PTO-1390 (Rev. 09-08)
Approved for use through 2/28/2010. OMB 0651-0021
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	
BRK-PU-001-US1	
U.S. APPLICATION NO. (If known, see 37 CFR 1.5)	

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/IL2007/000244	22nd February 2007	22nd February 2006

TITLE OF INVENTION
WIRELESS INTERNET SYSTEM AND METHOD

APPLICANT(S) FOR DO/EO/US
BARKAN, Elad

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☑ This is a **FIRST** submission of items concerning a submission under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a submission under 35 U.S.C. 371.
3. ☑ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☑ The US has been elected (Article 31).
5. ☑ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☑ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☑ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☑ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☑ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☑ A preliminary amendment.
14. ☑ An Application Data Sheet under 37 CFR 1.76.
15. ☐ A substitute specification.
16. ☑ A power of attorney and/or change of address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821- 1.825.
18. ☐ A second copy of the published International Application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
	PCT/IL2007/000244	BRK-PU-001-US1

20. Other items or information:

Petition for revival of an International Application for Patent Designating the U.S. abandoned unintentionally under 37 CFR 1.137(b) with accompanying fees and documents

The following fees have been submitted	CALCULATIONS	PTO USE ONLY
21. ☑ Basic national fee (37 CFR 1.492(a)) **$330**	$ 330	
22. ☑ Examination fee (37 CFR 1.492(c)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... **$0** All other situations **$220**	$ 220	
23. ☑ Search fee (37 CFR 1.492(b)) If the written opinion of the ISA/US or the International preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... **$0** Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority ..... **$100** International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB ..... **$430** All other situations **$540**	$ 100	
TOTAL OF 21, 22 and 23 =		
☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)). The fee is **$270** for each additional 50 sheets of paper or fraction thereof.		

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof (round up to a whole number)	RATE	
95 - 100 =	/50 =		x $270	$

Surcharge of **$130.00** for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	20 - 20 =		x $ 52	$	
Independent claims	3 - 3 =		x $220	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $390	$	
			TOTAL OF ABOVE CALCULATIONS =	$	
☑ Applicant claims small entity status. See 37 CFR 1.27. Fees above are reduced by ½.					
			SUBTOTAL =	$ 325	
Processing fee of **$130.00** for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i)). +				$	
			TOTAL NATIONAL FEE =	$ 325	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$	
			TOTAL FEES ENCLOSED =	$ 325	
			Amount to be refunded:	$	
			Amount to be charged	$	

a. ☐ A check in the amount of $ _____ to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees.

c. ☐ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. _____.

d. ☑ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

ADVISORY: If filing by EFS-Web, do **NOT** attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is **not** recommended and by doing so your **credit card information may be displayed via PAIR.** To protect your information, it is recommended paying fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

SEND ALL CORRESPONDENCE TO:

PROFESSIONAL PATENT SOLUTIONS
P.O. Box 654
Herzeliya Pituah, 46105
ISRAEL

SIGNATURE

VLADIMIR SHERMAN

NAME

43,116

REGISTRATION NUMBER

PTO/SB/64/PCT (05-07)
Approved for use through 02/28/2010. OMB 0651-0021
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PETITION FOR REVIVAL OF AN INTERNATIONAL APPLICATION FOR PATENT DESIGNATING THE U.S. ABANDONED UNINTENTIONALLY UNDER 37 CFR 1.137(b)

Docket Number (Optional) BRK-PU-001-US1

First Named Inventor: BARKAN, Elad

International (PCT) Application No.: PCT/IL2007/000244 U.S. Application No.: _____ (if known)

Filed: 22nd February 2007

Title: WIRELESS INTERNET SYSTEM AND METHOD

Attention: PCT Legal Staff
Mail Stop PCT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

The above-identified application became abandoned as to the United States because the fees and documents required by 35 U.S.C. 371(c) were not filed prior to the expiration of the time set in 37 CFR 1.495(b) or (c) as applicable. The date of abandonment is the day after the date on which the 35 U.S.C. 371(c) requirements were due. See 37 CFR 1.495(h).

APPLICANT HEREBY PETITIONS FOR REVIVAL OF THIS APPLICATION

NOTE: A grantable petition requires the following items:
(1) Petition fee
(2) Proper reply
(3) Terminal disclaimer with disclaimer fee which is required for all international applications having an international filing date before June 8, 1995; and
(4) Statement that the entire delay was unintentional.

1. Petition fee

☑ Small entity - fee $ 810 (37 CFR 1.17(m)). Applicant claims small entity status. See 37 CFR 1.27.

☐ Other than small entity - fee $_____(37 CFR 1.17(m))

2. Proper reply

A. The proper reply (the missing 35 U.S.C. 371(c) requirement(s)) in the form of Application Transmittal Letter, Application and Fees (identify type of reply):

☐ has been filed previously on _____.

☑ is enclosed herewith.

3. Terminal disclaimer with disclaimer fee

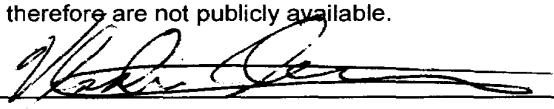
☑ Since this international application has an international filing date on or after June 8, 1995, no terminal disclaimer is required.

☐ A terminal disclaimer (and disclaimer fee (37 CFR 1.20(d)) of $ _____ for a small entity or $_____ for other than a small entity) disclaiming the required period of time is enclosed herewith (see PTO/SB/63).

4. Statement. The entire delay in filing the required reply from the due date for the required reply until the filing of a grantable petition under 37 CFR 1.137(b) was unintentional.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.



Signature

22/12/09

Date

Vladimir Sherman

Typed or Printed Name

43,116

Registration Number, if applicable

Address

Telephone Number

Address

Enclosures:
☑ Response
☑ Fee Payment
☐ Terminal Disclaimer
☑ Other (please identify): STATEMENT IN SUPPORT OF A PETITION FOR REVIVAL OF AN INTERNATIONAL APPLICATION FOR PATENT DESIGNATING THE U.S. ABANDONED UNINTENTIONALLY UNDER 37 CFR 1.137(b)

Attorney Docket No.: BRK-PU-001-US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	BARKAN. Elad	Examiner:	Not Yet Assigned
Serial No.:	Not Yet Assigned	Group Art Unit:	Not Yet Assigned
Filed:	Herewith		
International Application No:	PCT/IL2007/000244		
Title:	WIRELESS INTERNET SYSTEM AND METHOD		

STATEMENT IN SUPPORT OF A PETITION FOR REVIVAL OF AN INTERNATIONAL APPLICATION FOR PATENT DESIGNATING THE U.S. ABANDONED UNINTENTIONALLY UNDER 37 CFR 1.137(b)

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

This statement is being filed in support of a Petition for Revival of an International Application for Patent Designating the U.S. Abandoned Unintentionally under 37 CFR 1.137(b). The Petition is being submitted with all the required items including the transmittal of the request for entry into the National Phase in the United States of International Application PCT/IL2007/000244 and accompanying application documents, and the required fees.

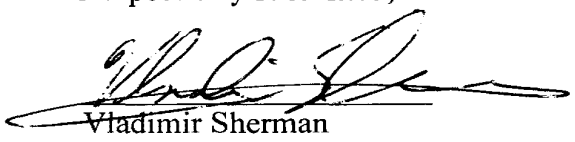
Applicant submits that despite the aforementioned International Application being in the care of a Patent Attorney registered in Israel, he did not receive any communication or reminders from the Patent Attorney that was responsible for filing the International Application, outlining the deadlines for filing National Phase Applications. Applicant further submits that he did not receive any other communication regarding the International Application from the aforementioned Patent Attorney during the lifespan of the International Application or at any time thereafter. Applicant submits that as a result of the lack of

communication from the Patent Attorney, Applicant unintentionally failed to timely file National Phase Applications in any jurisdiction.

Applicant further submits that he became aware of the lapse of the deadline to file National Phase Applications, including the U.S. National Phase Application of International Application PCT/IL2007/000244 on 14th December 2009, upon undertaking a due diligence.

Applicant submits that the entire delay in filing the National Phase Application was unintentional. The Undersigned became aware of the failure to file National Phase Applications of International Application PCT/IL2007/000244 on the 15th December 2009. Since becoming aware of the failure to file National Phase Applications, Applicant together with the Undersigned have worked to promptly transmit the National Phase Application, which is submitted herewith along with an official petition to revive form and the required application and petition fees.

Respectfully submitted,



Vladimir Sherman
Attorney for Applicant(s)
Registration No. 43,116

Dated: December 22nd, 2009

PTO/SB/01A (01-09)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	WIRELESS INTERNET SYSTEM AND METHOD

As the below named inventor(s), I/we declare that:

This declaration is directed to:

☐ The attached application, or

☒ Application No. PCT/IL2007/000244 filed on 22nd February 2007

☒ As amended on 20th December 2009 (if applicable);

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

All statements made herein of my/our own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR(S)

Inventor one: BARKAN, Elad Date: DEC 22, 2009

Signature: Elad Barkan Citizen of: Israel

Inventor two: _____ Date: _____

Signature: _____ Citizen of: _____

☐ Additional inventors or a legal representative are being named on _____ additional form(s) attached hereto.

PTO/SB/14 (11-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	BRK-PU-001-US1
	Application Number	
Title of Invention	WIRELESS INTERNET SYSTEM AND METHOD	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Elad		Barkan	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Kfar-Sirkin	Country Of Residence	IL
Citizenship under 37 CFR 1.41(b)	IL		

Mailing Address of Applicant:

Address 1	12 Habanim Street		
Address 2			
City	Kfar-Sirkin	State/Province	
Postal Code	49935	Country	IL

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	60956		
Email Address	ppsoffice@propats.com	Add Email	Remove Email

Application Information:

Title of the Invention	WIRELESS INTERNET SYSTEM AND METHOD		
Attorney Docket Number	BRK-PU-001-US1	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	22	Suggested Figure for Publication (if any)	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	BRK-PU-001-US1
	Application Number	
Title of Invention	WIRELESS INTERNET SYSTEM AND METHOD	

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	**Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S. C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	60956		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	a 371 of international	PCT/IL2007/000244	2007-02-22
Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
PCT/IL2007/000244	non provisional of	60775321	2006-02-22
Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
PCT/IL2007/000244	non provisional of	60794135	2006-04-24

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

			Remove
Application Number	Country[i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			◉ Yes ○ No

PTO/SB/14 (11-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	BRK-PU-001-US1
	Application Number	
Title of Invention	WIRELESS INTERNET SYSTEM AND METHOD	

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1

If the Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information:

Address 1			
Address 2			
City		**State/Province**	
Country		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button.

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/V.K.S./			Date (YYYY-MM-DD)	2009-12-22
First Name	Vladimir	Last Name	Sherman	Registration Number	43116

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Attorney Docket No.: BRK-PU-001-US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	BARKAN. Elad	Examiner:	Not Yet Assigned
Serial No.:	Not Yet Assigned	Group Art Unit:	Not Yet Assigned
Filed:	Herewith		
International Application No:	PCT/IL2007/000244		
Title:	WIRELESS INTERNET SYSTEM AND METHOD		

PRELIMINARY AMENDMENT

Mail Stop Amendment
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

Prior to Examination, kindly amend the above-identified application as follows:

Amendments to the Specification begin on page 2 of this Amendment.

Amendments to the Claims are reflected in the listing of claims which begins on page 3 of this paper.

Remarks/Arguments begin on page 12 of this paper.

AMENDMENTS TO SPECIFICATION

In the Cross Reference:

Please replace the Cross-Reference with the following Cross-Reference:

--CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a National Phase Application of PCT International Application No. PCT/IL2007/000244, International Filing Date 22nd February 2007, which claims priority from provisional Patent Applications, 60/775,321, filed 22nd February 2006, and 60/794,135, filed 24th April 2006, all of which are hereby incorporated by reference in their entirety.--

AMENDMENTS TO THE CLAIMS

Please add or amend the claims to read as follows, and cancel without prejudice or disclaimer to resubmission in a divisional or continuation application, claims 16, 17, 19, 20, 25-42 indicated as cancelled:

1. (Original) A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising:

a. wirelessly connecting a first STA to the Internet through a first AP with a first SSID;

b. remaining connected to the first Access Point (AP), the first STA creates a software-based wireless AP with a second SSID for wirelessly connecting other STAs to the Internet through the first STA.

2. (Original) The method for providing a wireless Internet connections to STAs according to claim 1, further including the step of:

c. a software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein.

3. (Currently amended) The method for providing a wireless Internet connection to STAs according to claim 1 [or 2], wherein each STA can be a laptop computer, PDA, wireless camera, wireless phone or a wireless device.

4. (Original) The method for providing a wireless Internet connection to STAs according to claim 1, wherein the first STA includes means for simultaneously connecting to the first AP and for opening the second AP, and means for transferring Internet packets between the first and second APs, while decrypting and encrypting the packets as needed based on the security parameters of the first and second AP, in addition to any communications with the Internet as required by a user of that STA.

5. (Original) The method for providing a wireless Internet connection to STAs according to claim 1, wherein activating, in the first STA, a single wireless card so as to operate in two modes at the same time, a STA mode and an AP mode.

6. (Original) The method for providing a wireless Internet connection to STAs according to claim 1, wherein the first AP does not provide wide, unconditional access to all.

7. (Original) The method for providing a wireless Internet connection to STAs according to claim 6, wherein a remote database may be accessed to determine if a STA without the software module should be allowed access, and how wide that access should be.

8. (Currently Amended) The method for providing a wireless Internet connection to STAs according to claim 1, [2, 3, 4 or 5,] wherein the software module, upon detecting that the other STA does not have the software module therein, allows to install and activate the software module in the other STA and then provides wide access to the other STA.

9. (Original) The method for providing a wireless Internet connection to STAs according to claim 6, wherein the software module, upon detecting that the other STA does not have the software module therein:

c1. presents to the user of the other STA a message indicating that wide Internet access is possible upon loading a copy of the software module;

c2. waiting for that user's permission;

c3. after receiving that user's permission, the other STA. STA downloads, installs and activates a copy of the software module to gain a wide Internet access to the other STA.

10. (Currently Amended) The method for providing a wireless Internet connection to STAs according to claim 1, [2, 3, 4 or 5] wherein the step of connecting another STA comprises:

c1. the first STA connects the other STA, while limiting the set of Internet addresses and/or Internet sites the other STA can access, and wherein the accessible sites include a special web site from which the other STA can download the software module;

c2. the other STA downloads, installs and activates the software module therein;

c3. the first STA, upon detecting the installed and active software module in the other STA, then removes the limitations on the set of Internet addresses
and/or Internet sites the other STA can access.

11. (Currently Amended) The method for providing a wireless Internet connection to STAs according to claim 1, [2, 3, 4 or 5] wherein the step of connecting another STA comprises:

cl. the first STA connects the other STA to the Internet, while limiting the set of Internet addresses and/or Internet sites the other STA can access, and wherein the accessible sites include a special web site from which the other STA can download the software module;

c2. if so instructed by the user of the other STA, the other STA downloads, installs and activates the software module therein;

c3. the first STA, upon detecting the installed and active software module in the other STA, then removes the limitations on the set of Internet addresses and/or Internet sites the other STA can access.

12. (Currently Amended) The method for providing a wireless Internet connection to STAs according to claim 10 [or 11] wherein the first STA, upon detecting the installed and active software module in the other STA, then removes part of the limitations on the set of Internet addresses and/or Internet sites the other STA can access, so as to keep some sites and/or addresses private to the first STA.

13. (Original) A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising:

a. activate in a first STA a software module for connecting with other STAs and to the Internet;

b. when required by the user to connect to the Internet and upon connecting with another STA which is already connected to the Internet and has a copy of the software module active therein, signal to the other STA that the first STA has a copy of the software module, and request to connect to the Internet through the other STA;

c. connect the first STA to the Internet through the second STA;

d. the software module in the first STA opens a second, software-based wireless Access Point (AP) at the first STA for connecting other STAs to the Internet through the first STA, and wherein the software module only provides wide Internet access to other STAs which each has a copy of the software module installed and active therein.

14. (Original) A method for providing a wireless Internet connection to WiFi-enabled devices (STAs), comprising:

a. activate in a first STA a software module for connecting with other STAs and to the Internet;

b. connect the first STA to the Internet and open a second, software-based wireless AP for connecting other STAs to the Internet through the first STA;

c. when another STA connects with the first STA through the second AP and requests access to the Internet:

1) check whether the other STA has a copy of the software module installed and active therein;

2) if the answer is positive, then connect the other STA to the Internet;

3) if the answer is negative, then support the other STA in loading, installing and activating a copy of the software module therein and, after the software module is active in the second STA, provide wide Internet access to the other STA.

15. (Currently Amended) The method for providing a wireless Internet connection to STAs according to claim 13 [or 14], wherein each STA may include a Portable computer, a Laptop, a PDA or a wireless phone.

16. (Cancelled) The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein each STA includes means for simultaneously connecting to the first AP and for opening the second AP, and means for transferring Internet packets between the first and second APs, in addition to any communications with the Internet as require by a user of that STA.

17. (Cancelled) The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein activating, in the first STA, a wireless card so as to operate in two modes at the same time, a STA mode and an AP mode.

18. [(Currently Amended) The method for providing a wireless Internet connection to STAs according to claim 13 [or 14], wherein a STA connects to the Internet through two or more STAs simultaneously.

19. (Cancelled) The method for providing a wireless Internet connection to STAs according to claim 18, wherein a STA repeats the connecting stage two or more times to connect to the Internet through two or more APs simultaneously.

20. (Cancelled)The method for providing a wireless Internet connection to STAs according to claim 18 or 19, wherein a STA performs a fast handover by continuously searching for new APs to connect therethrough and connecting to newly available APs as older APs may become inaccessible.

21. (Currently Amended) The method for providing a wireless Internet connection to STAs according to claim 13 [or 14], wherein the first STA prevents other STAs from accessing its inner network by limiting the access rights of the other STAs.

22. (Currently Amended) The method for providing a wireless Internet connection to STAs according to claim 13 [or 14], wherein the other STA prevents the first STA from eavesdropping on its communications by tunneling its sensitive traffic to a trusted network site, and accesses the Internet through its tunnel to the trusted network site which acts as a proxy for it.

23. (Currently Amended) The method for providing a wireless Internet connection to STAs according to claim 13 [or 14], wherein preventing STAs from using other STAs for their

primary network connection for a long period of time, by detecting that a STA is connected to the Internet through the same STA for a long period of time, and disconnecting that STA.

24. (Currently Amended) The method for providing a wireless Internet connection to STAs according to claim 13 [or 14], wherein preventing STAs from using other STAs for their primary network connection for a long period of time, by detecting that a STA is connected to the Internet through the same STA for a long period of time, and disconnecting that STA if it refuses to pay for the continued use of that connection.

25. (Cancelled) In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for configuring STAs to connect to a wireless network, comprising:

a. activating a software module in first STA, which is already configured to access an Access Point (AP);

b. the software module copies the security information from the personal computer to another STA, thus setting the security parameters for the other STA as to allow access to the AP.

26. (Cancelled) The method for configuring STAs according to claim 25, further including an authentication phase in which the other STA is authenticated by the software module or by a remote server before copying the security information.

27. (Cancelled) In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for configuring STAs to connect to a wireless network, comprising:

a. a customer first connects a STA by wire to its network, (or the STA first connects using a connection it establishes through an already connected device, such as a personal computer or laptop);

b. a software on the STA copies to the STA the security information gained through the wired connection, thus setting the security parameters for the STA.

28. (Cancelled) In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for performing fast handover for a first STA, from being connected to a first Access Point (AP) to a second AP, comprising:

a. a first STA communicates with a Termination Node (TN) and is in contact with a Governing Node (GN), wherein GN is non-exclusively responsible for the mobility management in a certain geographic area for a given time and wherein the GN is in contact with another STA in the coverage area of the second AP;

b. the other STA receives instructions from GN to impersonate the first STA towards the second AP and to complete a connection process with the second AP on behalf of the first STA;

c. the other STA communicates the connection parameters to the GN and, once the parameters are communicated, the other STA returns to its real identity;

d. the GN communicates the parameters to the first STA, thereby eliminating the need for the first STA to perform the connection process itself;

e. when the first STA reaches the perimeter of the coverage of the first AP, it can immediately use the new parameters and continue communications with the second AP, without any delay.

29. (Cancelled) The fast handover method according to claim 28, wherein the first STA alerts the TN before the handover, so it can start sending information packets to the new location.

30. (Cancelled) The fast handover method according to claim 28, wherein the TN sends information in parallel to the old and the new location, and ceases transmitting to the old location once the handover is complete.

31. (Cancelled) The fast handover method according to claim 28, wherein the other STA further opens a Transmission Control Protocol (TCP) as used in the Internet or sends a User Datagram Protocol (UDP) packet on behalf of the first STA, if required.

32. (Cancelled) The fast handover method according to claim 28, wherein the connection process performed by the other STA on behalf of the first STA includes authentication, association, receiving an IP address and performing any second authentication/log-in procedure.

33. (Cancelled) The fast handover method according to claim 28, wherein the connection process performed by the other STA on behalf of the first STA further includes opening connections or "punching holes" in the firewall.

34. (Cancelled) The fast handover method according to claim 28, wherein the connection waits for the first STA until it reaches the second AP and, if there is a timeout on these connections (either due to protocol, or due to firewalls), the other STA or yet other bypassing STAs can send and receive -keep-alive- messages on behalf of the first STA.

35. (Cancelled) The fast handover method according to claim 34, wherein the timeout for each AP is stored in the GN for future use.

36. (Cancelled) The fast handover method according to claim 34, wherein the value of the timeout is transmitted by the GN to the first STA.

37. (Cancelled) The first handover method according to claim 34, wherein the connections parameters are not limited in use for the first STA, but are also available for the use of other STAs.

38. (Cancelled) In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for fast uploading of information from STAs to the Internet, comprising:

a. a first STA connects to the Internet;

b. a second STA wirelessly connects to the first STA, and uploads the information using the fast and direct-wireless connection between the STAs;

c. The first STA temporarily stores the information;

d. The first STA uploads the information to the Internet through its backhaul.

39. (Cancelled) The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the first STA includes a laptop or a personal computer, the second STA includes a digital camera or a digital video camera, and the information includes digital pictures or digital clips.

40. (Cancelled) The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the second STA disconnects from the first STA after completing to upload the information to the first STA, but before the first STA completes the upload of information to the Internet; the first STA completes the upload of information from its temporary storage.

41. (Cancelled) The method for fast uploading of information from STAs to the Internet according to Claim 38, further including the step:

c. at a later time, the second STA connects to the Internet and verifies that the information was uploaded correctly.

42. (Cancelled) The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the information is encrypted by the second STA before being transmitted.

REMARKS

Applicants request entry of the Preliminary Amendment.

Applicants have cancelled claims 16, 17, 19, 20, 25-42 without prejudice or disclaimer.

Should the Examiner have any question or comment as to the form, content or entry of this Amendment, the Examiner is respectfully requested to contact the undersigned.

Respectfully submitted,

Vladimir Sherman
Attorney for Applicant(s)
Registration No. 43, 116

Dated: December 20, 2009

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2007 (30.08.2007)

PCT

(10) International Publication Number
WO 2007/096884 A2

(51) International Patent Classification:
H04J 13/00 (2006.01)

(21) International Application Number:
PCT/IL2007/000244

(22) International Filing Date:
22 February 2007 (22.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/775,321 22 February 2006 (22.02.2006) US
60/794,135 24 April 2006 (24.04.2006) US

(71) Applicant and
(72) Inventor: **BARKAN, Elad** [IL/IL]; C/O Marc Zuta, Patent Attorney, P.O. Box 2162, 49120 Petah-Tikva (IL).

(74) Agent: **ZUTA, Marc**; Marc Zuta, Patent Attorney, P.O. Box 2162, 49120 Petah-Tikva (IL).

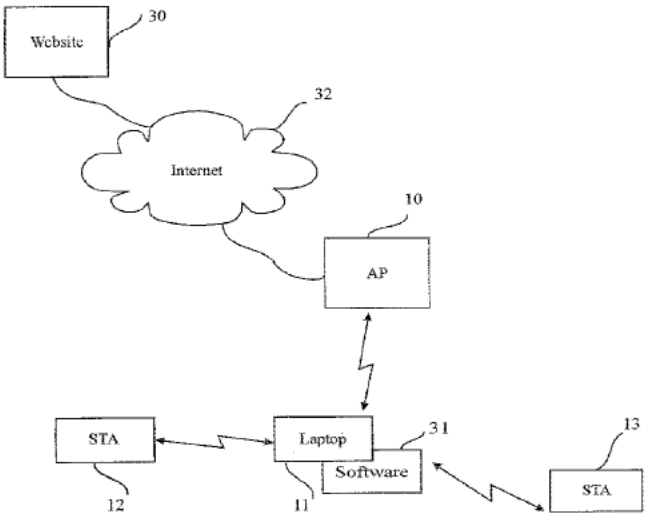
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: WIRELESS INTERNET SYSTEM AND METHOD



(57) Abstract: A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising: wirelessly connecting a first STA to the Internet through a first AP with a first SSID; remaining connected to the first Access Point (AP), the first STA creates a software-based wireless AP with a second SSID for wirelessly connecting other STAs to the Internet through the first STA. A software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein. A method for configuring STAs to connect to a wireless network, comprising: a customer first connects a STA by wire to its network; a software on the STA copies to the STA the security information gained through the wired connection, thus setting the security parameters for the STA.

WO 2007/096884 A2

Wireless Internet system and method

Cross-Reference to Related Applications

The present application is related to, and claims priority from, the provisional patent applications filed by the present applicant in U.S.A.: Application US 60/775,321 filed on 22 February 2006, and Application US 60/794,135 filed on 24 April 2006.

Technical Field

The present invention relates to a wireless Internet system and method, and more particularly to such systems for providing wireless Internet connection to roaming devices such as Portable computers, Laptops, PDAs and phones, and the deployment of such a system in a fast spreading manner (a viral-like method), in a client software-only manner such that the existing access points are not changed at all.

Background Art

Currently, there is a growing number of WiFi public hot-spots (or Access Points - "AP"). These APs allow WiFi-enabled devices (which we refer to as STA) that are in their coverage area to Connect to the internet.

Some of the APs are operated as a business, service, or as part of a community, either with or without a charge to the STA's owner. Other APs are placed by individuals in their premises, but are not "locked", i.e., they are "open", allowing bypassing STAs to utilize them. Other APs placed by individuals are "locked" (or "closed"), thus not allowing passing STAs to utilize them.

As APs are being deployed in growing numbers, many individuals lock their APs for fear of unfair use of their network resources, and due to security concerns. For instance, there have been cases where a person places an open AP, and his neighbor uses this AP as its internet connection on a full-time basis without the consent of the first person, thus abusing and degrading the service of the first individual. In other cases, the neighbor hacked into the computer of the first person through the network. Thus, as time passes, most APs are either locked, or a payment is required to use them. Although the total number of APs and their area of coverage is growing fast, a larger percent of the APs are becoming locked and inaccessible to roaming STAs.

A prior art approach for allowing roaming customers to access the Internet is taken by Fon (www.fon.com). It allows individuals to download a new software into their APs, which makes their APs a pay-for-use APs for STAs that roam in their vicinity, and in addition, they receive a username and password for free access to other APs which are operated by Fon or utilize their software. It also allows users to enjoy part of some of the payments made by other users to use the network. However, roaming STAs are forced either to find an open AP, find an AP for which they have an account, or pay for access in case there is a pay-for AP.

It is an aim of the current disclosure to provide a system and a method for deployment of APs for the purpose of connecting STAs to the Internet.

Roaming customers that connect to an AP are often far from the AP and have borderline reception conditions. As a result, the connection quality is very poor, and the user may experience a slow service or no service at all. It is another aim of the current disclosure to provide a system and a method for improving the connection quality for roaming STAs.

Another aspect of this invention refers to systems and methods for fast handovers in wireless networks such as 802.11 networks, specifically in un-managed wireless networks, and more particularly such systems and methods which allow extremely fast handovers in these networks without any changes to existing 802.11 base stations. The invention also

concerns efficient performance with regards to power consumption, coverage, security, installation, capacity and availability of wireless networks such as 802.11.
The invention can achieve these goals without any change to the WiFi access point.

Currently, there is a growing number of WiFi public hot-spots (or Access Points - "AP"). These APs allow WiFi enabled devices (which we refer to as STA) that are in their coverage area to connect to the internet.

Some of the APs are operated as a business, service, or as part of a community, either with or without a charge to the STA's owner. Other APs are placed by individuals in their premises, but are not "locked", i.e., they allow bypassing STAs to utilize them. The cumulative connectivity provided by the APs is enormous and growing fast, thus, it is tempting to use this cumulative connectivity to compete with other wireless technologies. For example, it would be tempting to have a STA that looks like a cellular handset (i.e., a WiFi Handset, or WiFi Phone), where the WiFi handset uses the free connectivity to provide a "free" service that competes with or complements the cellular service.

One of the major difficulties of achieving this vision is that the coverage of a single WiFi AP is very small (about a few hundreds to a few thousands of square meters). When a user goes out of this area, his connectivity is lost. A natural naive approach to solve this problem is performing a handover (sometimes also called handoff) to another AP with a better radio connection to the user. Another approach is to have a handset which supports both WiFi and Cellular, and handover the conversation from WiFi to Cellular [See: WO 2004/036770], this way, WiFi extends the coverage of cellular, and conversation is handed over from WiFi to cellular, when there is no WiFi coverage. However, the problem of performing handover between one WiFi AP to another WiFi AP remains when appropriate cellular coverage is not available (or there is no cooperation from the cellular company). The same idea applies when cellular is replaced by other access technology, such as satellite communications.

The concept of handover is taken from cellular networks. Handovers usually work well in

managed networks, such as cellular networks, campuses, or office environment., where the entire network is usually owned by the same operator.
The network operator in many cases chooses to add cells where coverage or capacity are needed. In managed networks, the APs (or the cellular cells) are synchronized and communicate with each other through a backbone, and are usually controlled by some other network entity (e.g., BSC - base station controller in cellular systems). For example, the APs can communicate with each other, for example using the IEEE 802.11F protocol - the Inter-AP protocol, which involves a RADIUS (Remote Authentication Dial In User Service, see RFC 2138, 2865, and 2866) server.

The APs can also employ a radio resource management such as IEEE 802.11K, or fast roaming using IEEE 802.11R, etc. However, in unmanaged networks, the APs can be deployed by many unrelated entities, such as by private individuals.

There is usually no entity that synchronizes the APs. The APs can be manufactured by various manufacturers, use various security mechanisms etc. In unmanaged networks, the handovers are typically very slow, as in the process of handover, it takes time for the STA to re-connect to the internet in the new AP (and it must disconnect from the previous AP). In such a handover in an unmanaged network, the IP address often changes. Therefore, a mechanism such as mobile IP must be used (as described later). This mechanism is limited with respect to the frequency in which the IP address can change, and a large latency (disconnection time) may result during the handover process. During the latency, the STA cannot receive any incoming messages.

A handover process is typically composed of the station STA connecting to a new AP, and disconnecting from the old AP. If STA is connected in parallel to both AP the handover is called soft-handover, and if STA first abandons the old AP and then connects to the new AP, the handover is called a hard-handover. Soft handovers require the ability of STA to communicate in parallel with at least two APs.

The process of connecting to a new AP is usually composed of the following steps:

1. STA performs a scanning process to discover neighboring APs.
2. STA chooses a new AP, and performs authentication with the AP, in which the AP verifies that STA is allowed to access the AP.
3. If the authentication is successful, STA performs an association process, in which the AP acknowledges that STA is connected to it (association requires the AP to allocate resources to the STA, and the 802.11 standard allows up to 2007 STAs to be associated with an AP).
4. Once STA is associated with the AP, the STA makes sure that it has all the information that it requires to communicate over the internet, for example, it must have an IP address, and it must update servers that govern its location (such as Mobile IP, as discussed later). In some cases, the user should go through a second authentication procedure (usually with a RADIUS server). Many times, this procedure is performed over a web interface, which is called a Captive Portal.

When a captive portal is used by the AP, the user needs to surf into the captive portal and perform a log-in to connect his IP address to the Internet. In some implementations, the user's web browser is forwarded to the captive portal regardless of the internet site that it tries to surf into. Some APs allow the STA to surf in some limited number of internet sites before they complete the second authentication procedure (for example, if the AP is in an hotel, it might allow surfing into the hotel's website, or affiliated news web sites). The procedure at the captive portal typically includes authentication, payment, or agreeing to terms of usage. Once the authentication is completed, the IP address of the STA is connected to the Internet (usually by reconfiguring the firewall that controls the communications of the AP). Each sub-process takes time to complete, resulting in a total delay of over several seconds to complete the entire process.

In managed networks, Step 4 can be performed once in a certain amount or time (or for a certain area), as moving between APs of the managed network does not necessarily change the parameters of the STA such as IP address etc. However, in un-managed networks (and sometimes also in managed networks), the STA must gain a new IP address and other parameters, usually through DHCP (Dynamic Host

Configuration Protocol, see RFC 1541). Completing the DHCP protocol can take up to several seconds. Sometimes, obtaining an IP is not enough, and a second authentication is needed. In other cases, a proxy server or a Socks server should be set for the communication. The entire process can consume a few seconds, which are intolerable in a streaming two-way application such as a voice conversation.

Many protocols that are used in the Internet require that the IP address of the STA would remain fixed during communications (for example, TCP - Transport Control Protocol, see RFC 793). However, a handover might result in the change of the IP address. This change of IP address causes a break in the communication as the communication needs to be restarted.

One solution to this problem is provided by the Mobile IP standard (see RFC 2002): in this solution the STA updates a server with its current IP address, every time that the IP address changes. As a preparation for roaming, the server allocates to the STA (in addition to the STA's current IP address) an IP address that remains fixed, even when the real IP address of the STA changes. This fixed IP address is also known as a "care of" address. From this moment on, the STA keeps the server posted of the real IP address of the STA, and the STA can use (in its communications with the rest of the Internet) the "care of" address (or its home address) as if it was its own fixed address.

Any IP data packet that is sent to the care-of IP address is tunneled by the Mobile-IP server to the current IP address of the STA. For packets originating from the STA to the Internet, the STA can tunnel the packets to the Mobile-IP server, which replaces the IP address with the care-of address. However, many times the STA can simply write its care-of IP address as the source address of the IP data packet, as many times, the source address of IP packets is not checked what-so-ever in the course of routing the IP data packet in the Internet.

The Mobile-IP solution can be applied as long as the handovers are not

performed too often. However, it incurs the punishment of routing all incoming packets through a server, causing both an increased travel time for the data packets, as well as latency (or disconnection) for the time that the real IP address changed, but the server is not informed yet. If the round-trip-time of the packets between the STA and the server is longer than the time a STA stays with the same IP, this method fails, as by the time packets reach the reported location of the STA, the STA is already in another location.

For many applications, such as voice, it is of utmost importance to minimize the time spent on the handover process. The time consumed by the handover process is usually dominated by the scanning step (Step 1 as mentioned above), and by Step 4 (specifically in case of an unmanaged network). There are many solutions that address fast handovers in cellular networks, and a few solutions that address fast handovers in managed WiFi networks (for example, see: WO2004/054283, which reduces Step 1 (mentioned above) by selective scanning but requires modifying the AP). None of these solutions deal with the delay due to Step 4.

It is an object of this invention to provide very fast handovers even in unmanaged networks.

Another barrier for wireless applications is that WiFi coverage might exists, and security policy might allow the STA to connect, but the AP might be out of resources (for example, there are 2007 associated STAs, and therefore it has no resources left, or that it has a limited IP address space which was already allocated through DHCP, and it has no IP address to allocate). It is an object of this invention to provide a system and method that allows STAs to use the services of the AP even when some of its resources are exhausted.

Another barrier for many wireless applications is the complex configuration of wireless parameters of STA, especially the security parameters. A user that purchases a new STA and has an existing AP, might wish to configure his new STA to work with his AP. This configuration includes entering into the STA the

encryption key and authentication key that would allow it to use the AP. Existing solutions require a change in the AP and STA, such that a special key can be pressed simultaneously at both ends to perform automatic configuration (like Buffalo INC's AirStation OneTouch Secure System - AOSS, or Broadcom's SecureEasySetup). Without such a solution, the user is usually forced to punch into his STA the security codes (which are typically long). The problem worsens when the STA moves between APs that use different security settings.

It is an object of this invention to provide for easy configuration on both levels: at the initial setup and while roaming.

Another barrier for many wireless applications is that WiFi coverage might exist, but it is locked and unavailable for use for the STA.It is an object of this invention to provide a solution for (legally) accessing locked APs.

Another problem with WiFi is that the WiFi protocol is not optimized for low battery consumption (compared to cellular protocols such as GSM). In current solutions, if the STA moves between APs and changes its IP, it must use mobile IP and inform an entity (server) in the network of its current IP (we refer to this process as "location update", as the STA updates the network entity of its location). Frequent location updates exhaust the STA's battery. Another problem with frequent location updates is that they create a heavy load on the network and on the network entities that manage and keep track of the STA's location.

The situation in WiFi is very different from the situation in cellular networks in two ways. Both of the ways cause an increase in the number of location updates in WiFi: First, in cellular network, the cells are typically much larger than a "cell" that is created by a WiFi AP. Therefore, in cellular networks, there are fewer transitions between cells, and hence less location updates. Second, cellular protocols allow defining a "location area" that encompasses several cells, and the STA is required to perform location update

only when moving between location areas, and thus reducing the number of location updates. Current WiFi protocols are not built to support location areas.

It is an object of this invention to provide a method that reduces the number of location updates required for STAs while moving between APs.

It is an object of the current invention to provide solutions to the above mentioned problems, using both a centralized (server based) approach, and also by providing a method for performing the solutions using a distributed peer-to-peer network. Therefore, no huge servers and no large investments are required.

Disclosure of Invention

The invention is described by way of example, but it should be obvious to persons skilled in the art that many variations thereof may be implemented.

A novel aspect of the invention relating to the deployment of APs is that devices function at the same time as STAs and as APs. This allows a STA to also create a new AP for connecting other STAs to the Internet therethrough. It is known in the art that a STA wireless card can operate in one of two modes, STA or AP. The present inventor has found a way to activate a device simultaneously in both modes.

According to another novel aspect, a connecting STA can limit the set of Internet addresses or internet sites that other STAs which connect through it can access, but the set of allowed addresses includes a special web site from which other STAs can download the Vagabee(TM) software. Vagabee software includes the functionality of the software of the first STA, to open new APs and further spread the Vagabee.

Once the new STAs download and execute the Vagabee software, the first STA

detects that the software is running on the new STAs, and allows them a wider access to the internet. Therefore, new STAs must download and run the Vagabee software to get wide access to the internet. As the new STAs run Vagabee, they become APs in their own right and allow other STAs to download and connect through them to the internet in the current location of these STAs, as well as in any other location they go.

Another novel method of the present invention allows a STA to connect through two or more APs simultaneously. Thus, a STA can enjoy a more stable connection even if part of the connections are of borderline quality. Furthermore, more connections may achieve a broader connection to the Internet, or may balance its traffic such that each STA carry a lighter burden with regards to the extra bandwidth they carry due to a new STA.

Multiple connections also allow faster handovers, as if a STA is moving from one place to the other it can first establish a new connection and then the old connection is terminated, practically leaving the STA connected.

In a further development of the novel method, a laptop (the terms STA and laptops are interchangeable, we use laptop rather than STA as in the preferred embodiment these cases the STA would be a laptop) can connect with another laptop directly or through a STA, such that both enjoy the Internet connection of the other. As the internet connection is not used all the time (typical laptop uses on average a few percents of its maximum bandwidth), both laptops will experience a much faster connection to the Internet.

Another important issue is the security of the system. A Laptop might agree to act as an APs, but it does not agree to allow other STAs to access its inner network (i.e., the laptop owner wishes to allows these STAs to access the internet through its private network but does not allow them to access computers on its private network. Another security concern is that the new

STAs may desire to prevent the first STA from tapping into their Communications, i.e., they do not want the first STA to be able to tap into communications that the first STA relays. The current disclosure provides novel method to deal with these two problems.

First, external STAs (new STAs) are not allowed access to computers in the inner network by having the first STA drop data packets from the external STAs that are designated to local IP addresses on the inner network. Second, a new STA's privacy is protected by tunneling its sensitive traffic to a trusted network site, and the new site accesses the Internet through his tunnel to the trusted network site which acts as a proxy for it.

An important issue is to prevent STAs from using other laptops for their primary network connection for a long period of time. A novel method detects that a STA is connected to the internet through the same laptop for a long period of time, and disconnects the STA. Alternatively, the STA has to pay to continue and use the network. The pricing can be such as to encourage the STA's user to purchase his own connection from an independent Internet Service Provider (ISP).

In yet another novel method, the software running on a laptop can replace the commercial banners that appear in the web pages the laptop surfs into, as well as the web pages that connected STAs surf into. The banners can be stopped, replaced, and made specially targeted to the user, for example based on his location.

A further novel method is that the wireless internet coverage that is obtained using laptops can be used by devices such as wireless IP phones to make phone calls using the wireless internet coverage, cellular phones that have built-in WiFi connection, or digital cameras with WiFi that wish to upload the data stored in them. Other devices might include for example, radio or TV broadcast capabilities.

For example, Digital cameras might be equipped with WiFi. The owner of such a

camera would like to upload his pictures from the camera to a server that stores the pictures on the Internet - the reasons for this may vary from being able to share the photos while on vacation with family members left at home, backup the pictures from the digital camera to the Internet server, or simply because the memory card on the camera is running out of space. A major problem is that to upload the pictures to the Internet may take a very long time, as pictures consume megabytes to store. In the novel method, the camera can send the photos to the laptop over WiFi (this connection is very fast), then disconnect and move on. Then, the laptop uploads the pictures to the Internet server (this process can take a long time as it involves uploading a lot of data), but the laptop owner would not feel it as a burden, since the pictures can be uploaded when his Internet connection is not used for other purposes.

Improvements to this method may include: The camera can encrypt the pictures so that the laptop owner cannot see them. The pictures can be still stored in the camera after being uploaded to the laptop, as the laptop might fail to upload them. The next time the camera connects to the Internet, it can check with the Internet server that the pictures arrived correctly to the server. If that is so, the pictures may be erased from the camera. Otherwise, the camera can re-transmit the pictures.

To have faster uploads, the camera can upload the pictures to several laptops that would upload the picture to the server.

Another novel method relates to configuring STAs to connect to a wireless network. The configuration, and especially the security configuration of STAs to connect to a wireless Internet connection such as WiFi is cumbersome and annoying to most users. Assume a STA belongs to the same user (or user group) of the owner of a laptop. Then, by a special logging into a website, the configuration of the laptop can be copied to the STA, thus configuring it to use the AP (i.e., allowing a connection without the laptop).

Another novel method allows devices with a trusted hardware to receive information that instructs them how to directly connect to AP, by providing them with the needed settings and security information.

One of the novel aspects of a very fast handover is to practically "almost complete" the process of the handover before it even started, possibly with the assistance of another STA that is already in the new AP's coverage (further details are described later).

Another novel aspect is that the same MAC address and IP address can actually be used by more than one STA. The differentiation between the STAs can be performed by using higher protocol identification, such as different port numbers (for example TCP ports), as detailed later.

It is useful for a station STA to know the identity of the adjacent APs that the STA might hand over to. The identity of an AP can be established in several ways, as disclosed herein. The SSID (Service Set ID) of the AP is usually broadcasted by the AP using periodical transmissions known as beacon. However, two adjacent AP may have the same SSID. In such a case, the MAC address of each AP is different, and APs can be differentiated based on their MAC address (which serves as a globally unique identification parameter). Some APs do not transmit beacon, and only respond when they are addressed using their SSID. In this case, a priory -knowledge is needed, see below.

Another aspect of the invention is for a STA to selectively scan for a neighboring AP in the following novel way. Assume that a STA scans to see if it can receive the beacon of a second AP, where the scanning will be performed exactly when the second AP is expected to transmit its beacon, therefore, the disconnection from the first AP will be minimal. The novel method consists of scanning and storing (in network entities) information about the relative time

between adjacent APs, and their relative clock drift. This information is retrieved at the appropriate time such that the STA knows to wait for the beacon just before it is transmitted.

Another aspect of the invention is to prevent exhaustion of resources at the APs. GN keeps a pool of MAC addresses with associated IP address. Just before a STA enters the AP, GN sends it a MAC address and an IP address that are already associated with the AP. Therefore, the STA can connect even if the AP has no resources left for new STAs.

Another novel aspect of the invention is to save Battery Power and reduce network load by reducing the number of Location Updates in WiFi. A location update is the process in which a STA informs an entity in the network on its current location (the notification can take many forms, including opening a TCP connection, or sending UDP packets). In prior art for 802.11 networks, a location update is required whenever the IP address of the STA changes (for example, when moving between APs of different subnets) - even if the STA is idle (not transmitting or receiving data). The novel method allows to define a location area for WiFi, such that an idle STA needs to perform location update only when it moves between APs that belong to different location areas, but does not need to perform location update when it moves between APs of the same location area, even if its IP address changes. See further details later.

A pseudo-beacon is another aspect of the invention which allows reducing the number of Location Updates. It is a message that GN can periodically transmit in each AP. While some APs might permit a remote node to transmit a message in the AP, other APs might not allow it. In the novel method, a certain MAC address, IP address, and possibly a port number, are allocated in each AP for the purpose of pseudo-beacon transmission. Further details are described later.

Configuring the security in new STAs to work with an existing AP might be a

tedious job, as the security (authentication/encryption) code might be very long as known in the art, and the user might need to punch it into the STA. A novel solution for easy configuration is disclosed. Unlike previous solutions, the novel method does not require changing the existing AP of the customer. In one embodiment, software is run on a personal computer of the user (that is already configured to access the WiFi). Then, the software establishes a secure channel with the STA, and copies the security information from the personal computer to the STA. In this way, the STA learns the security parameters. An authentication phase in which the STA is authenticated by the software or a remote server can be added before copying the security information.

In another embodiment, the customer first connects the STA by wire to its network (or alternatively, the STA first connects using a connection it establishes through an already connected device, such as a personal computer or laptop).

As the STA can receive and transmit signals on the wireless network and it is connected to the internet (through the other connection) at the same time, it tries to locate the web configuration of the AP on the wired network (most APs have a web interface). In most cases, it is an easy job for the STA, as either the STA can locate the AP as it is the default gateway of the wired network, or it can try to find its IP by performing RARP (Reverse Address Resolution Protocol) using the wireless MAC address of the AP (which it can see off-the-air). Further details are described later.

Another novel method for gaining access to locked networks is disclosed. While performing the above described easy setup (or at any other time), the user is prompted, if he wishes, to join a swapping service. The swapping service allows the user to gain access to many locked networks (the locked networks of the other users that joined the swapping service), in return he allows users to use his network for the purpose of connecting to the Internet. If the user agrees, the access parameters to his network (encryption key, MAC address,

default gateway, etc.) are securely stored in the network (for example in GN, and a backup server). The security information will be securely sent directly into the hardware of other STAs, when they need to connect using his AP. Further details are described later.

Another novel aspect of the invention takes advantage of the fact that the wireless network is local in nature, as the APs are geographically adjacent. As a result, the methods that are disclosed can be implemented by many small devices on the Internet, each responsible for a geographic area. The devices form a peer-to-peer network that implement the methods, without the need to rely heavily on large servers.

Another novel aspect of the invention is to have a STA which has a capability of communicating in two or more channels in parallel. This capability can enable a STA to be connected to two APs in parallel without the need to implement sophisticated mechanisms that actually simulate this situation. Thus, a STA can connect with future APs while maintaining a connection through its serving APs. Being connected to two APs simultaneously allows greater bandwidth by utilizing two connections instead of one, and soft-handovers, i.e., the STA stays connected through one AP, while disconnecting from the second AP in the process of handover.

The new system and method refers, among others, to the following innovative features:

1. A viral-like fast spread method for the Vagabee(tm) software:
- at the network level
- at the already connected PC
- at a connecting PC, already having the Vagabee software
- at a connecting PC, not yet having the Vagabee software
- details of the software package being loaded on a new computer: functions, operation, how installs, how spreads further away to other PCs.

2. Detail the viral spread method:
- use of existing standards; "as is" or with modifications
- method of reporting to user and getting a user's approval
- interaction with firewall and antivirus programs in the PC

3. Vagabee in use, with flow charts:
- manage communications with presently connected PCs
- add new PC
- remove a PC. Recover chain, reestablish communications when intermediary PC disconnects
- resolve conflicts where there are several Vagabee systems in one area.
Method of operation, so the networks will not interfere with each other,
rather they may assist each other and maybe provide backup functions.
- Knowing the identity of adjacent APs and the location of STAs.
- handoff to another local Vagabee network

4. Vagabee in use, system design:
- workload on the various PCs in the chain (the workload increases as one moves closer to the AP, the Internet connection)
- overhead, signaling and control, traffic control. Define signals, method of operation
- permission to access more sites on the Internet after a new PC downloads and activates Vagabee - how implemented.
- reliability issues

5. System design for various configurations
The basic assumptions greatly affect the performance of the network systems which may be formed:
- a PC connects to only one additional PC
- a PC may connect to one or two additional PCs
- a PC may connect to more than two additional PCs

6. Bandwidth control
Bandwidth request and allocation. For the various PCs in the chain.
Methods for improved channel use. How is implemented.

7. Privacy issues - how the inner/outer areas are implemented.
Protection from viruses and eavesdropping, passwords protection, etc.
Damage control, Recovery from a virus attack.
This is a vital aspect of the new technology.

8. User control and supervision
- the user of a PC decides whether to install Vagabee
- the user of a PC decides whether to allow additional users to connect, with what parameters (bandwidth allocation, etc.)
- incentives for a user to allow his computer to connect others.
- the user allows or forbids additional users, according to circumstances - how important his present activity is, what is the quality and bandwidth allocated to that user (how much spare bandwidth there is)

9. Details of implementation - software
- New software
- Modified existing software
- Method of use of existing software, standards

10. Functions, benefits to users - detail methods to implement them
- free internet connection
- enhanced bandwidth, reliability
- provide additional services - locate gas stations, Pizza Hut, restaurants.

Brief Description of Drawings

Figs. 1 and 2 illustrate a wireless system for connecting mobile devices to the Internet through an access point

Fig. 3 illustrates an expanded wireless system for connecting mobile devices to the internet through more than one access point

Fig. 4 details a method for fast spreading the Vagabee software by providing free wireless access to the Internet.

Fig. 5 details the dual mode connectivity of a STA also functioning as an AP with the Vagabee method and software

Figs. 6A to 6F detail stages in a wireless network evolvement and spreading of the Vagabee software

Fig. 7 details a method addressing control and security aspects of the Vagabee spreading method

Fig. 8 details a method addressing coordination and control aspects of the Vagabee spreading method for the first, connecting STA

Fig. 9 details multi-AP, fast configuration setting and handover aspects of the Vagabee spreading method for the second, to be connected STA

Fig. 10 details multi-AP, fast secure configuration setting and redirection aspects of the Vagabee spreading method for the first, connecting STA

Fig. 11 details multi-AP and fast configuration setting aspects of the Vagabee spreading method for the second, to be connected STA

Fig. 12 illustrates a system including mobile stations (STAs) and their Access Points (APs), with one STA moving from the coverage of one AP to the coverage of another

Fig. 13 illustrates a wireless system facilitating handover and including a STA, a Governing Node (GN) and another user, Termination Node (TN)

Fig. 14 details the handover method

Fig. 15 details a method for implementing two connections with a STA.

Fig. 16 details a method for connecting other STAs

Fig. 17 details another method for connecting other STAs

Fig. 18 details a method for configuring other STAs to directly connect to the AP

Fig. 19 details another method for configuring other STAs to directly connect to the AP

Fig. 20 details yet another method for configuring other STAs to directly connect to the AP

Best Mode for Carrying Out the Invention

A preferred embodiment of the present invention will now be described by way of example and with reference to the accompanying drawings.

Dual use laptop simultaneously connected to the internet and serving as AP

Figs. 1 and 2 illustrate a wireless system for connecting mobile devices to

the Internet through an access point. It may use a novel method for performing the deployment of APs, i.e., the method that allows devices to function at the same time as STAs and as APs. For example, a laptop 11 is connected to the Internet through access point AP 10, and at the same time, laptop 11 shares its connection for other STAs by operating as an AP. Thus, other STAs 12 and 13 look at laptop 11 as an AP, and can connect through it to the Internet.

When laptop 11 is connected to AP 10 through a wired connection, it can simply set its wireless connection as an AP (Infrastructure mode). However, when laptop 11 is connected to AP 10 through a wireless connection, the situation is more complex. Disclosed is a novel method in which laptop 11 can be connected to AP 10 and serve as an AP using only a single wireless network card. Laptop 11 connects to AP 10 just like any other STA, and at the same time runs the protocol stack of an AP.

Laptop 11 uses the same channel as AP 10, and transmits a beacon message such that the beacon of AP 10 and the beacon of laptop 11 are expected not to collide in time. Laptop 11 derives and updates its internal clock from AP 10, but adds a constant delay (to make his beacon appear with a delay after AP 10). In another embodiment, laptop 11 does not add a delay to the time of AP 10, but sets the beacon period to a value, such that the greatest common denominator (GCD) between its beacon period and the beacon period of AP 10 is the smallest that is possible. Such a choice of beacon period ensures minimal collisions between the beacons.

In the preferred embodiment, laptop 11 will run a Network Address Translation (NAT) and a DHCP server as part of his protocol stack. Running DHCP enables laptop 11 to provide an Internet address to STAs that connect to it. Running a NAT allows laptop 11 to connect other STAs through it, while keeping conformance with regards to AP 10 - To AP 10 all the communication appears to be originating form laptop 11.

The software package 31 may be contained in the laptop 11, or in the laptop 11

and the STA 12, for example.

Viral Spreading

Many networks suffer from the network effect in their infancy, in which the first users have no incentive to join the network. However, the network is of great value once many users are in the network.

The following method and system attracts the first users, and provide an increasing value as the network grows. The first very few laptops with the software are installed and deployed in key areas by the network initiator. The software running on the laptop 11 has functionality 31 as follows (explained through an example):

Laptop 11 acts as an AP and allows other STAs to connect to it. To further lure STAs, the SSID (Service Set Identification - this is the name of the network that users see when looking for an available network) can be set to "Free Internet" or another name that will attract roaming laptop users to log-into it while searching for wireless networks.

Assume a user using a laptop called STA 12 connects as described above. Once STA 12 is connected to the laptop 11 (laptop 11 serves as an AP), no matter which web site the user tries to enter, the software 31 on laptop 11 forwards

the connection to a special web site 30. The web site 30 informs the user (STA 12) that, in order to use the free connection, it must install a software with functionality 31. The deal is that the user is allowed the free access at this location, but it is requested to share his own connection when he has one at his disposal. The user then downloads and installs the software with functionality 31 (See Fig 1.B which shows software with functionality 31 running on STA 12. Once laptop 11 identifies that STA 12 has functionality 31

running, it allows it a wider access to the internet (or a full access to the public Internet).

Thus STA 12, which originally did not have functionality 31 running, but its user wished to connect to the internet, ended up with functionality 31 installed and running on STA 12, and the user received a working internet connection. When the user moves STA 12 to another area in which it connects directly to an AP (which might be locked), it shares its connection with other STAs, which are also motivated to install functionality 31. Thus, functionality 31 can spread quickly among STAs, and the total area that is served grows larger, where each additional STA spreads the network further.

Laptop 11 together with its software might need to use two different security parameters at the same time - one towards AP 10 (which might be locked), and open security towards other laptops - so they can connect with no security settings. Once functionality 31 is running, it can establish a secure connection with laptop 11 as a secure layer on top of the fundamental insecure wireless.

Connection through multiple access points

Another novel method of the present disclosure allows STA 14 to connect simultaneously through two or more APs, see Fig. 3. For example, STA 14 connects through both laptop 11 and laptop 21 to the internet. Thus, STA 14 can enjoy a more stable connection even if both connections (through laptop 11 and 21) are in borderline quality. Furthermore, even in case the connections are not in borderline quality, they can be used to provide STA 14 a broader connection to the internet, or balance his traffic such that laptop 11 and laptop 21 carry a lighter burden per laptop with regards to the extra bandwidth they carry due to STA 14.

Multiple connections also allow handovers. When a STA is moving from one place

to another, it can first establish a new connection and then the old connection is terminated, practically leaving the STA connected.

When laptop 11 and laptop 21 use the same WiFi channel, STA 14 connects to both laptops by creating two protocol stacks on the MAC (Media Access Control) layer. When laptop 11 and laptop 21 operate on different channels, STA 14 agrees with laptop 11 and laptop 21 on period of times in which laptop 11 sends packets to STA 14, and periods of time in which laptop 21 sends packets to STA 14. STA 14 makes sure that these periods of times do not overlap, thus, STA 14 sets the channel according to the period, such that it listens on the channel of the laptop that might transmit to it. If the laptop has packets pending for STA 14 it queues them for transmission in the transmission period.

In order to have a faster connection through the two (or more) connections, STA 14 downloads/uploads some of the information through one connection, and the rest through the other connection. For example, when downloading a web page, STA 14 can download the text through one connection, and download the images through the other connection.

In another embodiment a remote site 50 with a fast Internet connection acts as a proxy of STA 14. Incoming and outgoing packets are forwarded between STA 14 and remote site 50. The packets are sent using error-correction codes that allow reconstructing the data even if some packets are lost on one connection, but some packets reach the destination using the other connections. The role of remote site 50 can be assumed by a service provider, by computer with a software that the user installs in his premise, or by another user with high bandwidth.

When the STA moves from one location to another, new connections are being established, while other connections are being disconnected. However, as long as there is at least one active connection, the STA will stay connected to the Internet continuously and seamlessly.

Sharing Internet Connection between Laptops

When laptops 21 and 11 are within radio (wireless) contact (or through the mitigation of other STAs), each laptop can treat the other as another connection at his disposal. Thus, the maximum data rate available for each laptop can be significantly extended, much like the case with a STA connected to two laptops.

Fig. 4 details a method for fast spreading the Vagabee software by providing free wireless access to the Internet. The method includes:

a. First STA transmits "AP available" WIFI info 41
b. Info is presented to Guest 42
c. Guest chooses our AP? 43
d. Allow limited access to Guest including our Web site 44
e. Guest agrees to use our service? 45
f. Download connectivity software to Guest and activate it 46
g. Connect Guest to Internet and allow wider access 47
h. Guest transmits "AP available" info and further spreads our service 48
** End of method **

Note: It is not mandatory to perform all the above stages. The more important steps are 45 - 47 or any similar implementation.

Fig. 5 details the dual mode connectivity of a STA also functioning as an AP with the Vagabee method and software. The method includes:

a. First STA associates with an AP as a regular STA 411
b. First STA activates "AP" protocol stack with open security 412
c. Guest chooses our AP? 42
d Address translation to connect Guest to our Website 445

** End of method **

The above method has been implemented by the present inventor on a communication device using the Intel 2200 chipset, just as an example to show that it can be done. The present inventive approach and method may be used towards similar implementations with other communication devices.

Figs. 6A to 6F detail stages in a wireless network evolvement and spreading of the Vagabee software, including:

FIG. 6A: There is a Laptop 11 connected to the internet by wireless through the access point AP 10.

FIG. 6B: The Laptop 11 also functions as AP using the Vagabee software, thus allowing free access for STA 12 through Laptop 11.

FIG. 6C: STA 12 joined the Vagabee group, created a new AP to also connect Laptop 121. A long chain can thus be formed.

FIG. 6D: each AP can connect several new devices, as illustrated here with Laptop 122.

FIG. 6E: a multi-AP network may be configured, with a plurality of devices being connected through both AP 10 and AP 20. A device such as Laptop 122 can be simultaneously connected through more than one AP to the internet.

FIG. 6F: As the initiated device Laptop 124 moves to another location and connects to AP 24 (maybe it has a license or privileged access there, while Latop 125 and STA 126 cannot connect directly to AP 24 due to distance or lack of security parameters), the Vagabee software in device 124 opens a free AP at

that location, now being utilized by Laptop 125 and STA 126 to connect to the internet. At a separate location, AP 10 may still operate and connect STA 12, Laptop 121 etc.

Security

Another important issue is the security of the system. Consider a situation (shown in Fig.2) in which laptop 11 agrees to act as an APs, but it does not agree to allow STA 13 and STA 14 to access his inner network (i.e., it allows STA 13 and STA 14 to access the internet through his network but does not allow them to access computers in his network. For example, a private server 40 should not be accessible to them). On the other hand, STA 13 wishes to use laptop's 11 network, but might not wish laptop 11 to be able to tap into the data that STA 13 exchanges with Internet servers. The current disclosure addresses these two problems using a novel method. First, external STAs are not allowed to access to the inner network by not allowing them to access to local IP addresses. Second, STA 13's privacy is protected by tunneling its sensitive traffic to a trusted network site 50, and STA 13 accesses the internet through its tunnel to the trusted network site 50, which acts as a proxy of STA 13.

To prevent STAs from accessing the inner network, laptop 11 blocks all traffic from the guest STAs to internal addresses (i.e., addresses that appear only in local networks and not in the public internet, such as 192.168.*.*, or 10.*.*.*, and 172.16.0.0 - 172.31.255.255). Another method, which can be applied independently, is to allow the connection if it is at least x hops into the Internet, where x is the maximum number of hops in the local network (which can be discovered by performing a traceroute command). Another method is to allow access to addresses which have an IP address with a different prefix, as internal networks typically have the same prefix on the IP address. In another method, laptop 11 allow only packets to and from known servers such as trusted server 50 (i.e., white listing the allowed addresses).

To protect the privacy of STA while it is surfing, its traffic can be tunneled to a trusted network site 50, which acts as its proxy. The network site can be replaced by simply tunneling the connection to another node in the network, and switching the network node once in a while. The access to the remote nodes is made without identifying the STA, but only proving that it belongs to the group of STAs, thus, its privacy is preserved. The frequent switching of remote nodes eliminates the possibility that a remote node can gather a significant amount of private information from peeking into the communication. The list of available remote nodes can be kept by a directory service, which can be distributed in a peer-to-peer fashion.

In another embodiment, the remote node is a trusted computer installed by the user. Such a configuration has the added benefit that the user can access internal nodes in his own private network, effectively having a Virtual Private Network (VPN) with his home network.

Fig. 7 details control and security aspects of the Vagabee spreading method including:

a. First STA transmits "AP available" WIFI info 41
b. Info is presented to Guest 42
c. Guest has Vagabee software? 425
d. Guest agrees to use our service? 45
e. Download connectivity software to Guest and activate it 46
f. Connect Guest to Internet and allow wider access, excluding private servers/sites 472
g. Guest transmits "AP available" info and further spreads our service 48
h. Guest uses encryption and secure website to preserve privacy from connecting STA 481
i. Establish best route for all STAs 482
adaptive to changes in network.

Load balancing.
Connections thru multiple routes.

j. Connection time > Ts ? 483
k. Disconnect/change connection 485
** End of method **

Note: Not all the steps above are mandatory; a method may implement only part of the steps in the above method.

Maintaining Fairness

It is desirable to avoid an unfair situation in which one user exploits the network by continuously using a connection without ever sharing a connection. If many users follow these lines, the network experience will degrade as there will be only a small number of laptops connected directly to APs. A novel mechanism detects that a STA is connected to the internet by noting that the same STA (using the same laptop) connects from the same small area (or through the same AP) for a long period of time (i.e., beyond a threshold). For example, this threshold can be set to two weeks. Once a STA passes the threshold, the functionality 31 notes the user that the threshold is reached. The user is then required to move to another area or pay a small fee to continue and access the AP.

Functionality 31 may note the user when the threshold is being approached, even before it actually reaches it. It can then give a pre-warning to the user.

The laptop is identified through his account information, through the MAC address of his network card, and other machine-specific information, such as the serial number of the hard-disk.

Fig. 8 details coordination and control aspects of the Vagabee spreading method for the first, connecting STA, including:

a. First STA connects to AP in "AP" mode 412

b. Set wireless connection as "Ad-Hoc" using the same channel as the AP 413

c. Transmit beacon message at a delay after AP or set beacon period so as to minimize collisions 415

d. Act as AP for additional STAs, while preventing them access to its inner network 416

e. Replace commercial banners for own site and also for STAs connected to this STA 417

f. Security Option: Allow connection of connected STAs only if it is at least X hops into the Internet 418

g. Maintaining fairness: demand a connected STA to disconnect or move or pay after a predefined time 419
** End of method **

Fig. 9 details multi-AP, fast configuration setting and handover aspects of the Vagabee spreading method for the second, to be connected STA, including:

a. Connect through a first AP 481

b. Activate Vagabee to provide AP service to other STAs 482

c. Search for additional paths to 483
establish multiple simultaneous connections thru multiple APs

d. Copy configuration of connecting STA, 484
to gain direct access to the initial AP, or receive connecting instructions for STAs with trusted hardware

e. Preserve privacy using tunneling 485
to a trusted network site for sensitive traffic

f. Perform handover whenever necessary 486

g. When moving to a new location: 487
establishing a connection with available AP,
Activate Vagabee to provide AP service to other STAs

h. Maintaining fairness: demand a connected STA 419
to disconnect or move or pay after a predefined time

i. Control over advertisements (optional)
** End of method **

In a novel method hereby disclosed, the functionality 31 can scan the web pages that pass through it and block or replace the advertisements on the page depending on various data such as the user name, the user location, etc. The advertisements can be performed in collaboration with the web site that is being surfed into, or without.

Note: the functionality (or software module) 31 is an important part of the present method, a minimum requirement to allow Xiopea(tm) spreading. Moreover, module 31 need not include all the possible things that this

functionality can include, rather just the bare minimum directed toward allowing a connection to a STA in return to supporting the spreading of the this software.

The site 30 can instruct functionality 31 as to which advertisements should be removed or changed, and which advertisements should be placed. New advertisements can also be added in places that there were no advertisements to begin with.

The software 31 running on laptop 11 can replace the commercial banners that appear in the web pages that laptop 11 surfs into, as well as the web pages that STA 13 surfs into. The banners can be stopped, replaced, and made specially targeted to the user, for example based on his location.

Configuration of Wireless Networks

An annoying task associated with wireless networks is the configuration of a STA to work with a network. The security settings are especially annoying, and currently, many people avoid securing their network due to the cumbersome setting procedure.

A novel method is disclosed to perform easy configuration of a wireless settings. The method is composed of two parts, the first is establishing the settings for the first device, and the second part is establishing the settings for the rest of the devices. First part: Assume a user on laptop 11 is connected to his wireless AP 10. If AP 10 is not set to use encryption, the user can ask (or be offered) to secure his network. Functionality 31 automatically accesses the interface of AP 10 and configures it with security settings. Laptop 11 is also set with the security settings. The settings are also stored in an account in web site 30, for future use. Site 30 can also provide functionality 31 with the information on how to set the security setting on the specific model of AP 10.

Second part: When the user uses another device STA 12, he connects to the network through functionality 31 on laptop 11, which redirects him to web site 30. On the site, he can log-in using his account details. Web site 30, through functionality 31 which is running on laptop 11, discovers that the two devices (laptop 11 and STA 12) are both connected through AP 10, and both belong to the same user account. As a result, web site 30 offers the user to reconfigure STA 12 to work directly with AP 10. The user is advised to download functionality 31 to STA 12, and run it. Once functionality 31 is running on STA 12, it configures STA 12 with the settings of the network (which are retrieved from web site 30, or directly from laptop 11).

Fig. 10 details multi-AP, fast secure configuration setting and redirection aspects of the Vagabee spreading method for the first, connecting STA, including:

a. First STA connects to AP in "AP" mode 412

b. Establish settings for first STA: 511
configure AP with secure settings, set STA with secure settings.
Store settings in web site.

c. Redirect a connecting STA to the web site 512
to configure it with secure settings.
** End of method **

Fig. 11 details multi-AP and fast configuration setting aspects of the Vagabee spreading method for the second, to be connected STA, including:

a. Connect through a first/available AP 481

b. STA has secure sub-system trusted by the web site? 482

c. Web site allow it to retrieve the 483
settings of the network for direct connection

d. Both STAs use the same AP 484
and same user account?

e. Agrees to connect directly to AP? 485

f. Download functionality and activate it 486

g. Configure STA with the settings of the network 487
** End of method **

Many variations can follow to the above procedure, and should be clear to those skilled in the art. For example, the settings may be stored on laptop 11 instead on web site 30, the settings may be encrypted, and the sequence of events can be changed. The result is an easy configuration of the network by the user.

Fig. 12 illustrates the mobile stations (STA) with their covering Access Points (AP), where STA 11 is moving from the coverage of AP 31 to the coverage of AP 312. STA 12 is already in the coverage of AP 312, and another AP 313 has a coverage that intersects with both the coverage of AP 31 and AP 312.

A network infrastructure for other devices

Functionality 31 may allow devices that do not have the functionality 31 to access the network. Such a device receives a capability to be identified as eligible to access the network towards functionality 31, and it identifies as eligible to access towards functionality 31 on the laptop in order to gain access to the network. Such identification may include cryptographic means,

such as a digital certificate signed by an appropriate certification authority (CA) which gives the device the capability to be identified. Alternatively, the devices can be identified based on their MAC address. A username/password can be added for additional security.

Configuration of secure devices

It might be desirable to allow a device to directly connect to an AP, rather than connect through a laptop. When devices have a secure sub-system, i.e., a sub-system that is trusted by web site 30, web site 30 may allow it to retrieve the settings of the network (assuming that they are stored on web site 30), and configure the device to use the network.

As the device has a trusted sub-system, the settings can be stored in the sub-system, such that they do not leak outside.

Alternatively, functionality 31 can reconfigure the AP to allow access to a roaming device.

Displaying the coverage map

A problem often faced by users that wish to connect through wireless internet is that they cannot connect to the internet in their current location because the coverage in their area is locked, and they do not have access rights. A novel method and system helps users find the nearest location from which they can connect. Web site 30 holds a list of all access points from which users can successfully connect, together with all the list of APs from which are closed. The list includes the MAC address of each AP. Parts or all of this list can be downloaded in advance to a device, such as into laptop 11.

Then, laptop 11 uses the beacons of the APs which might be locked to determine its position (for example, www.SkyHookWireless.com uses beacons to determine

the location of a STA). Then, laptop 11 can display on a map the location of the user, and the locations of near by access point in which it can connect to the internet. The user can then go to the nearby locations and connect to the Internet. The list in site 30 can be constantly updated by information that STAs receive.

In another embodiment, the list of APs in site 30 can also hold the probability that the AP is accessible. The probability can change if the access is provided by a laptop rather than an AP, and the laptop may be present or not. An area covered by several independent APs, each with low probability, results in an area with higher probability of accessibility in the intersection of these areas. The probability of accessibility can be depicted in the map shown to the user, for example, by different colors representing the different probabilities.

It is understood that the method and system in the present disclosure may be used for the transmission of voice, data, multimedia or a combination thereof.

Gathering Physical Location

To display a map of coverage, the real-world physical location of STAs needs to be known. A novel idea is to use STAs that are equipped with both GPS (Global Positioning System) and WiFi to report back to a server (for example, web server 20), a scanning result and the physical location in which the scan was performed. The server can extract the physical location of the fixed APs and store it in a database. At a later time, when a WiFi-equipped STA that lacks a GPS receiver performs a WiFi AP scan, it can report the results to the server, which can use the database to determine the physical location of the STA. This physical location can be used to provide location-based services.

Fast Handover

A novel aspect of very fast handover is to practically almost complete the process of the handover before it even started.

Consider an example depicted in Figs 12 and 13, in which STA 11 is in conversation with TN 41 (TN - Termination node, the node with which STA 11 communicates, shown in Fig. 13), and STA 11 is moving from AP 31 towards AP 32. Also assume that a node GN 21 (GN - Governing Node, a node that is non-exclusively responsible for the mobility management in a certain geographic area for a given time, shown in Fig. 13) is in contact with STA 11, and it is assisting STA 11 during the handover process. STA 11 currently has an IP address, which was allocated to it by AP 31.

To complete the handover, STA 11 should be associated with AP 32, have an IP address assigned by AP 32, complete any second authentication that is required, and have TN 41 be aware of the new IP address, so it can forward the conversation to the new location. Note that in some scenarios (in some cases when there are firewalls or NAT devices between AP 32 and TN 41, the connection between STA 11 and TN 41 must be started from within AP 32 towards TN 41).

According to prior art, it appears that STA 11 cannot begin the handover process until it reaches the coverage of AP 32, since it cannot start the connection process. One novel solution (that requires changing the software of the AP) is to allow STA 11 to perform the connection process through the Internet, instead of performing it wirelessly. In this way, once STA 11 reaches radio connection with AP 32, it can start working immediately.

However, we are more interested in solutions where there is no need to change the AP. To achieve this goal, assume the existence of a non-moving STA 12 in

the coverage of AP 32 (we will somewhat soften this assumption later). According to the present invention STA 12 is in contact with GN 21, and receives instructions to impersonate STA 11 towards AP 32 (we will later discuss how to make it possible), and complete a connection process with AP 32 on behalf of STA 11 (including authentication, association, receiving an IP address, performing any second authentication/log-in procedure, and perhaps even opening connections or "punching holes" in the firewall).

Then, STA 12 communicates these parameters to GN 21 (once the parameters are communicated, STA 12 can return to its real identity). GN 21 communicates the parameters to STA 11 (and perhaps to TN 41), and thus, STA 11 does no longer need to perform the connection process, and once it reaches the perimeter of the coverage (we will later discuss how to identify this situation) it can immediately use the new parameters and continue communications without any delay. STA 11 (or GN 21) can alert TN 41 before the handover, so it can start and send information packets to the new location.

TN 41 may send the information in parallel to the old and the new location, and cease transmitting to the old location once the handover is complete (e.g., when it receives information from STA 11 with its address from the new AP). STA 12 may even open a TCP (Transmission Control Protocol, as used in the Internet) connection or send a UDP (User Datagram Protocol) packet on behalf of STA 11, if required.

This connection may wait for STA 11 until it reaches AP 32. If there is a timeout on these connections (either due to protocol, or due to firewalls), STA 12 or other bypassing STAs can send and receive -keep-alive- messages on behalf of STA 11 (as is instructed by GN 21). The timeout for each AP can be discovered over time by trial and error (or by discovering the APs type), and storing this information in GN 21 for future use. GN 21 can notify the STAs on the value of the timeout.

How STA 12 can impersonate STA 11:

To understand how STA 12 can impersonate STA 11 towards AP 32, we must understand how identity is established in the network. The basic identity in the network is the physical address which is known as MAC Address (Media Access Control Address), which is globally unique. Each manufacturer is allocated a portion of the address space and allocates a unique MAC address to every network card (including WiFi network card) that it manufactures. Then, the manufacturer burns the allocated address into the network card. However, in most network cards, an application can (temporarily) change the MAC address of the card to another MAC address.

The MAC address is not used for end-to-end communications over the internet, but usually only for communications within the same physical network. For example, STA 12 communicates with AP 32 using MAC address, but GN 21 is not usually aware of the MAC address of STA 12. The MAC address is universally unique. We use the feature of temporarily changing the MAC address in the network cards in a novel way, allowing STA 12 to impersonate STA 11.

Therefore, in the instructions that GN 21 gives to STA 12, it mentions the MAC address of STA 11, so STA 12 can assume the MAC identity of STA 11. Then, STA 12 can complete the association with AP 32 (using the MAC address of STA 11)), in which it receives the Association ID (AID), and completes a DHCP protocol in which it receives an IP address to be used with the MAC of STA 11 while it is using AP 32. STA 12 can also perform a second authentication and log-in on behalf of STA 11.

STA 12 sends the connection information back to GN 21, which forwards it to STA 11. STA 12 can return to its original MAC address, but the allocated resources at AP 32 remain allocated, as from the point of view of AP 32, STA 11 is already connected and in coverage. In order to avoid losing messages that are sent to STA 12 during its impersonation to STA 11, it can either

continue and listen using both its own MAC address and STA 11's MAC address, or it can issue a -power-save- mode command to its serving AP. The power save mode indicates the AP that the STA is sleeping for a while, in which time the AP is buffering the incoming data packets. Therefore, even if STA 12 is connected to the internet using another AP, it can issue a power-save mode command, possibly change the frequency, and perform the connection on behalf of STA 12. It can return to its serving AP once the connection is established, or pool for incoming messages once in a while.

First Softening of the Assumption that STA 12 is in the coverage of AP 32: What if STA 12 is not in the coverage of AP 32, and there is no other station in AP 32's coverage- The following process can be performed in advance, well before a handover is needed. GN 21 can ask (in advance) stations that pass through AP 32 to connect and receive an IP address from AP 32 using some MAC address. The MAC address is not necessarily the MAC address of STA 11, as the process is not specific to STA 11. The stations send the connection details to GN 21, which stores the AID, the MAC, the IP address and other connections details in a pool for future use.

The pool may even contain UDP or TCP connections, which may be kept alive by bypassing STAs (against timeouts of firewalls, Network Address Translator devices (NAT), and protocol timeouts). UDP and TCP connections in the pool are targeted to some node in the network that can forward information for other nodes (for example TN 41). When a connection is required by some STA, the pool is queried, and a resource can be allocated and applied by a STA. As a result, a station might change its MAC address and IP address every time it moves between APs. If the station moves very fast between these access points, GN 21 can predict the direction in which the station is moving based on past movements, inform TN 41 of the possible future addresses.

Using this method, TN 41 can send data to the new address even before the

station actually moved there. In some implementations of the APs and firewalls between AP 32 and TN 41 the STA must first send data before it can receive any data, otherwise, the firewall may block the incoming data, or a NAT (Network Address Translator) device might not know where to forward the data. The restriction, that the STA must be the first to send data, is usually required due to security policy that allows only outgoing connections, or due to NAT device that need to relate an internal IP address and port number with an external IP address and port number.

For example, in most NAT implementations a connection must be established from within the NATed zone (e.g., the AP coverage) towards the internet. Many firewalls also require that the connection is established from the private network towards the internet (rather than allowing incoming connections from the internet towards the private networks). In these cases, the data that TN 41 sends is not transmitted by AP 32 until the station reaches the access point and transmits information back to TN 41. Depending on the type of firewalls and NAT devices, TN 41 might be able to predict a port number to which it should send such messages before the first outgoing data packet is transmitted.

Another associated novel disclosure is that the same MAC address and IP address can actually be used by more than one STA. The differentiation between the STAs can be performed by using higher protocol identities such as different ports (for example TCP ports). Using the same MAC and IP address in more than one STA is not problematic for packets that are sent from the STA.

However, while receiving an incoming packet, only one STA should send an acknowledgement. As each STA knows the ports that are in use, it only acknowledges messages that are designated to it. GN 21 can coordinate between the STAs such that they do not use the same ports. For example, if there are at most n stations using the same MAC and IP address, station i will allocate port numbers that are equal to i modulo n. Another solution is to choose the

port number at random. If each STA uses one port at random, according to the birthday paradox, port collisions occur with very low probability as long as the number of connections is smaller than about the square root of 65536 (i.e., when there are less than 256 connections using the same IP).

Another idea is to change the software at the AP such that it can communicate with GN 21 and perform the connection procedure on behalf of STA 11.

Knowing who are the adjacent APs and the location of a STA:
It is useful for a station STA 11 to know the identity of the adjacent APs that the station might hand over to. The identity of an AP can be established in several ways: The SSID (Service Set ID) of the AP is usually broadcasted by the AP using periodical transmissions known as beacon. However, two adjacent AP may have the same SSID. In such a case, the MAC address of each AP is different, and APs can be differentiated based on their MAC address. Some APs do not transmit their SSID, but they still broadcast beacon messages with their MAC address. Even if the AP is locked and encrypted the MAC address is transmitted, and it is transmitted without any encryption. In this way, STA 11 can know the identity of adjacent APs, and infer its location.

Scanning by Idle STAs:

In a preferred embodiment, GN 21 collects information about APs which are adjacent. Idle stations (i.e. stations which are not in an intensive data transfer) can perform a scanning operation once in a while. As a result they learn the MAC address (and possibly the SSIDs) of the APs within radio reach. The STAs can then send this information to GN 21 which collects it. The idle STAs can also perform tests to check what is the accessibility parameters of an AP (e.g., is it an open and free AP, is it a locked AP and the password is available from GN 21, is it locked and there is no free access to the AP, is there a captive portal, does GN 21 have a username/password available for the

captive portal, etc.). All this discovered information is sent to GN 21.

When handovers are performed, GN 21 takes note of the sequence of handovers that occur, and can learn common paths which are taken (for example, a road or a crosswalk might cause more likely paths than others).

It is very important that GN 21 knows in advance the AP to which STA 11 will be handed over to and when the handover will occur. Such a knowledge allows, for example, to alert TN 41 of the new location in advance. Gaining accuracy in the prediction of the handover (when and where) translates to better performance, as GN 21 needs to allocate a MAC address and an IP address to STA 11 in the new AP, and TN 41 might start to send data to the new location.

Therefore, knowing who the neighboring APs are, and their reception quality at STA 11 is very important.

Scanning by a non-Idle STA

In principle, STA 11 can scan the surroundings once in a while and look for the beacons of adjacent APs, and thus measure the reception quality from each AP. However, such a scanning takes a lot of time (might even take couple of seconds for a full scan). Selective scanning for APs which are expected to be neighbors can reduce the scanning time, but it can still stay in the magnitude of a few hundred milliseconds. It is important to understand that during a contemporary scanning using current technology, STA 11 cannot receive or send messages from or to AP 31, which means that the scanning time must be reduced to reduce this disconnection time.

The novel disclosed method is that STA 11 will selectively scan for a neighboring AP in the following special way. Assume that STA 11 scans to see

if it can receive the beacon of AP 33, where the scanning is performed exactly when the AP 33 is expected to transmit its beacon. Therefore, the disconnection from AP 31 will be minimal. The problem is, however, that although the beacons are transmitted periodically, STA 11 does not know when a beacon is expected to be transmitted from AP 33. As the beacons are transmitted about every 102.4 ms (milliseconds); (many variations are possible)., STA 11 might be forced to wait on average 51.2 ms, which is a prohibitively long time to wait.

STA 11 may also transmit a Probe message to force a beacon to be sent especially for it- but a probe message requires a transmission that has implication on battery life. Furthermore, for the purpose of location finding, STA 11 might wish to be able to receive beacons of APs that will not answer the probe (due to range, policies, etc.)

We can safely assume that other STAs visited the area of AP 33 before STA 11, and that they have reported the rate of the beacons of AP 33 (e.g., a beacon every 102.4 ms). A problem that remains is that the beacons are scheduled according to the internal clock of AP 33, which might tick at a different rate than other clocks (and clocks tend to tick at different rates). Moreover, the clock of the visiting STAs is probably not exactly synchronized with the clock of STA 11, which makes the process inaccurate.

That is, even if STA 11 knows that at a specific time according to some STA's internal clock a beacon was transmitted, STA 11 will not know how to translate this information to his clock, as the clocks are probably not synchronized to such great accuracy (network time synchronization services such as the network time protocol (NTP) cannot be more accurate than a couple of tens of milliseconds, where in this case we need an accuracy of around one millisecond). The following novel method allows accuracy of microseconds.

The novel approach for time synchronization is to rely on a relatively accurate clock already available to STA 11: The 802.11 standard requires each AP to transmit in its beacon its clock (referred to in the 802.11 standard as timestamp). This clock must be the internal clock of the AP at the time of transmission in units of microseconds. Therefore, STAs can specify the value of the clock of AP 33 in terms of the value of the clock at the adjacent AP 31.

By measuring the timestamp of AP 31 and AP 33 at two different times T311 and T312 (based on the clock of AP 31), in which the time value of AP 33 T331 and T332, respectively, it can be established with reasonable accuracy that AP 33 clock ticks approximately r33/31=(T332- T331)/(T312-T311) times for every clock tick of AP 31. At time T313 in the future, the clock of AP 33 can be estimated as T333=T332+(r33/31)(T313-T312). Similarly, at time T334 the clock of AP 31 can be estimated as T314= T312+(1/r33/31)(T334-T332).

Beacons are scheduled to transmission when the clock of the AP modulo the beacon interval is zero, where the beacon interval is measured in microseconds according to the clock of the AP, it is fixed for an AP, and the value of the beacon interval is transmitted in the beacon. Therefore, GN 21 stores the relation r33/31 together with T332 and T312 and the beacon interval of AP 33 and AP 31, and reports it to STA 11 such that it can extrapolate the time at AP 33 and infer the time of the beacon transmission.

Once STA 11 succeeds in receiving a beacon from AP 33 it can report the times to GN 21, so that GN 21 can keep its time tracking accurate. Furthermore, the scanning allows GN 21 and STA 11 to make the best handover decisions based on the knowledge of the approximate location of STA 11 with respect to the neighboring APs.

A technical problem to be solved is that a STA can know the value T311 but cannot measure the value of T331 at exactly the same time of T311 , as these values are carried on the beacons of APs, which are transmitted at different times.

A solution is to measure the time of AP 33 T331' at a time close to T331, and note the time difference between the two measurements according to the STA's internal timer. As the measurements are very close to each other, the clock drift between the STA's timer and AP 33's timer is negligible, and we can estimate that T331= T331'+timediff, where timediff is the time difference between the measurements of T331 and T331' according to the timer of the STA. If there is a large clock drift after all (although it is not expected), it can be corrected by calculating the r value between the clock at AP 33 and the STA in a similar way to the way done for APs.

The location of STA 11 can be deduced from the reception quality, the reception strength and the identity of the neighboring APs. This location information can be taken into account while performing handover decisions, as well as for location based services or for other network applications.

It should also be noted that in Frequency Hopping, knowing the time of the AP has another special importance, as the frequency that the AP works in might depend on the time.

Fig. 14 details a preferred embodiment of the handover method, including:

a. STA prepares in advance for a handover: 541
* Assisted by another STA (or STAs)
* Optional: use the same MAC and IP addresses in more than one STA
* Learn the identity of adjacent APs
* Measure beacon strength from other APs

b. GN supports handover: 542
* GN keeps a pool of MAC and IP addresses
* GN sends the addresses to STA just before it enters the AP

c. STA reduces the number of Location Updates 543
by only updating when changing location area

d. GN transmits a pseudo-beacon including 544
MAC address, IP address, port number

e. Easy security configuration: 545
* The AP of the customer is not changed
* Establish secure channel with STA and Copy security information, or
* Connect the STA initially by wire

f. Gain access to locked networks 546
by joining the Vagabee service

g. Maintain simultaneous communication with 547
more than one AP.
Update net configuration responsive to changing circumstances
** End of method **

Fig. 15 details a method for implementing two connections with a STA.
The method includes:

a. Load BSS firmware to the NIC 415

b. Associate with AP using a first SSID 416

c. Load IBSS firmware to the NIC, but do not perform 417
dissociation from AP before loading the IBSS

d. Create an ad-hoc network using a second SSID 418

e. Communicate with AP and STA that connect to 419
the second SSID
** End of method **

Fig. 16 details a method for connecting other STAs, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs to connect to the Internet by 492
allowing them to connect to the second SSID.
The first STA decrypts and encrypts data packets as needed based on the security parameters of the first and second SSID (or APs), and performs address translations and forward packets between the second and first SSID to facilitate this connection for other STAs.
** End of method **

Fig. 17 details another method for connecting other STAs, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by 492
allowing them to connect to the second SSID. The limited access includes the ability to download a software that implements the current method.

The first STA decrypts and encrypts data packets as
needed based on the security parameters of the first and second SSID (or APs),
and performs address translations and forward packets between the second and

first SSID to facilitate this limited connection for other STAs.

c. When the first STA detects that another STA 493
has a software (which implements the current method) installed, the first STA allows the other STA a wider access to the Internet.
** End of method **

Fig. 18 details a method for configuring other STAs to directly connect to the AP, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by 492
allowing them to connect to the second SSID.
The limited access includes the ability to request an ability to access the first SSID directly, i.e. not through the second SSID and the first STA.

c. The first STA decrypts and encrypts data packets as needed based on the security parameters of the first and second SSID (or APs), and performs address translations and forward packets between the second and first SSID to facilitate this limited connection for other STAs.

d. Another STA requests an ability for direct access to 494
the first SSID

e. First STA prompts user: To 495
allow this access?

f. Security access parameters to access the first SSID are copied 496

from the first STA to the other STA

g. The other STA can access the first SSID directly 497
** End of method **

Fig. 19 details another method for configuring other STAs to directly connect to the AP, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by 492
allowing them to connect to the second SSID.

c. First STA's user can view a list of 498
connected STAs and can choose to allow access directly through the first SSID
to a chosen other STA

d. Security access parameters to access the first SSID are copied 496
from the first STA to the other STA

e. The other STA can access the first SSID directly 497
** End of method **

Fig. 20 details yet another method for configuring other STAs to directly connect to the AP, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by allowing them to connect to the second SSID. 492

c. Security access parameters to access the first SSID are copied to the other STA 496

d. The other STA can access the first SSID directly 497

** End of method **

Preventing Exhaustion of Resources at the AP

As discussed in the "Background" section, each AP has a limited number of Association IDs (AID) and usually, even a smaller pool of IP addresses (available through DHCP). Once this number of resources is exhausted, the AP might not be able to serve new STAs. A situation where IP addresses are exhausted can happen very quickly: for example, consider an AP in a very busy location, where there are many STAs that connect to the AP only for a short period of time. Each STA performs the connection process and obtains an IP address using DHCP, but as it disconnects it might not release the IP address.

The pool of IP addresses in an unmanaged AP is usually limited to about 200 addresses, with many consumer APs supporting only tens of addresses. A device is assigned the IP address for a given period of time (known as the lease time). Many times, the lease time is set in a magnitude of days (although the granularity is seconds), and in many other instances the lease time is set to a magnitude of hours. In such a situation the pool of IP addresses runs empty very fast.

However, in this disclosure for fast handovers, GN 21 keeps a pool of MAC addresses with associated IP address. Just before a STA enters the AP, GN 21 can send it a MAC address and an IP address that are already associated with

the AP. Therefore, the STA can connect even if the AP has no resources left for new STAs. Combined with the above disclosure that allows several STAs to share the same MAC address and IP address, an AP can serve more APs than its IP resources, even above its limit on the number of associated STAs.

Saving Battery Power by Reducing Location Updates

A novel disclosure of this invention is a method to reduce the number of location updates that are needed in WiFi, when a STA is idle. A location update is the process in which a STA informs an entity in the network of the current location of the STA (the notification can take many forms, including opening a TCP connection, or sending UDP packets). In prior art for WiFi networks (with for example mobile IP, or SIP - Session Initiation Protocol), a location update is required whenever the IP address of the STA changes (for example, when moving between APs of different subnets) - even if the STA is idle.

The novel method allows defining a location area for WiFi, such that a STA needs to perform location update only when it moves between APs that belong to different location areas, but does not need to perform location update when it moves between APs of the same location area as long as it's idle.

We assume that the APs are divided into location areas, and for each location area there is a node in the network that is in charge of this location area. For example, assume GN 21 is in charge of a location area composed of AP 31, AP 32, and AP 33.
How does a STA know which AP belongs to the location area- Either GN 21 gives it a list of all the APs that belong to the location area, or GN 21 transmits a pseudo-beacon in each AP.

A pseudo-beacon is a novel disclosure of this invention. It is a message that GN 21 can periodically transmit in each AP. While some APs might permit a remote node to transmit a message in the AP, other APs might not allow it. In

the novel method, a certain MAC address, IP address, and possibly port are allocated in each AP for the purpose of pseudo-beacon transmission. GN 21 asks some STA to open a connection using these resources to GN 21, and GN 21 sends the pseudo-beacon messages using this transmission. Each pseudo-beacon contains the parameters needed to listen to the pseudo-beacons in the adjacent APs. A STA that lacks these parameters can contact GN 21 and receive them.

From that moment on, the STA can move between APs in the same location area, and receive the parameters that are needed to listen to the pseudo-beacon from other pseudo beacons. For example, assume that STA 11 is located in AP 31 and is moving to AP 32. STA 11 listens to the pseudo-beacon at AP 31, and from the pseudo-beacon learns the parameters that are needed to listen to the pseudo-beacon of AP 32. Thus, STA 11 can move to AP 32 without any transmission.

Which STAs of the stations in AP 31 should acknowledge the pseudo-beacon- Preferably, none. However, some firewalls require minimum rate of outgoing packets to maintain an open connection. In such a case, once in a while GN 21 sends on the pseudo-beacon a message that asks any station to send an acknowledgement with some probability p. The probability that GN 21 states should be accommodated to the expected number of stations in AP 31 (GN 21 might not exactly know how many STAs are in the AP). If no STA acknowledges the pseudo-beacon for over the needed time, and the timeout of firewalls stop the incoming messages, then no pseudo-beacons are transmitted. In this case, a roaming STA will contact GN 21 after a certain period of time of probing for the pseudo-beacon has passed (and no pseudo-beacon is seen). GN 21 can request the STA to reopen the connection for the pseudo-beacon transmission.

If the STA is in a session with TN 41 with many packets received (e.g., above a certain threshold), it is considered non-idle (which we also refer to as "In conversation") and is treated as described above in "Fast handover".

However, assume that STA 11 is in idle mode (e.g., incoming packets below a threshold), it can move between APs of the same location area without performing location update. When a node TN 41 wishes to send data to STA 11, STA 11 should change its state from idle to in conversation. TN 41 contacts GN 21 (TN 41 might be forwarded to GN 21 through a system such as dynamic DNS (Directory Name Service) or another method, such as a Distributed Hash Table - DHT, or a peer-to-peer network).

GN 21 sends a paging message for STA 11 on the pseudo-beacon of all the APs in the location area. As STA 11 listens to one of the pseudo-beacons, STA 11 will receive the paging message. Then, STA 11 responds preferably to GN 21 (or to TN 41, depending on what is written in the paging message) by initiating an outgoing connection as described below. It should be noted that GN 21 can first page for STA 11 in the APs that have a higher chance covering STA 11, and the paging can repeat several times until STA 11 replies.

When a STA is required to initiate an outgoing connection it can use a resource (MAC, IP, or TCP/UDP with port, user/password) that is listed as available on the pseudo-beacon or on the paging message, or it can request its own resources from the AP. If two (or more) STAs use the same resources for a connection at the same time, GN 21 will detect it, and in the acknowledge message (or second message of the TCP handshake) will announce the identity of the STA that it answers to. The other STA is required to initiate an outgoing connection again. Once a connection with GN 21 is established, GN 21 can allocate resources to the STA such that it moves to be in conversation status. One of the resources that are allocated is GN 21 attention to accompany the STA as it might need to perform handover to another AP.

It should be noted that the location areas can overlap, meaning a single AP can belong to more than one location area. Upon the policy of the network, STA 11 might be required to perform location update when it reaches such a APs, or it may just give helpful information. If possible, a STA might prefer

to park on an AP that is within the same location area as its current AP, such that a location update is avoided.

It should also be noted that there is a tradeoff between the overhead that is spent during paging and establishing the connection, and the overhead that is being spent to keep a steady connection for each AP. The optimal point on the tradeoff depends on the rate that the AP switches APs as well as on the number of packets it receives and sends.

Easy Configuration of STA

When purchasing a new STA, it is required to configure the STA with the security settings of the existing network (in case the network is secure). If the network is not secure, the new owner usually only needs to select his network from the list of available networks that is received by the wireless network card.

Configuring the security might be a tedious job, as the security (authentication/encryption) code might be very long as known in the art, which the user might need to punch in. A novel solution for easy configuration is disclosed. Unlike previous solutions, the novel method does not require changing the existing AP of the customer. In one embodiment, software is run on a personal computer of the user (that is already configured to access the WiFi). Then, the software establishes a secure channel with the STA, and copies the security information from the personal computer to the STA. In this way, the STA learns the security parameters.

In another embodiment, the customer first connects the STA by wire to its network (or alternatively, the STA first connects using a connection it establishes through an already connected device, such as a personal computer). As the STA can receive and transmit signals on the wireless network and it is connected to the internet (through the other connection) at the same time, it tries to locate the web configuration of the AP on the wired network (most APs

have a web interface). In most cases, it is an easy job for the STA, as either the STA can locate the AP as it is the default gateway of the wired network, or it can try to find its IP by performing RARP (Reverse Address Resolution Protocol) using the wireless MAC address of the AP (which it can see off-the-air).

If none succeeds the STA can perform exhaustive search on commonly used IP addresses, or on very probable addresses, like all the IP addresses of the same subnet. Once the AP web interface is found, the STA tries to log into the AP. It can guess the default address or find it on a database that can be built on the web, with common default passwords for each manufacturer (the manufacturer and model will be usually sent by the AP during the web login process, or can be found out using the MAC address, which is unique per manufacturer). If the password for the AP cannot be guessed, the user is prompted for its password to complete the log-in. Then, the STA navigates to the security settings page and retrieves the password needed for the wireless network.

In the event that the procedure fails, the user is prompted for the security settings (which would happen without using the above method). For most common users and setups, the method succeeds (and for unsophisticated customers, who do not change the passwords - it succeeds in the majority of the cases). Thus, in the majority of cases, the setup is made much simpler.

Once the STA has access to the setup of the AP, it can (with permission from the user), open holes or forward certain port to some IP address. This IP address and port can serve as way that GN 21 can send and broadcast the pseudo-beacon, without a STA first opening a connection from the AP, and without worrying about timeouts (provided that there are no other firewall between the AP and GN 21). Opened ports can also help during the fast handover, such that TN 41 can directly send packets to the new location without a need for STA 12 to open the connection.

In corporate settings, the company can set a special server which gives the configuration to the phone, over the network.

Gaining Access to Locked Networks

While performing the above easy setup (or at any other time), the user is prompted if he wishes to join a swapping service. The swapping service allows the user to gain access to many locked networks (the locked networks of the other users that joined the swapping service), in return that he allows users to use his network for the purpose of connecting to the internet. If the user agrees, the access parameters to his network (encryption key, MAC address, default gateway, etc.) are securely stored in the network (for example in GN 21, and a backup server). The security information is securely sent directly into the hardware (or network card) of other STAs, when they need to connect using his AP.

As the security parameters are sent directly to the STA's network hardware, it can make sure that the communication that is established is designated outside the user's network, and will not jeopardize the computers on the user's network. Furthermore, GN 21 can monitor the amount of bandwidth that is consumed by visiting users, and to make sure their hardware limits the amount of used bandwidth such that the user does not experience a degradation of quality of his connection. Alternatively, the security information can be sent to the other STAs using other security measures, as known in the art.

In many scenarios it is enough to trust the software that runs on the STA to make sure all communications are targeted outside the user's network, such that it does not jeopardize the computers on the user's network, and limit bandwidth used by the STA.

The secrecy of the security parameters (such as the encryption key) can be cryptographically protected while on transit and storage, as known in the art.

Some APs limit the access of the subscribers by making sure that only specific MAC addresses connect to the network. As our methods as described above allow

to use the same MAC address for several users, this specific MAC address can be used when using the network that restricts the use with specific MAC address.

In case a STA tries to connect to an AP with a captive portal, a special application on the STA is running and performs the authentication and log-in automatically. GN 21 can store typical portal appearances, such that it can guide the STA on how to perform the authentication/log-in process. If the STA comes across a captive portal which is unknown or unexpected, it can locally store the web pages that it received from the captive portal and later transfer them to GN 21. GN 21 accumulates the reports and guides STAs how to log-in to the captive portal in the future. As part of the swapping service, GN 21 can store username/passwords to enable connection through the captive portal automatically.

Special care for data

The above description works well for both voice and data. TN 41 might be a mobile node as well, or a fixed node in the network. The transferred information between STA 11 and GN 21 can be voice, data, or their combination.

In case STA 11 wishes to communicate with a node that is not aware of the novel network, it can do so through a node that is aware of the network. For example, TN 41 can serve as a proxy for STA 11 (in a similar way to mobile IP). The node that is not aware of the network communicates with TN 41. TN 41 forward the information to STA 11. TN 41 can allocate an IP address (perhaps using NAT, or allocate ports using its own IP address) that will serve STA 11.

To balance the communication load, STA 11 can have several network nodes such as TN 41, TN 42 (not shown), etc, to be its proxies in parallel. In fact, the resulting connection between STA 11 and TN 41 can be seen as a layer 2 (MAC) connection, on top of which the communication is performed. In this setup, TN 41 serves as the default gateway of STA 11, and optionally can run a DHCP server and a NAT server.

Executing the Invention over a Peer-to-peer network

Another novel aspect of the above novel methods takes advantage of the fact that the wireless network is local in nature, as the APs are geographically adjacent. The system and method as described in this disclosure allows GN 21 to be responsible over a small geographical area with little interaction with its neighbors. As a result, the methods that are disclosed can be implemented by many small devices forming a peer-to-peer network that implements the methods, without the need to rely heavily on large servers.

Many nodes GN 21, GN 22 (not shown), can each control a group of APs. To make the system grow "automatically", it is possible to give users a "base" that will act as their point of presence in the network. For example, the base can assume the role of TN 41 as a Mobile IP proxy. The base can connect to the wired network at the premises of the customer. Some bases will assume the role of a GN, where the GNs can be managed by either a network control center, or through peer-to-peer protocols.

In early stages of deployment of the system, when there is still a small number of GNs, each GN might need to cover a large number APs. A general server can back-up all information that the GNs hold. To avoid the situation, where a single GN needs to cover a huge number of APs with pseudo-beacons, the system might not use the pseudo-beacon mechanism (although, it should be noted that with moderate computing power and network resources, a GN might be able to cover a few thousands of APs). In the worst case scenario of a peer-to-peer network, there is one base (GN) for each STA, and this GN act as the GN for the APs in the proximity of the STA.

When the STA moves, the coverage area in the responsibility of the GN moves with it. In this case, the GN can fetch information on neighboring APs from

the general server. When GN abandons an AP, it can store the information it gathered about it in the general server, for later use by possibly other GNs. In a system which is not based on many small GNs, a large GN can assume the role of the smaller GNs.

It should be noted that it takes some time to gather the information on the APs (such as timing, default gateways, etc). However, once a single STA passes in an area, it obtains the needed information. This information is later stored in the GNs and general server, for the benefit of all STAs in the future.

If a STA needs to handover into an AP which has no STAs currently in it, it might not have the needed resources pre-allocated (such as an associated MAC address and IP address), and might therefore need to gain it by itself. However, in many cases the STA can obtain resources at one pass in the area, and these resources (such as IP address) will stay for the next pass in the area (which can be hours later).

An Alternate Fast Method for Connecting to an AP - Removing the Assumption on the Existence of STA 12 in the Coverage of the new AP

A possible drawback of the above method of fast handover is that it requires that the pool of resources that GN 21 holds should contain a valid IP address of the AP that STA is handing over to. If the DHCP lease time is long enough, having a valid IP might not be a problem, but on short lease times with only a few STAs roaming it is desirable to perform handovers even if there is no valid IP available in the pool. Unfortunately, a typical execution of the DHCP protocol can take several seconds to complete, which might be too long for a fast handover. Interestingly, we observe that many APs will forward information even if the IP that is being used was not allocated by DHCP.

Therefore, we disclose the following method:
Choose a MAC and associate it with the AP (or use an Associated MAC without an associated IP address), choose a random (but valid) IP address, and use it.
The STA must use the correct default gateway settings of the AP (these settings can be stored in GN 21). If the STA wishes to use DNS, it must have the DNS settings of the AP (which can be received from GN 21), or DNS services are provided through GN 21.

Choosing a valid IP at random results in a very low probability of colliding with another IP address that is used in the AP. Note, however, that the STA still needs to authenticate/log-in through the captive portal in case such portal exists.

Another method that can be used to quickly obtain an IP address, such that the IP address is not already allocated by the DHCP of the AP is disclosed. Most DHCP implementations of AP send an ICMP (Internet Control Message Protocol) Echo Request (ping) before allocating an IP address, to make sure that it is unused. Therefore, STA can begin the DHCP protocol, then, wait for the ICMP echo request that the AP sends, and understand the IP that is going to be allocated to it.

Therefore, a STA can start using the IP address and respond to the ICMP echo request. It can then prematurely terminate the DHCP protocol (as it already got an IP). Alternatively, STA can use the IP address from the ICMP echo request without responding to it, and complete the DHCP process. If the IP address that is allocated during the DHCP is identical to the IP address (vast majority of cases), then STA simply saved time. Otherwise, it can move from the IP address of the ICMP echo request to the IP address that was allocated.

If no connection to GN 21 is available, the default gateway address can be guessed, as in the majority of the cases the default gateway address is one out of only a few addresses. Common addresses are: 192.168.1.1, 192.168.2.1, 10.0.0.1, etc.

Moreover, the default gateway is usually the AP itself. Its MAC address is known (as it is broadcasted in the beacon). Therefore, in most cases it is enough to forward packets to this MAC address (without knowing its IP address).

A STA with a Capability to Connect on Two Channels in Parallel

The present application discloses a STA which has a capability of communicating in two or more channels in parallel (for example, by using two wireless network cards). This capability can enable a STA to be connected to two APs in parallel without the need to implement sophisticated mechanisms that actually simulate this situation. Thus, a STA can connect with future AP while maintaining a connection through its serving APs. Being connected to two or more APs simultaneously allows greater bandwidth by utilizing two connections instead of one, and the performance of soft-handovers, i.e., the STA stays connected through one AP, while disconnecting from the second AP in the process of handover.

Fast uploading of digital camera pictures

Digital cameras might be equipped with WiFi. The owner of such a camera would like to upload his pictures from the camera to a server that stores the pictures on the Internet - the reasons for this may vary from being able to share the photos while on vacation with family members left at home, back up the pictures from the digital camera to the Internet server, or simply because the memory card on the camera is running out of space. A major problem is that to upload the pictures to the Internet may take a very long time, as pictures consume megabytes to store.

Solution: The camera sends the photos to a laptop over WiFi (this connection is very fast), then disconnects and the camera's user may move on. Then, the laptop uploads the pictures to the Internet server (this process can take a long time as it involves uploading a lot of data), but the laptop owner would not feel it as a burden, since the pictures can be uploaded when his Internet connection is not used for other purposes.

Method for uploading data files

In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for fast uploading of information from STAs to the Internet, comprises:

a. a first STA, such as a laptop computer, connects to the Internet;

b. a second STA, such as a camera, wirelessly connects to the first STA, and uploads the information using the fast and direct-wireless connection between the STAs;

c. The first STA temporarily stores the information;

d. The first STA uploads the information to the Internet through its backhaul.

** End of method **

Notes:

1. In the above method, the first STA may include for example a laptop or a personal computer, the second STA may include a digital camera or a digital video camera, and the information may include digital pictures or digital clips.

2. The second STA preferably disconnects from the first STA after completing to upload the information to the first STA, but before the first STA completes the upload of information to the Internet; the first STA completes the upload of information from its temporary storage.

3. An additional step in the above method may include the following:

e. at a later time, the second STA connects to the Internet and verifies that the information was uploaded correctly.

4. The information may be encrypted by the second STA before being transmitted.

It will be recognized that the foregoing is but one example of an apparatus and method within the scope of the present invention and that various modifications will occur to those skilled in the art upon reading the disclosure set forth hereinbefore.

CLAIMS

1. A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising:

a. wirelessly connecting a first STA to the Internet through a first AP with a first SSID;

b. remaining connected to the first Access Point (AP), the first STA creates a software-based wireless AP with a second SSID for wirelessly connecting other STAs to the Internet through the first STA.

2. The method for providing a wireless Internet connections to STAs according to claim 1, further including the step of:

c. a software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein.

3. The method for providing a wireless Internet connection to STAs according to claim 1 or 2, wherein each STA can be a laptop computer, PDA, wireless camera, wireless phone or a wireless device.

4. The method for providing a wireless Internet connection to STAs according to claim 1, wherein the first STA includes means for simultaneously connecting to the first AP and for opening the second AP, and means for transferring Internet packets between the first and second APs, while decrypting and encrypting the packets as needed based on the security parameters of the first and second AP, in addition to any communications with the Internet as required by a user of that STA.

5. The method for providing a wireless Internet connection to STAs according to claim 1, wherein activating, in the first STA, a single wireless card so as to operate in two modes at the same time, a STA mode and an AP mode.

6. The method for providing a wireless Internet connection to STAs according to claim 1, wherein the first AP does not provide wide, unconditional access to all.

7. The method for providing a wireless Internet connection to STAs according to claim 6, wherein a remote database may be accessed to determine if a STA without the software module should be allowed access, and how wide that access should be.

8. The method for providing a wireless Internet connection to STAs according to claim 1, 2, 3, 4 or 5, wherein the software module, upon detecting that the other STA does not have the software module therein, allows to install and activate the software module in the other STA and then provides wide access to the other STA.

9. The method for providing a wireless Internet connection to STAs according to claim 6, wherein the software module, upon detecting that the other STA does not have the software module therein:

c1. presents to the user of the other STA a message indicating that wide Internet access is possible upon loading a copy of the software module;

c2. waiting for that user's permission;

c3. after receiving that user's permission, the other STA. STA downloads, installs and activates a copy of the software module to gain a wide Internet access to the other STA.

10. The method for providing a wireless Internet connection to STAs according to claim 1, 2, 3, 4 or 5 wherein the step of connecting another STA comprises:

c1. the first STA connects the other STA, while limiting the set of Internet addresses and/or Internet sites the other STA can access, and wherein the accessible sites include a special web site from which the other STA can download the software module;

c2. the other STA downloads, installs and activates the software module therein;

c3. the first STA, upon detecting the installed and active software module in the other STA, then removes the limitations on the set of Internet addresses

and/or Internet sites the other STA can access.

11. The method for providing a wireless Internet connection to STAs according to claim 1, 2, 3, 4 or 5 wherein the step of connecting another STA comprises:

c1. the first STA connects the other STA to the Internet, while limiting the set of Internet addresses and/or Internet sites the other STA can access, and wherein the accessible sites include a special web site from which the other STA can download the software module;

c2. if so instructed by the user of the other STA, the other STA downloads, installs and activates the software module therein;

c3. the first STA, upon detecting the installed and active software module in the other STA, then removes the limitations on the set of Internet addresses and/or Internet sites the other STA can access.

12. The method for providing a wireless Internet connection to STAs according to claim 10 or 11 wherein the first STA, upon detecting the installed and active software module in the other STA, then removes part of the limitations on the set of Internet addresses and/or Internet sites the other STA can access, so as to keep some sites and/or addresses private to the first STA.

13. A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising:

a. activate in a first STA a software module for connecting with other STAs and to the Internet;

b. when required by the user to connect to the Internet and upon connecting with another STA which is already connected to the Internet and has a copy of the software module active therein, signal to the other STA that the first STA has a copy of the software module, and request to connect to the Internet through the other STA;

c. connect the first STA to the Internet through the second STA;

d. the software module in the first STA opens a second, software-based

wireless Access Point (AP) at the first STA for connecting other STAs to the Internet through the first STA, and wherein the software module only provides wide Internet access to other STAs which each has a copy of the software module installed and active therein.

14. A method for providing a wireless Internet connection to WiFi-enabled devices (STAs), comprising:

a. activate in a first STA a software module for connecting with other STAs and to the Internet;

b. connect the first STA to the Internet and open a second, software-based wireless AP for connecting other STAs to the Internet through the first STA;

c. when another STA connects with the first STA through the second AP and requests access to the Internet:

1) check whether the other STA has a copy of the software module installed and active therein;

2) if the answer is positive, then connect the other STA to the Internet;

3) if the answer is negative, then support the other STA in loading, installing and activating a copy of the software module therein and, after the software module is active in the second STA, provide wide Internet access to the other STA.

15. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein each STA may include a Portable computer, a Laptop, a PDA or a wireless phone.

16. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein each STA includes means for simultaneously connecting to the first AP and for opening the second AP, and means for transferring Internet packets between the first and second APs, in addition to any communications with the Internet as require by a user of that STA.

17. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein activating, in the first STA, a wireless card so as

to operate in two modes at the same time, a STA mode and an AP mode.

18. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein a STA connects to the Internet through two or more STAs simultaneously.

19. The method for providing a wireless Internet connection to STAs according to claim 18, wherein a STA repeats the connecting stage two or more times to connect to the Internet through two or more APs simultaneously.

20. The method for providing a wireless Internet connection to STAs according to claim 18 or 19, wherein a STA performs a fast handover by continuously searching for new APs to connect therethrough and connecting to newly available APs as older APs may become inaccessible.

21. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein the first STA prevents other STAs from accessing its inner network by limiting the access rights of the other STAs.

22. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein the other STA prevents the first STA from eavesdropping on its communications by tunneling its sensitive traffic to a trusted network site, and accesses the Internet through its tunnel to the trusted network site which acts as a proxy for it.

23. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein preventing STAs from using other STAs for their primary network connection for a long period of time, by detecting that a STA is connected to the Internet through the same STA for a long period of time, and disconnecting that STA.

24. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein preventing STAs from using other STAs for their primary network connection for a long period of time, by detecting

that a STA is connected to the Internet through the same STA for a long period of time, and disconnecting that STA if it refuses to pay for the continued use of that connection.

25. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for configuring STAs to connect to a wireless network, comprising:

a. activating a software module in first STA, which is already configured to access an Access Point (AP);

b. the software module copies the security information from the personal computer to another STA, thus setting the security parameters for the other STA as to allow access to the AP.

26. The method for configuring STAs according to claim 25, further including an authentication phase in which the other STA is authenticated by the software module or by a remote server before copying the security information.

27. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for configuring STAs to connect to a wireless network, comprising:

a. a customer first connects a STA by wire to its network, (or the STA first connects using a connection it establishes through an already connected device, such as a personal computer or laptop);

b. a software on the STA copies to the STA the security information gained through the wired connection, thus setting the security parameters for the STA.

28. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for performing fast handover for a first STA, from being connected to a first Access Point (AP) to a second AP, comprising:

a. a first STA communicates with a Termination Node (TN) and is in contact with a

Governing Node (GN), wherein GN is non-exclusively responsible for the mobility management in a certain geographic area for a given time and wherein the GN is in contact with another STA in the coverage area of the second AP;

b. the other STA receives instructions from GN to impersonate the first STA towards the second AP and to complete a connection process with the second AP on behalf of the first STA;

c. the other STA communicates the connection parameters to the GN and, once the parameters are communicated, the other STA returns to its real identity;

d. the GN communicates the parameters to the first STA, thereby eliminating the need for the first STA to perform the connection process itself;

e. when the first STA reaches the perimeter of the coverage of the first AP, it can immediately use the new parameters and continue communications with the second AP, without any delay.

29. The fast handover method according to claim 28, wherein the first STA alerts the TN before the handover, so it can start sending information packets to the new location.

30. The fast handover method according to claim 28, wherein the TN sends information in parallel to the old and the new location, and ceases transmitting to the old location once the handover is complete.

31. The fast handover method according to claim 28, wherein the other STA further opens a Transmission Control Protocol (TCP) as used in the Internet or sends a User Datagram Protocol (UDP) packet on behalf of the first STA, if required.

32. The fast handover method according to claim 28, wherein the connection process performed by the other STA on behalf of the first STA includes authentication, association, receiving an IP address and performing any second authentication/log-in procedure.

33. The fast handover method according to claim 28, wherein the connection process performed by the other STA on behalf of the first STA further includes

opening connections or "punching holes" in the firewall.

34. The fast handover method according to claim 28, wherein the connection waits for the first STA until it reaches the second AP and, if there is a timeout on these connections (either due to protocol, or due to firewalls), the other STA or yet other bypassing STAs can send and receive -keep-alive-messages on behalf of the first STA.

35. The fast handover method according to claim 34, wherein the timeout for each AP is stored in the GN for future use.

36. The fast handover method according to claim 34, wherein the value of the timeout is transmitted by the GN to the first STA.

37. The first handover method according to claim 34, wherein the connections parameters are not limited in use for the first STA, but are also available for the use of other STAs.

38. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for fast uploading of information from STAs to the Internet, comprising:
a. a first STA connects to the Internet;
b. a second STA wirelessly connects to the first STA, and uploads the information using the fast and direct-wireless connection between the STAs;
c. The first STA temporarily stores the information;
d. The first STA uploads the information to the Internet through its backhaul.

39. The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the first STA includes a laptop or a personal computer, the second STA includes a digital camera or a digital video camera, and the information includes digital pictures or digital clips.

40. The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the second STA disconnects from the first STA after completing to upload the information to the first STA, but before the first STA completes the upload of information to the Internet; the first STA completes the upload of information from its temporary storage.

41. The method for fast uploading of information from STAs to the Internet according to Claim 38, further including the step:

e. at a later time, the second STA connects to the Internet and verifies that the information was uploaded correctly.

42. The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the information is encrypted by the second STA before being transmitted.

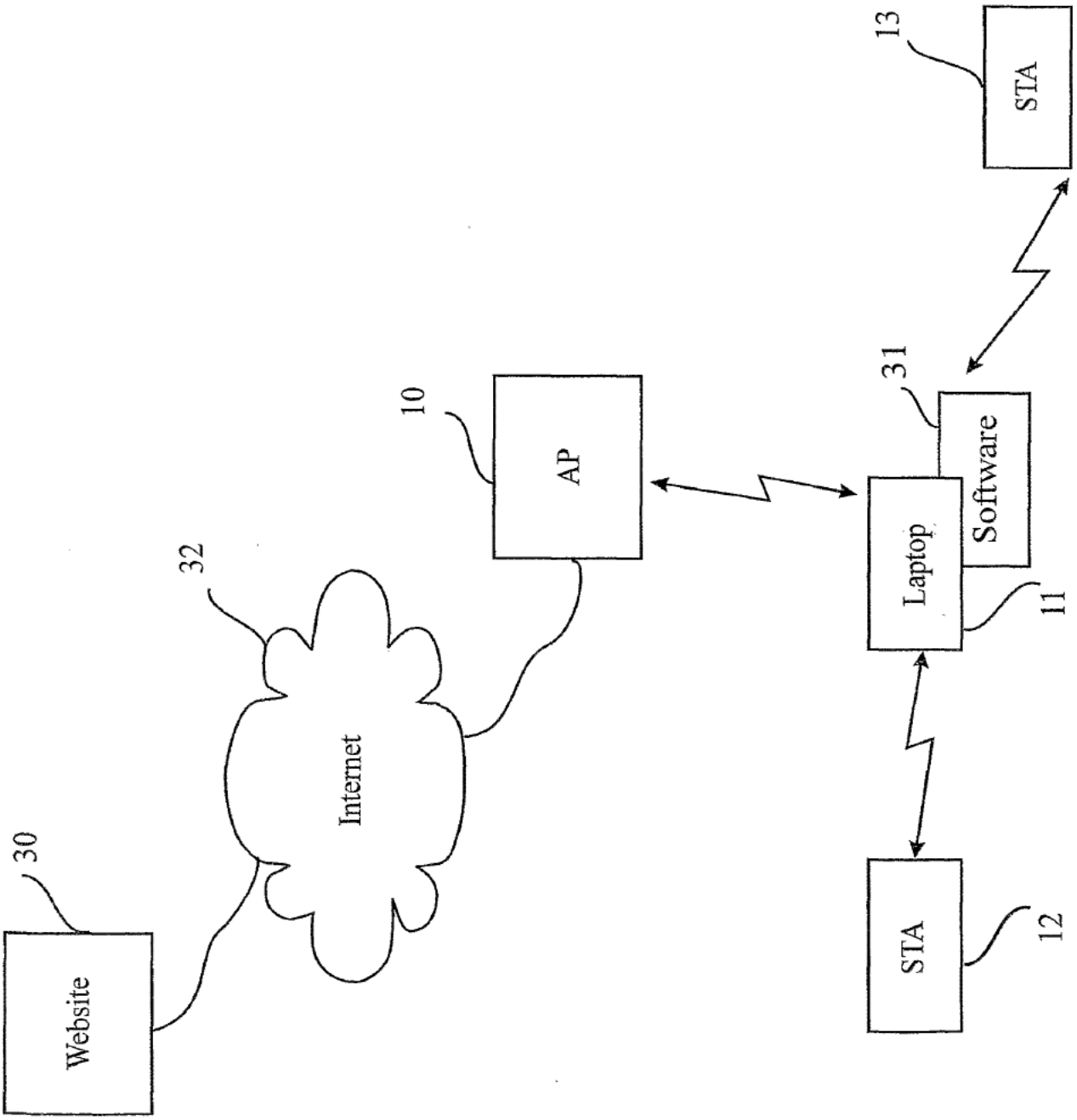

Website
30
Internet
32
AP
10
Laptop
Software
31
11
STA
12
STA
13

FIG. 1

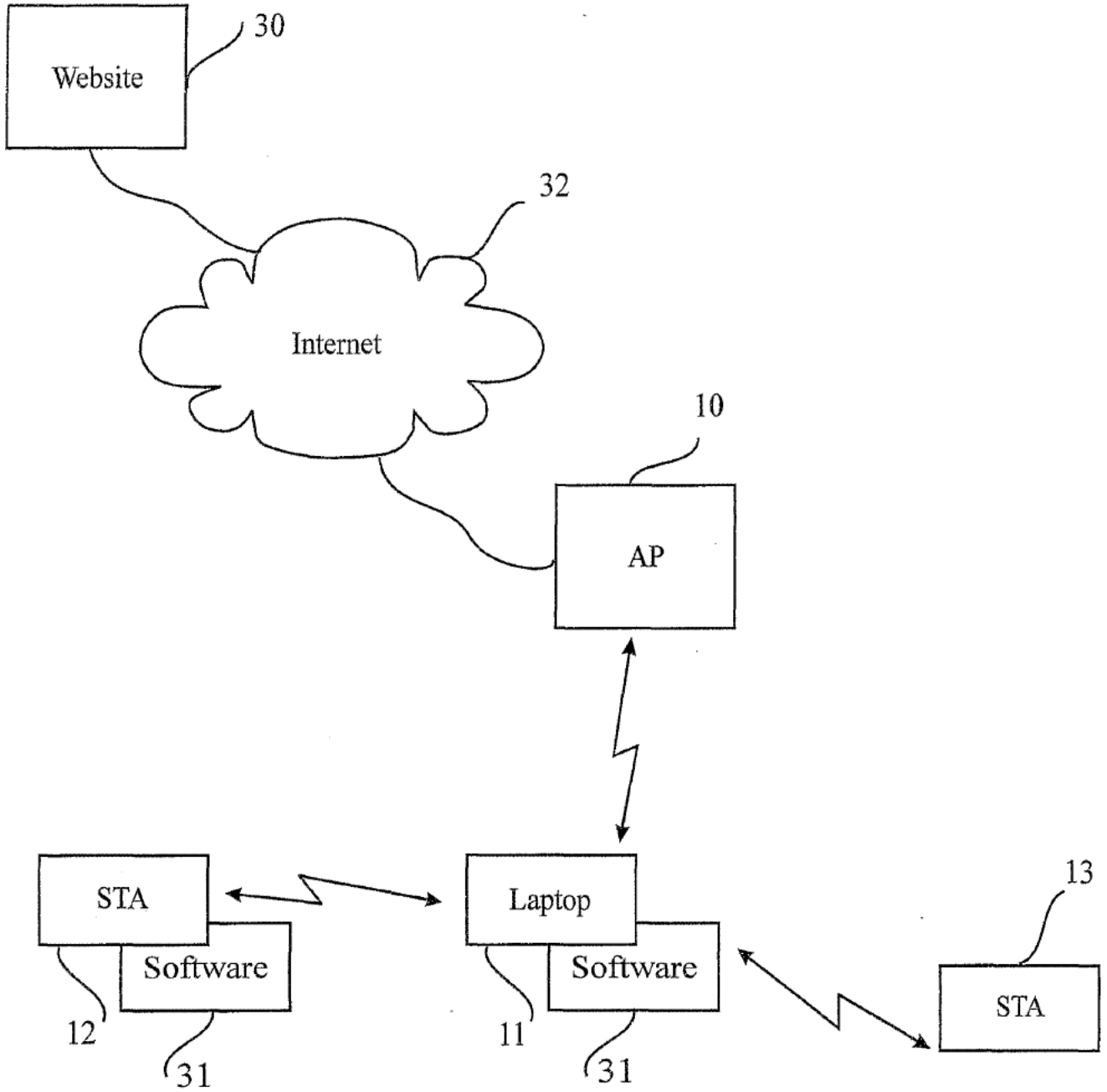

Website
30
32
Internet
10
AP
STA
Software
12
31
Laptop
Software
11
31
13
STA

FIG. 2

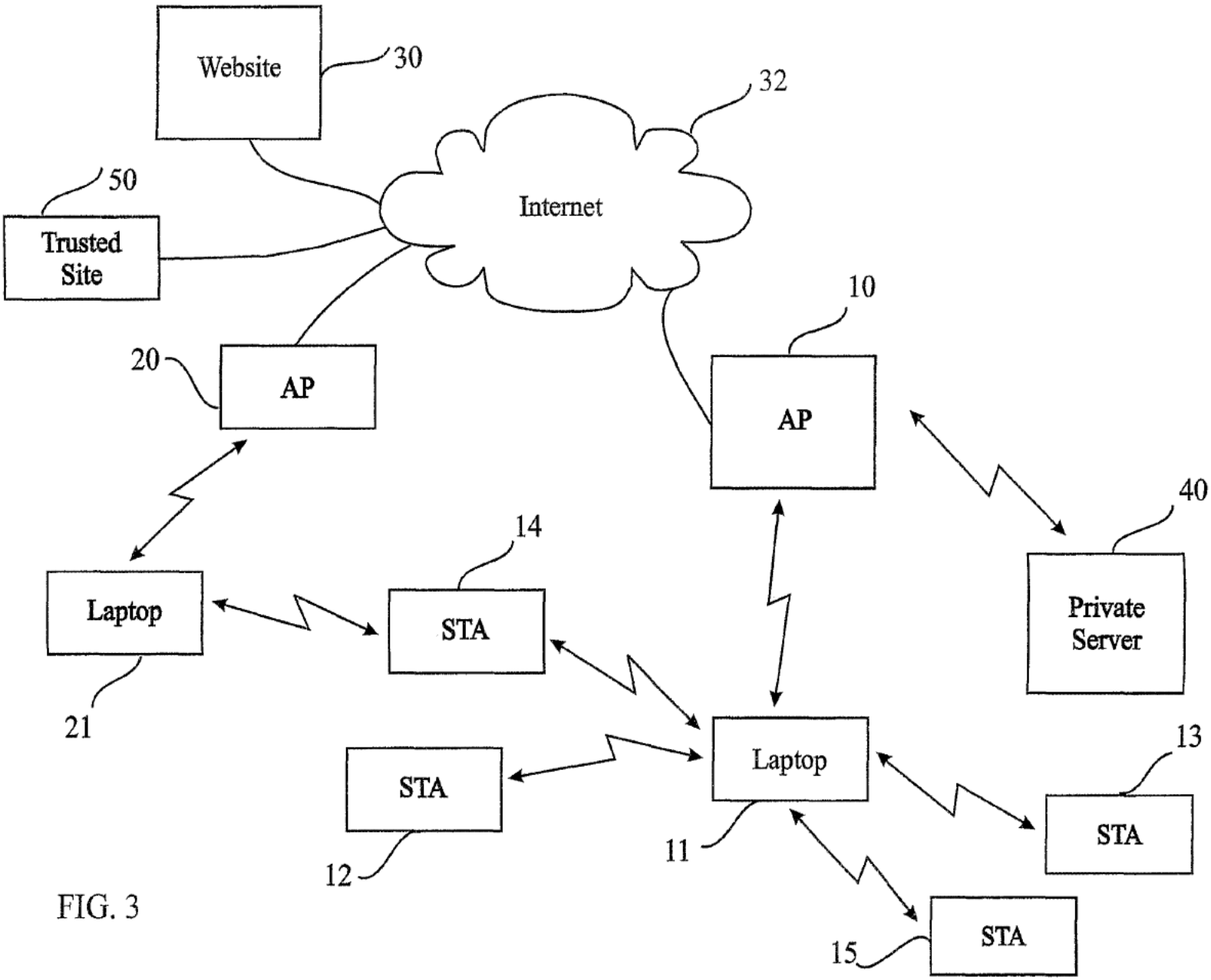


FIG. 3

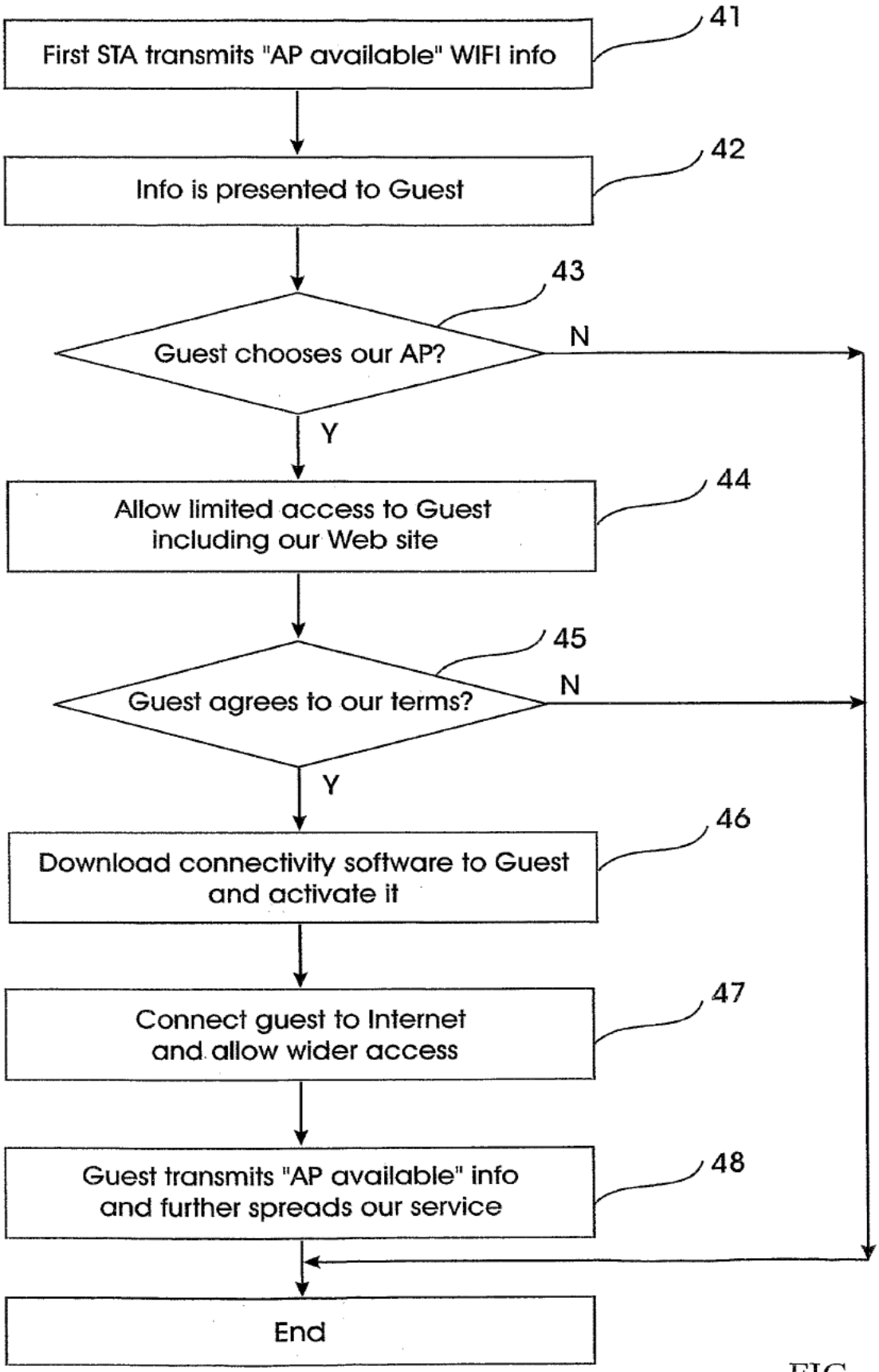

First STA transmits "AP available" WIFI info
41
Info is presented to Guest
42
Guest chooses our AP?
43
N
Y
Allow limited access to Guest including our Web site
44
Guest agrees to our terms?
45
N
Y
Download connectivity software to Guest and activate it
46
Connect guest to Internet and allow wider access
47
Guest transmits "AP available" info and further spreads our service
48
End

FIG. 4

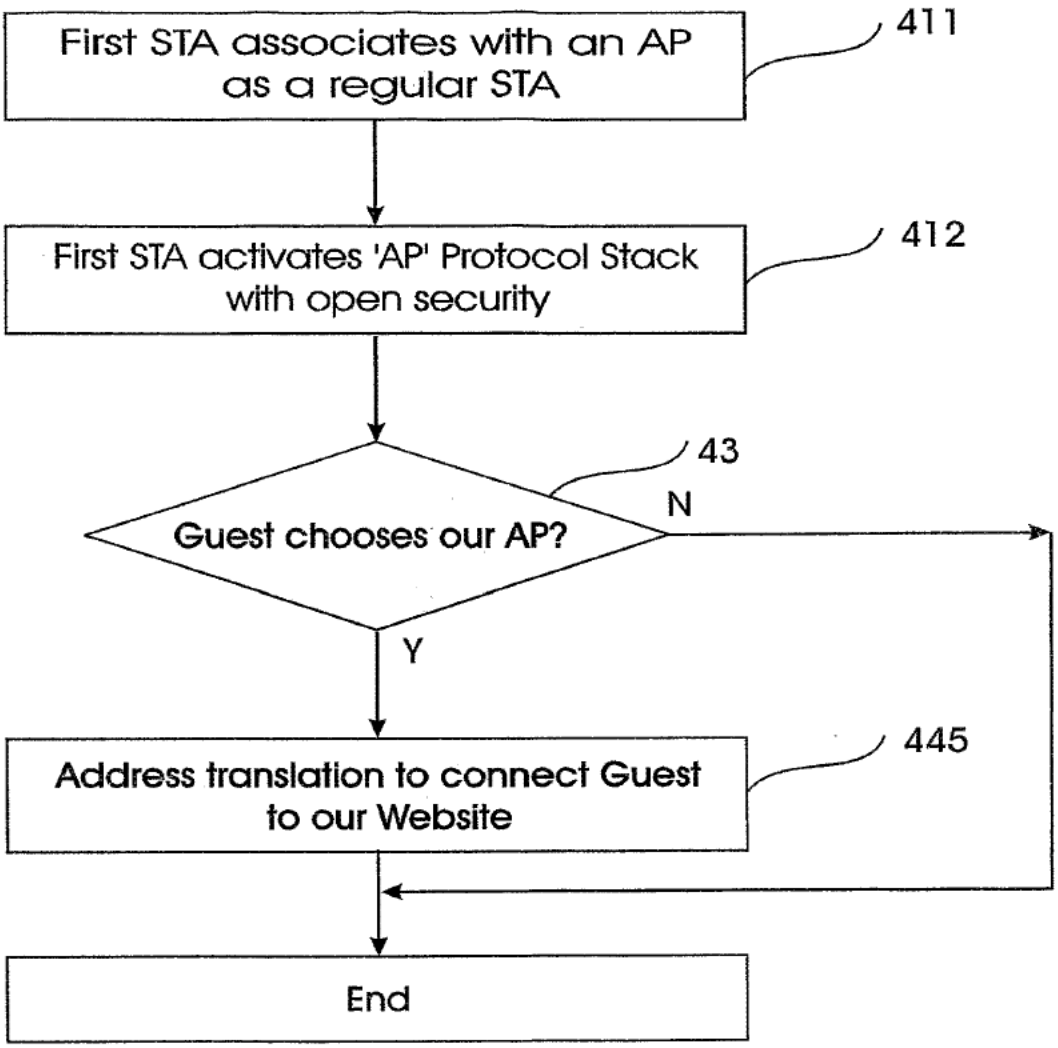

First STA associates with an AP as a regular STA
411
First STA activates 'AP' Protocol Stack with open security
412
Guest chooses our AP?
43
N
Y
Address translation to connect Guest to our Website
445
End

FIG. 5

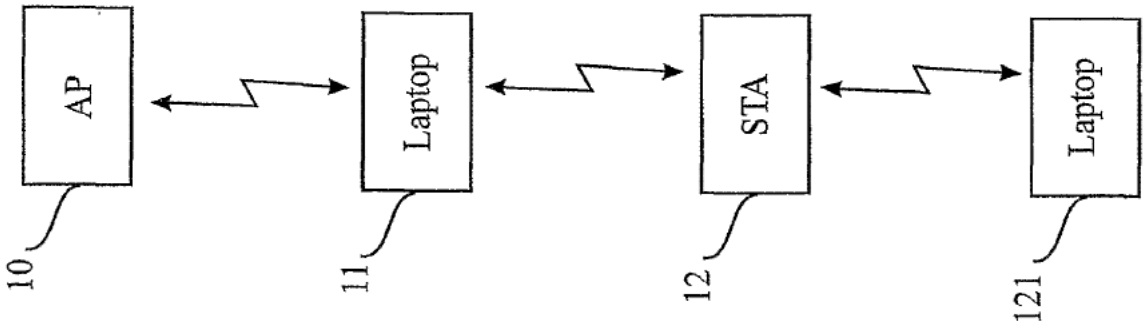


FIG. 6C

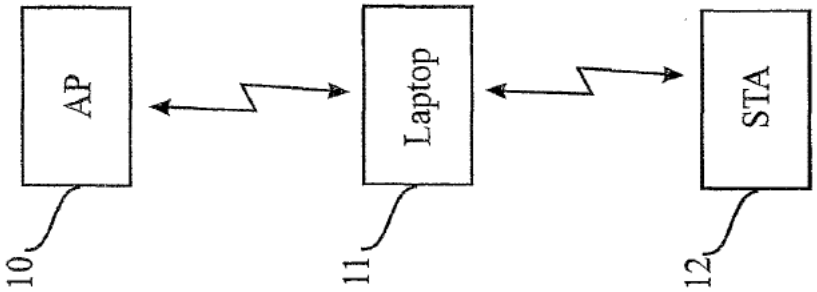


FIG. 6B

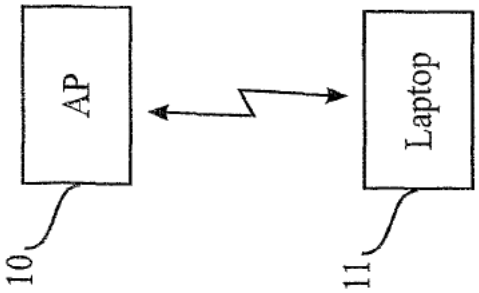


FIG. 6A

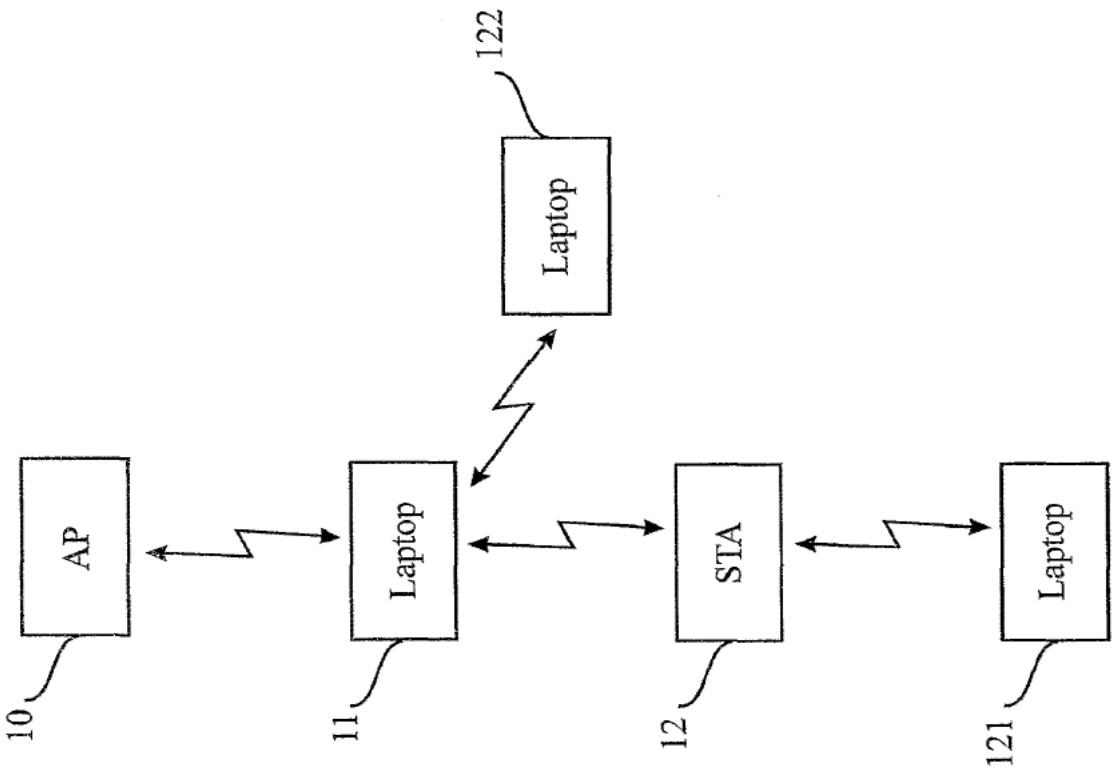


FIG. 6D

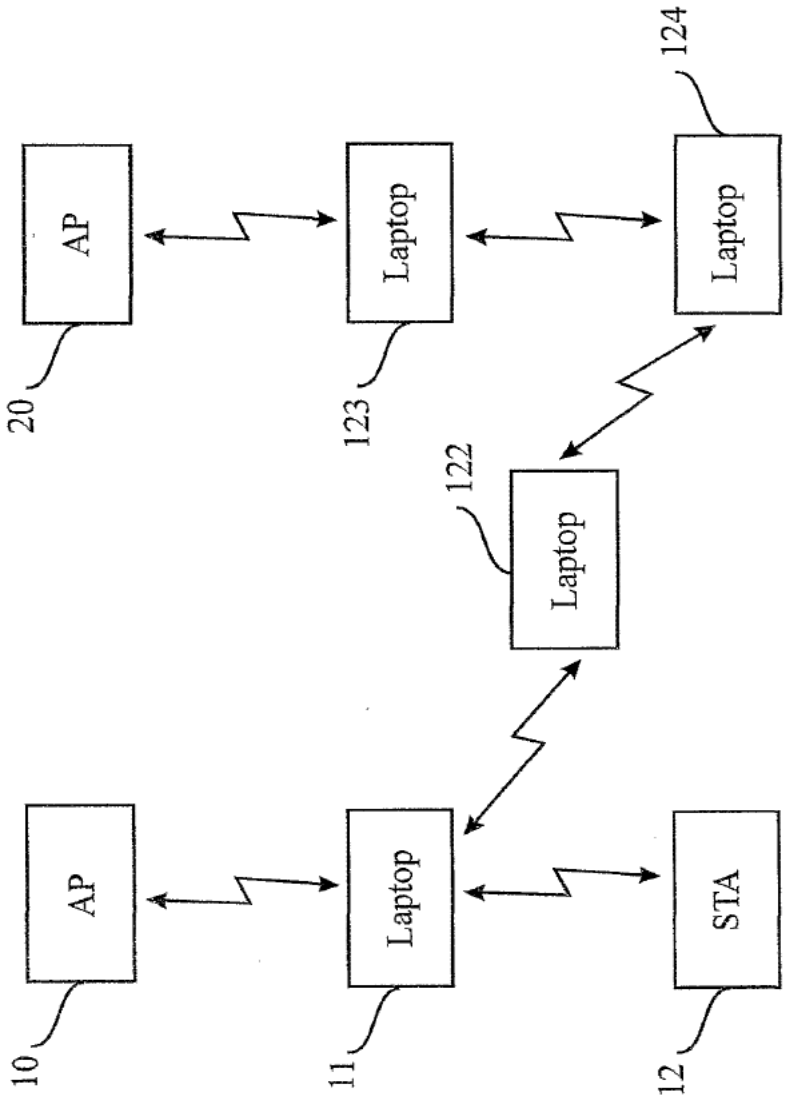


FIG. 6E

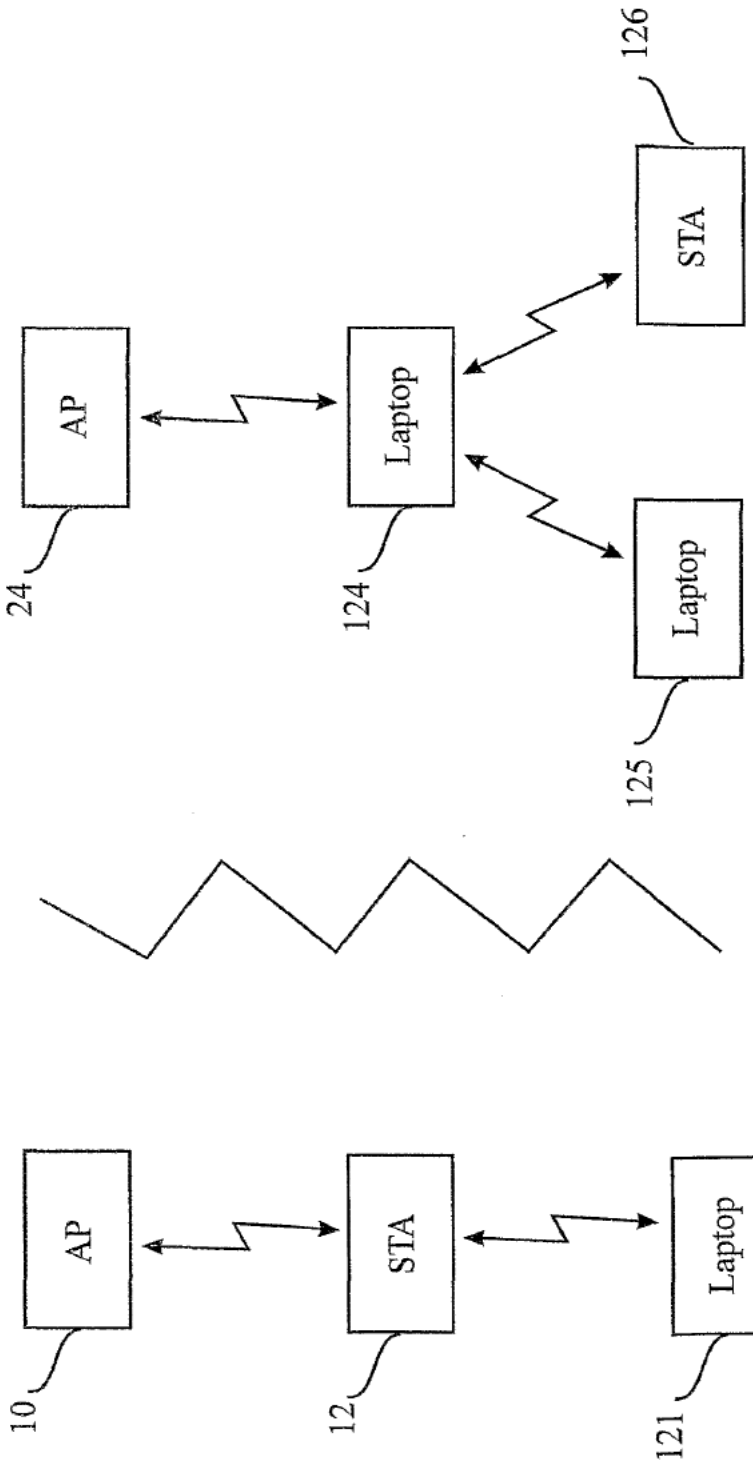


FIG. 6F

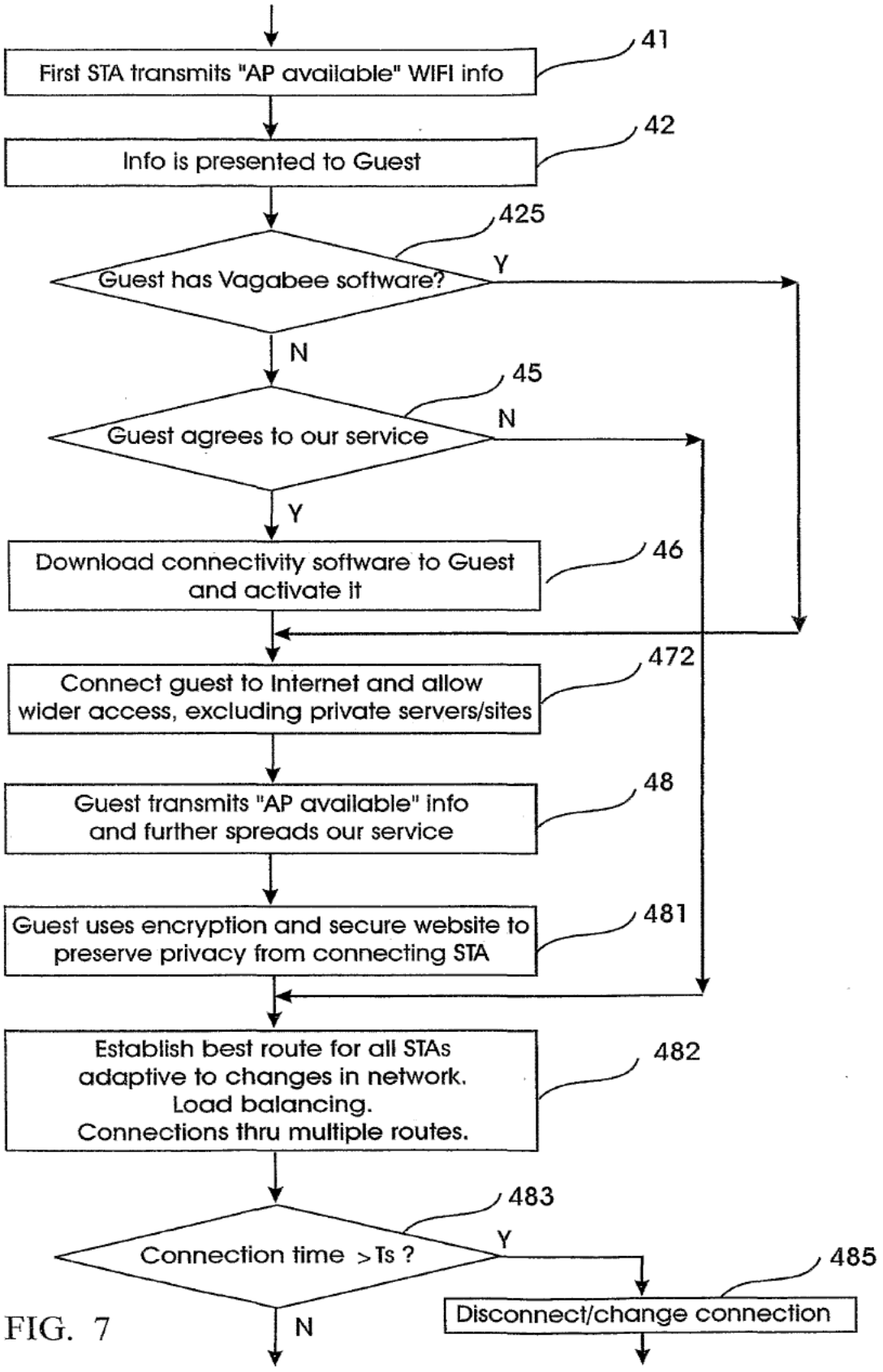

First STA transmits "AP available" WIFI info
41
Info is presented to Guest
42
Guest has Vagabee software?
425
Y
N
Guest agrees to our service
45
N
Y
Download connectivity software to Guest and activate it
46
Connect guest to Internet and allow wider access, excluding private servers/sites
472
Guest transmits "AP available" info and further spreads our service
48
Guest uses encryption and secure website to preserve privacy from connecting STA
481
Establish best route for all STAs adaptive to changes in network. Load balancing. Connections thru multiple routes.
482
Connection time >Ts ?
483
Y
N
Disconnect/change connection
485

FIG. 7

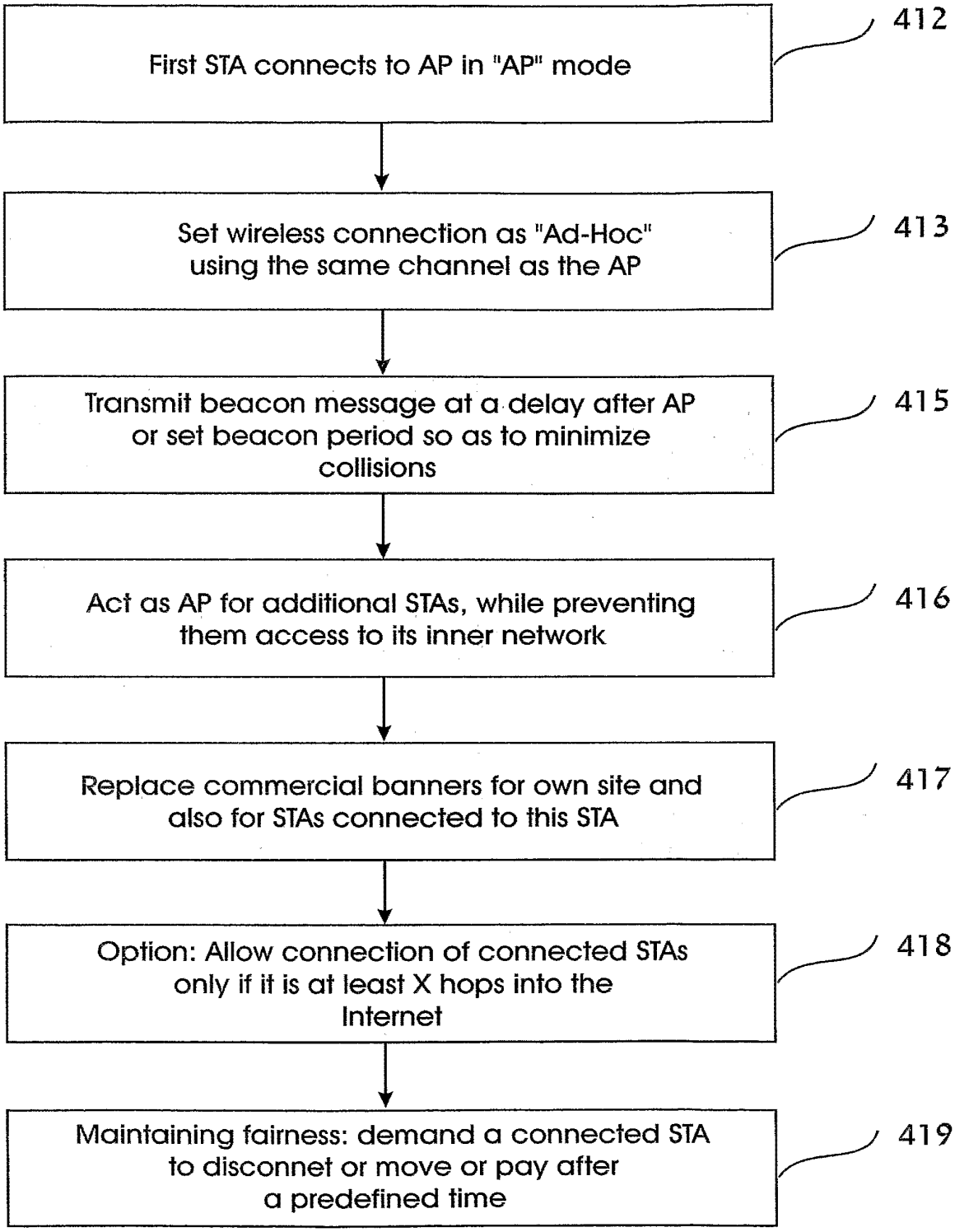

First STA connects to AP in "AP" mode
412
Set wireless connection as "Ad-Hoc" using the same channel as the AP
413
Transmit beacon message at a delay after AP or set beacon period so as to minimize collisions
415
Act as AP for additional STAs, while preventing them access to its inner network
416
Replace commercial banners for own site and also for STAs connected to this STA
417
Option: Allow connection of connected STAs only if it is at least X hops into the Internet
418
Maintaining fairness: demand a connected STA to disconnet or move or pay after a predefined time
419

FIG. 8

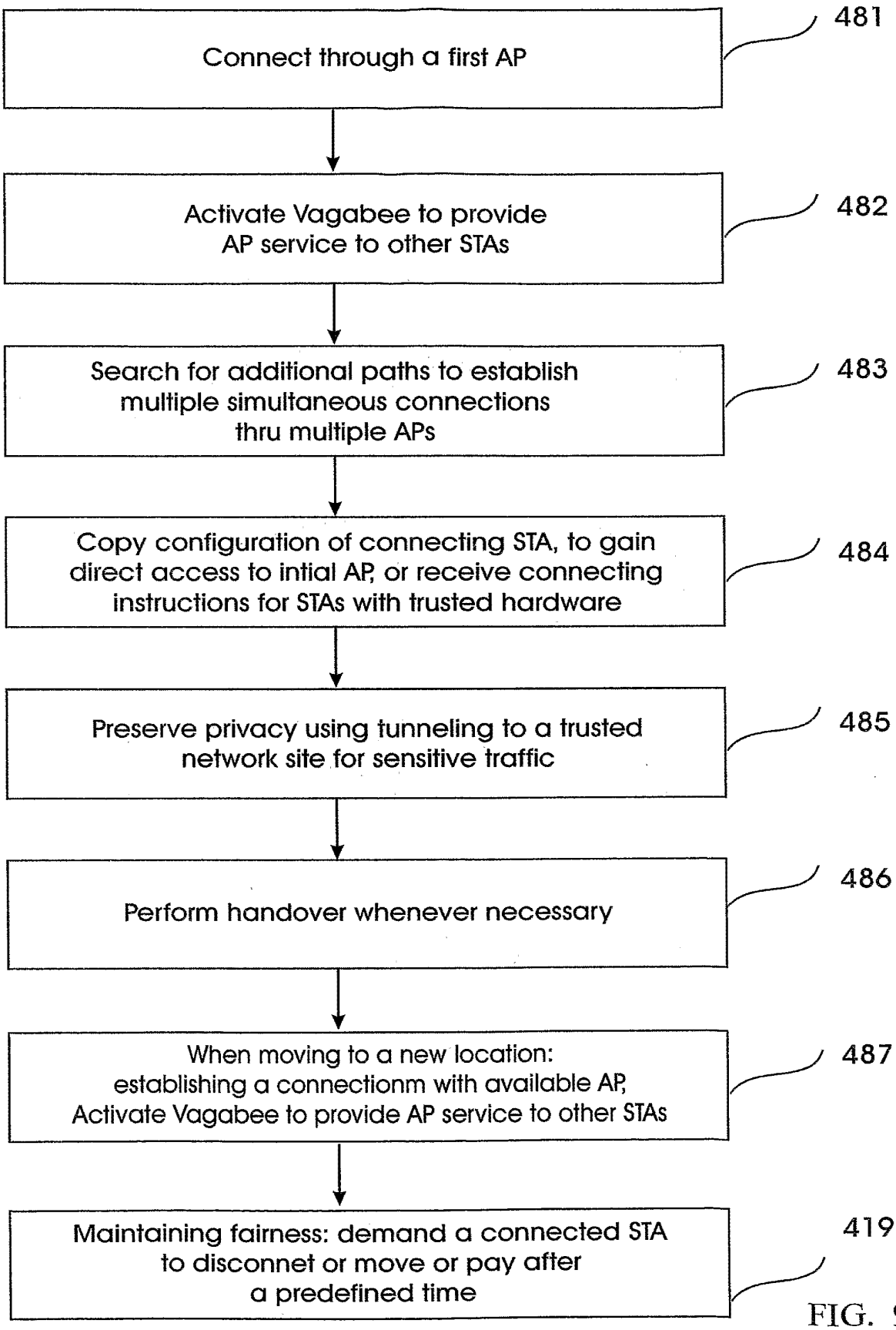

Connect through a first AP
481
Activate Vagabee to provide AP service to other STAs
482
Search for additional paths to establish multiple simultaneous connections thru multiple APs
483
Copy configuration of connecting STA, to gain direct access to intial AP, or receive connecting instructions for STAs with trusted hardware
484
Preserve privacy using tunneling to a trusted network site for sensitive traffic
485
Perform handover whenever necessary
486
When moving to a new location: establishing a connectionm with available AP, Activate Vagabee to provide AP service to other STAs
487
Maintaining fairness: demand a connected STA to disconnet or move or pay after a predefined time
419

FIG. 9

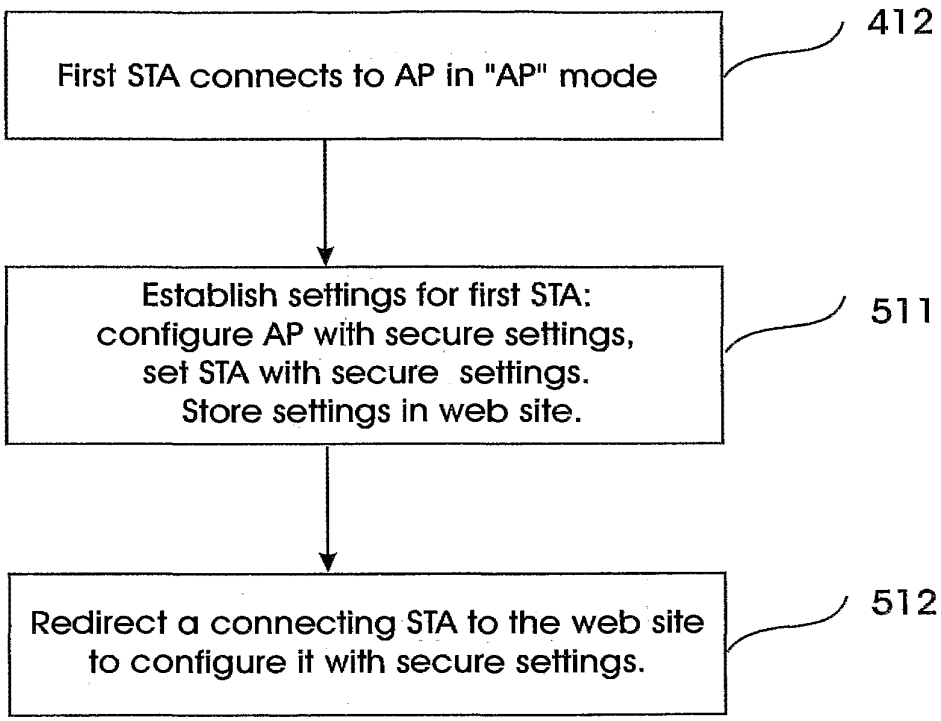

First STA connects to AP in "AP" mode
412
Establish settings for first STA:
configure AP with secure settings,
set STA with secure settings.
Store settings in web site.
511
Redirect a connecting STA to the web site
to configure it with secure settings.
512

FIG. 10

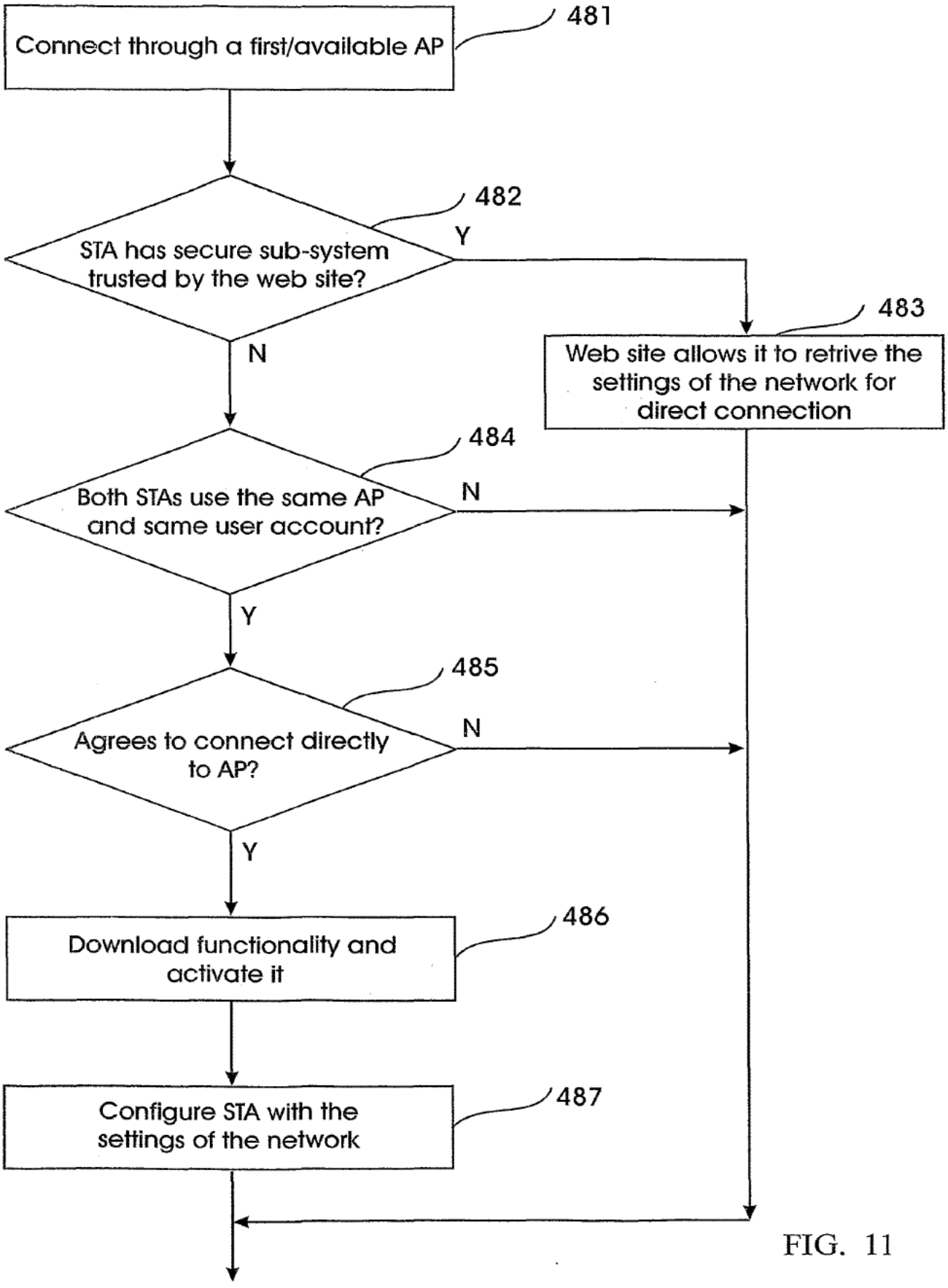

Connect through a first/available AP
481
STA has secure sub-system trusted by the web site?
482
Y
N
Web site allows it to retrive the settings of the network for direct connection
483
Both STAs use the same AP and same user account?
484
N
Y
Agrees to connect directly to AP?
485
N
Y
Download functionality and activate it
486
Configure STA with the settings of the network
487

FIG. 11

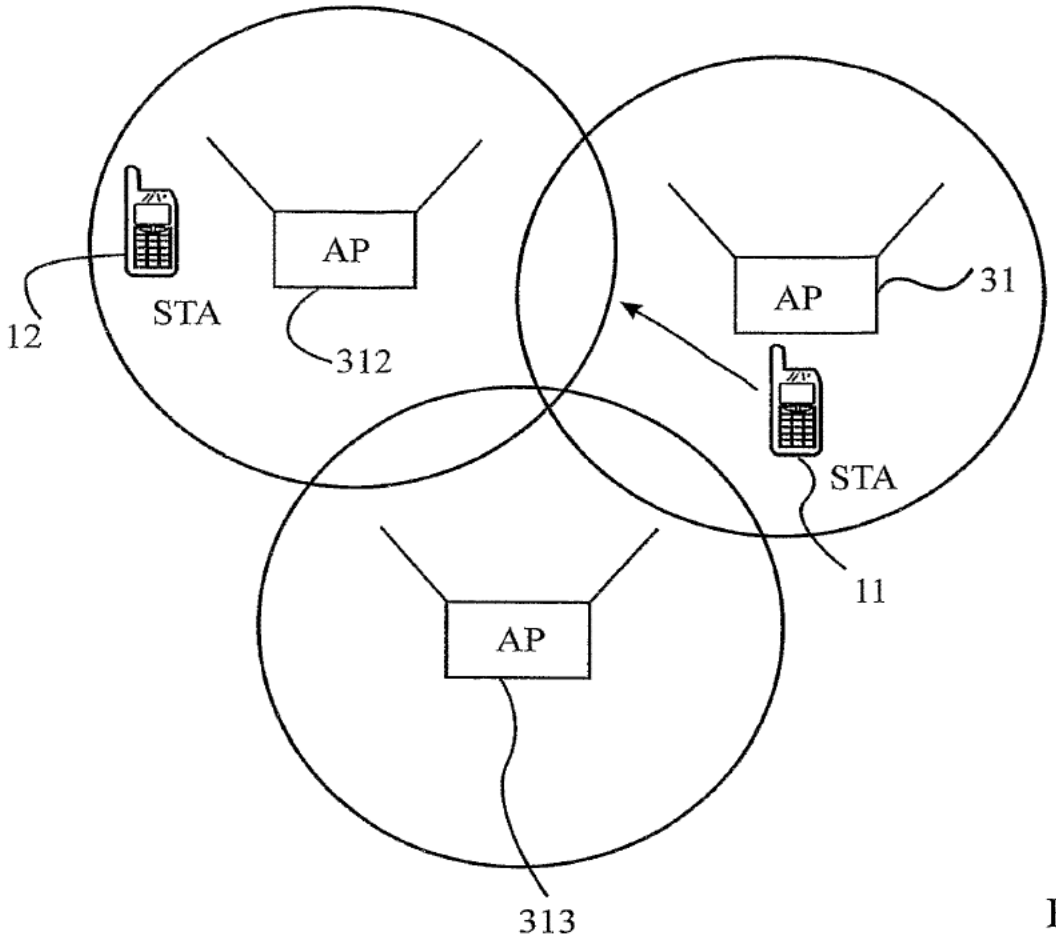

AP
STA
12
312
AP
31
STA
11
AP
313

FIG. 12

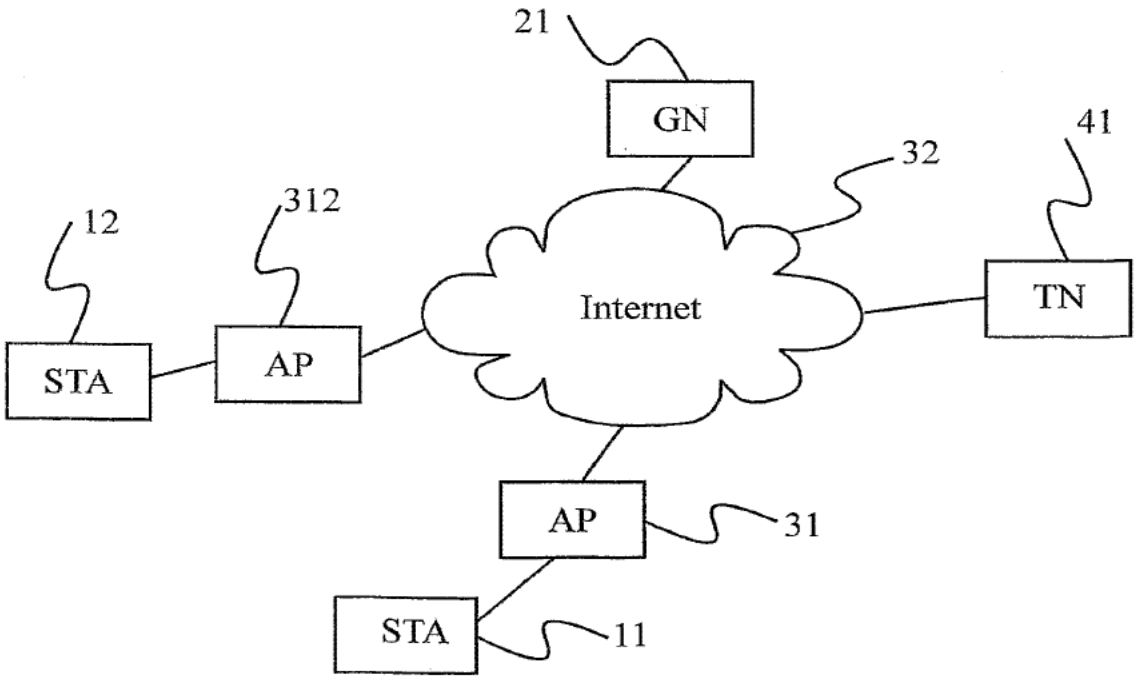

21
GN
41
32
312
12
Internet
TN
STA
AP
AP
31
STA
11

FIG. 13

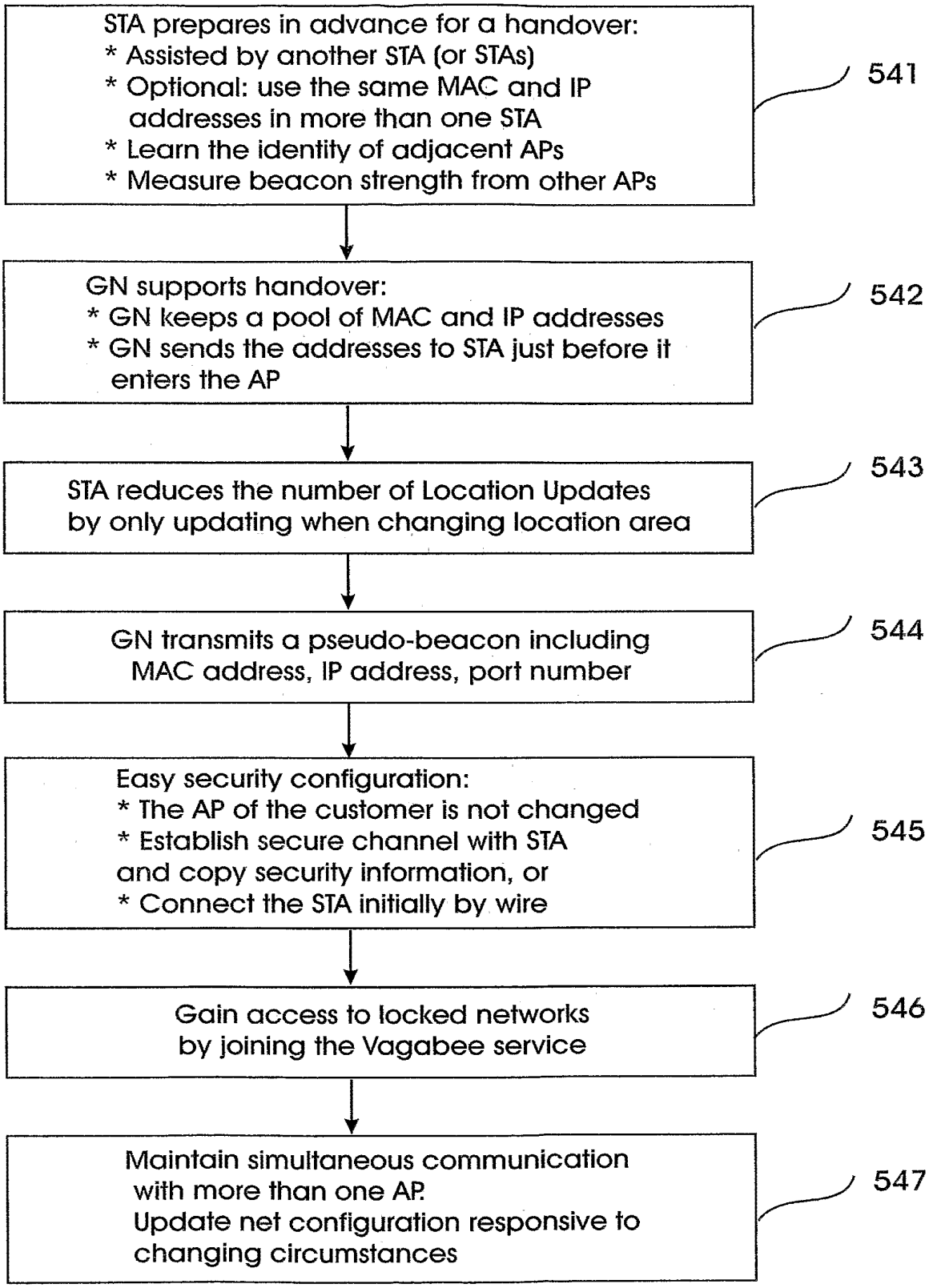

STA prepares in advance for a handover:
* Assisted by another STA (or STAs)
* Optional: use the same MAC and IP addresses in more than one STA
* Learn the identity of adjacent APs
* Measure beacon strength from other APs
541
GN supports handover:
* GN keeps a pool of MAC and IP addresses
* GN sends the addresses to STA just before it enters the AP
542
STA reduces the number of Location Updates by only updating when changing location area
543
GN transmits a pseudo-beacon including MAC address, IP address, port number
544
Easy security configuration:
* The AP of the customer is not changed
* Establish secure channel with STA and copy security information, or
* Connect the STA initially by wire
545
Gain access to locked networks by joining the Vagabee service
546
Maintain simultaneous communication with more than one AP.
Update net configuration responsive to changing circumstances
547

FIG. 14

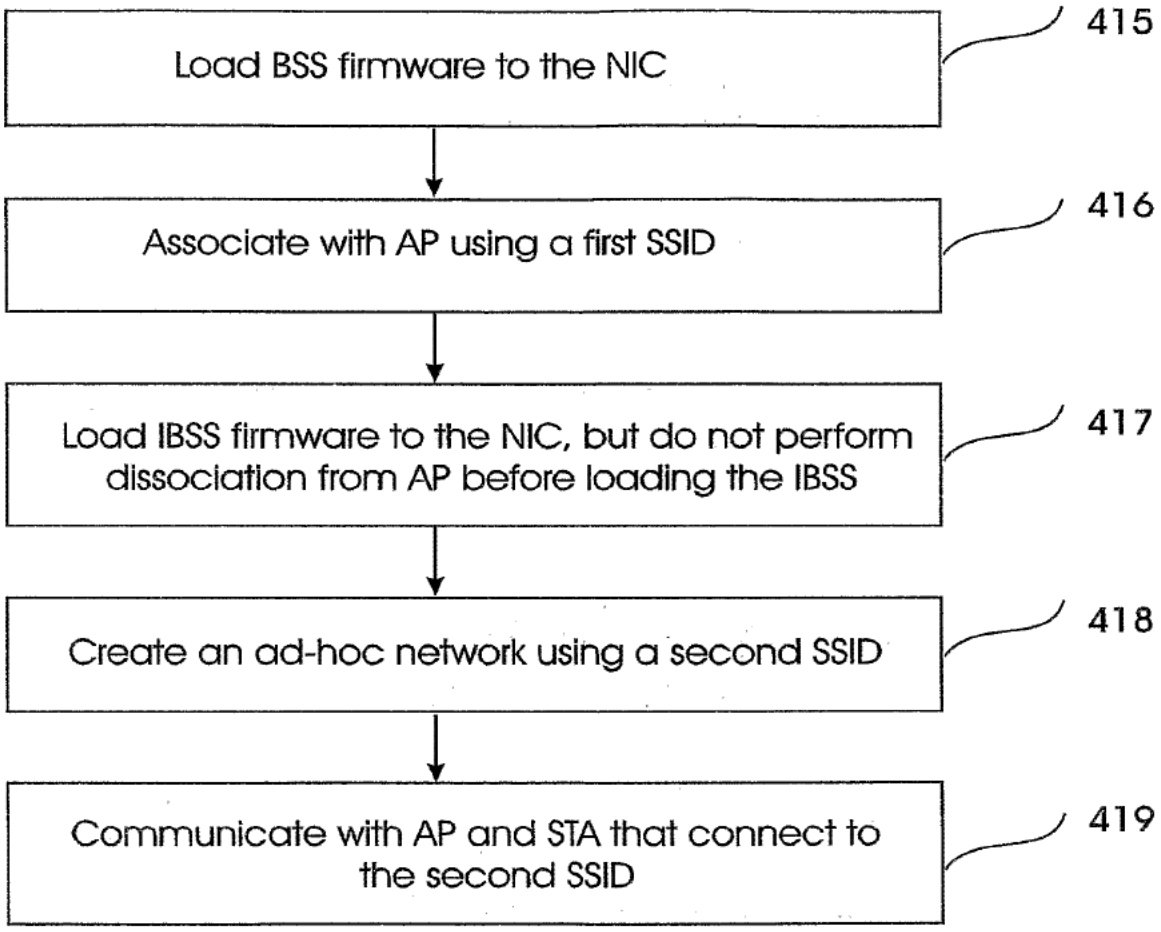

Load BSS firmware to the NIC
415
Associate with AP using a first SSID
416
Load IBSS firmware to the NIC, but do not perform dissociation from AP before loading the IBSS
417
Create an ad-hoc network using a second SSID
418
Communicate with AP and STA that connect to the second SSID
419

FIG. 15

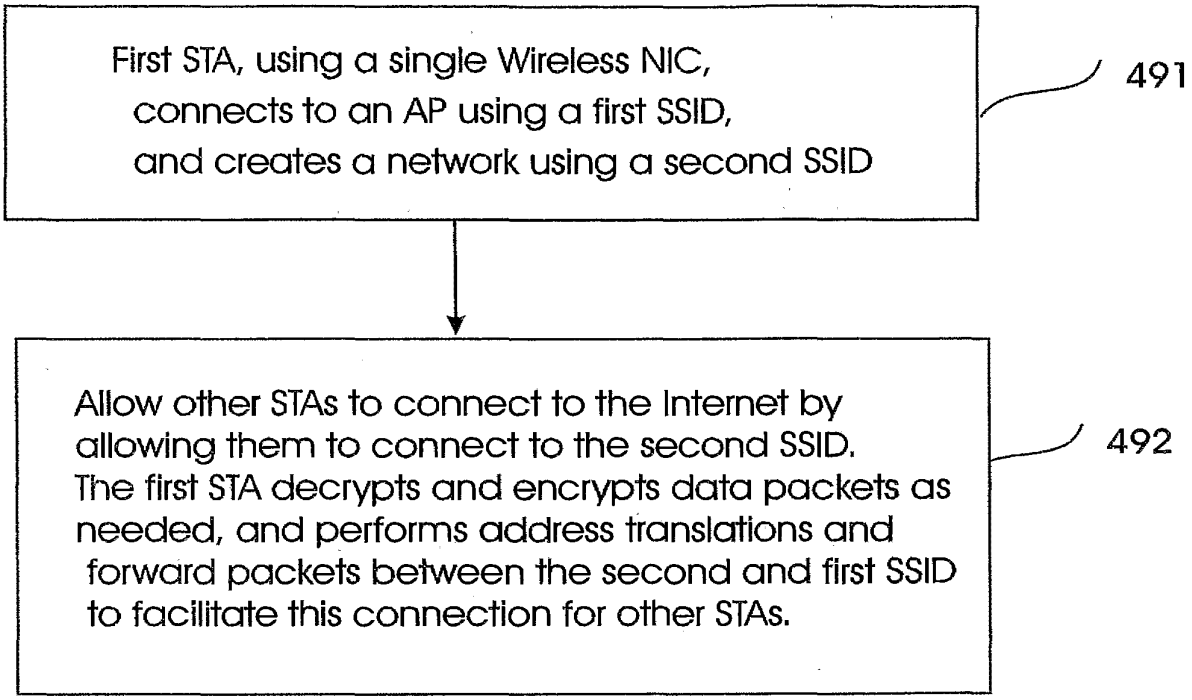

First STA, using a single Wireless NIC,
connects to an AP using a first SSID,
and creates a network using a second SSID
491
Allow other STAs to connect to the Internet by
allowing them to connect to the second SSID.
The first STA decrypts and encrypts data packets as
needed, and performs address translations and
forward packets between the second and first SSID
to facilitate this connection for other STAs.
492

FIG. 16

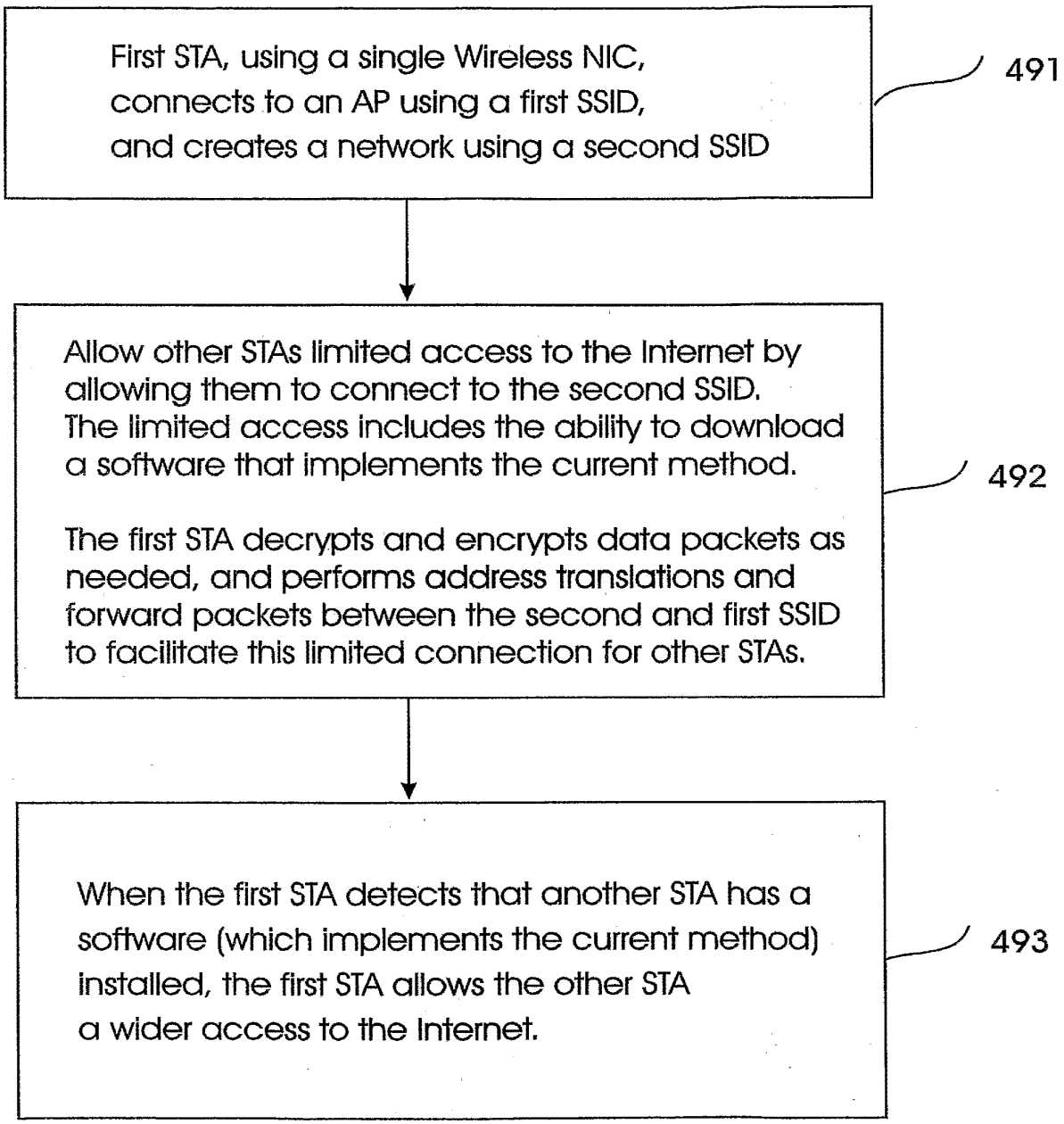

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID. The limited access includes the ability to download a software that implements the current method.
The first STA decrypts and encrypts data packets as needed, and performs address translations and forward packets between the second and first SSID to facilitate this limited connection for other STAs.
492
When the first STA detects that another STA has a software (which implements the current method) installed, the first STA allows the other STA a wider access to the Internet.
493

FIG. 17

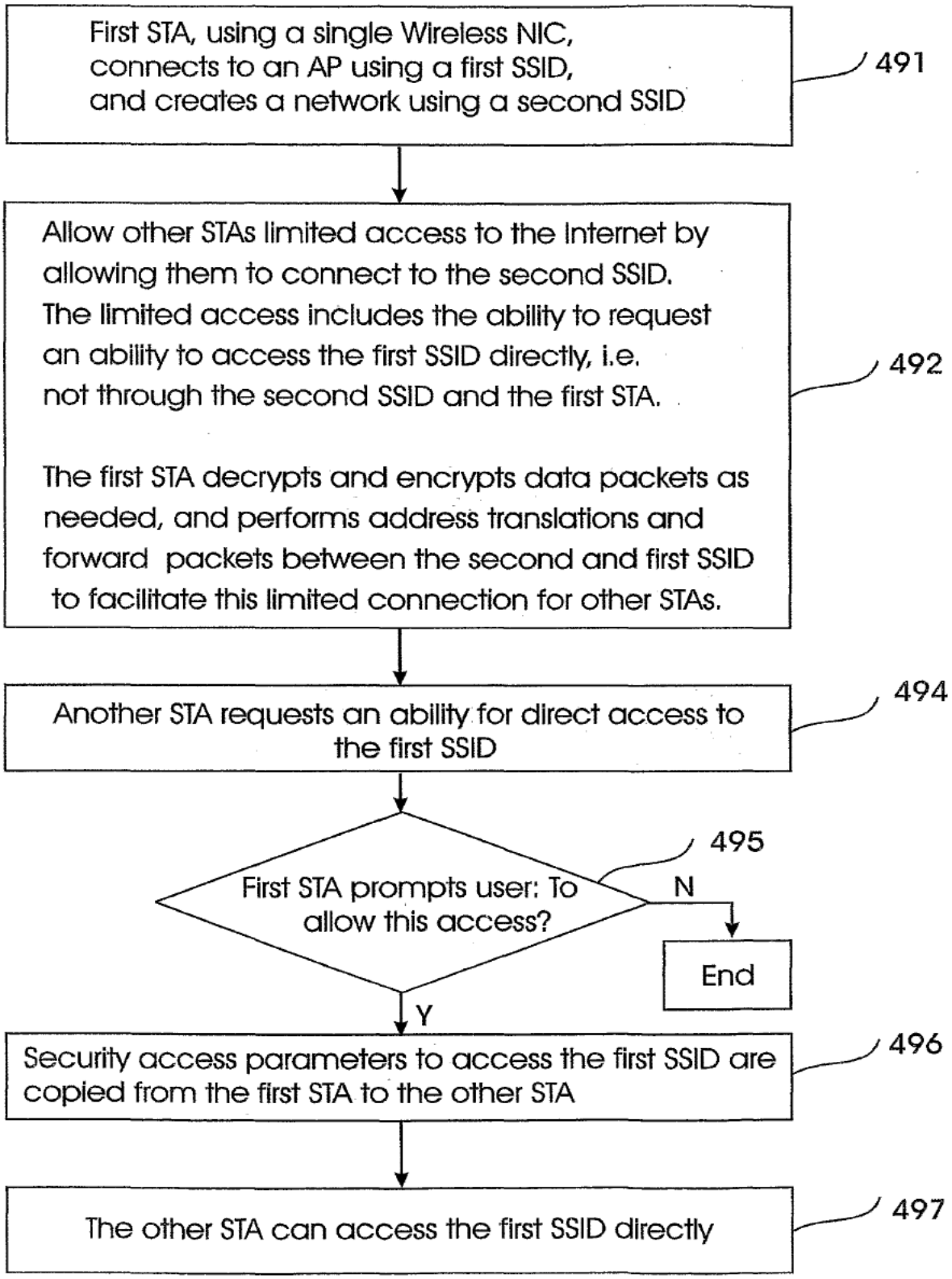

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID. The limited access includes the ability to request an ability to access the first SSID directly, i.e. not through the second SSID and the first STA.
The first STA decrypts and encrypts data packets as needed, and performs address translations and forward packets between the second and first SSID to facilitate this limited connection for other STAs.
492
Another STA requests an ability for direct access to the first SSID
494
First STA prompts user: To allow this access?
495
N
End
Y
Security access parameters to access the first SSID are copied from the first STA to the other STA
496
The other STA can access the first SSID directly
497

FIG. 18

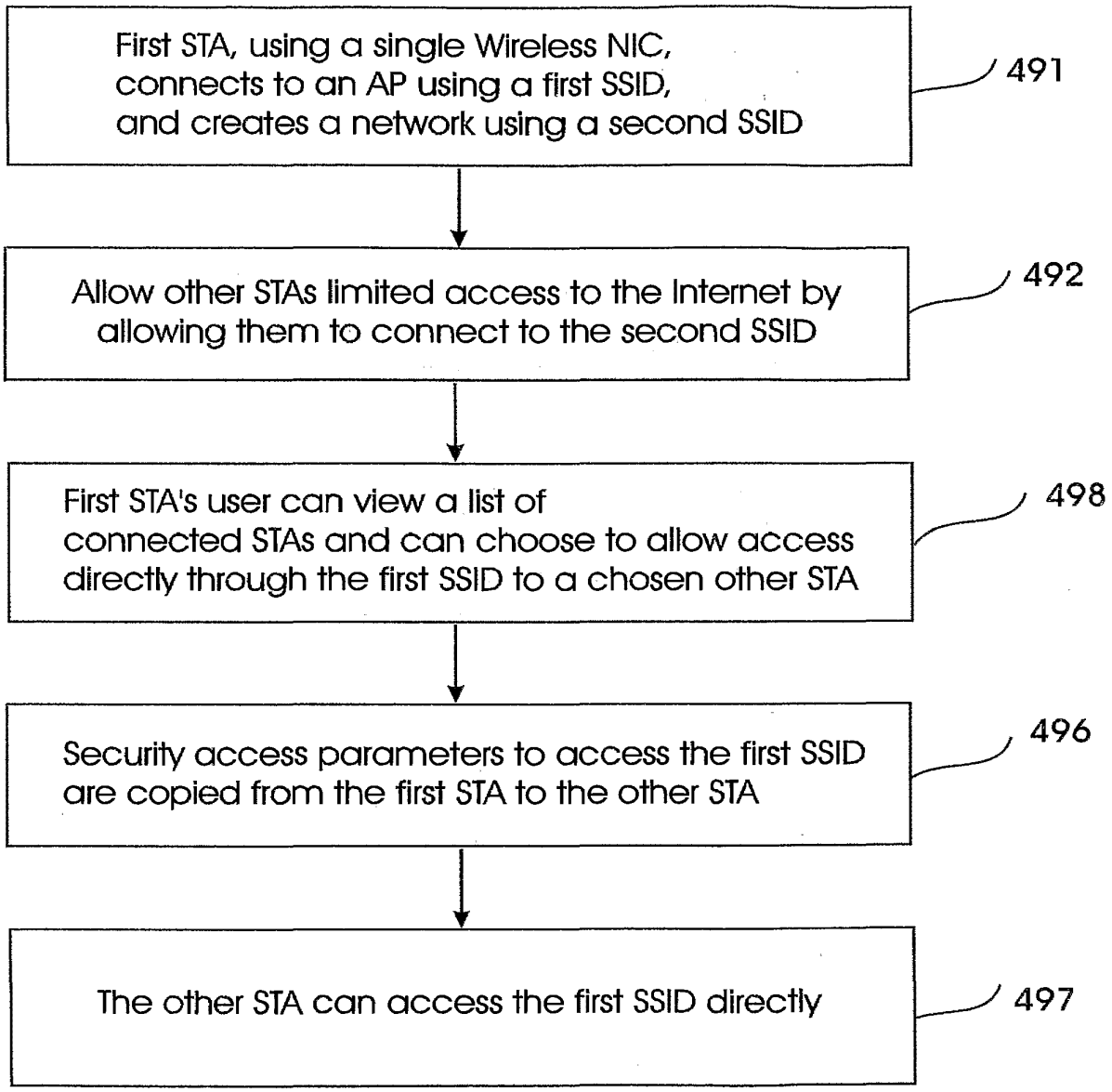

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID
492
First STA's user can view a list of connected STAs and can choose to allow access directly through the first SSID to a chosen other STA
498
Security access parameters to access the first SSID are copied from the first STA to the other STA
496
The other STA can access the first SSID directly
497

FIG. 19

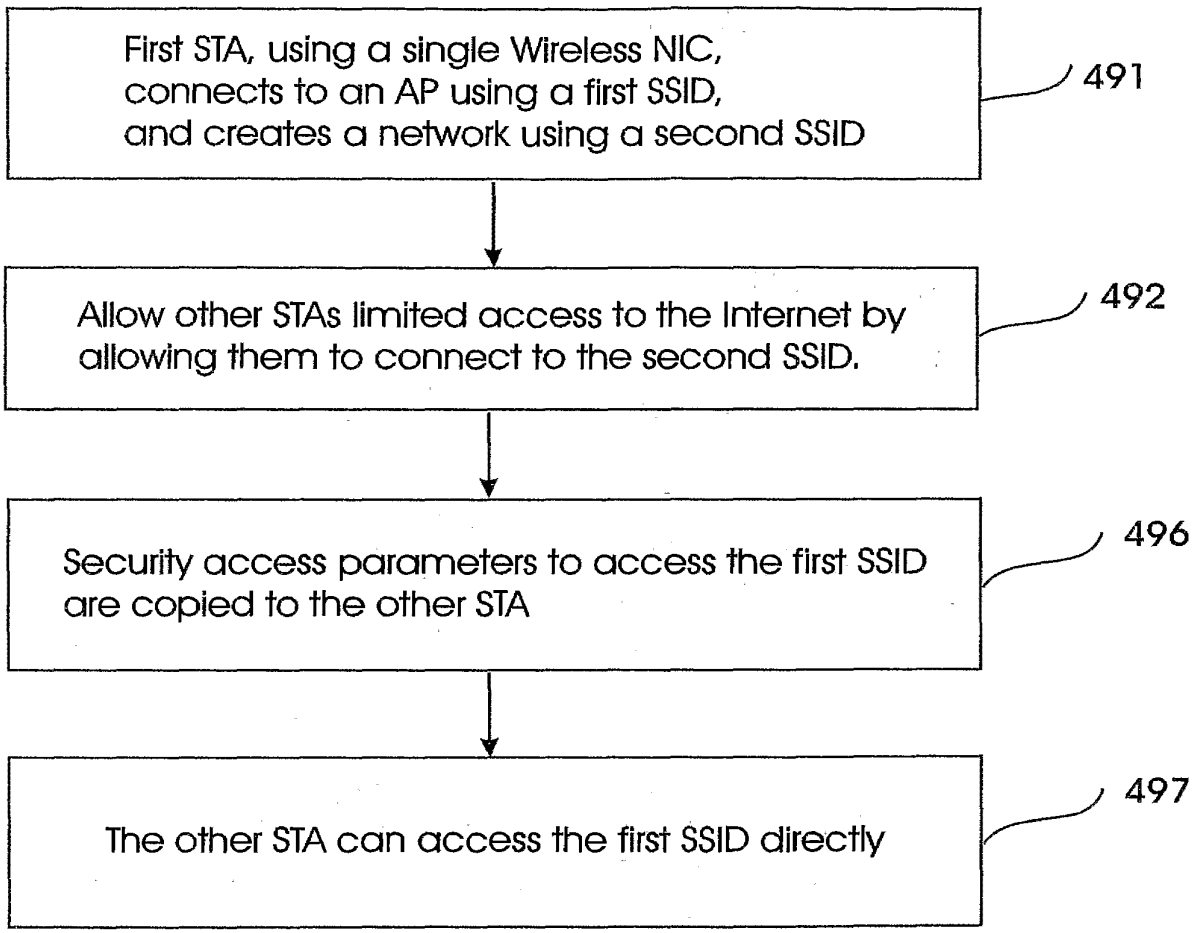

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID.
492
Security access parameters to access the first SSID are copied to the other STA
496
The other STA can access the first SSID directly
497

FIG. 20

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	WIRELESS INTERNET SYSTEM AND METHOD
First Named Inventor/Applicant Name:	Elad BARKAN
Filer:	Vladimir Sherman
Attorney Docket Number:	BRK-PU-001-US1

Filed as Small Entity

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Basic National Stage Fee	2631	1	165	165
Natl Stage Search Fee - U.S. was the ISA	2641	1	50	50
Natl Stage Exam Fee - all other cases	2633	1	110	110
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Petition-revive unintent. abandoned appl	2453	1	810	810

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1135**

Electronic Acknowledgement Receipt

EFS ID:	6686188
Application Number:	12665978
International Application Number:	PCT/IL07/00244
Confirmation Number:	5873
Title of Invention:	WIRELESS INTERNET SYSTEM AND METHOD
First Named Inventor/Applicant Name:	Elad BARKAN
Customer Number:	60956
Filer:	Vladimir Sherman
Filer Authorized By:	
Attorney Docket Number:	BRK-PU-001-US1
Receipt Date:	22-DEC-2009
Filing Date:	
Time Stamp:	11:40:15
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1135
RAM confirmation Number	8596
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Power of Attorney	BRK-PU-001-US1-POA.pdf	527636 9c1fc2e7017e074bf76c2786b1f58d5c796f93a7	no	1
Warnings:					
Information:					
2	Transmittal of New Application	BRK-PU-001-US1-AppTransmittal.pdf	160468 ff9b22a238bc81e07f03160678c1fb9ce3e83b14	no	3
Warnings:					
Information:					
3	Petition for review and processing by the PCT legal office.	BRK-PU-001-US1-PetitiontoRevive.pdf	103686 f1283e5717e6103985ee5b9f7c1fd5c2584d422b	no	2
Warnings:					
Information:					
4	Petition for review and processing by the PCT legal office.	BRK-PU-001-US1-PetitionStatement.pdf	69559 2a3cdcb6ed87af341a8491d67ccb1b0e76a73192	no	2
Warnings:					
Information:					
5	Oath or Declaration filed	BRK-PU-001-US1-Declaration.pdf	612047 7093e1effca841d962c3a8f46d9020737285d5ea	no	1
Warnings:					
Information:					
6	Application Data Sheet	BRK-PU-001-US1-ApplicationDataSheet.pdf	50594 6a81c7f553fee82f07fa6940f33284ff8461b8af	no	4
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
7		BRK-PU-001-US1-PrelimAmdt.pdf	438324 e4f169ace2e888c1ac1811195a1cd562e5382759	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Claims	2	11
	Applicant Arguments/Remarks Made in an Amendment	12	12

Warnings:
Information:

8		BRK-PU-001-US1-ApplicationSpecification.pdf	3934142 dbc6840e62d68d5a3d9ea6ee502c1d5af75bb6ea	yes	95

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Abstract	1	1
Specification	2	64
Claims	65	73
Drawings-only black and white line drawings	74	95

Warnings:

Information:

9	Fee Worksheet (PTO-875)	fee-info.pdf	36572 523f1174cba0dcc80530731c99ffeddcfb76d456	no	2

Warnings:

Information:

Total Files Size (in bytes):	5933028

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	
Filing Date	Herewith
First Named Inventor	BARKAN, Elad
Title	WIRELESS INTERNET SYSTEM AND METHOD
Art Unit	
Examiner Name	
Attorney Docket Number	BRK-PU-001-US1

I hereby revoke all previous powers of attorney given in the above-identified application.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

60956

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the:

☒ Applicant/Inventor.

OR

☐ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of Applicant or Assignee of Record

Signature	Elad BarKan	Date	Dec 22, 2009
Name	Elad BARKAN	Telephone	
Title and Company			

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2007 (30.08.2007)

PCT

(10) International Publication Number
WO 2007/096884 A2

(51) International Patent Classification:
H04J 13/00 (2006.01)

(21) International Application Number:
PCT/IL2007/000244

(22) International Filing Date:
22 February 2007 (22.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/775,321 22 February 2006 (22.02.2006) US
60/794,135 24 April 2006 (24.04.2006) US

(71) Applicant and
(72) Inventor: **BARKAN, Elad** [IL/IL]; C/O Marc Zuta, Patent Attorney, P.O. Box 2162, 49120 Petah-Tikva (IL).

(74) Agent: **ZUTA, Marc**; Marc Zuta, Patent Attorney, P.O. Box 2162, 49120 Petah-Tikva (IL).

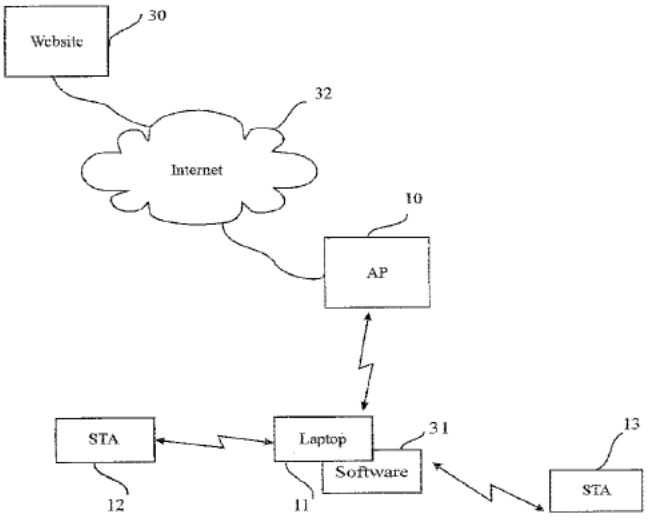
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** WIRELESS INTERNET SYSTEM AND METHOD



(57) **Abstract:** A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising: wirelessly connecting a first STA to the Internet through a first AP with a first SSID; remaining connected to the first Access Point (AP), the first STA creates a software-based wireless AP with a second SSID for wirelessly connecting other STAs to the Internet through the first STA. A software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein. A method for configuring STAs to connect to a wireless network, comprising: a customer first connects a STA by wire to its network; a software on the STA copies to the STA the security information gained through the wired connection, thus setting the security parameters for the STA.

WO 2007/096884 A2

Wireless Internet system and method

Cross-Reference to Related Applications

The present application is related to, and claims priority from, the provisional patent applications filed by the present applicant in U.S.A.:
Application US 60/775,321 filed on 22 February 2006, and
Application US 60/794,135 filed on 24 April 2006.

Technical Field

The present invention relates to a wireless Internet system and method, and more particularly to such systems for providing wireless Internet connection to roaming devices such as Portable computers, Laptops, PDAs and phones, and the deployment of such a system in a fast spreading manner (a viral-like method), in a client software-only manner such that the existing access points are not changed at all.

Background Art

Currently, there is a growing number of WiFi public hot-spots (or Access Points - "AP"). These APs allow WiFi-enabled devices (which we refer to as STA) that are in their coverage area to Connect to the internet.

Some of the APs are operated as a business, service, or as part of a community, either with or without a charge to the STA's owner. Other APs are placed by individuals in their premises, but are not "locked", i.e., they are "open", allowing bypassing STAs to utilize them. Other APs placed by individuals are "locked" (or "closed"), thus not allowing passing STAs to utilize them.

As APs are being deployed in growing numbers, many individuals lock their APs for fear of unfair use of their network resources, and due to security concerns. For instance, there have been cases where a person places an open AP, and his neighbor uses this AP as its internet connection on a full-time basis without the consent of the first person, thus abusing and degrading the service of the first individual. In other cases, the neighbor hacked into the computer of the first person through the network. Thus, as time passes, most APs are either locked, or a payment is required to use them. Although the total number of APs and their area of coverage is growing fast, a larger percent of the APs are becoming locked and inaccessible to roaming STAs.

A prior art approach for allowing roaming customers to access the Internet is taken by Fon (www.fon.com). It allows individuals to download a new software into their APs, which makes their APs a pay-for-use APs for STAs that roam in their vicinity, and in addition, they receive a username and password for free access to other APs which are operated by Fon or utilize their software. It also allows users to enjoy part of some of the payments made by other users to use the network. However, roaming STAs are forced either to find an open AP, find an AP for which they have an account, or pay for access in case there is a pay-for AP.

It is an aim of the current disclosure to provide a system and a method for deployment of APs for the purpose of connecting STAs to the Internet.

Roaming customers that connect to an AP are often far from the AP and have borderline reception conditions. As a result, the connection quality is very poor, and the user may experience a slow service or no service at all. It is another aim of the current disclosure to provide a system and a method for improving the connection quality for roaming STAs.

Another aspect of this invention refers to systems and methods for fast handovers in wireless networks such as 802.11 networks, specifically in un-managed wireless networks, and more particularly such systems and methods which allow extremely fast handovers in these networks without any changes to existing 802.11 base stations. The invention also

concerns efficient performance with regards to power consumption, coverage, security, installation, capacity and availability of wireless networks such as 802.11.
The invention can achieve these goals without any change to the WiFi access point.

Currently, there is a growing number of WiFi public hot-spots (or Access Points - "AP"). These APs allow WiFi enabled devices (which we refer to as STA) that are in their coverage area to connect to the internet.

Some of the APs are operated as a business, service, or as part of a community, either with or without a charge to the STA's owner. Other APs are placed by individuals in their premises, but are not "locked", i.e., they allow bypassing STAs to utilize them. The cumulative connectivity provided by the APs is enormous and growing fast, thus, it is tempting to use this cumulative connectivity to compete with other wireless technologies. For example, it would be tempting to have a STA that looks like a cellular handset (i.e., a WiFi Handset, or WiFi Phone), where the WiFi handset uses the free connectivity to provide a "free" service that competes with or complements the cellular service.

One of the major difficulties of achieving this vision is that the coverage of a single WiFi AP is very small (about a few hundreds to a few thousands of square meters). When a user goes out of this area, his connectivity is lost. A natural naive approach to solve this problem is performing a handover (sometimes also called handoff) to another AP with a better radio connection to the user. Another approach is to have a handset which supports both WiFi and Cellular, and handover the conversation from WiFi to Cellular [See: WO 2004/036770], this way, WiFi extends the coverage of cellular, and conversation is handed over from WiFi to cellular, when there is no WiFi coverage. However, the problem of performing handover between one WiFi AP to another WiFi AP remains when appropriate cellular coverage is not available (or there is no cooperation from the cellular company). The same idea applies when cellular is replaced by other access technology, such as satellite communications.

The concept of handover is taken from cellular networks. Handovers usually work well in

managed networks, such as cellular networks, campuses, or office environment., where the entire network is usually owned by the same operator.
The network operator in many cases chooses to add cells where coverage or capacity are needed. In managed networks, the APs (or the cellular cells) are synchronized and communicate with each other through a backbone, and are usually controlled by some other network entity (e.g., BSC - base station controller in cellular systems). For example, the APs can communicate with each other, for example using the IEEE 802.11F protocol - the Inter-AP protocol, which involves a RADIUS (Remote Authentication Dial In User Service, see RFC 2138, 2865, and 2866) server.

The APs can also employ a radio resource management such as IEEE 802.11K, or fast roaming using IEEE 802.11R, etc. However, in unmanaged networks, the APs can be deployed by many unrelated entities, such as by private individuals.

There is usually no entity that synchronizes the APs. The APs can be manufactured by various manufacturers, use various security mechanisms etc. In unmanaged networks, the handovers are typically very slow, as in the process of handover, it takes time for the STA to re-connect to the internet in the new AP (and it must disconnect from the previous AP). In such a handover in an unmanaged network, the IP address often changes. Therefore, a mechanism such as mobile IP must be used (as described later). This mechanism is limited with respect to the frequency in which the IP address can change, and a large latency (disconnection time) may result during the handover process. During the latency, the STA cannot receive any incoming messages.

A handover process is typically composed of the station STA connecting to a new AP, and disconnecting from the old AP. If STA is connected in parallel to both AP the handover is called soft-handover, and if STA first abandons the old AP and then connects to the new AP, the handover is called a hard-handover. Soft handovers require the ability of STA to communicate in parallel with at least two APs.

The process of connecting to a new AP is usually composed of the following steps:

1. STA performs a scanning process to discover neighboring APs.
2. STA chooses a new AP, and performs authentication with the AP, in which the AP verifies that STA is allowed to access the AP.
3. If the authentication is successful, STA performs an association process, in which the AP acknowledges that STA is connected to it (association requires the AP to allocate resources to the STA, and the 802.11 standard allows up to 2007 STAs to be associated with an AP).
4. Once STA is associated with the AP, the STA makes sure that it has all the information that it requires to communicate over the internet, for example, it must have an IP address, and it must update servers that govern its location (such as Mobile IP, as discussed later). In some cases, the user should go through a second authentication procedure (usually with a RADIUS server). Many times, this procedure is performed over a web interface, which is called a Captive Portal.

When a captive portal is used by the AP, the user needs to surf into the captive portal and perform a log-in to connect his IP address to the Internet. In some implementations, the user's web browser is forwarded to the captive portal regardless of the internet site that it tries to surf into. Some APs allow the STA to surf in some limited number of internet sites before they complete the second authentication procedure (for example, if the AP is in an hotel, it might allow surfing into the hotel's website, or affiliated news web sites). The procedure at the captive portal typically includes authentication, payment, or agreeing to terms of usage. Once the authentication is completed, the IP address of the STA is connected to the Internet (usually by reconfiguring the firewall that controls the communications of the AP). Each sub-process takes time to complete, resulting in a total delay of over several seconds to complete the entire process.

In managed networks, Step 4 can be performed once in a certain amount or time (or for a certain area), as moving between APs of the managed network does not necessarily change the parameters of the STA such as IP address etc. However, in un-managed networks (and sometimes also in managed networks), the STA must gain a new IP address and other parameters, usually through DHCP (Dynamic Host

Configuration Protocol, see RFC 1541). Completing the DHCP protocol can take up to several seconds. Sometimes, obtaining an IP is not enough, and a second authentication is needed. In other cases, a proxy server or a Socks server should be set for the communication. The entire process can consume a few seconds, which are intolerable in a streaming two-way application such as a voice conversation.

Many protocols that are used in the Internet require that the IP address of the STA would remain fixed during communications (for example, TCP - Transport Control Protocol, see RFC 793). However, a handover might result in the change of the IP address. This change of IP address causes a break in the communication as the communication needs to be restarted.

One solution to this problem is provided by the Mobile IP standard (see RFC 2002): in this solution the STA updates a server with its current IP address, every time that the IP address changes. As a preparation for roaming, the server allocates to the STA (in addition to the STA's current IP address) an IP address that remains fixed, even when the real IP address of the STA changes. This fixed IP address is also known as a "care of" address. From this moment on, the STA keeps the server posted of the real IP address of the STA, and the STA can use (in its communications with the rest of the Internet) the "care of" address (or its home address) as if it was its own fixed address.

Any IP data packet that is sent to the care-of IP address is tunneled by the Mobile-IP server to the current IP address of the STA. For packets originating from the STA to the Internet, the STA can tunnel the packets to the Mobile-IP server, which replaces the IP address with the care-of address. However, many times the STA can simply write its care-of IP address as the source address of the IP data packet, as many times, the source address of IP packets is not checked what-so-ever in the course of routing the IP data packet in the Internet.

The Mobile-IP solution can be applied as long as the handovers are not

performed too often. However, it incurs the punishment of routing all incoming packets through a server, causing both an increased travel time for the data packets, as well as latency (or disconnection) for the time that the real IP address changed, but the server is not informed yet. If the round-trip-time of the packets between the STA and the server is longer than the time a STA stays with the same IP, this method fails, as by the time packets reach the reported location of the STA, the STA is already in another location.

For many applications, such as voice, it is of utmost importance to minimize the time spent on the handover process. The time consumed by the handover process is usually dominated by the scanning step (Step 1 as mentioned above), and by Step 4 (specifically in case of an unmanaged network). There are many solutions that address fast handovers in cellular networks, and a few solutions that address fast handovers in managed WiFi networks (for example, see: WO2004/054283, which reduces Step 1 (mentioned above) by selective scanning but requires modifying the AP). None of these solutions deal with the delay due to Step 4.

It is an object of this invention to provide very fast handovers even in unmanaged networks.

Another barrier for wireless applications is that WiFi coverage might exists, and security policy might allow the STA to connect, but the AP might be out of resources (for example, there are 2007 associated STAs, and therefore it has no resources left, or that it has a limited IP address space which was already allocated through DHCP, and it has no IP address to allocate). It is an object of this invention to provide a system and method that allows STAs to use the services of the AP even when some of its resources are exhausted.

Another barrier for many wireless applications is the complex configuration of wireless parameters of STA, especially the security parameters. A user that purchases a new STA and has an existing AP, might wish to configure his new STA to work with his AP. This configuration includes entering into the STA the

encryption key and authentication key that would allow it to use the AP. Existing solutions require a change in the AP and STA, such that a special key can be pressed simultaneously at both ends to perform automatic configuration (like Buffalo INC's AirStation OneTouch Secure System - AOSS, or Broadcom's SecureEasySetup). Without such a solution, the user is usually forced to punch into his STA the security codes (which are typically long). The problem worsens when the STA moves between APs that use different security settings.

It is an object of this invention to provide for easy configuration on both levels: at the initial setup and while roaming.

Another barrier for many wireless applications is that WiFi coverage might exist, but it is locked and unavailable for use for the STA.It is an object of this invention to provide a solution for (legally) accessing locked APs.

Another problem with WiFi is that the WiFi protocol is not optimized for low battery consumption (compared to cellular protocols such as GSM). In current solutions, if the STA moves between APs and changes its IP, it must use mobile IP and inform an entity (server) in the network of its current IP (we refer to this process as "location update", as the STA updates the network entity of its location). Frequent location updates exhaust the STA's battery. Another problem with frequent location updates is that they create a heavy load on the network and on the network entities that manage and keep track of the STA's location.

The situation in WiFi is very different from the situation in cellular networks in two ways. Both of the ways cause an increase in the number of location updates in WiFi: First, in cellular network, the cells are typically much larger than a "cell" that is created by a WiFi AP. Therefore, in cellular networks, there are fewer transitions between cells, and hence less location updates. Second, cellular protocols allow defining a "location area" that encompasses several cells, and the STA is required to perform location update

only when moving between location areas, and thus reducing the number of location updates. Current WiFi protocols are not built to support location areas.

It is an object of this invention to provide a method that reduces the number of location updates required for STAs while moving between APs.

It is an object of the current invention to provide solutions to the above mentioned problems, using both a centralized (server based) approach, and also by providing a method for performing the solutions using a distributed peer-to-peer network. Therefore, no huge servers and no large investments are required.

Disclosure of Invention

The invention is described by way of example, but it should be obvious to persons skilled in the art that many variations thereof may be implemented.

A novel aspect of the invention relating to the deployment of APs is that devices function at the same time as STAs and as APs. This allows a STA to also create a new AP for connecting other STAs to the Internet therethrough. It is known in the art that a STA wireless card can operate in one of two modes, STA or AP. The present inventor has found a way to activate a device simultaneously in both modes.

According to another novel aspect, a connecting STA can limit the set of Internet addresses or internet sites that other STAs which connect through it can access, but the set of allowed addresses includes a special web site from which other STAs can download the Vagabee(TM) software. Vagabee software includes the functionality of the software of the first STA, to open new APs and further spread the Vagabee.

Once the new STAs download and execute the Vagabee software, the first STA

detects that the software is running on the new STAs, and allows them a wider access to the internet. Therefore, new STAs must download and run the Vagabee software to get wide access to the internet. As the new STAs run Vagabee, they become APs in their own right and allow other STAs to download and connect through them to the internet in the current location of these STAs, as well as in any other location they go.

Another novel method of the present invention allows a STA to connect through two or more APs simultaneously. Thus, a STA can enjoy a more stable connection even if part of the connections are of borderline quality. Furthermore, more connections may achieve a broader connection to the Internet, or may balance its traffic such that each STA carry a lighter burden with regards to the extra bandwidth they carry due to a new STA.

Multiple connections also allow faster handovers, as if a STA is moving from one place to the other it can first establish a new connection and then the old connection is terminated, practically leaving the STA connected.

In a further development of the novel method, a laptop (the terms STA and laptops are interchangeable, we use laptop rather than STA as in the preferred embodiment these cases the STA would be a laptop) can connect with another laptop directly or through a STA, such that both enjoy the Internet connection of the other. As the internet connection is not used all the time (typical laptop uses on average a few percents of its maximum bandwidth), both laptops will experience a much faster connection to the Internet.

Another important issue is the security of the system. A Laptop might agree to act as an APs, but it does not agree to allow other STAs to access its inner network (i.e., the laptop owner wishes to allows these STAs to access the internet through its private network but does not allow them to access computers on its private network. Another security concern is that the new

STAs may desire to prevent the first STA from tapping into their Communications, i.e., they do not want the first STA to be able to tap into communications that the first STA relays. The current disclosure provides novel method to deal with these two problems.

First, external STAs (new STAs) are not allowed access to computers in the inner network by having the first STA drop data packets from the external STAs that are designated to local IP addresses on the inner network. Second, a new STA's privacy is protected by tunneling its sensitive traffic to a trusted network site, and the new site accesses the Internet through his tunnel to the trusted network site which acts as a proxy for it.

An important issue is to prevent STAs from using other laptops for their primary network connection for a long period of time. A novel method detects that a STA is connected to the internet through the same laptop for a long period of time, and disconnects the STA. Alternatively, the STA has to pay to continue and use the network. The pricing can be such as to encourage the STA's user to purchase his own connection from an independent Internet Service Provider (ISP).

In yet another novel method, the software running on a laptop can replace the commercial banners that appear in the web pages the laptop surfs into, as well as the web pages that connected STAs surf into. The banners can be stopped, replaced, and made specially targeted to the user, for example based on his location.

A further novel method is that the wireless internet coverage that is obtained using laptops can be used by devices such as wireless IP phones to make phone calls using the wireless internet coverage, cellular phones that have built-in WiFi connection, or digital cameras with WiFi that wish to upload the data stored in them. Other devices might include for example, radio or TV broadcast capabilities.

For example, Digital cameras might be equipped with WiFi. The owner of such a

camera would like to upload his pictures from the camera to a server that stores the pictures on the Internet - the reasons for this may vary from being able to share the photos while on vacation with family members left at home, backup the pictures from the digital camera to the Internet server, or simply because the memory card on the camera is running out of space. A major problem is that to upload the pictures to the Internet may take a very long time, as pictures consume megabytes to store. In the novel method, the camera can send the photos to the laptop over WiFi (this connection is very fast), then disconnect and move on. Then, the laptop uploads the pictures to the Internet server (this process can take a long time as it involves uploading a lot of data), but the laptop owner would not feel it as a burden, since the pictures can be uploaded when his Internet connection is not used for other purposes.

Improvements to this method may include: The camera can encrypt the pictures so that the laptop owner cannot see them. The pictures can be still stored in the camera after being uploaded to the laptop, as the laptop might fail to upload them. The next time the camera connects to the Internet, it can check with the Internet server that the pictures arrived correctly to the server. If that is so, the pictures may be erased from the camera. Otherwise, the camera can re-transmit the pictures.

To have faster uploads, the camera can upload the pictures to several laptops that would upload the picture to the server.

Another novel method relates to configuring STAs to connect to a wireless network. The configuration, and especially the security configuration of STAs to connect to a wireless Internet connection such as WiFi is cumbersome and annoying to most users. Assume a STA belongs to the same user (or user group) of the owner of a laptop. Then, by a special logging into a website, the configuration of the laptop can be copied to the STA, thus configuring it to use the AP (i.e., allowing a connection without the laptop).

Another novel method allows devices with a trusted hardware to receive information that instructs them how to directly connect to AP, by providing them with the needed settings and security information.

One of the novel aspects of a very fast handover is to practically "almost complete" the process of the handover before it even started, possibly with the assistance of another STA that is already in the new AP's coverage (further details are described later).

Another novel aspect is that the same MAC address and IP address can actually be used by more than one STA. The differentiation between the STAs can be performed by using higher protocol identification, such as different port numbers (for example TCP ports), as detailed later.

It is useful for a station STA to know the identity of the adjacent APs that the STA might hand over to. The identity of an AP can be established in several ways, as disclosed herein. The SSID (Service Set ID) of the AP is usually broadcasted by the AP using periodical transmissions known as beacon. However, two adjacent AP may have the same SSID. In such a case, the MAC address of each AP is different, and APs can be differentiated based on their MAC address (which serves as a globally unique identification parameter). Some APs do not transmit beacon, and only respond when they are addressed using their SSID. In this case, a priory -knowledge is needed, see below.

Another aspect of the invention is for a STA to selectively scan for a neighboring AP in the following novel way. Assume that a STA scans to see if it can receive the beacon of a second AP, where the scanning will be performed exactly when the second AP is expected to transmit its beacon, therefore, the disconnection from the first AP will be minimal. The novel method consists of scanning and storing (in network entities) information about the relative time

between adjacent APs, and their relative clock drift. This information is retrieved at the appropriate time such that the STA knows to wait for the beacon just before it is transmitted.

Another aspect of the invention is to prevent exhaustion of resources at the APs. GN keeps a pool of MAC addresses with associated IP address. Just before a STA enters the AP, GN sends it a MAC address and an IP address that are already associated with the AP. Therefore, the STA can connect even if the AP has no resources left for new STAs.

Another novel aspect of the invention is to save Battery Power and reduce network load by reducing the number of Location Updates in WiFi. A location update is the process in which a STA informs an entity in the network on its current location (the notification can take many forms, including opening a TCP connection, or sending UDP packets). In prior art for 802.11 networks, a location update is required whenever the IP address of the STA changes (for example, when moving between APs of different subnets) - even if the STA is idle (not transmitting or receiving data). The novel method allows to define a location area for WiFi, such that an idle STA needs to perform location update only when it moves between APs that belong to different location areas, but does not need to perform location update when it moves between APs of the same location area, even if its IP address changes. See further details later.

A pseudo-beacon is another aspect of the invention which allows reducing the number of Location Updates. It is a message that GN can periodically transmit in each AP. While some APs might permit a remote node to transmit a message in the AP, other APs might not allow it. In the novel method, a certain MAC address, IP address, and possibly a port number, are allocated in each AP for the purpose of pseudo-beacon transmission. Further details are described later.

Configuring the security in new STAs to work with an existing AP might be a

tedious job, as the security (authentication/encryption) code might be very long as known in the art, and the user might need to punch it into the STA. A novel solution for easy configuration is disclosed. Unlike previous solutions, the novel method does not require changing the existing AP of the customer. In one embodiment, software is run on a personal computer of the user (that is already configured to access the WiFi). Then, the software establishes a secure channel with the STA, and copies the security information from the personal computer to the STA. In this way, the STA learns the security parameters. An authentication phase in which the STA is authenticated by the software or a remote server can be added before copying the security information.

In another embodiment, the customer first connects the STA by wire to its network (or alternatively, the STA first connects using a connection it establishes through an already connected device, such as a personal computer or laptop).

As the STA can receive and transmit signals on the wireless network and it is connected to the internet (through the other connection) at the same time, it tries to locate the web configuration of the AP on the wired network (most APs have a web interface). In most cases, it is an easy job for the STA, as either the STA can locate the AP as it is the default gateway of the wired network, or it can try to find its IP by performing RARP (Reverse Address Resolution Protocol) using the wireless MAC address of the AP (which it can see off-the-air). Further details are described later.

Another novel method for gaining access to locked networks is disclosed. While performing the above described easy setup (or at any other time), the user is prompted, if he wishes, to join a swapping service. The swapping service allows the user to gain access to many locked networks (the locked networks of the other users that joined the swapping service), in return he allows users to use his network for the purpose of connecting to the Internet. If the user agrees, the access parameters to his network (encryption key, MAC address,

default gateway, etc.) are securely stored in the network (for example in GN, and a backup server). The security information will be securely sent directly into the hardware of other STAs, when they need to connect using his AP. Further details are described later.

Another novel aspect of the invention takes advantage of the fact that the wireless network is local in nature, as the APs are geographically adjacent. As a result, the methods that are disclosed can be implemented by many small devices on the Internet, each responsible for a geographic area. The devices form a peer-to-peer network that implement the methods, without the need to rely heavily on large servers.

Another novel aspect of the invention is to have a STA which has a capability of communicating in two or more channels in parallel. This capability can enable a STA to be connected to two APs in parallel without the need to implement sophisticated mechanisms that actually simulate this situation. Thus, a STA can connect with future APs while maintaining a connection through its serving APs. Being connected to two APs simultaneously allows greater bandwidth by utilizing two connections instead of one, and soft-handovers, i.e., the STA stays connected through one AP, while disconnecting from the second AP in the process of handover.

The new system and method refers, among others, to the following innovative features:

1. A viral-like fast spread method for the Vagabee(tm) software:
- at the network level
- at the already connected PC
- at a connecting PC, already having the Vagabee software
- at a connecting PC, not yet having the Vagabee software
- details of the software package being loaded on a new computer: functions, operation, how installs, how spreads further away to other PCs.

2. Detail the viral spread method:
- use of existing standards; "as is" or with modifications
- method of reporting to user and getting a user's approval
- interaction with firewall and antivirus programs in the PC

3. Vagabee in use, with flow charts:
- manage communications with presently connected PCs
- add new PC
- remove a PC. Recover chain, reestablish communications when intermediary PC disconnects
- resolve conflicts where there are several Vagabee systems in one area.
Method of operation, so the networks will not interfere with each other,
rather they may assist each other and maybe provide backup functions.
- Knowing the identity of adjacent APs and the location of STAs.
- handoff to another local Vagabee network

4. Vagabee in use, system design:
- workload on the various PCs in the chain (the workload increases as one moves closer to the AP, the Internet connection)
- overhead, signaling and control, traffic control. Define signals, method of operation
- permission to access more sites on the Internet after a new PC downloads and activates Vagabee - how implemented.
- reliability issues

5. System design for various configurations
The basic assumptions greatly affect the performance of the network systems which may be formed:
- a PC connects to only one additional PC
- a PC may connect to one or two additional PCs
- a PC may connect to more than two additional PCs

6. Bandwidth control
Bandwidth request and allocation. For the various PCs in the chain.
Methods for improved channel use. How is implemented.

7. Privacy issues - how the inner/outer areas are implemented.
Protection from viruses and eavesdropping, passwords protection, etc.
Damage control, Recovery from a virus attack.
This is a vital aspect of the new technology.

8. User control and supervision
- the user of a PC decides whether to install Vagabee
- the user of a PC decides whether to allow additional users to connect, with what parameters (bandwidth allocation, etc.)
- incentives for a user to allow his computer to connect others.
- the user allows or forbids additional users, according to circumstances - how important his present activity is, what is the quality and bandwidth allocated to that user (how much spare bandwidth there is)

9. Details of implementation - software
- New software
- Modified existing software
- Method of use of existing software, standards

10. Functions, benefits to users - detail methods to implement them
- free internet connection
- enhanced bandwidth, reliability
- provide additional services - locate gas stations, Pizza Hut, restaurants.

Brief Description of Drawings

Figs. 1 and 2 illustrate a wireless system for connecting mobile devices to the Internet through an access point

Fig. 3 illustrates an expanded wireless system for connecting mobile devices to the internet through more than one access point

Fig. 4 details a method for fast spreading the Vagabee software by providing free wireless access to the Internet.

Fig. 5 details the dual mode connectivity of a STA also functioning as an AP with the Vagabee method and software

Figs. 6A to 6F detail stages in a wireless network evolvement and spreading of the Vagabee software

Fig. 7 details a method addressing control and security aspects of the Vagabee spreading method

Fig. 8 details a method addressing coordination and control aspects of the Vagabee spreading method for the first, connecting STA

Fig. 9 details multi-AP, fast configuration setting and handover aspects of the Vagabee spreading method for the second, to be connected STA

Fig. 10 details multi-AP, fast secure configuration setting and redirection aspects of the Vagabee spreading method for the first, connecting STA

Fig. 11 details multi-AP and fast configuration setting aspects of the Vagabee spreading method for the second, to be connected STA

Fig. 12 illustrates a system including mobile stations (STAs) and their Access Points (APs), with one STA moving from the coverage of one AP to the coverage of another

Fig. 13 illustrates a wireless system facilitating handover and including a STA, a Governing Node (GN) and another user, Termination Node (TN)

Fig. 14 details the handover method

Fig. 15 details a method for implementing two connections with a STA.

Fig. 16 details a method for connecting other STAs

Fig. 17 details another method for connecting other STAs

Fig. 18 details a method for configuring other STAs to directly connect to the AP

Fig. 19 details another method for configuring other STAs to directly connect to the AP

Fig. 20 details yet another method for configuring other STAs to directly connect to the AP

Best Mode for Carrying Out the Invention

A preferred embodiment of the present invention will now be described by way of example and with reference to the accompanying drawings.

Dual use laptop simultaneously connected to the internet and serving as AP

Figs. 1 and 2 illustrate a wireless system for connecting mobile devices to

the Internet through an access point. It may use a novel method for performing the deployment of APs, i.e., the method that allows devices to function at the same time as STAs and as APs. For example, a laptop 11 is connected to the Internet through access point AP 10, and at the same time, laptop 11 shares its connection for other STAs by operating as an AP. Thus, other STAs 12 and 13 look at laptop 11 as an AP, and can connect through it to the Internet.

When laptop 11 is connected to AP 10 through a wired connection, it can simply set its wireless connection as an AP (Infrastructure mode). However, when laptop 11 is connected to AP 10 through a wireless connection, the situation is more complex. Disclosed is a novel method in which laptop 11 can be connected to AP 10 and serve as an AP using only a single wireless network card. Laptop 11 connects to AP 10 just like any other STA, and at the same time runs the protocol stack of an AP.

Laptop 11 uses the same channel as AP 10, and transmits a beacon message such that the beacon of AP 10 and the beacon of laptop 11 are expected not to collide in time. Laptop 11 derives and updates its internal clock from AP 10, but adds a constant delay (to make his beacon appear with a delay after AP 10). In another embodiment, laptop 11 does not add a delay to the time of AP 10, but sets the beacon period to a value, such that the greatest common denominator (GCD) between its beacon period and the beacon period of AP 10 is the smallest that is possible. Such a choice of beacon period ensures minimal collisions between the beacons.

In the preferred embodiment, laptop 11 will run a Network Address Translation (NAT) and a DHCP server as part of his protocol stack. Running DHCP enables laptop 11 to provide an Internet address to STAs that connect to it. Running a NAT allows laptop 11 to connect other STAs through it, while keeping conformance with regards to AP 10 - To AP 10 all the communication appears to be originating form laptop 11.

The software package 31 may be contained in the laptop 11, or in the laptop 11

and the STA 12, for example.

Viral Spreading

Many networks suffer from the network effect in their infancy, in which the first users have no incentive to join the network. However, the network is of great value once many users are in the network.

The following method and system attracts the first users, and provide an increasing value as the network grows. The first very few laptops with the software are installed and deployed in key areas by the network initiator. The software running on the laptop 11 has functionality 31 as follows (explained through an example):

Laptop 11 acts as an AP and allows other STAs to connect to it. To further lure STAs, the SSID (Service Set Identification - this is the name of the network that users see when looking for an available network) can be set to "Free Internet" or another name that will attract roaming laptop users to log-into it while searching for wireless networks.

Assume a user using a laptop called STA 12 connects as described above. Once STA 12 is connected to the laptop 11 (laptop 11 serves as an AP), no matter which web site the user tries to enter, the software 31 on laptop 11 forwards

the connection to a special web site 30. The web site 30 informs the user (STA 12) that, in order to use the free connection, it must install a software with functionality 31. The deal is that the user is allowed the free access at this location, but it is requested to share his own connection when he has one at his disposal. The user then downloads and installs the software with functionality 31 (See Fig 1.B which shows software with functionality 31 running on STA 12. Once laptop 11 identifies that STA 12 has functionality 31

running, it allows it a wider access to the internet (or a full access to the public Internet).

Thus STA 12, which originally did not have functionality 31 running, but its user wished to connect to the internet, ended up with functionality 31 installed and running on STA 12, and the user received a working internet connection. When the user moves STA 12 to another area in which it connects directly to an AP (which might be locked), it shares its connection with other STAs, which are also motivated to install functionality 31. Thus, functionality 31 can spread quickly among STAs, and the total area that is served grows larger, where each additional STA spreads the network further.

Laptop 11 together with its software might need to use two different security parameters at the same time - one towards AP 10 (which might be locked), and open security towards other laptops - so they can connect with no security settings. Once functionality 31 is running, it can establish a secure connection with laptop 11 as a secure layer on top of the fundamental insecure wireless.

Connection through multiple access points

Another novel method of the present disclosure allows STA 14 to connect simultaneously through two or more APs, see Fig. 3. For example, STA 14 connects through both laptop 11 and laptop 21 to the internet. Thus, STA 14 can enjoy a more stable connection even if both connections (through laptop 11 and 21) are in borderline quality. Furthermore, even in case the connections are not in borderline quality, they can be used to provide STA 14 a broader connection to the internet, or balance his traffic such that laptop 11 and laptop 21 carry a lighter burden per laptop with regards to the extra bandwidth they carry due to STA 14.

Multiple connections also allow handovers. When a STA is moving from one place

to another, it can first establish a new connection and then the old connection is terminated, practically leaving the STA connected.

When laptop 11 and laptop 21 use the same WiFi channel, STA 14 connects to both laptops by creating two protocol stacks on the MAC (Media Access Control) layer. When laptop 11 and laptop 21 operate on different channels, STA 14 agrees with laptop 11 and laptop 21 on period of times in which laptop 11 sends packets to STA 14, and periods of time in which laptop 21 sends packets to STA 14. STA 14 makes sure that these periods of times do not overlap, thus, STA 14 sets the channel according to the period, such that it listens on the channel of the laptop that might transmit to it. If the laptop has packets pending for STA 14 it queues them for transmission in the transmission period.

In order to have a faster connection through the two (or more) connections, STA 14 downloads/uploads some of the information through one connection, and the rest through the other connection. For example, when downloading a web page, STA 14 can download the text through one connection, and download the images through the other connection.

In another embodiment a remote site 50 with a fast Internet connection acts as a proxy of STA 14. Incoming and outgoing packets are forwarded between STA 14 and remote site 50. The packets are sent using error-correction codes that allow reconstructing the data even if some packets are lost on one connection, but some packets reach the destination using the other connections. The role of remote site 50 can be assumed by a service provider, by computer with a software that the user installs in his premise, or by another user with high bandwidth.

When the STA moves from one location to another, new connections are being established, while other connections are being disconnected. However, as long as there is at least one active connection, the STA will stay connected to the Internet continuously and seamlessly.

Sharing Internet Connection between Laptops

When laptops 21 and 11 are within radio (wireless) contact (or through the mitigation of other STAs), each laptop can treat the other as another connection at his disposal. Thus, the maximum data rate available for each laptop can be significantly extended, much like the case with a STA connected to two laptops.

Fig. 4 details a method for fast spreading the Vagabee software by providing free wireless access to the Internet. The method includes:

a. First STA transmits "AP available" WIFI info 41
b. Info is presented to Guest 42
c. Guest chooses our AP? 43
d. Allow limited access to Guest including our Web site 44
e. Guest agrees to use our service? 45
f. Download connectivity software to Guest and activate it 46
g. Connect Guest to Internet and allow wider access 47
h. Guest transmits "AP available" info and further spreads our service 48
** End of method **

Note: It is not mandatory to perform all the above stages. The more important steps are 45 - 47 or any similar implementation.

Fig. 5 details the dual mode connectivity of a STA also functioning as an AP with the Vagabee method and software. The method includes:

a. First STA associates with an AP as a regular STA 411
b. First STA activates "AP" protocol stack with open security 412
c. Guest chooses our AP? 42
d Address translation to connect Guest to our Website 445

** End of method **

The above method has been implemented by the present inventor on a communication device using the Intel 2200 chipset, just as an example to show that it can be done. The present inventive approach and method may be used towards similar implementations with other communication devices.

Figs. 6A to 6F detail stages in a wireless network evolvement and spreading of the Vagabee software, including:

FIG. 6A: There is a Laptop 11 connected to the internet by wireless through the access point AP 10.

FIG. 6B: The Laptop 11 also functions as AP using the Vagabee software, thus allowing free access for STA 12 through Laptop 11.

FIG. 6C: STA 12 joined the Vagabee group, created a new AP to also connect Laptop 121. A long chain can thus be formed.

FIG. 6D: each AP can connect several new devices, as illustrated here with Laptop 122.

FIG. 6E: a multi-AP network may be configured, with a plurality of devices being connected through both AP 10 and AP 20. A device such as Laptop 122 can be simultaneously connected through more than one AP to the internet.

FIG. 6F: As the initiated device Laptop 124 moves to another location and connects to AP 24 (maybe it has a license or privileged access there, while Latop 125 and STA 126 cannot connect directly to AP 24 due to distance or lack of security parameters), the Vagabee software in device 124 opens a free AP at

that location, now being utilized by Laptop 125 and STA 126 to connect to the internet. At a separate location, AP 10 may still operate and connect STA 12, Laptop 121 etc.

Security

Another important issue is the security of the system. Consider a situation (shown in Fig.2) in which laptop 11 agrees to act as an APs, but it does not agree to allow STA 13 and STA 14 to access his inner network (i.e., it allows STA 13 and STA 14 to access the internet through his network but does not allow them to access computers in his network. For example, a private server 40 should not be accessible to them). On the other hand, STA 13 wishes to use laptop's 11 network, but might not wish laptop 11 to be able to tap into the data that STA 13 exchanges with Internet servers. The current disclosure addresses these two problems using a novel method. First, external STAs are not allowed to access to the inner network by not allowing them to access to local IP addresses. Second, STA 13's privacy is protected by tunneling its sensitive traffic to a trusted network site 50, and STA 13 accesses the internet through its tunnel to the trusted network site 50, which acts as a proxy of STA 13.

To prevent STAs from accessing the inner network, laptop 11 blocks all traffic from the guest STAs to internal addresses (i.e., addresses that appear only in local networks and not in the public internet, such as 192.168.*.*, or 10.*.*.*, and 172.16.0.0 - 172.31.255.255). Another method, which can be applied independently, is to allow the connection if it is at least x hops into the Internet, where x is the maximum number of hops in the local network (which can be discovered by performing a traceroute command). Another method is to allow access to addresses which have an IP address with a different prefix, as internal networks typically have the same prefix on the IP address. In another method, laptop 11 allow only packets to and from known servers such as trusted server 50 (i.e., white listing the allowed addresses).

To protect the privacy of STA while it is surfing, its traffic can be tunneled to a trusted network site 50, which acts as its proxy. The network site can be replaced by simply tunneling the connection to another node in the network, and switching the network node once in a while. The access to the remote nodes is made without identifying the STA, but only proving that it belongs to the group of STAs, thus, its privacy is preserved. The frequent switching of remote nodes eliminates the possibility that a remote node can gather a significant amount of private information from peeking into the communication. The list of available remote nodes can be kept by a directory service, which can be distributed in a peer-to-peer fashion.

In another embodiment, the remote node is a trusted computer installed by the user. Such a configuration has the added benefit that the user can access internal nodes in his own private network, effectively having a Virtual Private Network (VPN) with his home network.

Fig. 7 details control and security aspects of the Vagabee spreading method including:

a. First STA transmits "AP available" WIFI info 41
b. Info is presented to Guest 42
c. Guest has Vagabee software? 425
d. Guest agrees to use our service? 45
e. Download connectivity software to Guest and activate it 46
f. Connect Guest to Internet and allow wider access, excluding private servers/sites 472
g. Guest transmits "AP available" info and further spreads our service 48
h. Guest uses encryption and secure website to preserve privacy from connecting STA 481
i. Establish best route for all STAs 482
adaptive to changes in network.

Load balancing.
Connections thru multiple routes.

j. Connection time > Ts ? 483
k. Disconnect/change connection 485
** End of method **

Note: Not all the steps above are mandatory; a method may implement only part of the steps in the above method.

Maintaining Fairness

It is desirable to avoid an unfair situation in which one user exploits the network by continuously using a connection without ever sharing a connection. If many users follow these lines, the network experience will degrade as there will be only a small number of laptops connected directly to APs. A novel mechanism detects that a STA is connected to the internet by noting that the same STA (using the same laptop) connects from the same small area (or through the same AP) for a long period of time (i.e., beyond a threshold). For example, this threshold can be set to two weeks. Once a STA passes the threshold, the functionality 31 notes the user that the threshold is reached. The user is then required to move to another area or pay a small fee to continue and access the AP.

Functionality 31 may note the user when the threshold is being approached, even before it actually reaches it. It can then give a pre-warning to the user.

The laptop is identified through his account information, through the MAC address of his network card, and other machine-specific information, such as the serial number of the hard-disk.

Fig. 8 details coordination and control aspects of the Vagabee spreading method for the first, connecting STA, including:

a. First STA connects to AP in "AP" mode 412

b. Set wireless connection as "Ad-Hoc" using the same channel as the AP 413

c. Transmit beacon message at a delay after AP or set beacon period so as to minimize collisions 415

d. Act as AP for additional STAs, while preventing them access to its inner network 416

e. Replace commercial banners for own site and also for STAs connected to this STA 417

f. Security Option: Allow connection of connected STAs only if it is at least X hops into the Internet 418

g. Maintaining fairness: demand a connected STA to disconnect or move or pay after a predefined time 419
** End of method **

Fig. 9 details multi-AP, fast configuration setting and handover aspects of the Vagabee spreading method for the second, to be connected STA, including:

a. Connect through a first AP 481

b. Activate Vagabee to provide AP service to other STAs 482

c. Search for additional paths to 483
establish multiple simultaneous connections thru multiple APs

d. Copy configuration of connecting STA, 484
to gain direct access to the initial AP, or receive connecting instructions for STAs with trusted hardware

e. Preserve privacy using tunneling 485
to a trusted network site for sensitive traffic

f. Perform handover whenever necessary 486

g. When moving to a new location: 487
establishing a connection with available AP,
Activate Vagabee to provide AP service to other STAs

h. Maintaining fairness: demand a connected STA 419
to disconnect or move or pay after a predefined time

i. Control over advertisements (optional)
** End of method **

In a novel method hereby disclosed, the functionality 31 can scan the web pages that pass through it and block or replace the advertisements on the page depending on various data such as the user name, the user location, etc. The advertisements can be performed in collaboration with the web site that is being surfed into, or without.

Note: the functionality (or software module) 31 is an important part of the present method, a minimum requirement to allow Xiopea(tm) spreading. Moreover, module 31 need not include all the possible things that this

functionality can include, rather just the bare minimum directed toward allowing a connection to a STA in return to supporting the spreading of the this software.

The site 30 can instruct functionality 31 as to which advertisements should be removed or changed, and which advertisements should be placed. New advertisements can also be added in places that there were no advertisements to begin with.

The software 31 running on laptop 11 can replace the commercial banners that appear in the web pages that laptop 11 surfs into, as well as the web pages that STA 13 surfs into. The banners can be stopped, replaced, and made specially targeted to the user, for example based on his location.

Configuration of Wireless Networks

An annoying task associated with wireless networks is the configuration of a STA to work with a network. The security settings are especially annoying, and currently, many people avoid securing their network due to the cumbersome setting procedure.

A novel method is disclosed to perform easy configuration of a wireless settings. The method is composed of two parts, the first is establishing the settings for the first device, and the second part is establishing the settings for the rest of the devices. First part: Assume a user on laptop 11 is connected to his wireless AP 10. If AP 10 is not set to use encryption, the user can ask (or be offered) to secure his network. Functionality 31 automatically accesses the interface of AP 10 and configures it with security settings. Laptop 11 is also set with the security settings. The settings are also stored in an account in web site 30, for future use. Site 30 can also provide functionality 31 with the information on how to set the security setting on the specific model of AP 10.

Second part: When the user uses another device STA 12, he connects to the network through functionality 31 on laptop 11, which redirects him to web site 30. On the site, he can log-in using his account details. Web site 30, through functionality 31 which is running on laptop 11, discovers that the two devices (laptop 11 and STA 12) are both connected through AP 10, and both belong to the same user account. As a result, web site 30 offers the user to reconfigure STA 12 to work directly with AP 10. The user is advised to download functionality 31 to STA 12, and run it. Once functionality 31 is running on STA 12, it configures STA 12 with the settings of the network (which are retrieved from web site 30, or directly from laptop 11).

Fig. 10 details multi-AP, fast secure configuration setting and redirection aspects of the Vagabee spreading method for the first, connecting STA, including:

a. First STA connects to AP in "AP" mode 412

b. Establish settings for first STA: 511
configure AP with secure settings, set STA with secure settings.
Store settings in web site.

c. Redirect a connecting STA to the web site 512
to configure it with secure settings.
** End of method **

Fig. 11 details multi-AP and fast configuration setting aspects of the Vagabee spreading method for the second, to be connected STA, including:

a. Connect through a first/available AP 481

b. STA has secure sub-system trusted by the web site? 482

c. Web site allow it to retrieve the 483
settings of the network for direct connection

d. Both STAs use the same AP 484
and same user account?

e. Agrees to connect directly to AP? 485

f. Download functionality and activate it 486

g. Configure STA with the settings of the network 487
** End of method **

Many variations can follow to the above procedure, and should be clear to those skilled in the art. For example, the settings may be stored on laptop 11 instead on web site 30, the settings may be encrypted, and the sequence of events can be changed. The result is an easy configuration of the network by the user.

Fig. 12 illustrates the mobile stations (STA) with their covering Access Points (AP), where STA 11 is moving from the coverage of AP 31 to the coverage of AP 312. STA 12 is already in the coverage of AP 312, and another AP 313 has a coverage that intersects with both the coverage of AP 31 and AP 312.

A network infrastructure for other devices

Functionality 31 may allow devices that do not have the functionality 31 to access the network. Such a device receives a capability to be identified as eligible to access the network towards functionality 31, and it identifies as eligible to access towards functionality 31 on the laptop in order to gain access to the network. Such identification may include cryptographic means,

such as a digital certificate signed by an appropriate certification authority (CA) which gives the device the capability to be identified. Alternatively, the devices can be identified based on their MAC address. A username/password can be added for additional security.

Configuration of secure devices

It might be desirable to allow a device to directly connect to an AP, rather than connect through a laptop. When devices have a secure sub-system, i.e., a sub-system that is trusted by web site 30, web site 30 may allow it to retrieve the settings of the network (assuming that they are stored on web site 30), and configure the device to use the network.

As the device has a trusted sub-system, the settings can be stored in the sub-system, such that they do not leak outside.

Alternatively, functionality 31 can reconfigure the AP to allow access to a roaming device.

Displaying the coverage map

A problem often faced by users that wish to connect through wireless internet is that they cannot connect to the internet in their current location because the coverage in their area is locked, and they do not have access rights. A novel method and system helps users find the nearest location from which they can connect. Web site 30 holds a list of all access points from which users can successfully connect, together with all the list of APs from which are closed. The list includes the MAC address of each AP. Parts or all of this list can be downloaded in advance to a device, such as into laptop 11.

Then, laptop 11 uses the beacons of the APs which might be locked to determine its position (for example, www.SkyHookWireless.com uses beacons to determine

the location of a STA). Then, laptop 11 can display on a map the location of the user, and the locations of near by access point in which it can connect to the internet. The user can then go to the nearby locations and connect to the Internet. The list in site 30 can be constantly updated by information that STAs receive.

In another embodiment, the list of APs in site 30 can also hold the probability that the AP is accessible. The probability can change if the access is provided by a laptop rather than an AP, and the laptop may be present or not. An area covered by several independent APs, each with low probability, results in an area with higher probability of accessibility in the intersection of these areas. The probability of accessibility can be depicted in the map shown to the user, for example, by different colors representing the different probabilities.

It is understood that the method and system in the present disclosure may be used for the transmission of voice, data, multimedia or a combination thereof.

Gathering Physical Location

To display a map of coverage, the real-world physical location of STAs needs to be known. A novel idea is to use STAs that are equipped with both GPS (Global Positioning System) and WiFi to report back to a server (for example, web server 20), a scanning result and the physical location in which the scan was performed. The server can extract the physical location of the fixed APs and store it in a database. At a later time, when a WiFi-equipped STA that lacks a GPS receiver performs a WiFi AP scan, it can report the results to the server, which can use the database to determine the physical location of the STA. This physical location can be used to provide location-based services.

Fast Handover

A novel aspect of very fast handover is to practically almost complete the process of the handover before it even started.

Consider an example depicted in Figs 12 and 13, in which STA 11 is in conversation with TN 41 (TN - Termination node, the node with which STA 11 communicates, shown in Fig. 13), and STA 11 is moving from AP 31 towards AP 32. Also assume that a node GN 21 (GN - Governing Node, a node that is non-exclusively responsible for the mobility management in a certain geographic area for a given time, shown in Fig. 13) is in contact with STA 11, and it is assisting STA 11 during the handover process. STA 11 currently has an IP address, which was allocated to it by AP 31.

To complete the handover, STA 11 should be associated with AP 32, have an IP address assigned by AP 32, complete any second authentication that is required, and have TN 41 be aware of the new IP address, so it can forward the conversation to the new location. Note that in some scenarios (in some cases when there are firewalls or NAT devices between AP 32 and TN 41, the connection between STA 11 and TN 41 must be started from within AP 32 towards TN 41).

According to prior art, it appears that STA 11 cannot begin the handover process until it reaches the coverage of AP 32, since it cannot start the connection process. One novel solution (that requires changing the software of the AP) is to allow STA 11 to perform the connection process through the Internet, instead of performing it wirelessly. In this way, once STA 11 reaches radio connection with AP 32, it can start working immediately.

However, we are more interested in solutions where there is no need to change the AP. To achieve this goal, assume the existence of a non-moving STA 12 in

the coverage of AP 32 (we will somewhat soften this assumption later). According to the present invention STA 12 is in contact with GN 21, and receives instructions to impersonate STA 11 towards AP 32 (we will later discuss how to make it possible), and complete a connection process with AP 32 on behalf of STA 11 (including authentication, association, receiving an IP address, performing any second authentication/log-in procedure, and perhaps even opening connections or "punching holes" in the firewall).

Then, STA 12 communicates these parameters to GN 21 (once the parameters are communicated, STA 12 can return to its real identity). GN 21 communicates the parameters to STA 11 (and perhaps to TN 41), and thus, STA 11 does no longer need to perform the connection process, and once it reaches the perimeter of the coverage (we will later discuss how to identify this situation) it can immediately use the new parameters and continue communications without any delay. STA 11 (or GN 21) can alert TN 41 before the handover, so it can start and send information packets to the new location.

TN 41 may send the information in parallel to the old and the new location, and cease transmitting to the old location once the handover is complete (e.g., when it receives information from STA 11 with its address from the new AP). STA 12 may even open a TCP (Transmission Control Protocol, as used in the Internet) connection or send a UDP (User Datagram Protocol) packet on behalf of STA 11, if required.

This connection may wait for STA 11 until it reaches AP 32. If there is a timeout on these connections (either due to protocol, or due to firewalls), STA 12 or other bypassing STAs can send and receive -keep-alive- messages on behalf of STA 11 (as is instructed by GN 21). The timeout for each AP can be discovered over time by trial and error (or by discovering the APs type), and storing this information in GN 21 for future use. GN 21 can notify the STAs on the value of the timeout.

How STA 12 can impersonate STA 11:
To understand how STA 12 can impersonate STA 11 towards AP 32, we must understand how identity is established in the network. The basic identity in the network is the physical address which is known as MAC Address (Media Access Control Address), which is globally unique. Each manufacturer is allocated a portion of the address space and allocates a unique MAC address to every network card (including WiFi network card) that it manufactures. Then, the manufacturer burns the allocated address into the network card. However, in most network cards, an application can (temporarily) change the MAC address of the card to another MAC address.

The MAC address is not used for end-to-end communications over the internet, but usually only for communications within the same physical network. For example, STA 12 communicates with AP 32 using MAC address, but GN 21 is not usually aware of the MAC address of STA 12. The MAC address is universally unique. We use the feature of temporarily changing the MAC address in the network cards in a novel way, allowing STA 12 to impersonate STA 11.

Therefore, in the instructions that GN 21 gives to STA 12, it mentions the MAC address of STA 11, so STA 12 can assume the MAC identity of STA 11. Then, STA 12 can complete the association with AP 32 (using the MAC address of STA 11)), in which it receives the Association ID (AID), and completes a DHCP protocol in which it receives an IP address to be used with the MAC of STA 11 while it is using AP 32. STA 12 can also perform a second authentication and log-in on behalf of STA 11.

STA 12 sends the connection information back to GN 21, which forwards it to STA 11. STA 12 can return to its original MAC address, but the allocated resources at AP 32 remain allocated, as from the point of view of AP 32, STA 11 is already connected and in coverage. In order to avoid losing messages that are sent to STA 12 during its impersonation to STA 11, it can either

continue and listen using both its own MAC address and STA 11's MAC address, or it can issue a -power-save- mode command to its serving AP. The power save mode indicates the AP that the STA is sleeping for a while, in which time the AP is buffering the incoming data packets. Therefore, even if STA 12 is connected to the internet using another AP, it can issue a power-save mode command, possibly change the frequency, and perform the connection on behalf of STA 12. It can return to its serving AP once the connection is established, or pool for incoming messages once in a while.

First Softening of the Assumption that STA 12 is in the coverage of AP 32: What if STA 12 is not in the coverage of AP 32, and there is no other station in AP 32's coverage- The following process can be performed in advance, well before a handover is needed. GN 21 can ask (in advance) stations that pass through AP 32 to connect and receive an IP address from AP 32 using some MAC address. The MAC address is not necessarily the MAC address of STA 11, as the process is not specific to STA 11. The stations send the connection details to GN 21, which stores the AID, the MAC, the IP address and other connections details in a pool for future use.

The pool may even contain UDP or TCP connections, which may be kept alive by bypassing STAs (against timeouts of firewalls, Network Address Translator devices (NAT), and protocol timeouts). UDP and TCP connections in the pool are targeted to some node in the network that can forward information for other nodes (for example TN 41). When a connection is required by some STA, the pool is queried, and a resource can be allocated and applied by a STA. As a result, a station might change its MAC address and IP address every time it moves between APs. If the station moves very fast between these access points, GN 21 can predict the direction in which the station is moving based on past movements, inform TN 41 of the possible future addresses.

Using this method, TN 41 can send data to the new address even before the

station actually moved there. In some implementations of the APs and firewalls between AP 32 and TN 41 the STA must first send data before it can receive any data, otherwise, the firewall may block the incoming data, or a NAT (Network Address Translator) device might not know where to forward the data. The restriction, that the STA must be the first to send data, is usually required due to security policy that allows only outgoing connections, or due to NAT device that need to relate an internal IP address and port number with an external IP address and port number.

For example, in most NAT implementations a connection must be established from within the NATed zone (e.g., the AP coverage) towards the internet. Many firewalls also require that the connection is established from the private network towards the internet (rather than allowing incoming connections from the internet towards the private networks). In these cases, the data that TN 41 sends is not transmitted by AP 32 until the station reaches the access point and transmits information back to TN 41. Depending on the type of firewalls and NAT devices, TN 41 might be able to predict a port number to which it should send such messages before the first outgoing data packet is transmitted.

Another associated novel disclosure is that the same MAC address and IP address can actually be used by more than one STA. The differentiation between the STAs can be performed by using higher protocol identities such as different ports (for example TCP ports). Using the same MAC and IP address in more than one STA is not problematic for packets that are sent from the STA.

However, while receiving an incoming packet, only one STA should send an acknowledgement. As each STA knows the ports that are in use, it only acknowledges messages that are designated to it. GN 21 can coordinate between the STAs such that they do not use the same ports. For example, if there are at most n stations using the same MAC and IP address, station i will allocate port numbers that are equal to i modulo n. Another solution is to choose the

port number at random. If each STA uses one port at random, according to the birthday paradox, port collisions occur with very low probability as long as the number of connections is smaller than about the square root of 65536 (i.e., when there are less than 256 connections using the same IP).

Another idea is to change the software at the AP such that it can communicate with GN 21 and perform the connection procedure on behalf of STA 11.

Knowing who are the adjacent APs and the location of a STA:
It is useful for a station STA 11 to know the identity of the adjacent APs that the station might hand over to. The identity of an AP can be established in several ways: The SSID (Service Set ID) of the AP is usually broadcasted by the AP using periodical transmissions known as beacon. However, two adjacent AP may have the same SSID. In such a case, the MAC address of each AP is different, and APs can be differentiated based on their MAC address. Some APs do not transmit their SSID, but they still broadcast beacon messages with their MAC address. Even if the AP is locked and encrypted the MAC address is transmitted, and it is transmitted without any encryption. In this way, STA 11 can know the identity of adjacent APs, and infer its location.

Scanning by Idle STAs:

In a preferred embodiment, GN 21 collects information about APs which are adjacent. Idle stations (i.e. stations which are not in an intensive data transfer) can perform a scanning operation once in a while. As a result they learn the MAC address (and possibly the SSIDs) of the APs within radio reach. The STAs can then send this information to GN 21 which collects it. The idle STAs can also perform tests to check what is the accessibility parameters of an AP (e.g., is it an open and free AP, is it a locked AP and the password is available from GN 21, is it locked and there is no free access to the AP, is there a captive portal, does GN 21 have a username/password available for the

captive portal, etc.). All this discovered information is sent to GN 21.

When handovers are performed, GN 21 takes note of the sequence of handovers that occur, and can learn common paths which are taken (for example, a road or a crosswalk might cause more likely paths than others).

It is very important that GN 21 knows in advance the AP to which STA 11 will be handed over to and when the handover will occur. Such a knowledge allows, for example, to alert TN 41 of the new location in advance. Gaining accuracy in the prediction of the handover (when and where) translates to better performance, as GN 21 needs to allocate a MAC address and an IP address to STA 11 in the new AP, and TN 41 might start to send data to the new location.

Therefore, knowing who the neighboring APs are, and their reception quality at STA 11 is very important.

Scanning by a non-Idle STA

In principle, STA 11 can scan the surroundings once in a while and look for the beacons of adjacent APs, and thus measure the reception quality from each AP. However, such a scanning takes a lot of time (might even take couple of seconds for a full scan). Selective scanning for APs which are expected to be neighbors can reduce the scanning time, but it can still stay in the magnitude of a few hundred milliseconds. It is important to understand that during a contemporary scanning using current technology, STA 11 cannot receive or send messages from or to AP 31, which means that the scanning time must be reduced to reduce this disconnection time.

The novel disclosed method is that STA 11 will selectively scan for a neighboring AP in the following special way. Assume that STA 11 scans to see

if it can receive the beacon of AP 33, where the scanning is performed exactly when the AP 33 is expected to transmit its beacon. Therefore, the disconnection from AP 31 will be minimal. The problem is, however, that although the beacons are transmitted periodically, STA 11 does not know when a beacon is expected to be transmitted from AP 33. As the beacons are transmitted about every 102.4 ms (milliseconds); (many variations are possible)., STA 11 might be forced to wait on average 51.2 ms, which is a prohibitively long time to wait.

STA 11 may also transmit a Probe message to force a beacon to be sent especially for it- but a probe message requires a transmission that has implication on battery life. Furthermore, for the purpose of location finding, STA 11 might wish to be able to receive beacons of APs that will not answer the probe (due to range, policies, etc.)

We can safely assume that other STAs visited the area of AP 33 before STA 11, and that they have reported the rate of the beacons of AP 33 (e.g., a beacon every 102.4 ms). A problem that remains is that the beacons are scheduled according to the internal clock of AP 33, which might tick at a different rate than other clocks (and clocks tend to tick at different rates). Moreover, the clock of the visiting STAs is probably not exactly synchronized with the clock of STA 11, which makes the process inaccurate.

That is, even if STA 11 knows that at a specific time according to some STA's internal clock a beacon was transmitted, STA 11 will not know how to translate this information to his clock, as the clocks are probably not synchronized to such great accuracy (network time synchronization services such as the network time protocol (NTP) cannot be more accurate than a couple of tens of milliseconds, where in this case we need an accuracy of around one millisecond). The following novel method allows accuracy of microseconds.

The novel approach for time synchronization is to rely on a relatively accurate clock already available to STA 11: The 802.11 standard requires each AP to transmit in its beacon its clock (referred to in the 802.11 standard as timestamp). This clock must be the internal clock of the AP at the time of transmission in units of microseconds. Therefore, STAs can specify the value of the clock of AP 33 in terms of the value of the clock at the adjacent AP 31.

By measuring the timestamp of AP 31 and AP 33 at two different times T311 and T312 (based on the clock of AP 31), in which the time value of AP 33 T331 and T332, respectively, it can be established with reasonable accuracy that AP 33 clock ticks approximately r33/31=(T332- T331)/(T312-T311) times for every clock tick of AP 31. At time T313 in the future, the clock of AP 33 can be estimated as T333=T332+(r33/31)(T313-T312). Similarly, at time T334 the clock of AP 31 can be estimated as T314= T312+(1/r33/31)(T334-T332).

Beacons are scheduled to transmission when the clock of the AP modulo the beacon interval is zero, where the beacon interval is measured in microseconds according to the clock of the AP, it is fixed for an AP, and the value of the beacon interval is transmitted in the beacon. Therefore, GN 21 stores the relation r33/31 together with T332 and T312 and the beacon interval of AP 33 and AP 31, and reports it to STA 11 such that it can extrapolate the time at AP 33 and infer the time of the beacon transmission.

Once STA 11 succeeds in receiving a beacon from AP 33 it can report the times to GN 21, so that GN 21 can keep its time tracking accurate. Furthermore, the scanning allows GN 21 and STA 11 to make the best handover decisions based on the knowledge of the approximate location of STA 11 with respect to the neighboring APs.

A technical problem to be solved is that a STA can know the value T311 but cannot measure the value of T331 at exactly the same time of T311 , as these values are carried on the beacons of APs, which are transmitted at different times.

A solution is to measure the time of AP 33 T331' at a time close to T331, and note the time difference between the two measurements according to the STA's internal timer. As the measurements are very close to each other, the clock drift between the STA's timer and AP 33's timer is negligible, and we can estimate that T331= T331'+timediff, where timediff is the time difference between the measurements of T331 and T331' according to the timer of the STA. If there is a large clock drift after all (although it is not expected), it can be corrected by calculating the r value between the clock at AP 33 and the STA in a similar way to the way done for APs.

The location of STA 11 can be deduced from the reception quality, the reception strength and the identity of the neighboring APs. This location information can be taken into account while performing handover decisions, as well as for location based services or for other network applications.

It should also be noted that in Frequency Hopping, knowing the time of the AP has another special importance, as the frequency that the AP works in might depend on the time.

Fig. 14 details a preferred embodiment of the handover method, including:

a. STA prepares in advance for a handover: 541
* Assisted by another STA (or STAs)
* Optional: use the same MAC and IP addresses in more than one STA
* Learn the identity of adjacent APs
* Measure beacon strength from other APs

b. GN supports handover: 542
* GN keeps a pool of MAC and IP addresses
* GN sends the addresses to STA just before it enters the AP

c. STA reduces the number of Location Updates 543
by only updating when changing location area

d. GN transmits a pseudo-beacon including 544
MAC address, IP address, port number

e. Easy security configuration: 545
* The AP of the customer is not changed
* Establish secure channel with STA and Copy security information, or
* Connect the STA initially by wire

f. Gain access to locked networks 546
by joining the Vagabee service

g. Maintain simultaneous communication with 547
more than one AP.
Update net configuration responsive to changing circumstances
** End of method **

Fig. 15 details a method for implementing two connections with a STA.
The method includes:

a. Load BSS firmware to the NIC 415

b. Associate with AP using a first SSID 416

c. Load IBSS firmware to the NIC, but do not perform 417
dissociation from AP before loading the IBSS

d. Create an ad-hoc network using a second SSID 418

e. Communicate with AP and STA that connect to 419
the second SSID
** End of method **

Fig. 16 details a method for connecting other STAs, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs to connect to the Internet by 492
allowing them to connect to the second SSID.
The first STA decrypts and encrypts data packets as needed based on the security parameters of the first and second SSID (or APs), and performs address translations and forward packets between the second and first SSID to facilitate this connection for other STAs.
** End of method **

Fig. 17 details another method for connecting other STAs, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by 492
allowing them to connect to the second SSID. The limited access includes the ability to download a software that implements the current method.

The first STA decrypts and encrypts data packets as
needed based on the security parameters of the first and second SSID (or APs),
and performs address translations and forward packets between the second and

first SSID to facilitate this limited connection for other STAs.

c. When the first STA detects that another STA 493
has a software (which implements the current method) installed, the first STA allows the other STA a wider access to the Internet.
** End of method **

Fig. 18 details a method for configuring other STAs to directly connect to the AP, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by 492
allowing them to connect to the second SSID.
The limited access includes the ability to request an ability to access the first SSID directly, i.e. not through the second SSID and the first STA.

c. The first STA decrypts and encrypts data packets as needed based on the security parameters of the first and second SSID (or APs), and performs address translations and forward packets between the second and first SSID to facilitate this limited connection for other STAs.

d. Another STA requests an ability for direct access to 494
the first SSID

e. First STA prompts user: To 495
allow this access?

f. Security access parameters to access the first SSID are copied 496

from the first STA to the other STA

g. The other STA can access the first SSID directly 497
** End of method **

Fig. 19 details another method for configuring other STAs to directly connect to the AP, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by 492
allowing them to connect to the second SSID.

c. First STA's user can view a list of 498
connected STAs and can choose to allow access directly through the first SSID
to a chosen other STA

d. Security access parameters to access the first SSID are copied 496
from the first STA to the other STA

e. The other STA can access the first SSID directly 497
** End of method **

Fig. 20 details yet another method for configuring other STAs to directly connect to the AP, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by allowing them to connect to the second SSID. 492

c. Security access parameters to access the first SSID are copied to the other STA 496

d. The other STA can access the first SSID directly 497

** End of method **

Preventing Exhaustion of Resources at the AP

As discussed in the "Background" section, each AP has a limited number of Association IDs (AID) and usually, even a smaller pool of IP addresses (available through DHCP). Once this number of resources is exhausted, the AP might not be able to serve new STAs. A situation where IP addresses are exhausted can happen very quickly: for example, consider an AP in a very busy location, where there are many STAs that connect to the AP only for a short period of time. Each STA performs the connection process and obtains an IP address using DHCP, but as it disconnects it might not release the IP address.

The pool of IP addresses in an unmanaged AP is usually limited to about 200 addresses, with many consumer APs supporting only tens of addresses. A device is assigned the IP address for a given period of time (known as the lease time). Many times, the lease time is set in a magnitude of days (although the granularity is seconds), and in many other instances the lease time is set to a magnitude of hours. In such a situation the pool of IP addresses runs empty very fast.

However, in this disclosure for fast handovers, GN 21 keeps a pool of MAC addresses with associated IP address. Just before a STA enters the AP, GN 21 can send it a MAC address and an IP address that are already associated with

the AP. Therefore, the STA can connect even if the AP has no resources left for new STAs. Combined with the above disclosure that allows several STAs to share the same MAC address and IP address, an AP can serve more APs than its IP resources, even above its limit on the number of associated STAs.

Saving Battery Power by Reducing Location Updates

A novel disclosure of this invention is a method to reduce the number of location updates that are needed in WiFi, when a STA is idle. A location update is the process in which a STA informs an entity in the network of the current location of the STA (the notification can take many forms, including opening a TCP connection, or sending UDP packets). In prior art for WiFi networks (with for example mobile IP, or SIP - Session Initiation Protocol), a location update is required whenever the IP address of the STA changes (for example, when moving between APs of different subnets) - even if the STA is idle.

The novel method allows defining a location area for WiFi, such that a STA needs to perform location update only when it moves between APs that belong to different location areas, but does not need to perform location update when it moves between APs of the same location area as long as it's idle.

We assume that the APs are divided into location areas, and for each location area there is a node in the network that is in charge of this location area. For example, assume GN 21 is in charge of a location area composed of AP 31, AP 32, and AP 33.
How does a STA know which AP belongs to the location area- Either GN 21 gives it a list of all the APs that belong to the location area, or GN 21 transmits a pseudo-beacon in each AP.

A pseudo-beacon is a novel disclosure of this invention. It is a message that GN 21 can periodically transmit in each AP. While some APs might permit a remote node to transmit a message in the AP, other APs might not allow it. In

the novel method, a certain MAC address, IP address, and possibly port are allocated in each AP for the purpose of pseudo-beacon transmission. GN 21 asks some STA to open a connection using these resources to GN 21, and GN 21 sends the pseudo-beacon messages using this transmission. Each pseudo-beacon contains the parameters needed to listen to the pseudo-beacons in the adjacent APs. A STA that lacks these parameters can contact GN 21 and receive them.

From that moment on, the STA can move between APs in the same location area, and receive the parameters that are needed to listen to the pseudo-beacon from other pseudo beacons. For example, assume that STA 11 is located in AP 31 and is moving to AP 32. STA 11 listens to the pseudo-beacon at AP 31, and from the pseudo-beacon learns the parameters that are needed to listen to the pseudo-beacon of AP 32. Thus, STA 11 can move to AP 32 without any transmission.

Which STAs of the stations in AP 31 should acknowledge the pseudo-beacon- Preferably, none. However, some firewalls require minimum rate of outgoing packets to maintain an open connection. In such a case, once in a while GN 21 sends on the pseudo-beacon a message that asks any station to send an acknowledgement with some probability p. The probability that GN 21 states should be accommodated to the expected number of stations in AP 31 (GN 21 might not exactly know how many STAs are in the AP). If no STA acknowledges the pseudo-beacon for over the needed time, and the timeout of firewalls stop the incoming messages, then no pseudo-beacons are transmitted. In this case, a roaming STA will contact GN 21 after a certain period of time of probing for the pseudo-beacon has passed (and no pseudo-beacon is seen). GN 21 can request the STA to reopen the connection for the pseudo-beacon transmission.

If the STA is in a session with TN 41 with many packets received (e.g., above a certain threshold), it is considered non-idle (which we also refer to as "In conversation") and is treated as described above in "Fast handover".

However, assume that STA 11 is in idle mode (e.g., incoming packets below a threshold), it can move between APs of the same location area without performing location update. When a node TN 41 wishes to send data to STA 11, STA 11 should change its state from idle to in conversation. TN 41 contacts GN 21 (TN 41 might be forwarded to GN 21 through a system such as dynamic DNS (Directory Name Service) or another method, such as a Distributed Hash Table - DHT, or a peer-to-peer network).

GN 21 sends a paging message for STA 11 on the pseudo-beacon of all the APs in the location area. As STA 11 listens to one of the pseudo-beacons, STA 11 will receive the paging message. Then, STA 11 responds preferably to GN 21 (or to TN 41, depending on what is written in the paging message) by initiating an outgoing connection as described below. It should be noted that GN 21 can first page for STA 11 in the APs that have a higher chance covering STA 11, and the paging can repeat several times until STA 11 replies.

When a STA is required to initiate an outgoing connection it can use a resource (MAC, IP, or TCP/UDP with port, user/password) that is listed as available on the pseudo-beacon or on the paging message, or it can request its own resources from the AP. If two (or more) STAs use the same resources for a connection at the same time, GN 21 will detect it, and in the acknowledge message (or second message of the TCP handshake) will announce the identity of the STA that it answers to. The other STA is required to initiate an outgoing connection again. Once a connection with GN 21 is established, GN 21 can allocate resources to the STA such that it moves to be in conversation status. One of the resources that are allocated is GN 21 attention to accompany the STA as it might need to perform handover to another AP.

It should be noted that the location areas can overlap, meaning a single AP can belong to more than one location area. Upon the policy of the network, STA 11 might be required to perform location update when it reaches such a APs, or it may just give helpful information. If possible, a STA might prefer

to park on an AP that is within the same location area as its current AP, such that a location update is avoided.

It should also be noted that there is a tradeoff between the overhead that is spent during paging and establishing the connection, and the overhead that is being spent to keep a steady connection for each AP. The optimal point on the tradeoff depends on the rate that the AP switches APs as well as on the number of packets it receives and sends.

Easy Configuration of STA

When purchasing a new STA, it is required to configure the STA with the security settings of the existing network (in case the network is secure). If the network is not secure, the new owner usually only needs to select his network from the list of available networks that is received by the wireless network card.

Configuring the security might be a tedious job, as the security (authentication/encryption) code might be very long as known in the art, which the user might need to punch in. A novel solution for easy configuration is disclosed. Unlike previous solutions, the novel method does not require changing the existing AP of the customer. In one embodiment, software is run on a personal computer of the user (that is already configured to access the WiFi). Then, the software establishes a secure channel with the STA, and copies the security information from the personal computer to the STA. In this way, the STA learns the security parameters.

In another embodiment, the customer first connects the STA by wire to its network (or alternatively, the STA first connects using a connection it establishes through an already connected device, such as a personal computer). As the STA can receive and transmit signals on the wireless network and it is connected to the internet (through the other connection) at the same time, it tries to locate the web configuration of the AP on the wired network (most APs

have a web interface). In most cases, it is an easy job for the STA, as either the STA can locate the AP as it is the default gateway of the wired network, or it can try to find its IP by performing RARP (Reverse Address Resolution Protocol) using the wireless MAC address of the AP (which it can see off-the-air).

If none succeeds the STA can perform exhaustive search on commonly used IP addresses, or on very probable addresses, like all the IP addresses of the same subnet. Once the AP web interface is found, the STA tries to log into the AP. It can guess the default address or find it on a database that can be built on the web, with common default passwords for each manufacturer (the manufacturer and model will be usually sent by the AP during the web login process, or can be found out using the MAC address, which is unique per manufacturer). If the password for the AP cannot be guessed, the user is prompted for its password to complete the log-in. Then, the STA navigates to the security settings page and retrieves the password needed for the wireless network.

In the event that the procedure fails, the user is prompted for the security settings (which would happen without using the above method). For most common users and setups, the method succeeds (and for unsophisticated customers, who do not change the passwords - it succeeds in the majority of the cases). Thus, in the majority of cases, the setup is made much simpler.

Once the STA has access to the setup of the AP, it can (with permission from the user), open holes or forward certain port to some IP address. This IP address and port can serve as way that GN 21 can send and broadcast the pseudo-beacon, without a STA first opening a connection from the AP, and without worrying about timeouts (provided that there are no other firewall between the AP and GN 21). Opened ports can also help during the fast handover, such that TN 41 can directly send packets to the new location without a need for STA 12 to open the connection.

In corporate settings, the company can set a special server which gives the configuration to the phone, over the network.

Gaining Access to Locked Networks

While performing the above easy setup (or at any other time), the user is prompted if he wishes to join a swapping service. The swapping service allows the user to gain access to many locked networks (the locked networks of the other users that joined the swapping service), in return that he allows users to use his network for the purpose of connecting to the internet. If the user agrees, the access parameters to his network (encryption key, MAC address, default gateway, etc.) are securely stored in the network (for example in GN 21, and a backup server). The security information is securely sent directly into the hardware (or network card) of other STAs, when they need to connect using his AP.

As the security parameters are sent directly to the STA's network hardware, it can make sure that the communication that is established is designated outside the user's network, and will not jeopardize the computers on the user's network. Furthermore, GN 21 can monitor the amount of bandwidth that is consumed by visiting users, and to make sure their hardware limits the amount of used bandwidth such that the user does not experience a degradation of quality of his connection. Alternatively, the security information can be sent to the other STAs using other security measures, as known in the art.

In many scenarios it is enough to trust the software that runs on the STA to make sure all communications are targeted outside the user's network, such that it does not jeopardize the computers on the user's network, and limit bandwidth used by the STA.

The secrecy of the security parameters (such as the encryption key) can be cryptographically protected while on transit and storage, as known in the art.

Some APs limit the access of the subscribers by making sure that only specific MAC addresses connect to the network. As our methods as described above allow

to use the same MAC address for several users, this specific MAC address can be used when using the network that restricts the use with specific MAC address.

In case a STA tries to connect to an AP with a captive portal, a special application on the STA is running and performs the authentication and log-in automatically. GN 21 can store typical portal appearances, such that it can guide the STA on how to perform the authentication/log-in process. If the STA comes across a captive portal which is unknown or unexpected, it can locally store the web pages that it received from the captive portal and later transfer them to GN 21. GN 21 accumulates the reports and guides STAs how to log-in to the captive portal in the future. As part of the swapping service, GN 21 can store username/passwords to enable connection through the captive portal automatically.

Special care for data

The above description works well for both voice and data. TN 41 might be a mobile node as well, or a fixed node in the network. The transferred information between STA 11 and GN 21 can be voice, data, or their combination.

In case STA 11 wishes to communicate with a node that is not aware of the novel network, it can do so through a node that is aware of the network. For example, TN 41 can serve as a proxy for STA 11 (in a similar way to mobile IP). The node that is not aware of the network communicates with TN 41. TN 41 forward the information to STA 11. TN 41 can allocate an IP address (perhaps using NAT, or allocate ports using its own IP address) that will serve STA 11.

To balance the communication load, STA 11 can have several network nodes such as TN 41, TN 42 (not shown), etc, to be its proxies in parallel. In fact, the resulting connection between STA 11 and TN 41 can be seen as a layer 2 (MAC) connection, on top of which the communication is performed. In this setup, TN 41 serves as the default gateway of STA 11, and optionally can run a DHCP server and a NAT server.

Executing the Invention over a Peer-to-peer network

Another novel aspect of the above novel methods takes advantage of the fact that the wireless network is local in nature, as the APs are geographically adjacent. The system and method as described in this disclosure allows GN 21 to be responsible over a small geographical area with little interaction with its neighbors. As a result, the methods that are disclosed can be implemented by many small devices forming a peer-to-peer network that implements the methods, without the need to rely heavily on large servers.

Many nodes GN 21, GN 22 (not shown), can each control a group of APs. To make the system grow "automatically", it is possible to give users a "base" that will act as their point of presence in the network. For example, the base can assume the role of TN 41 as a Mobile IP proxy. The base can connect to the wired network at the premises of the customer. Some bases will assume the role of a GN, where the GNs can be managed by either a network control center, or through peer-to-peer protocols.

In early stages of deployment of the system, when there is still a small number of GNs, each GN might need to cover a large number APs. A general server can back-up all information that the GNs hold. To avoid the situation, where a single GN needs to cover a huge number of APs with pseudo-beacons, the system might not use the pseudo-beacon mechanism (although, it should be noted that with moderate computing power and network resources, a GN might be able to cover a few thousands of APs). In the worst case scenario of a peer-to-peer network, there is one base (GN) for each STA, and this GN act as the GN for the APs in the proximity of the STA.

When the STA moves, the coverage area in the responsibility of the GN moves with it. In this case, the GN can fetch information on neighboring APs from

the general server. When GN abandons an AP, it can store the information it gathered about it in the general server, for later use by possibly other GNs. In a system which is not based on many small GNs, a large GN can assume the role of the smaller GNs.

It should be noted that it takes some time to gather the information on the APs (such as timing, default gateways, etc). However, once a single STA passes in an area, it obtains the needed information. This information is later stored in the GNs and general server, for the benefit of all STAs in the future.

If a STA needs to handover into an AP which has no STAs currently in it, it might not have the needed resources pre-allocated (such as an associated MAC address and IP address), and might therefore need to gain it by itself. However, in many cases the STA can obtain resources at one pass in the area, and these resources (such as IP address) will stay for the next pass in the area (which can be hours later).

An Alternate Fast Method for Connecting to an AP - Removing the Assumption on the Existence of STA 12 in the Coverage of the new AP

A possible drawback of the above method of fast handover is that it requires that the pool of resources that GN 21 holds should contain a valid IP address of the AP that STA is handing over to. If the DHCP lease time is long enough, having a valid IP might not be a problem, but on short lease times with only a few STAs roaming it is desirable to perform handovers even if there is no valid IP available in the pool. Unfortunately, a typical execution of the DHCP protocol can take several seconds to complete, which might be too long for a fast handover. Interestingly, we observe that many APs will forward information even if the IP that is being used was not allocated by DHCP.

Therefore, we disclose the following method:
Choose a MAC and associate it with the AP (or use an Associated MAC without an associated IP address), choose a random (but valid) IP address, and use it.
The STA must use the correct default gateway settings of the AP (these settings can be stored in GN 21). If the STA wishes to use DNS, it must have the DNS settings of the AP (which can be received from GN 21), or DNS services are provided through GN 21.

Choosing a valid IP at random results in a very low probability of colliding with another IP address that is used in the AP. Note, however, that the STA still needs to authenticate/log-in through the captive portal in case such portal exists.

Another method that can be used to quickly obtain an IP address, such that the IP address is not already allocated by the DHCP of the AP is disclosed. Most DHCP implementations of AP send an ICMP (Internet Control Message Protocol) Echo Request (ping) before allocating an IP address, to make sure that it is unused. Therefore, STA can begin the DHCP protocol, then, wait for the ICMP echo request that the AP sends, and understand the IP that is going to be allocated to it.

Therefore, a STA can start using the IP address and respond to the ICMP echo request. It can then prematurely terminate the DHCP protocol (as it already got an IP). Alternatively, STA can use the IP address from the ICMP echo request without responding to it, and complete the DHCP process. If the IP address that is allocated during the DHCP is identical to the IP address (vast majority of cases), then STA simply saved time. Otherwise, it can move from the IP address of the ICMP echo request to the IP address that was allocated.

If no connection to GN 21 is available, the default gateway address can be guessed, as in the majority of the cases the default gateway address is one out of only a few addresses. Common addresses are: 192.168.1.1, 192.168.2.1, 10.0.0.1, etc.

Moreover, the default gateway is usually the AP itself. Its MAC address is known (as it is broadcasted in the beacon). Therefore, in most cases it is enough to forward packets to this MAC address (without knowing its IP address).

A STA with a Capability to Connect on Two Channels in Parallel

The present application discloses a STA which has a capability of communicating in two or more channels in parallel (for example, by using two wireless network cards). This capability can enable a STA to be connected to two APs in parallel without the need to implement sophisticated mechanisms that actually simulate this situation. Thus, a STA can connect with future AP while maintaining a connection through its serving APs. Being connected to two or more APs simultaneously allows greater bandwidth by utilizing two connections instead of one, and the performance of soft-handovers, i.e., the STA stays connected through one AP, while disconnecting from the second AP in the process of handover.

Fast uploading of digital camera pictures

Digital cameras might be equipped with WiFi. The owner of such a camera would like to upload his pictures from the camera to a server that stores the pictures on the Internet - the reasons for this may vary from being able to share the photos while on vacation with family members left at home, back up the pictures from the digital camera to the Internet server, or simply because the memory card on the camera is running out of space. A major problem is that to upload the pictures to the Internet may take a very long time, as pictures consume megabytes to store.

Solution: The camera sends the photos to a laptop over WiFi (this connection is very fast), then disconnects and the camera's user may move on. Then, the laptop uploads the pictures to the Internet server (this process can take a long time as it involves uploading a lot of data), but the laptop owner would not feel it as a burden, since the pictures can be uploaded when his Internet connection is not used for other purposes.

Method for uploading data files

In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for fast uploading of information from STAs to the Internet, comprises:

a. a first STA, such as a laptop computer, connects to the Internet;

b. a second STA, such as a camera, wirelessly connects to the first STA, and uploads the information using the fast and direct-wireless connection between the STAs;

c. The first STA temporarily stores the information;

d. The first STA uploads the information to the Internet through its backhaul.

** End of method **

Notes:

1. In the above method, the first STA may include for example a laptop or a personal computer, the second STA may include a digital camera or a digital video camera, and the information may include digital pictures or digital clips.

2. The second STA preferably disconnects from the first STA after completing to upload the information to the first STA, but before the first STA completes the upload of information to the Internet; the first STA completes the upload of information from its temporary storage.

3. An additional step in the above method may include the following:

e. at a later time, the second STA connects to the Internet and verifies that the information was uploaded correctly.

4. The information may be encrypted by the second STA before being transmitted.

It will be recognized that the foregoing is but one example of an apparatus and method within the scope of the present invention and that various modifications will occur to those skilled in the art upon reading the disclosure set forth hereinbefore.

CLAIMS

1. A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising:

a. wirelessly connecting a first STA to the Internet through a first AP with a first SSID;

b. remaining connected to the first Access Point (AP), the first STA creates a software-based wireless AP with a second SSID for wirelessly connecting other STAs to the Internet through the first STA.

2. The method for providing a wireless Internet connections to STAs according to claim 1, further including the step of:

c. a software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein.

3. The method for providing a wireless Internet connection to STAs according to claim 1 or 2, wherein each STA can be a laptop computer, PDA, wireless camera, wireless phone or a wireless device.

4. The method for providing a wireless Internet connection to STAs according to claim 1, wherein the first STA includes means for simultaneously connecting to the first AP and for opening the second AP, and means for transferring Internet packets between the first and second APs, while decrypting and encrypting the packets as needed based on the security parameters of the first and second AP, in addition to any communications with the Internet as required by a user of that STA.

5. The method for providing a wireless Internet connection to STAs according to claim 1, wherein activating, in the first STA, a single wireless card so as to operate in two modes at the same time, a STA mode and an AP mode.

6. The method for providing a wireless Internet connection to STAs according to claim 1, wherein the first AP does not provide wide, unconditional access to all.

7. The method for providing a wireless Internet connection to STAs according to claim 6, wherein a remote database may be accessed to determine if a STA without the software module should be allowed access, and how wide that access should be.

8. The method for providing a wireless Internet connection to STAs according to claim 1, 2, 3, 4 or 5, wherein the software module, upon detecting that the other STA does not have the software module therein, allows to install and activate the software module in the other STA and then provides wide access to the other STA.

9. The method for providing a wireless Internet connection to STAs according to claim 6, wherein the software module, upon detecting that the other STA does not have the software module therein:

c1. presents to the user of the other STA a message indicating that wide Internet access is possible upon loading a copy of the software module;

c2. waiting for that user's permission;

c3. after receiving that user's permission, the other STA. STA downloads, installs and activates a copy of the software module to gain a wide Internet access to the other STA.

10. The method for providing a wireless Internet connection to STAs according to claim 1, 2, 3, 4 or 5 wherein the step of connecting another STA comprises:

c1. the first STA connects the other STA, while limiting the set of Internet addresses and/or Internet sites the other STA can access, and wherein the accessible sites include a special web site from which the other STA can download the software module;

c2. the other STA downloads, installs and activates the software module therein;

c3. the first STA, upon detecting the installed and active software module in the other STA, then removes the limitations on the set of Internet addresses

and/or Internet sites the other STA can access.

11. The method for providing a wireless Internet connection to STAs according to claim 1, 2, 3, 4 or 5 wherein the step of connecting another STA comprises:

c1. the first STA connects the other STA to the Internet, while limiting the set of Internet addresses and/or Internet sites the other STA can access, and wherein the accessible sites include a special web site from which the other STA can download the software module;

c2. if so instructed by the user of the other STA, the other STA downloads, installs and activates the software module therein;

c3. the first STA, upon detecting the installed and active software module in the other STA, then removes the limitations on the set of Internet addresses and/or Internet sites the other STA can access.

12. The method for providing a wireless Internet connection to STAs according to claim 10 or 11 wherein the first STA, upon detecting the installed and active software module in the other STA, then removes part of the limitations on the set of Internet addresses and/or Internet sites the other STA can access, so as to keep some sites and/or addresses private to the first STA.

13. A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising:

a. activate in a first STA a software module for connecting with other STAs and to the Internet;

b. when required by the user to connect to the Internet and upon connecting with another STA which is already connected to the Internet and has a copy of the software module active therein, signal to the other STA that the first STA has a copy of the software module, and request to connect to the Internet through the other STA;

c. connect the first STA to the Internet through the second STA;

d. the software module in the first STA opens a second, software-based

wireless Access Point (AP) at the first STA for connecting other STAs to the Internet through the first STA, and wherein the software module only provides wide Internet access to other STAs which each has a copy of the software module installed and active therein.

14. A method for providing a wireless Internet connection to WiFi-enabled devices (STAs), comprising:

a. activate in a first STA a software module for connecting with other STAs and to the Internet;

b. connect the first STA to the Internet and open a second, software-based wireless AP for connecting other STAs to the Internet through the first STA;

c. when another STA connects with the first STA through the second AP and requests access to the Internet:

1) check whether the other STA has a copy of the software module installed and active therein;

2) if the answer is positive, then connect the other STA to the Internet;

3) if the answer is negative, then support the other STA in loading, installing and activating a copy of the software module therein and, after the software module is active in the second STA, provide wide Internet access to the other STA.

15. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein each STA may include a Portable computer, a Laptop, a PDA or a wireless phone.

16. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein each STA includes means for simultaneously connecting to the first AP and for opening the second AP, and means for transferring Internet packets between the first and second APs, in addition to any communications with the Internet as require by a user of that STA.

17. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein activating, in the first STA, a wireless card so as

to operate in two modes at the same time, a STA mode and an AP mode.

18. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein a STA connects to the Internet through two or more STAs simultaneously.

19. The method for providing a wireless Internet connection to STAs according to claim 18, wherein a STA repeats the connecting stage two or more times to connect to the Internet through two or more APs simultaneously.

20. The method for providing a wireless Internet connection to STAs according to claim 18 or 19, wherein a STA performs a fast handover by continuously searching for new APs to connect therethrough and connecting to newly available APs as older APs may become inaccessible.

21. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein the first STA prevents other STAs from accessing its inner network by limiting the access rights of the other STAs.

22. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein the other STA prevents the first STA from eavesdropping on its communications by tunneling its sensitive traffic to a trusted network site, and accesses the Internet through its tunnel to the trusted network site which acts as a proxy for it.

23. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein preventing STAs from using other STAs for their primary network connection for a long period of time, by detecting that a STA is connected to the Internet through the same STA for a long period of time, and disconnecting that STA.

24. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein preventing STAs from using other STAs for their primary network connection for a long period of time, by detecting

that a STA is connected to the Internet through the same STA for a long period of time, and disconnecting that STA if it refuses to pay for the continued use of that connection.

25. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for configuring STAs to connect to a wireless network, comprising:

a. activating a software module in first STA, which is already configured to access an Access Point (AP);

b. the software module copies the security information from the personal computer to another STA, thus setting the security parameters for the other STA as to allow access to the AP.

26. The method for configuring STAs according to claim 25, further including an authentication phase in which the other STA is authenticated by the software module or by a remote server before copying the security information.

27. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for configuring STAs to connect to a wireless network, comprising:

a. a customer first connects a STA by wire to its network, (or the STA first connects using a connection it establishes through an already connected device, such as a personal computer or laptop);

b. a software on the STA copies to the STA the security information gained through the wired connection, thus setting the security parameters for the STA.

28. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for performing fast handover for a first STA, from being connected to a first Access Point (AP) to a second AP, comprising:

a. a first STA communicates with a Termination Node (TN) and is in contact with a

Governing Node (GN), wherein GN is non-exclusively responsible for the mobility management in a certain geographic area for a given time and wherein the GN is in contact with another STA in the coverage area of the second AP;

b. the other STA receives instructions from GN to impersonate the first STA towards the second AP and to complete a connection process with the second AP on behalf of the first STA;

c. the other STA communicates the connection parameters to the GN and, once the parameters are communicated, the other STA returns to its real identity;

d. the GN communicates the parameters to the first STA, thereby eliminating the need for the first STA to perform the connection process itself;

e. when the first STA reaches the perimeter of the coverage of the first AP, it can immediately use the new parameters and continue communications with the second AP, without any delay.

29. The fast handover method according to claim 28, wherein the first STA alerts the TN before the handover, so it can start sending information packets to the new location.

30. The fast handover method according to claim 28, wherein the TN sends information in parallel to the old and the new location, and ceases transmitting to the old location once the handover is complete.

31. The fast handover method according to claim 28, wherein the other STA further opens a Transmission Control Protocol (TCP) as used in the Internet or sends a User Datagram Protocol (UDP) packet on behalf of the first STA, if required.

32. The fast handover method according to claim 28, wherein the connection process performed by the other STA on behalf of the first STA includes authentication, association, receiving an IP address and performing any second authentication/log-in procedure.

33. The fast handover method according to claim 28, wherein the connection process performed by the other STA on behalf of the first STA further includes

opening connections or "punching holes" in the firewall.

34. The fast handover method according to claim 28, wherein the connection waits for the first STA until it reaches the second AP and, if there is a timeout on these connections (either due to protocol, or due to firewalls), the other STA or yet other bypassing STAs can send and receive -keep-alive-messages on behalf of the first STA.

35. The fast handover method according to claim 34, wherein the timeout for each AP is stored in the GN for future use.

36. The fast handover method according to claim 34, wherein the value of the timeout is transmitted by the GN to the first STA.

37. The first handover method according to claim 34, wherein the connections parameters are not limited in use for the first STA, but are also available for the use of other STAs.

38. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for fast uploading of information from STAs to the Internet, comprising:
a. a first STA connects to the Internet;
b. a second STA wirelessly connects to the first STA, and uploads the information using the fast and direct-wireless connection between the STAs;
c. The first STA temporarily stores the information;
d. The first STA uploads the information to the Internet through its backhaul.

39. The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the first STA includes a laptop or a personal computer, the second STA includes a digital camera or a digital video camera, and the information includes digital pictures or digital clips.

40. The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the second STA disconnects from the first STA after completing to upload the information to the first STA, but before the first STA completes the upload of information to the Internet; the first STA completes the upload of information from its temporary storage.

41. The method for fast uploading of information from STAs to the Internet according to Claim 38, further including the step:

e. at a later time, the second STA connects to the Internet and verifies that the information was uploaded correctly.

42. The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the information is encrypted by the second STA before being transmitted.

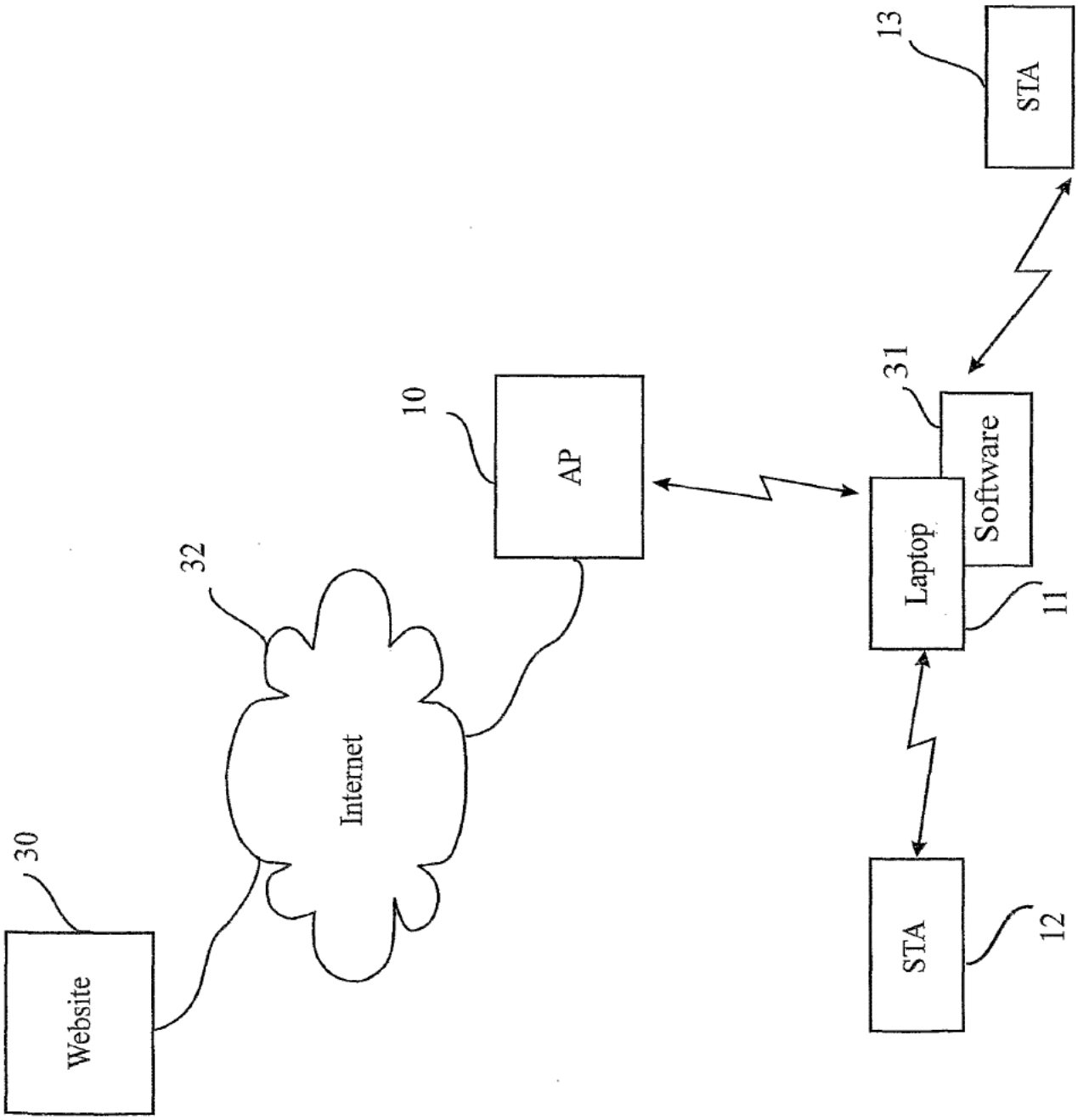

Website
30
Internet
32
AP
10
Laptop
Software
31
11
STA
12
STA
13

FIG. 1

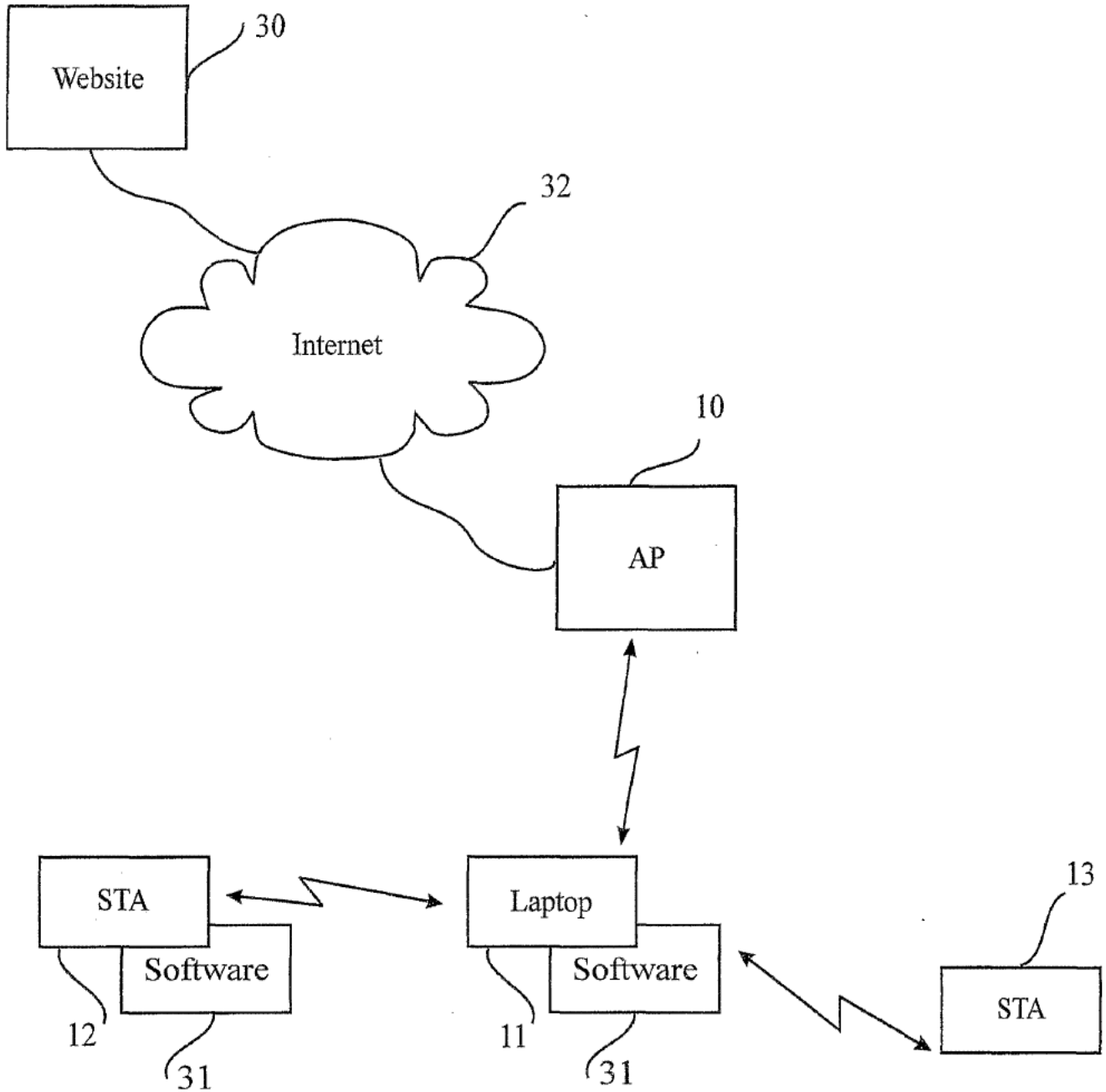

Website
30
32
Internet
10
AP
STA
Software
12
31
Laptop
Software
11
31
13
STA

FIG. 2

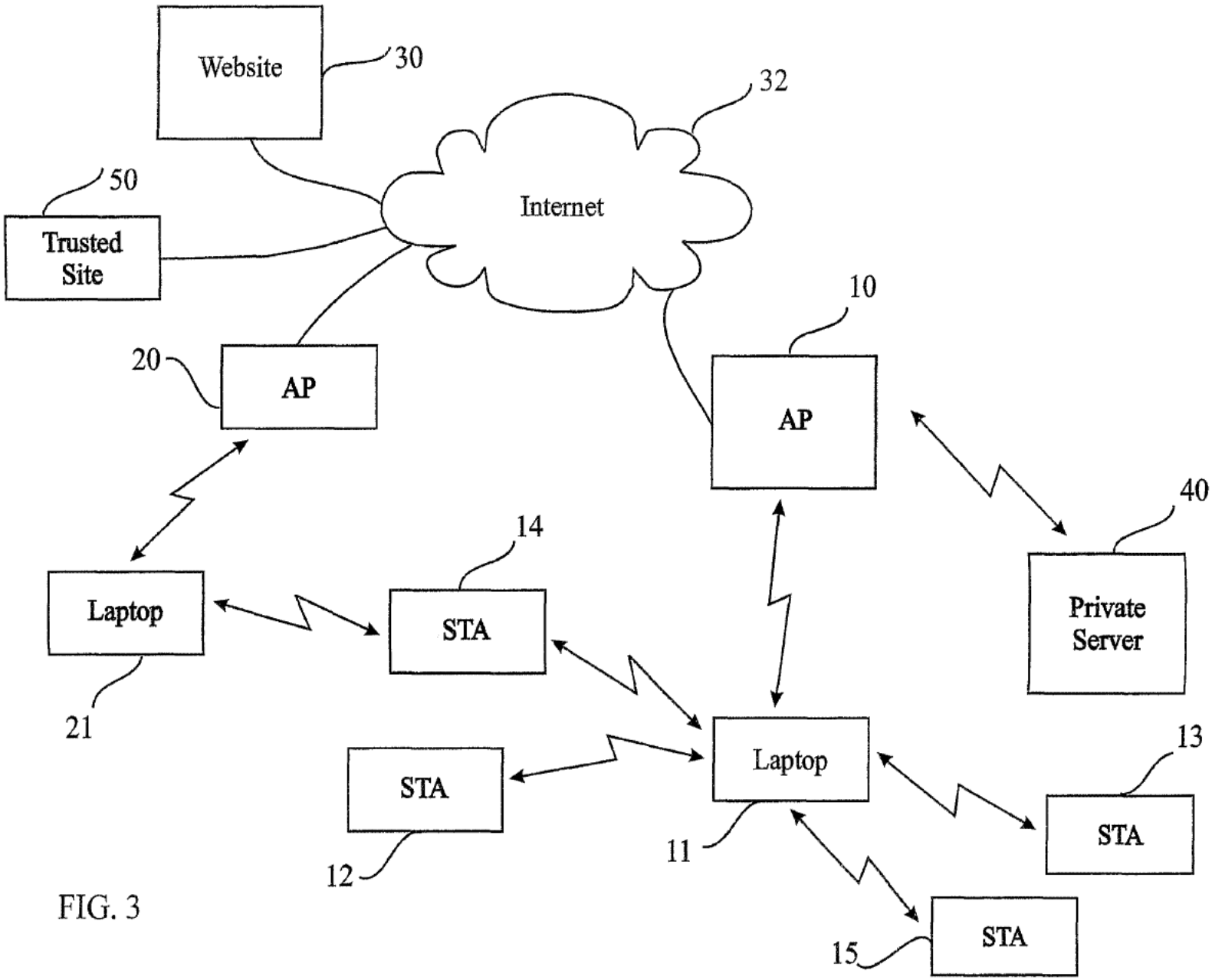

Website
30
32
Internet
50
Trusted Site
10
20
AP
AP
40
14
Laptop
STA
Private Server
21
13
STA
Laptop
STA
11
12
15
STA

FIG. 3

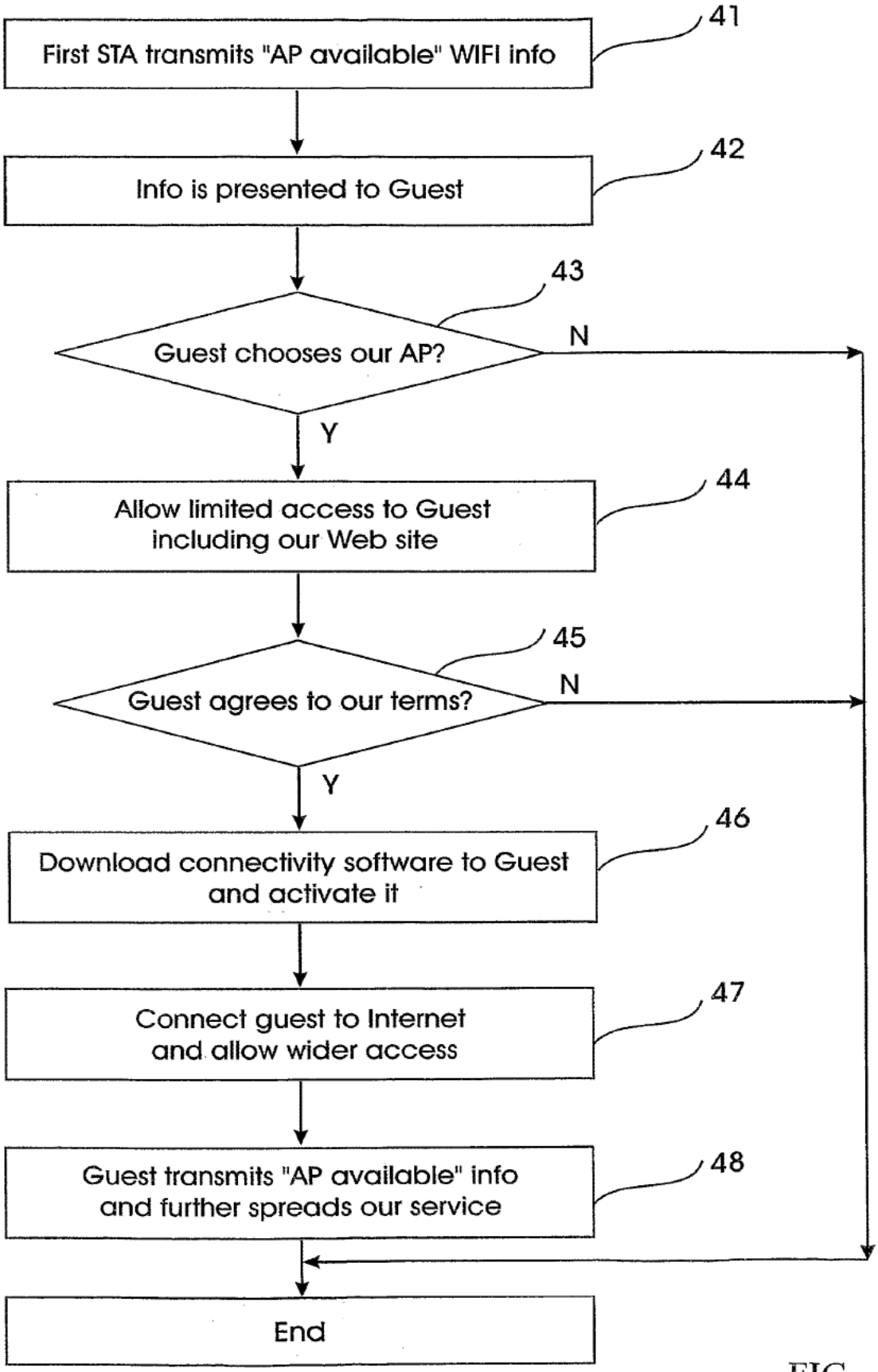

First STA transmits "AP available" WIFI info
41
Info is presented to Guest
42
Guest chooses our AP?
43
N
Y
Allow limited access to Guest including our Web site
44
Guest agrees to our terms?
45
N
Y
Download connectivity software to Guest and activate it
46
Connect guest to Internet and allow wider access
47
Guest transmits "AP available" info and further spreads our service
48
End

FIG. 4

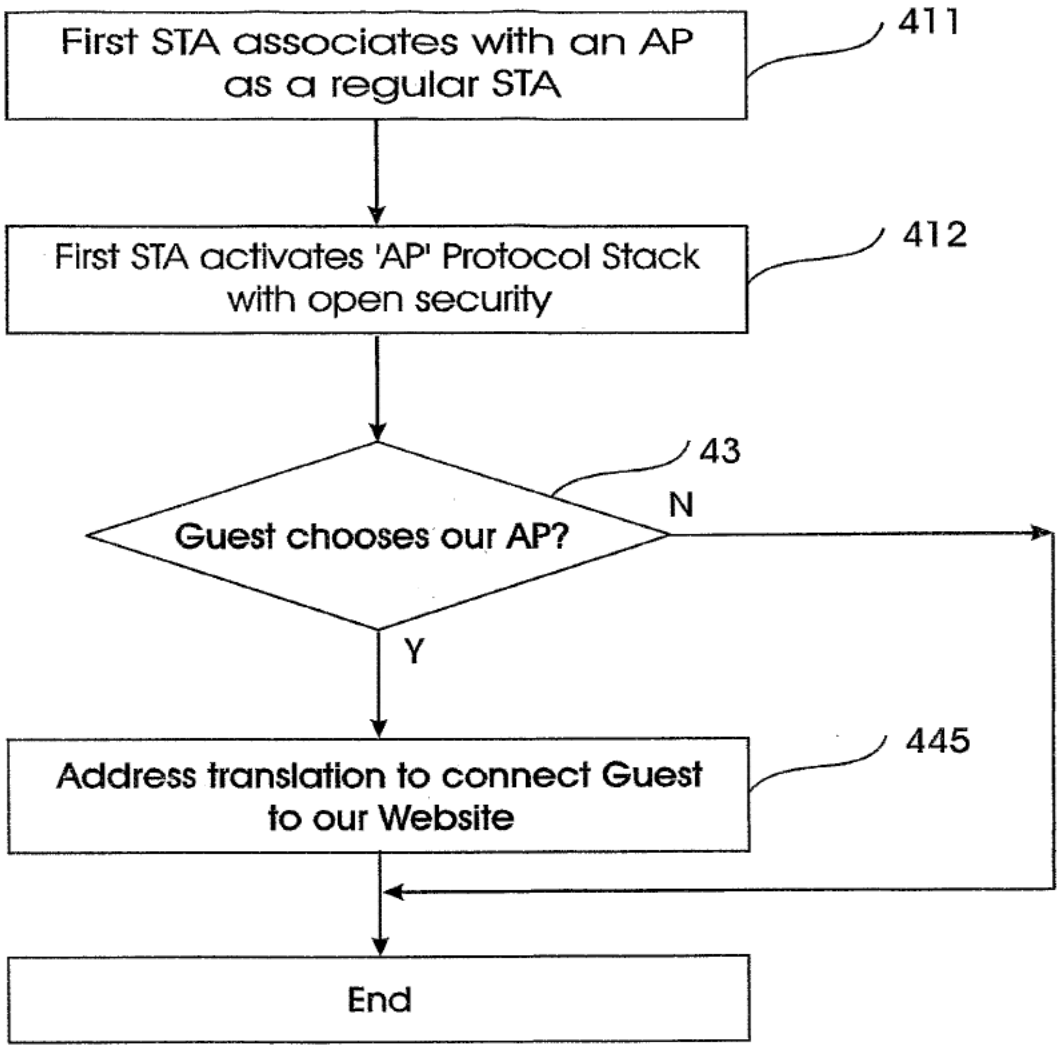

First STA associates with an AP as a regular STA
411
First STA activates 'AP' Protocol Stack with open security
412
Guest chooses our AP?
43
N
Y
Address translation to connect Guest to our Website
445
End

FIG. 5

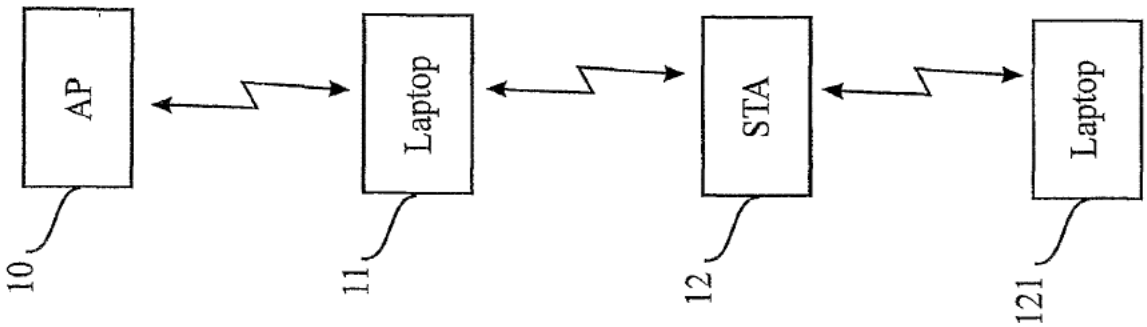


FIG. 6C

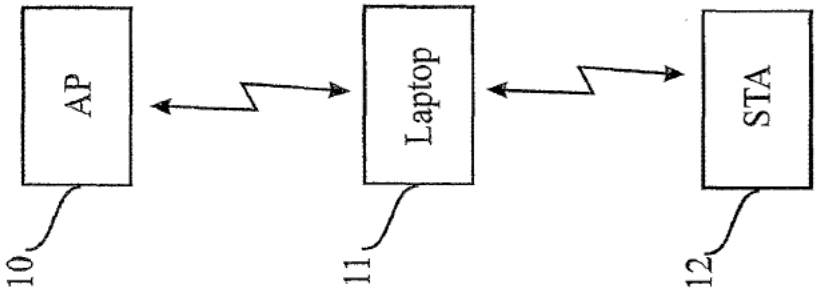


FIG. 6B

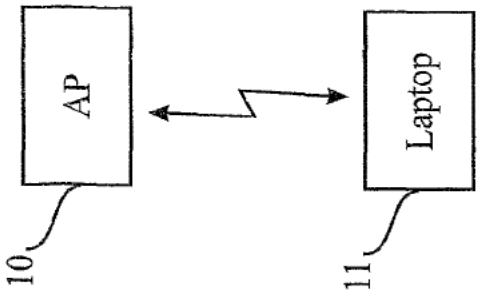


FIG. 6A

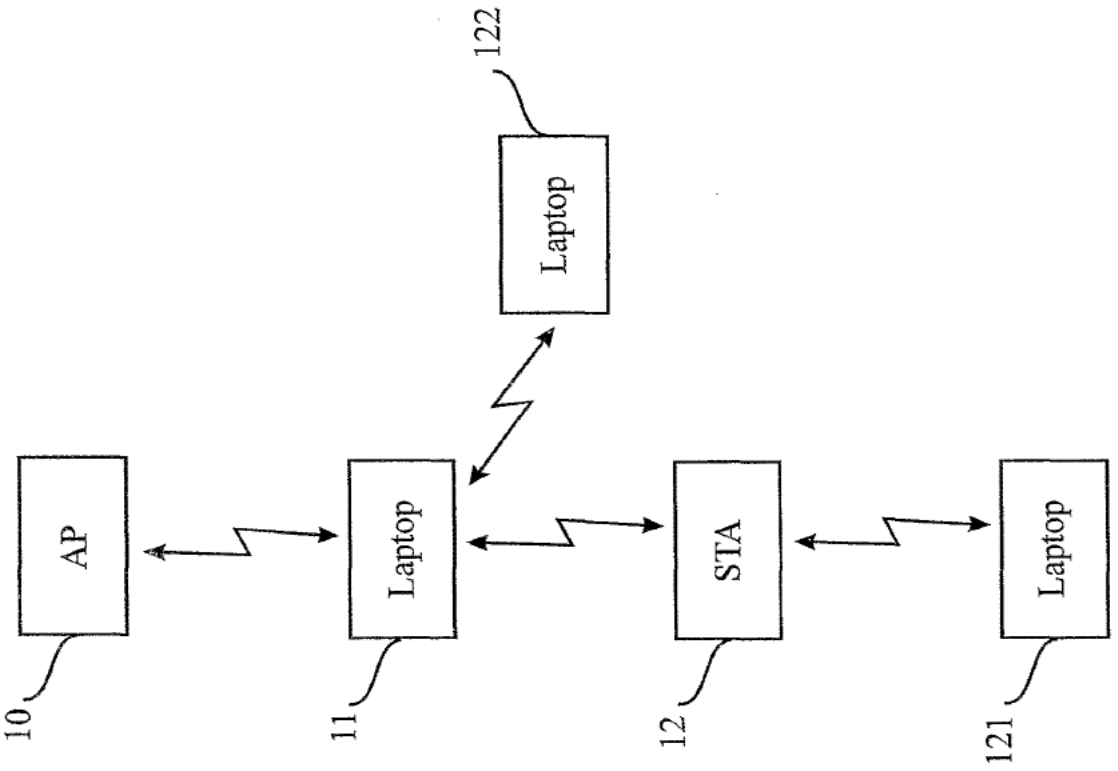


FIG. 6D

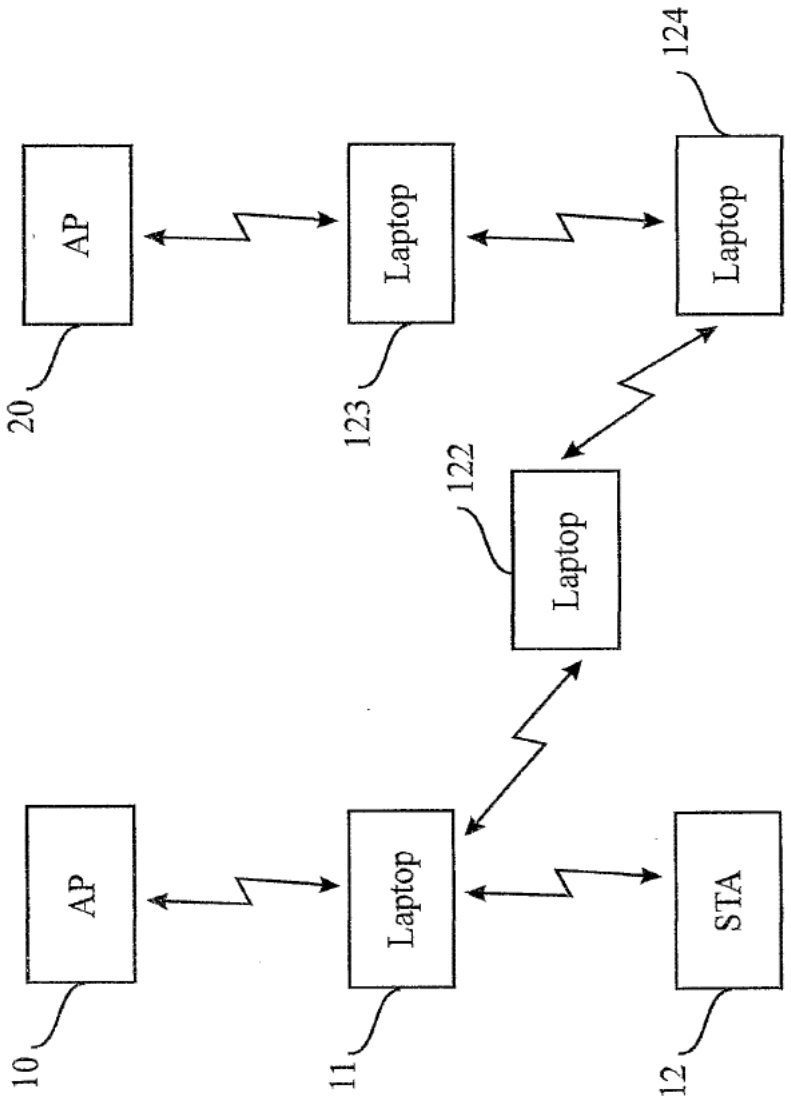


FIG. 6E

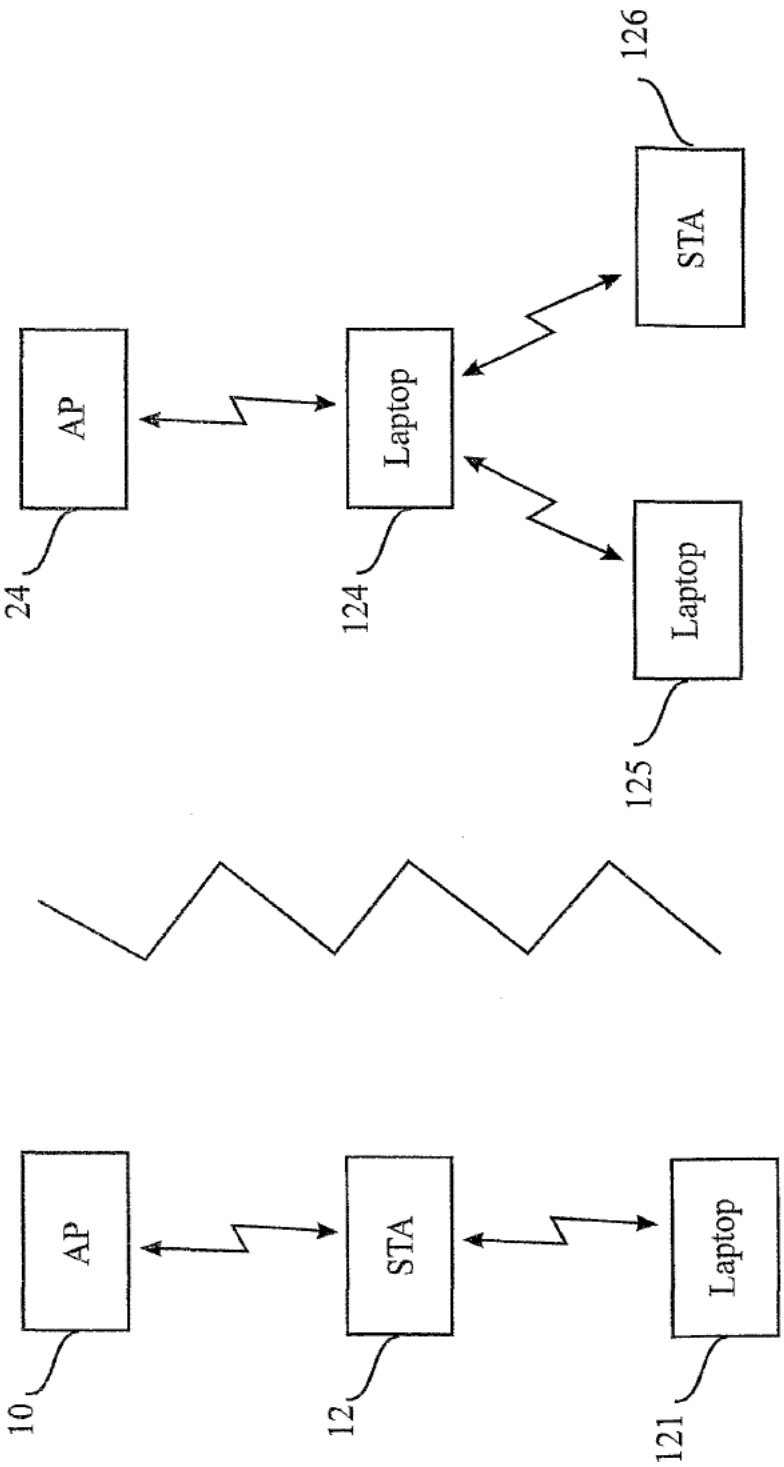


FIG. 6F

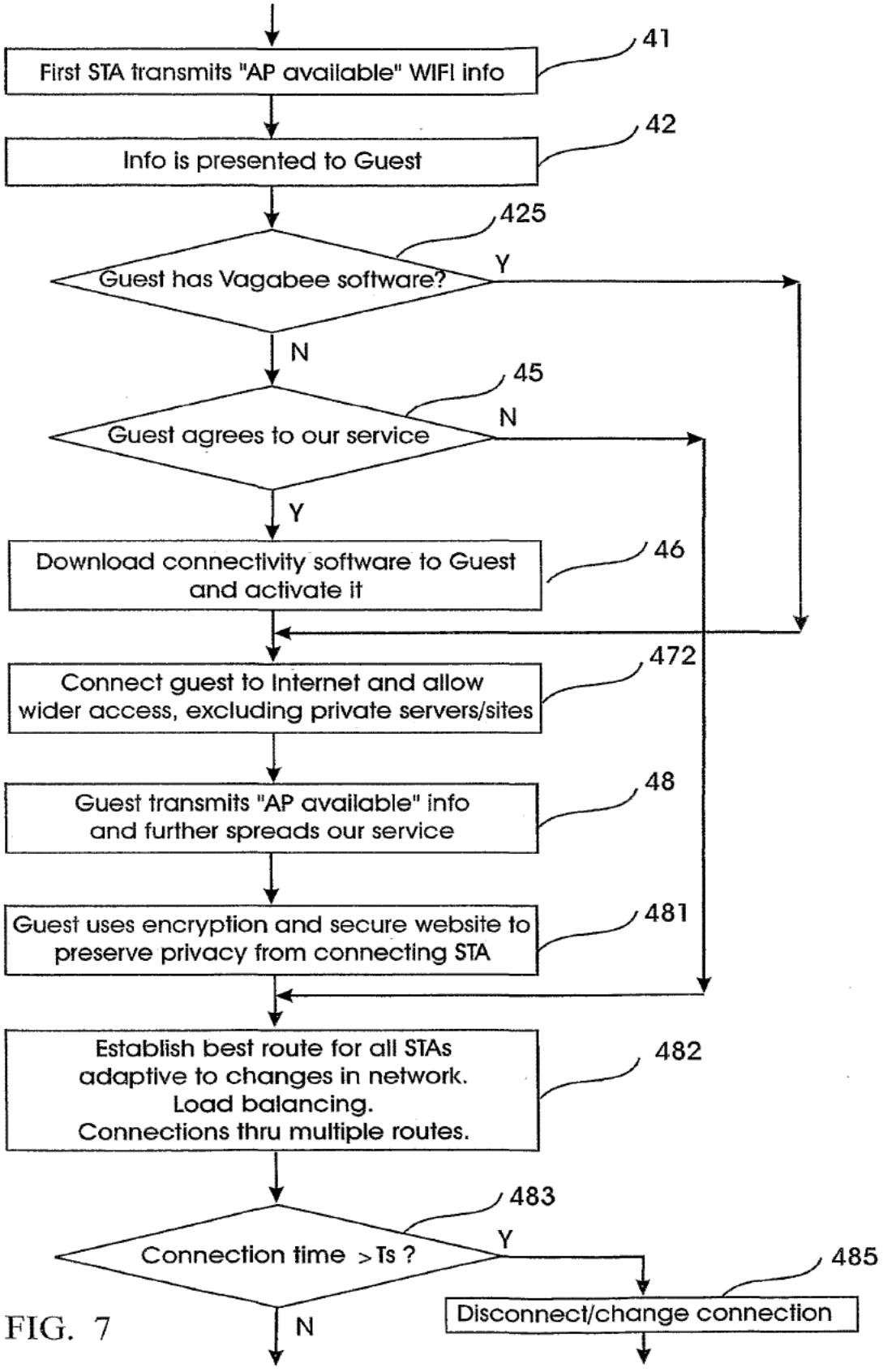

First STA transmits "AP available" WIFI info
41
Info is presented to Guest
42
Guest has Vagabee software?
425
Y
N
Guest agrees to our service
45
N
Y
Download connectivity software to Guest and activate it
46
Connect guest to Internet and allow wider access, excluding private servers/sites
472
Guest transmits "AP available" info and further spreads our service
48
Guest uses encryption and secure website to preserve privacy from connecting STA
481
Establish best route for all STAs adaptive to changes in network. Load balancing. Connections thru multiple routes.
482
Connection time >Ts ?
483
Y
N
Disconnect/change connection
485

FIG. 7

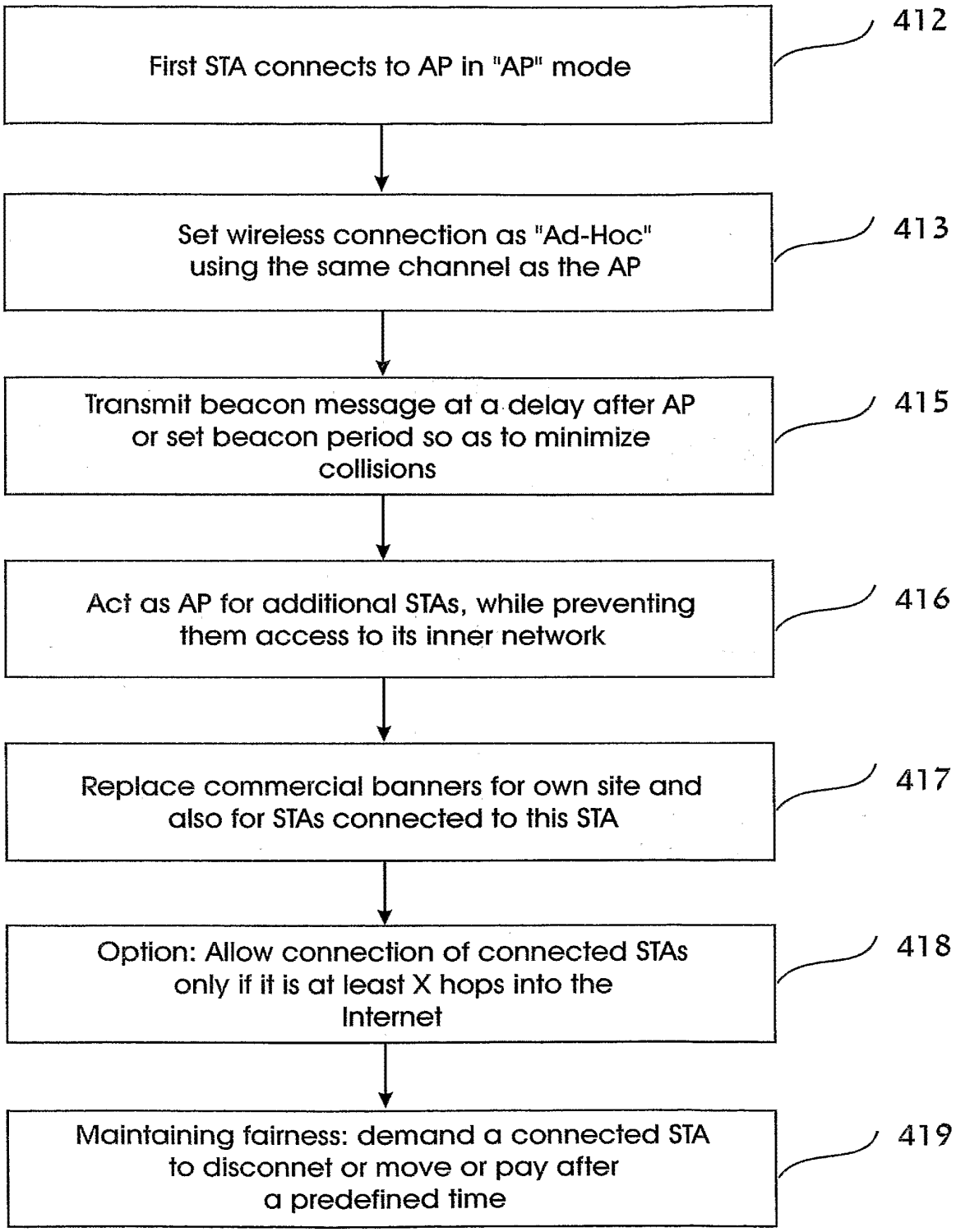

First STA connects to AP in "AP" mode
412
Set wireless connection as "Ad-Hoc" using the same channel as the AP
413
Transmit beacon message at a delay after AP or set beacon period so as to minimize collisions
415
Act as AP for additional STAs, while preventing them access to its inner network
416
Replace commercial banners for own site and also for STAs connected to this STA
417
Option: Allow connection of connected STAs only if it is at least X hops into the Internet
418
Maintaining fairness: demand a connected STA to disconnet or move or pay after a predefined time
419

FIG. 8

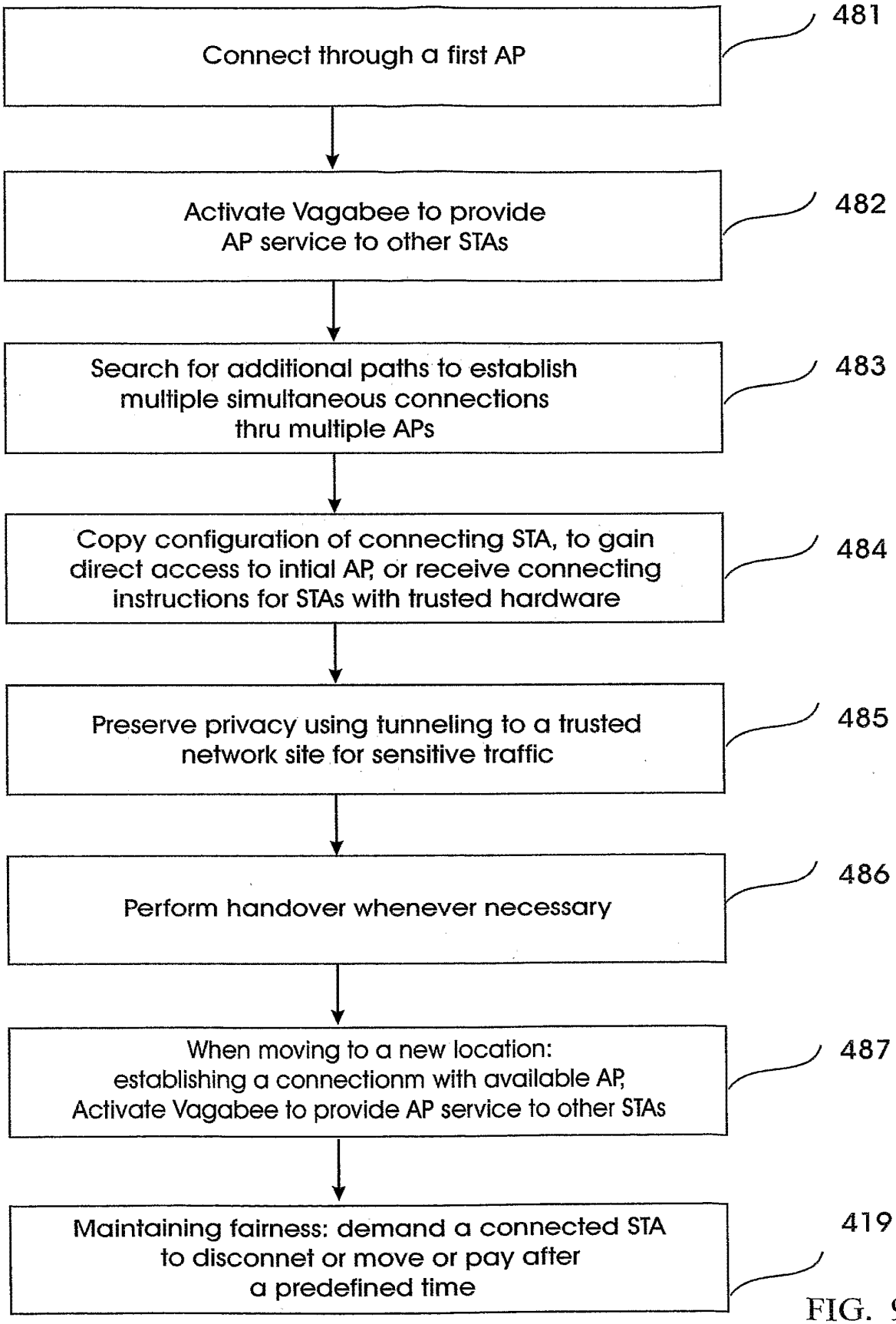

Connect through a first AP
481
Activate Vagabee to provide AP service to other STAs
482
Search for additional paths to establish multiple simultaneous connections thru multiple APs
483
Copy configuration of connecting STA, to gain direct access to intial AP, or receive connecting instructions for STAs with trusted hardware
484
Preserve privacy using tunneling to a trusted network site for sensitive traffic
485
Perform handover whenever necessary
486
When moving to a new location: establishing a connectionm with available AP, Activate Vagabee to provide AP service to other STAs
487
Maintaining fairness: demand a connected STA to disconnet or move or pay after a predefined time
419

FIG. 9

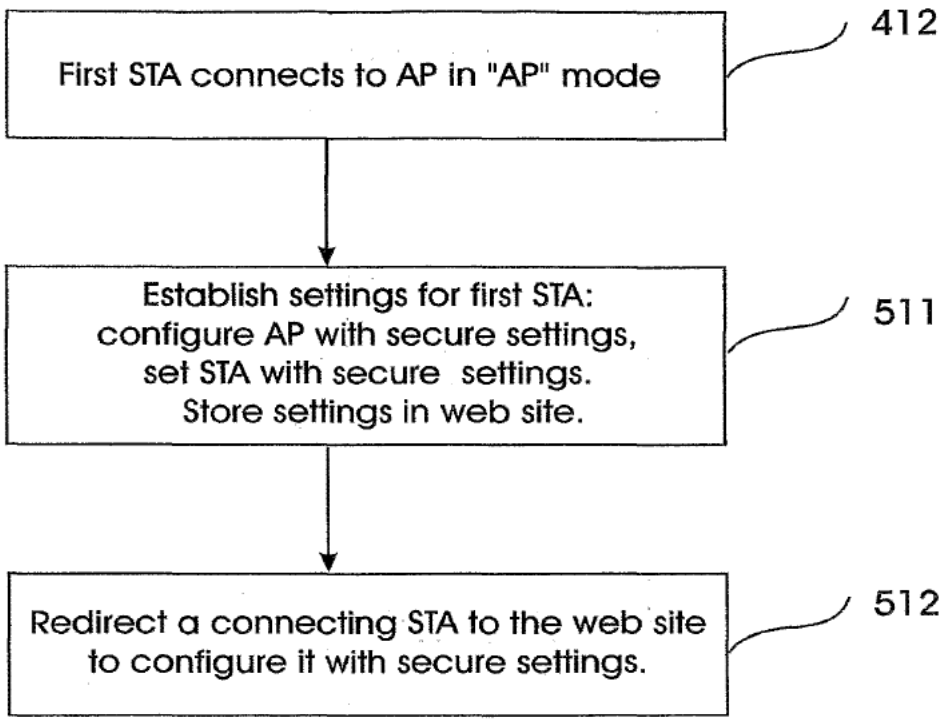

First STA connects to AP in "AP" mode
412
Establish settings for first STA:
configure AP with secure settings,
set STA with secure settings.
Store settings in web site.
511
Redirect a connecting STA to the web site
to configure it with secure settings.
512

FIG. 10

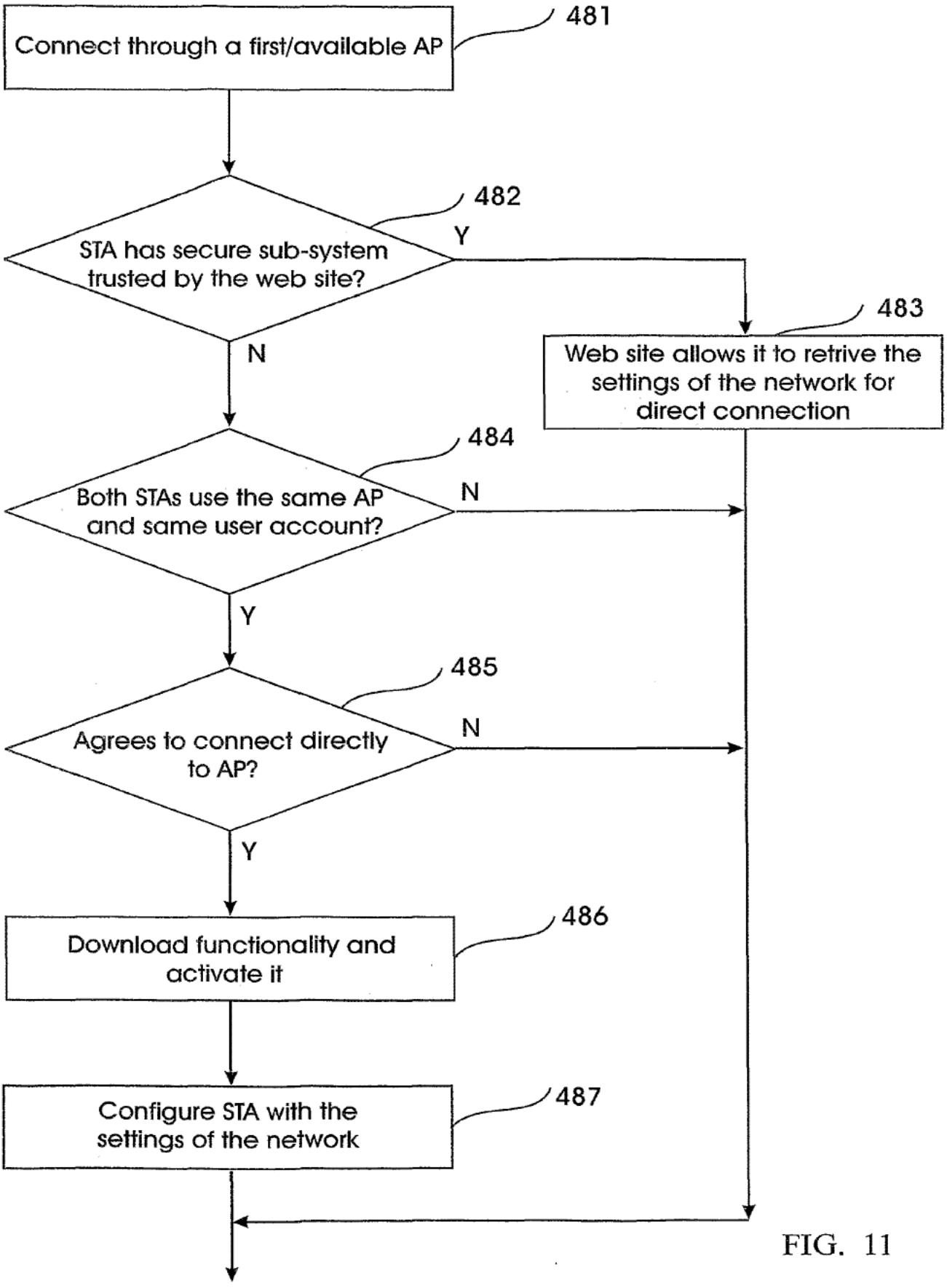

Connect through a first/available AP
481
STA has secure sub-system trusted by the web site?
482
Y
N
Web site allows it to retrive the settings of the network for direct connection
483
Both STAs use the same AP and same user account?
484
N
Y
Agrees to connect directly to AP?
485
N
Y
Download functionality and activate it
486
Configure STA with the settings of the network
487

FIG. 11

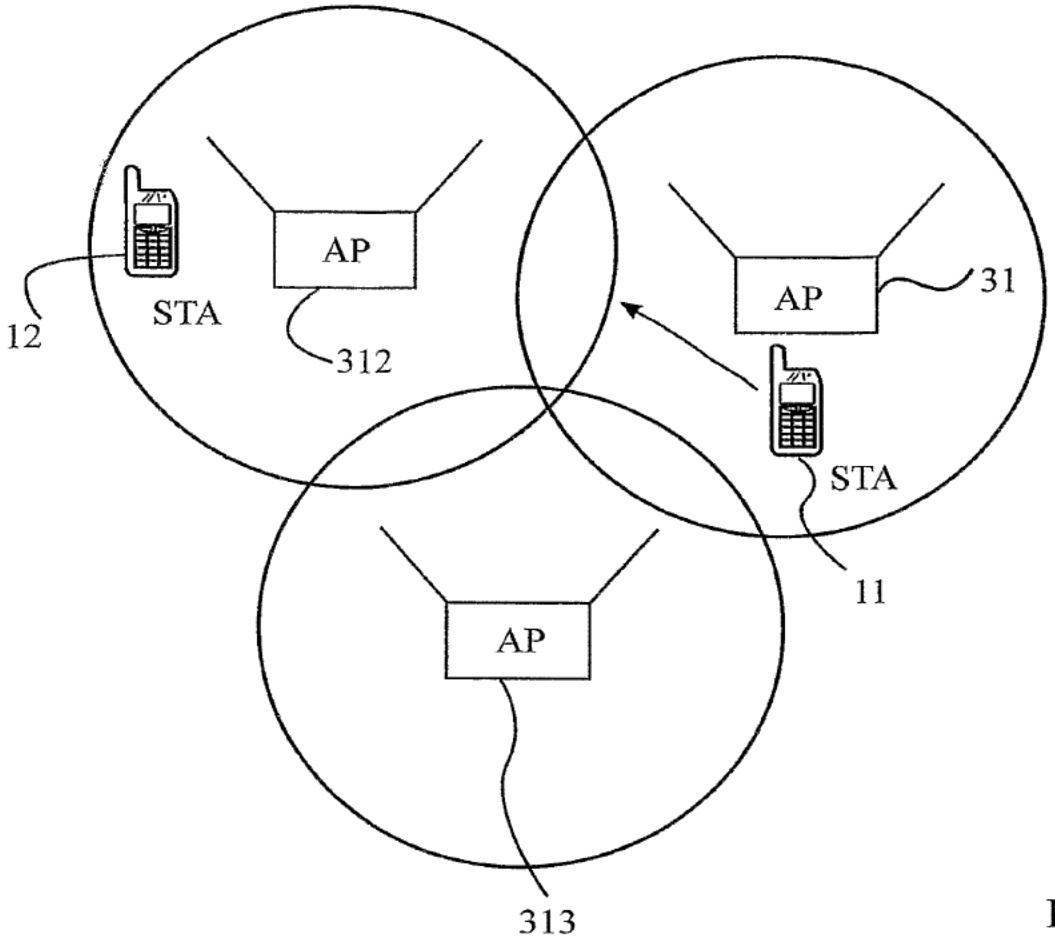

AP
STA
12
312
AP
31
STA
11
AP
313

FIG. 12

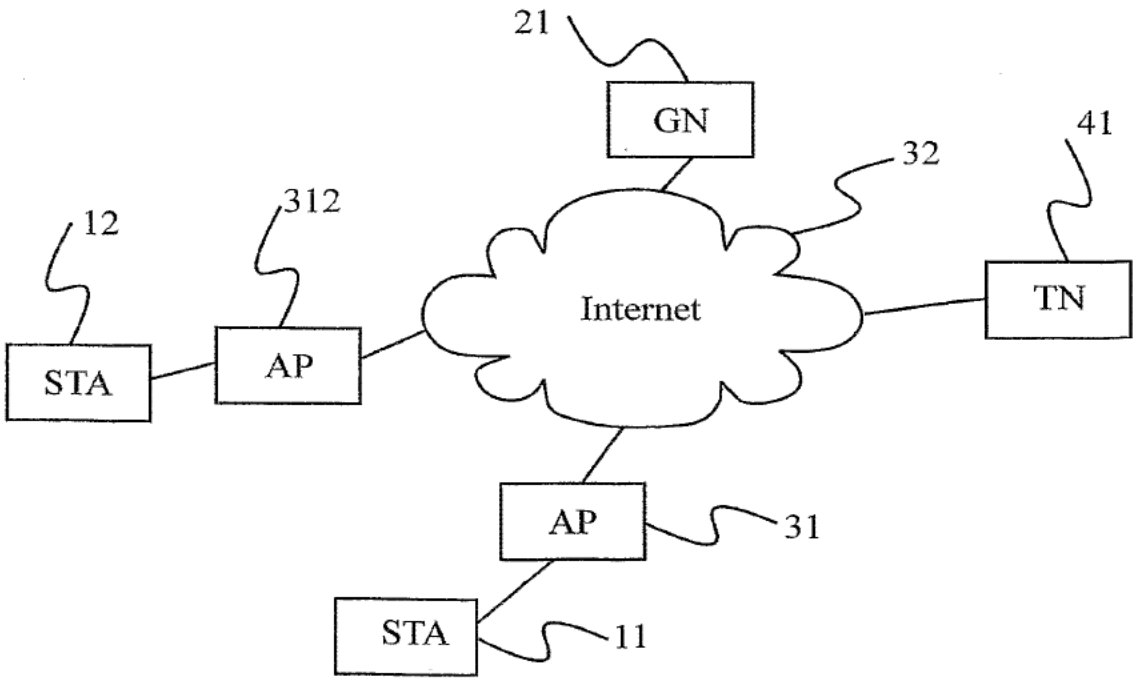

21
GN
41
32
312
12
Internet
TN
STA
AP
AP
31
STA
11

FIG. 13

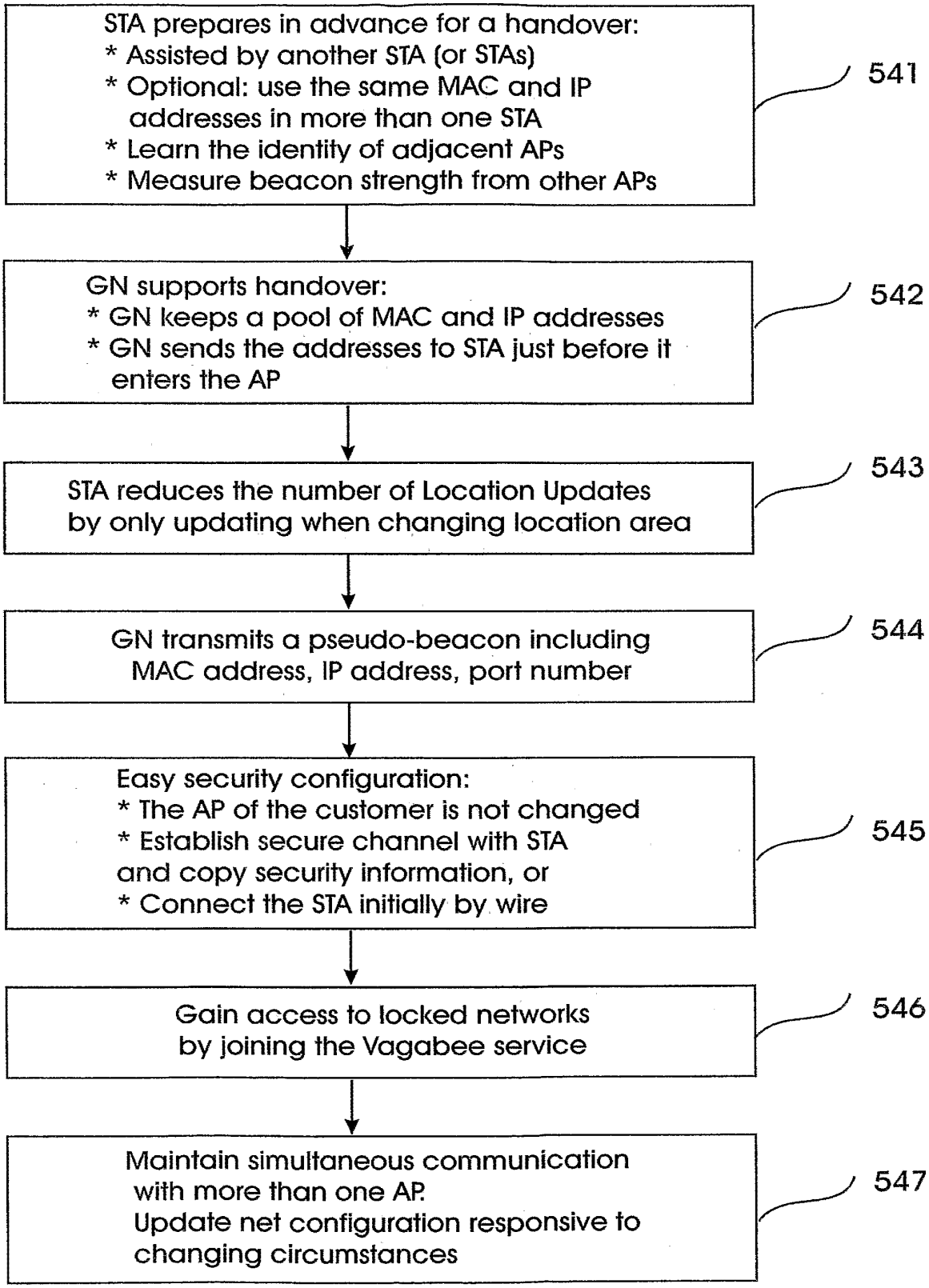

STA prepares in advance for a handover:
* Assisted by another STA (or STAs)
* Optional: use the same MAC and IP addresses in more than one STA
* Learn the identity of adjacent APs
* Measure beacon strength from other APs
541
GN supports handover:
* GN keeps a pool of MAC and IP addresses
* GN sends the addresses to STA just before it enters the AP
542
STA reduces the number of Location Updates by only updating when changing location area
543
GN transmits a pseudo-beacon including MAC address, IP address, port number
544
Easy security configuration:
* The AP of the customer is not changed
* Establish secure channel with STA and copy security information, or
* Connect the STA initially by wire
545
Gain access to locked networks by joining the Vagabee service
546
Maintain simultaneous communication with more than one AP.
Update net configuration responsive to changing circumstances
547

FIG. 14

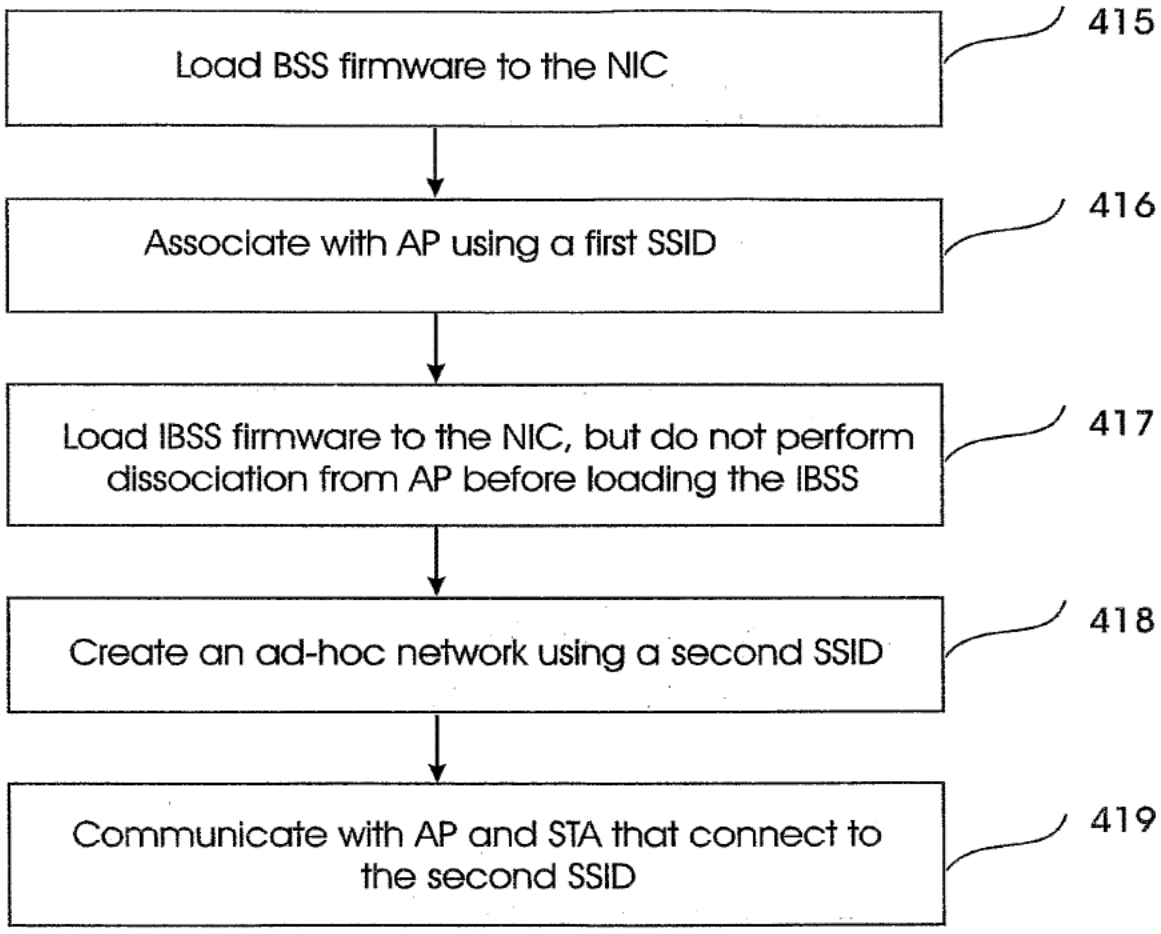

Load BSS firmware to the NIC
415
Associate with AP using a first SSID
416
Load IBSS firmware to the NIC, but do not perform dissociation from AP before loading the IBSS
417
Create an ad-hoc network using a second SSID
418
Communicate with AP and STA that connect to the second SSID
419

FIG. 15

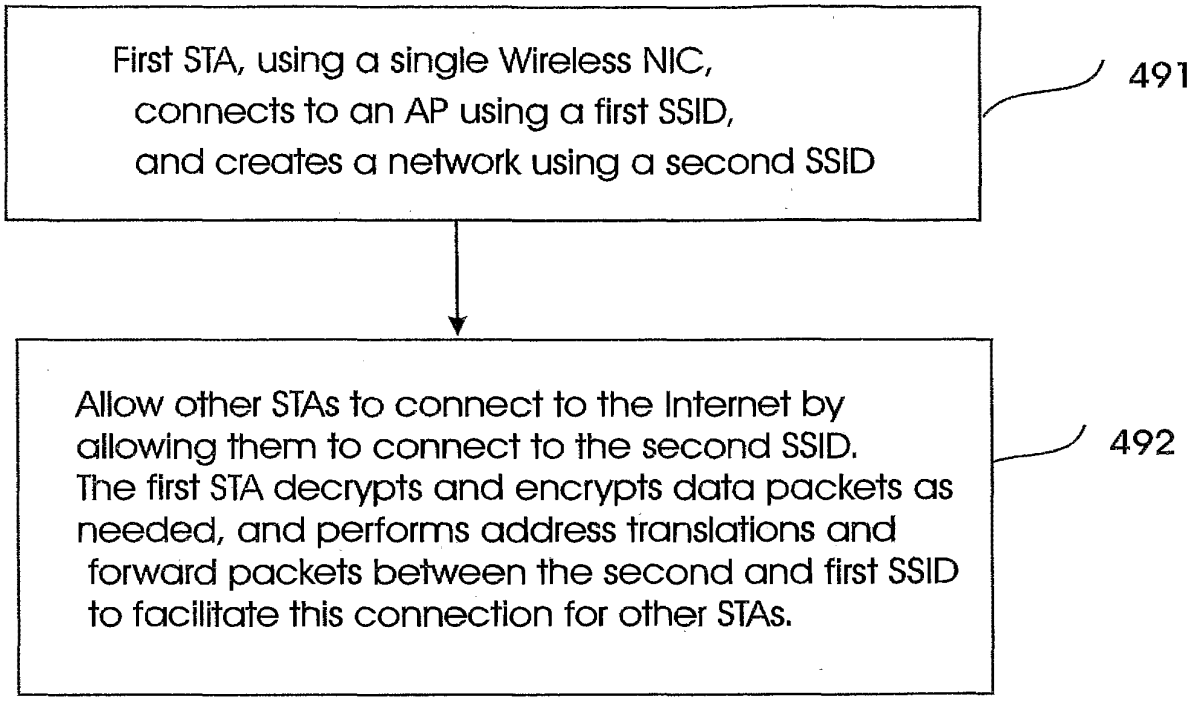

First STA, using a single Wireless NIC,
connects to an AP using a first SSID,
and creates a network using a second SSID
491
Allow other STAs to connect to the Internet by
allowing them to connect to the second SSID.
The first STA decrypts and encrypts data packets as
needed, and performs address translations and
forward packets between the second and first SSID
to facilitate this connection for other STAs.
492

FIG. 16

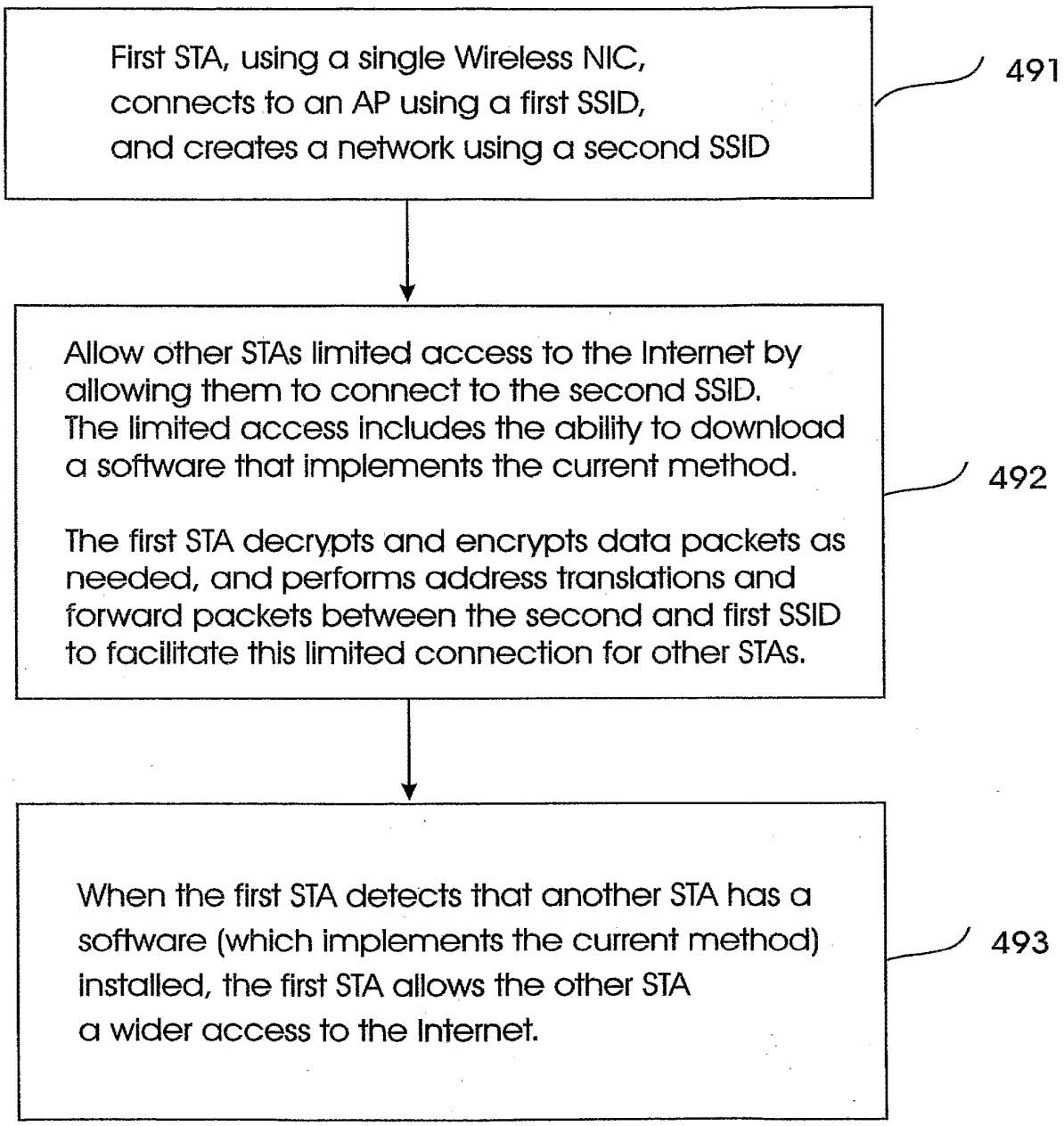

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID. The limited access includes the ability to download a software that implements the current method.
The first STA decrypts and encrypts data packets as needed, and performs address translations and forward packets between the second and first SSID to facilitate this limited connection for other STAs.
492
When the first STA detects that another STA has a software (which implements the current method) installed, the first STA allows the other STA a wider access to the Internet.
493

FIG. 17

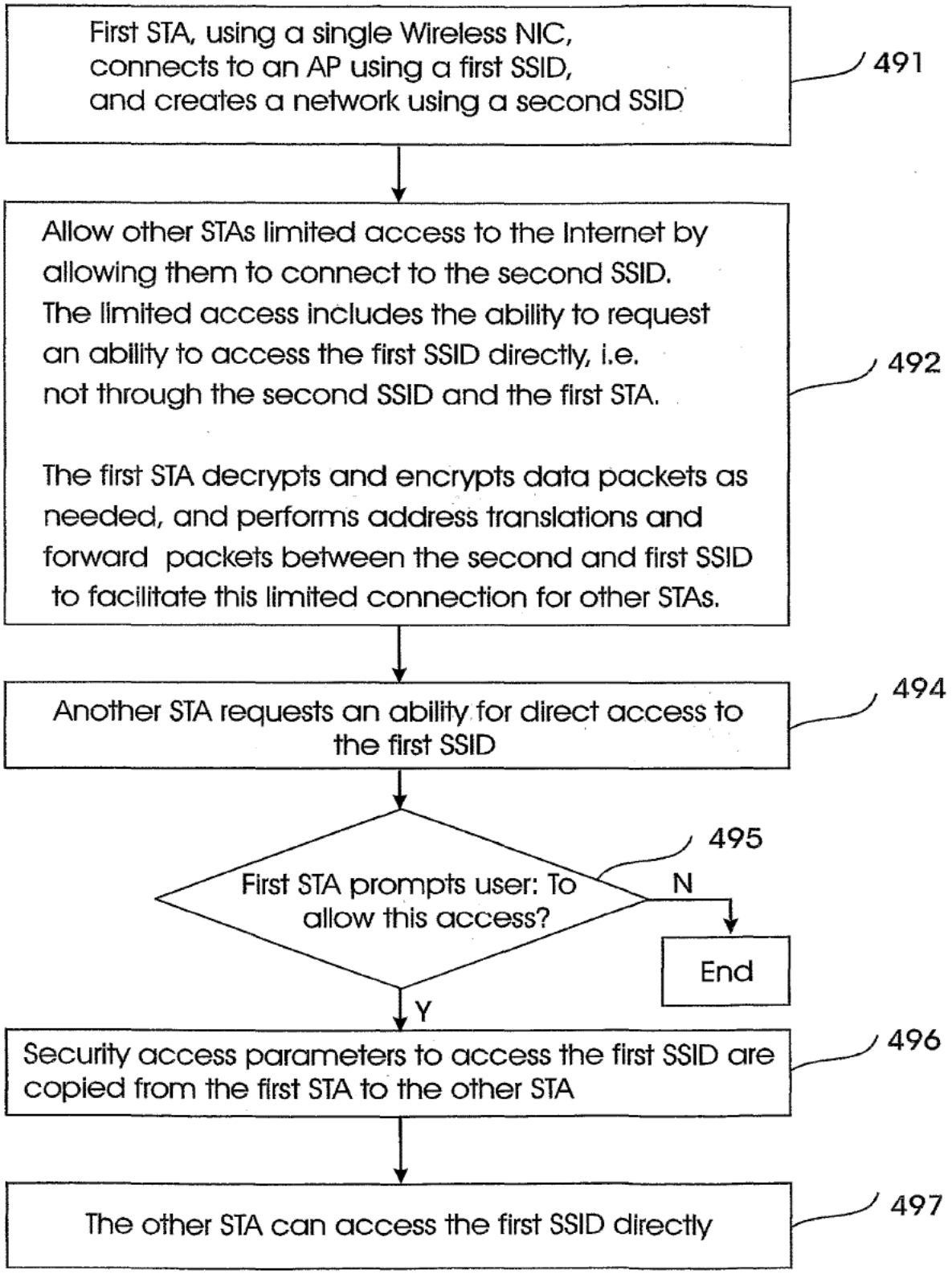

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID. The limited access includes the ability to request an ability to access the first SSID directly, i.e. not through the second SSID and the first STA.
The first STA decrypts and encrypts data packets as needed, and performs address translations and forward packets between the second and first SSID to facilitate this limited connection for other STAs.
492
Another STA requests an ability for direct access to the first SSID
494
First STA prompts user: To allow this access?
495
N
End
Y
Security access parameters to access the first SSID are copied from the first STA to the other STA
496
The other STA can access the first SSID directly
497

FIG. 18

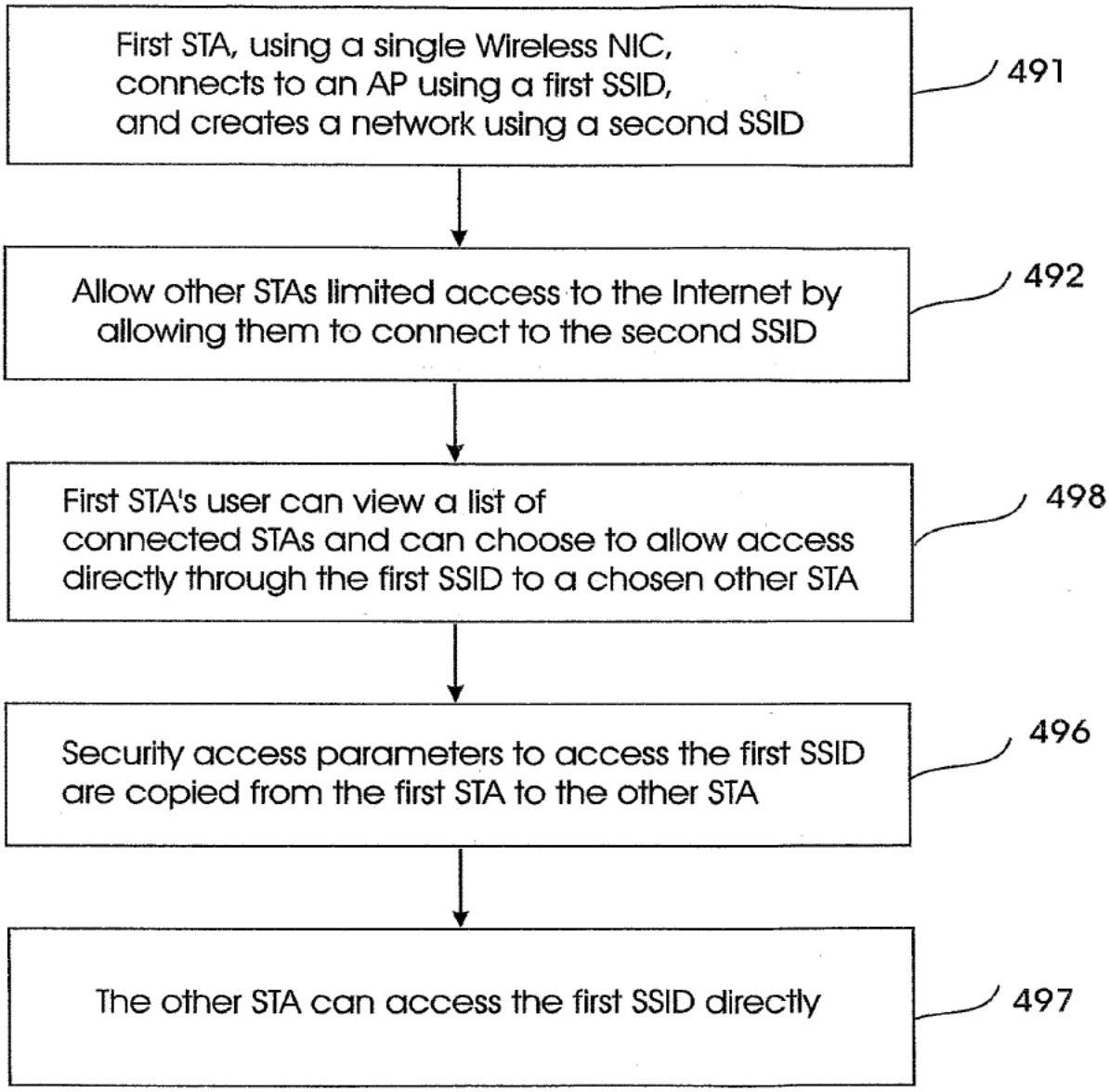

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID
492
First STA's user can view a list of connected STAs and can choose to allow access directly through the first SSID to a chosen other STA
498
Security access parameters to access the first SSID are copied from the first STA to the other STA
496
The other STA can access the first SSID directly
497

FIG. 19

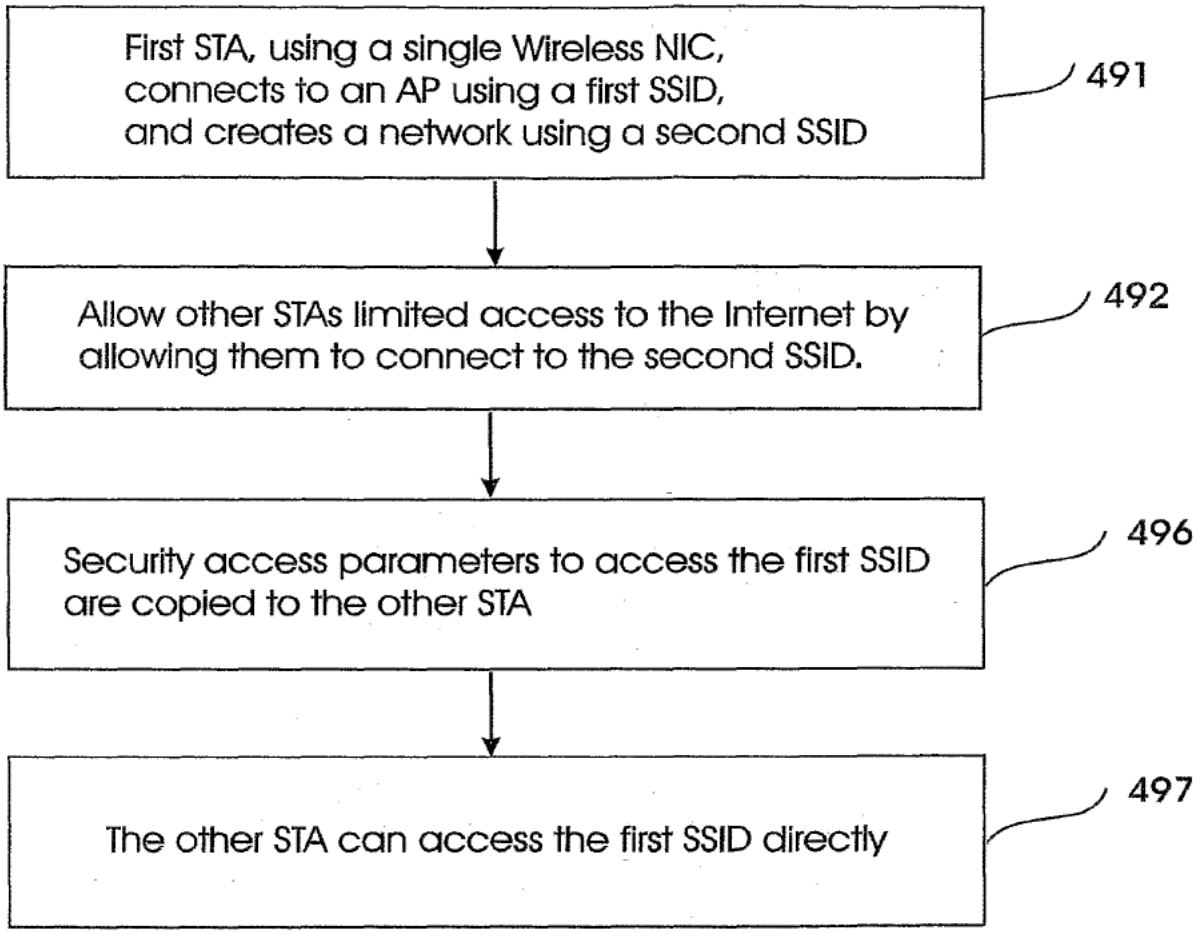

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID.
492
Security access parameters to access the first SSID are copied to the other STA
496
The other STA can access the first SSID directly
497

FIG. 20

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2007 (30.08.2007)

PCT

(10) International Publication Number
WO 2007/096884 A3

(51) International Patent Classification:
H04Q 7/24 (2006.01)

(21) International Application Number:
PCT/IL2007/000244

(22) International Filing Date:
22 February 2007 (22.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/775,321 22 February 2006 (22.02.2006) US
60/794,135 24 April 2006 (24.04.2006) US

(71) Applicant and
(72) Inventor: **BARKAN, Elad** [IL/IL]; C/O Marc Zuta, Patent Attorney, P.O. Box 2162, 49120 Petah-Tikva (IL).

(74) Agent: **ZUTA, Marc**; Marc Zuta, Patent Attorney, P.O. Box 2162, 49120 Petah-Tikva (IL).

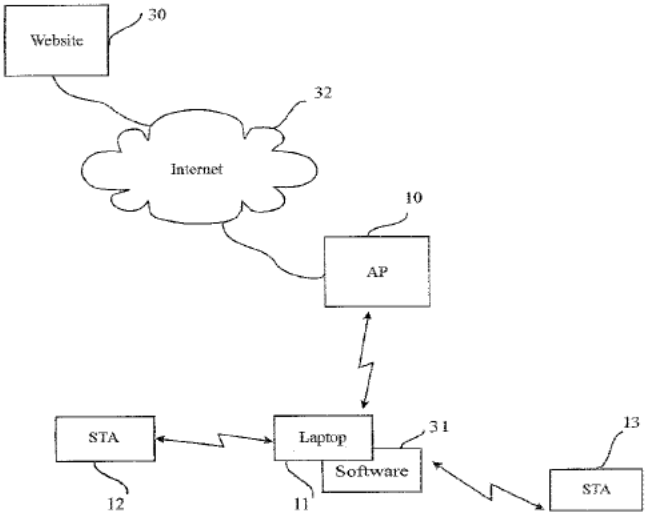
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
9 April 2009

(54) Title: WIRELESS INTERNET SYSTEM AND METHOD



(57) Abstract: A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising: wirelessly connecting a first STA to the Internet through a first AP with a first SSID; remaining connected to the first Access Point (AP), the first STA creates a software-based wireless AP with a second SSID for wirelessly connecting other STAs to the Internet through the first STA. A software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein. A method for configuring STAs to connect to a wireless network, comprising: a customer first connects a STA by wire to its network; a software on the STA copies to the STA the security information gained through the wired connection, thus setting the security parameters for the STA.

WO 2007/096884 A3

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/IL2007/000244

International filing date: 22 February 2007 (22.02.2007)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/775,321
Filing date: 22 February 2006 (22.02.2006)

Date of receipt at the International Bureau: 23 May 2007 (23.05.2007)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PA 1600860

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

April 23, 2007

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/775,321***
FILING DATE: ***February 22, 2006***

THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS ***US60/775,321***

By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office

L. Edelen

L. EDELEN
Certifying Officer

PTO/SB/16 (10-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 1 of 2

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. FEDEX 8547 7688 0082

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
ELAD	BARKAN	KFAR-SIRKIN, ISRAEL

Additional inventors are being named on the _____ *separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max):

FAST HANDOVER IN WIRELESS NETWORKS

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ The address corresponding to Customer Number: _____

OR

☑ Firm or Individual Name ELAD BARKAN

Address 12 HABANIM St.

City KFAR-SIRKIN | State | Zip 44935

Country ISRAEL | Telephone +972-54-5204112 | Email MCTIP@BARKAN.ORG

ENCLOSED APPLICATION PARTS *(check all that apply)*

☐ Application Data Sheet. See 37 CFR 1.76

☐ Specification *Number of Pages* 27

☐ Drawing(s) *Number of Sheets* 1

☐ CD(s), Number of CDs _____

☐ Other (specify) _____

Fees Due: Filing Fee of $200 ($100 for small entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

METHOD OF PAYMENT OF THE FILING FEE AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT

☑ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check or money order is enclosed to cover the filing fee and application size fee (if applicable).

☑ Payment by credit card. Form PTO-2038 is attached

☐ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: _____. A duplicative copy of this form is enclosed for fee processing.

100.00

TOTAL FEE AMOUNT ($)

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PROVISIONAL APPLICATION COVER SHEET
Page 2 of 2

PTO/SB/16 (10-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☑ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

SIGNATURE E. Barkan Date Feb 20, 2006

TYPED or PRINTED NAME ELAD BARKAN REGISTRATION NO. _____ *(if appropriate)*

TELEPHONE +(972)-54-520-4121 Docket Number: _____

Provisional Application For Paten

Title: Fast Handover in Wireless Networks

Date: February 20, 2006

Inventor: **Elad Barkan**

12 Habanim St.
Kfar Sirkin 49935
Israel

Tel: +(972)-54-520-4121
Fax: +(972)-3-933-2284
Email: moti@barkan.org

Fast Handover in Wireless Networks

Technical Field

This invention concerns systems and methods for fast handovers in wireless networks such as 802.11 networks, specifically in un-managed wireless networks, and more particularly such systems and methods which allow extremely fast handovers in these networks without any changes to existing 802.11 base stations. The invention also concerns efficient performance with regards to power consumption, coverage, security, installation, capacity and availability of wireless networks such as 802.11. The invention can achieve these goals without any change to the WiFi access point.

Background Art

Currently, there is a growing number of WiFi public hot-spots (or Access Points – "AP"). These APs allow WiFi enabled devices (which we refer to as STA) that are in their coverage area to connect to the internet.

Some of the APs are operated as a business, service, or as part of a community, either with or without a charge to the STA's user. Other APs are placed by individuals in their premises, but are not "locked", i.e., they allow bypassing STAs to utilize them. The cumulative connectivity provided by the APs is enormous and growing fast, thus, it is tempting to use this cumulative connectivity to compete with other wireless technologies. For example, it would be tempting to have a STA that looks like a cellular handset, where the WiFi handset uses the free connectivity to provide a "free" service that competes with or complements the cellular service.

One of the major difficulties of achieving this vision is that the coverage of a single WiFi AP is very small (about a few hundreds meters). When a user goes out of this area, his connectivity is lost. A natural approach to solve this problem is performing a *handover* (sometimes also called *handoff*) to another AP with a better radio connection to the user. Another approach is to have a handset which supports both WiFi and Cellular, and handover the conversation from WiFi to Cellular [See: WO 2004/036770], this way, WiFi extends the coverage of cellular, and conversation is handed over from WiFi to cellular, when there is no WiFi coverage. However, the

problem of performing handover between one WiFi AP to another WiFi AP remains when appropriate cellular coverage is not available (or there is no cooperation from the cellular company). The same idea applies when cellular is replaced by other access technology, such as satellite communications.

The concept of handover is taken from cellular networks. Handovers usually work well in *managed* networks, such as cellular networks, campuses, or office environment., where the entire network is usually owned by the same operator. The network operator in many cases chooses to add cells where coverage or capacity are needed. In managed networks, the APs (or the cellular cells) are synchronized and communicate with each other, and are usually controlled by some other network entity. For examples, the APs can communicate with each other, for example using the IEEE 802.11F protocol – the Inter-AP protocol, which involves a RADIUS (Remote Authentication Dial In User Service, see RFC 2138, 2865, and 2866) server. The APs can also employ a radio resource management such as IEEE 802.11K, or fast roaming using IEEE 802.11R, etc. However, in *unmanaged* networks, the APs can be deployed by many unrelated entities, such as by private individuals. There is usually no entity that synchronizes the APs. The APs can be manufactured by various manufacturers, use various security mechanisms etc. In unmanaged networks, the handovers are typically very slow, as in the process of handover, it takes time for the STA to re-connect to the internet in the new AP (and it must disconnect from the previous AP). In such a handover in an unmanaged network, the IP address often changes, therefore, a mechanism such as mobile IP must be used (as described later). This mechanism is limited with respect to the frequency in which the IP address can change, and a large latency (disconnection time) may result during the handover process. During the latency, the STA cannot receive any incoming messages.

A handover process is typically composed of the station STA connecting to a new AP, and disconnecting from the old AP. If STA is connected in parallel to both AP the handover is called *soft-handover*, and if STA first abandons the old AP and then connects to the new AP, the handover is called a *hard-handover*. Soft handovers require the ability of STA to communicate in parallel with at least two APs.

The process of connecting to a new AP is usually composed of the following steps.

1. STA performs a scanning process to discover neighboring APs.
2. STA chooses a new AP, and performs *authentication* with the AP, in which the AP verifies that STA is allowed to access the AP.
3. If the authentication is successful, STA performs an *association* process, in which the AP acknowledges that STA is connected to it (association requires the AP to allocate resources to the STA, and the 802.11 standard allows up to 2007 STAs to be associated with an AP).
4. Once STA is associated with the AP, the STA makes sure that it has all the information that it requires to communicate over the internet, for example, it must have an IP address, and it must update servers that govern its location (such as Mobile IP, as discussed later). In some cases, the user should go through a second authentication procedure (usually with a RADIUS server). Many times, this procedure is performed over a web interface, which is called a *Captive Portal*.

When a captive portal is used by the AP, the user needs to surf into the captive portal and perform a log-in to connect his IP address to the internet. In some implementations, the user's web browser is forwarded to the captive portal regardless of the internet site that it tries to surf into. Some APs allow the STA to surf in some limited number of internet sites before they complete the second authentication procedure (for example, if the AP is in an hotel, it might allow surfing into the hotel's website, or affiliated news web sites). The procedure at the captive portal typically includes authentication, payment, or agreeing to terms of usage. Once the authentication is complete, the IP address of the STA is connected to the internet (usually by reconfiguring the firewall that controls the communications of the AP). Each sub process takes time to complete, resulting in a total of over several seconds to complete the entire process.

It is important to note that in managed networks, Step 4 can be performed once in a certain amount or time (or for a certain area), as moving between APs of the managed network does not necessarily change the parameters of the STA such as IP address etc. However, in un-managed networks (and sometimes also in managed networks), the STA must gain a new IP address and other parameters, usually through DHCP

(Dynamic Host Configuration Protocol, see RFC 1541). Completing the DHCP protocol can take up to several seconds. Sometimes, obtaining an IP is not enough, and a second authentication is needed. In other cases, a proxy server or a Socks server should be set for the communication. The whole process can consume a few seconds, which are intolerable in a streaming two-way application such as a voice conversation.

Many protocols that are used in the Internet require that the IP address of the user would remain fixed during communications (for example, TCP – Transport Control Protocol, see RFC 793). However, a handover might result in the change of the IP.

One solution to this problem is provided by the Mobile IP standard (see RFC 2002): in this solution the STA updates a server with its current IP address, every time that the IP address changes. As a preparation for roaming, the server allocates to the STA (in addition to the STA's current IP address) an IP address that remains fixed, even when the real IP address of the STA changes. This fixed IP address is also known as a "care of" address. From this moment on, the STA keeps the server posted of the real IP address of the STA, and the STA can use (in its communications with the rest of the internet) the care of address (or its home address) as if it was its own fixed address. Any IP data packet that is sent to the care of IP address is tunneled by the server to the current IP address of the STA. For packets originating from the STA to the Internet, the STA can tunnel the packets to the server, which replaces the IP address with the care of address. However, many times the STA can simply write its care of IP address as the source address of the IP data packet, as many times, this address is not checked what-so-ever in the course of routing the IP data packet in the Internet.

This solution can be applied as long as the handovers are not performed too often. However, it incurs the punishment of routing all incoming packets through a server, causing both an increased travel time for the data packets, as well as latency (or disconnection) for the time that the real IP address changed, but the server is not informed yet. If the round-trip-time of the packets between the STA and the server is longer than the time a STA stays with the same IP, this method fails, as by the time packets reach the reported location of the STA, the STA is already in another location.

For many applications, such as voice, it is of utmost importance to minimize the time spent on the handover process. The time consumed by the handover process is usually dominated by the scanning step (Step 1 as mentioned above), and by Step 4 (specifically in case of an unmanaged network). There are many solutions that address fast handovers in cellular networks, and a few solutions that address fast handovers in managed WiFi networks (for example, see: WO2004/054283, which reduces Step 1 (mentioned above) by selective scanning but requires modifying the AP). None of these solutions deal with the delay due to Step 4.

It is an object of this invention to provide very fast handovers even in unmanaged networks.

Another barrier for wireless applications is that WiFi coverage might exists, and security policy might allow the STA to connect, but the AP might be out of resources (for example, there are 2007 associated STAs, and therefore it has no resources left, or that it has a limited IP address space which was already allocated through DHCP, and it has no IP address to allocate). It is an object of this invention to provide a system and method that allows STAs to use the services of the AP even when some of its resources are exhausted.

Another barrier for many wireless applications is the complex configuration of STA, especially the security parameters. A user that purchases a new STA and has an existing AP, might wish to configure his new STA to work with his AP. This configuration includes entering into the STA the encryption key and authentication key that would allow it to use the AP. Existing solutions require a change in the AP and STA, such that a special key can be pressed simultaneously at both ends to perform automatic configuration (like Buffalo INC's AirStation OneTouch Secure System – AOSS, or Broadcom's SecureEasySetup). Without such a solution, the user is usually forced to punch into his STA the security codes (which are typically long). The problem worsens when the STA moves between APs that use different security settings.

It is an object of this invention to provide easy configuration on both levels: at the initial setup and while roaming.

Another barrier for many wireless applications is that WiFi coverage might exist, but it is locked and unavailable for use for the STA.It is an object of this invention to provide a solution for (legally) accessing locked APs.

Another problem with WiFi is that the WiFi protocol is not optimized for low battery consumption (compared to cellular protocols such as GSM). In current solutions, if the STA moves between APs and changes its IP, it must use mobile IP and inform an entity (server) in the network of its current IP (we refer this process *location update*, as the STA updates the network entity of its location). Frequent location updates exhaust the STA's battery. Another problem with frequent location updates is that they create a heavy load on the network and on the network entities that manage and keep track of the STA's location.

The situation in WiFi is very different from the situation in cellular networks in two ways. Both of the ways cause increase on the number of location updates in WiFi: First, in cellular network, the cells are typically much larger than a "cell" that is created by a WiFi AP. Therefore, in cellular there are fewer transitions between cells, and hence less location updates. Second, cellular protocols allow defining a "location area" that encompasses several cells, and the STA is required to perform location update only when moving between location areas, and thus reducing the number of location updates. Current WiFi protocols are not built to support location areas.

It is an object of this invention to provide a method that reduces the number of location updates required for STAs while moving between APs.

It is an object of the current invention to provide the solutions to the above mentioned problems, using both a centralized (server based) approach, and also by providing a method for performing the solutions using a distributed peer-to-peer network. Therefore, no huge servers and no large investments are required.

Disclosure of Invention

The invention is described by way of example, but it should be obvious to those skilled in the art that many variations follow.

One of the novel ideas behind very fast handover is to practically almost complete the process of the handover before it even started, possibly with the assistance of another STA that is already in the new AP's coverage (further details are described later).

Another associated novel idea is that the same MAC address and IP address can actually be used by more than one STA. The differentiation between the STAs can be performed by using higher protocol identification, such as different port numbers (for example TCP ports), as detailed later.

It is useful for a station STA11 to know the identity of the adjacent APs that the STA might hand over to. The identity of an AP can be established in several ways, as disclosed herein. The SSID (Service Set ID) of the AP is usually broadcasted by the AP using periodical transmissions known as beacon. However, two adjacent AP may have the same SSID. In such a case, the MAC address of each AP is different, and APs can be differentiated based on their MAC address (which serves as a globally unique identification parameter). Some APs do not transmit beacon, and only respond when they are addressed using their SSID. In this case, a pre-knowledge is needed, as described later.

Another novel idea is that STA11 will selectively scan for a neighboring AP in the following novel way. Assume that STA11 scans to see if it can receive the beacon of AP33, where the scanning will be performed exactly when the AP33 is expected to transmit its beacon, therefore, the disconnection from AP31 will be minimal. The novel method consists of scanning and storing (in network entities) information about the relative time between adjacent APs, and their relative clock drift. This information is retrieved in the appropriate time such that the STA knows to wait for the beacon just before it is transmitted. The details are disclosed in the sequel..

Another aspect of this invention is to prevent exhaustion of resources at the APs. GN21 keeps a pool of MAC addresses with associated IP address. Just before a STA enters the AP, GN21 sends it a MAC address and an IP address that are already associated with the AP. Therefore, the STA can connect even if the AP has no resources left for new STAs. See a detailed description later.

Another novel idea in this disclosure is to save Battery Power and reduce network load by reducing the number of Location Updates in WiFi. A location update is the process in which a STA informs an entity in the network on its current location (the notification can take many forms, including opening a TCP connection, or sending UDP packets). In prior art for 802.11 networks, a location update is required whenever the IP address of the STA changes (for example, when moving between APs of different subnets) – even if the STA is idle (not transmitting or receiving data). The novel method allows to define a *location area* for WiFi, such that an idle STA needs to perform location update only when it moves between APs that belong to different location areas, but does not need to perform location update when it moves between APs of the same location area. See further details later.

A *pseudo-beacon* is another novel idea of this invention which allows reducing the number of Location Updates. It is a message that GN21 can periodically transmit in each AP. While some APs might permit a remote node to transmit a message in the AP, other APs might not allow it. In the novel method, a certain MAC address, IP address, and possibly a port number, are allocated in each AP for the purpose of pseudo-beacon transmission. Further details are described later.

Configuring the security might be a tedious job, as the security (authentication/encryption) code might be very long as known in the art, which the user might need to punch in. A novel solution for easy configuration is disclosed. Unlike previous solutions, the novel method does not require changing the existing AP of the customer. In one embodiment, software is run on a personal computer of the user (that is already configured to access the WiFi). Then, the software establishes a secure channel with the STA, and copies the security information from the personal computer to the STA. In this way, the STA learns the security parameters.
In another embodiment, the customer first connects the STA by wire to its network (or alternatively, the STA first connects using a connection it establishes through an already connected device, such as a personal computer). As the STA can receive and transmit signals on the wireless network and it is connected to the internet (through the other connection) at the same time, it tries to locate the web configuration of the AP on the wired network (most APs have a web interface). In most cases, it is an easy

job for the STA, as either the STA can locate the AP as it is the default gateway of the wired network, or it can try to find its IP by performing RARP (Reverse Address Resolution Protocol) using the wireless MAC address of the AP (which it can see off-the-air). Further details are described later.

Another novel method for gaining access to locked networks is disclosed. While performing the above described easy setup (or at any other time), the user is prompted, if he wishes, to join a swapping service. The swapping service allows the user to gain access to many locked networks (the locked networks of the other users that joined the swapping service), in return he allows users to use his network for the purpose of connecting to the internet. If the user agrees, the access parameters to his network (encryption key, MAC address, default gateway, etc.) are securely stored in the network (for example in GN21, and a backup server). The security information will be securely sent directly into the hardware of other STAs, when they need to connect using his AP. Further details are described later.

Another novel aspect of the invention takes advantage of the fact that the wireless network is local in nature, as the APs are geographically adjacent. As a result, the methods that are disclosed can be implemented by many small devices on the internet, each responsible for a geographic area. The devices form a peer-to-peer network that implement the methods, without the need to rely heavily on large servers.

Another novel idea in the invention is to have a STA which has a capability of communicating in two or more channels in parallel. This capability can enable a STA to be connected to two APs in parallel without the need to implement sophisticated mechanisms that actually simulate this situation. Thus, a STA can connect with future AP while maintaining a connection through its serving APs. Being connected to two APs simultaneously allows greater bandwidth by utilizing two connections instead of one, and soft-handovers, i.e., the STA stays connected through one AP, while disconnecting from the second AP in the process of handover.

Brief Description of the Drawings

The invention will now be described by way of example and with reference to the accompanying drawings in which:

Fig. 1 illustrates the mobile stations (STA) in the covering cell performed by the "Access Point" (AP)

Fig. 2. illustrates the connection among STA11, a Governing Node (GN) and another user – Termination Node (TN).

Mode of Carrying out the Invention

A preferred embodiment of the present invention will now be described by way of example and with reference to the accompanying drawings.

It is understood that the method and system in the present disclosure may be used for the transmission of voice, data, multimedia or a combination thereof.

Fast Handover

One of the novel ideas behind very fast handover is to practically almost complete the process of the handover before it even started.

Consider an example depicted in Figure 1 and Figure 2, in which STA11 is in conversation with TN41 (TN – Termination node, the node with which STA11 communicates, shown in Fig. 2), and STA11 is moving from AP31 towards AP32. Also assume that a node GN21 (GN – Governing Node, a node that is non-exclusively responsible for the mobility management in a certain geographic area for a given time, shown in Fig. 2) is in contact with STA11, and it is assisting STA11 during the handover process. STA11 currently has an IP address, which was allocated to it by AP31. To complete the handover, STA11 should be associated with AP32, have an IP address assigned by AP32, complete any second authentication that is required, and have TN41 be aware of the new IP address, so it can forward the conversation to the new location. Note that in some scenarios (in some cases when there are firewalls or

NAT devices between AP32 and TN41, the connection between STA11 and TN41 must be started from within AP32 towards TN41).

According to prior art, it appears that STA11 cannot begin the handover process until it reaches the coverage of AP32, since it cannot start the connection process. One novel solution (that requires changing the software of the AP) is to allow STA11 to perform the connection process through the Internet, instead of performing it wirelessly. In this way, once STA11 reaches radio connection with AP32, it can start working immediately.

However, we are more interested in solutions where there is no need to change the AP. To achieve this goal, assume the existence of a non-moving STA12 in the coverage of AP32 (we will somewhat soften this assumption later). According to the present invention STA12 is in contact with GN21, and receives instructions to *impersonate* STA11 towards AP32 (we will later discuss how to make it possible), and complete a connection process with AP32 on behalf of STA11 (including authentication, association, receiving an IP address, performing any second authentication/log-in procedure, and perhaps even opening connections or "punching holes" in the firewall). Then, STA12 communicates this parameters to GN21 (once the parameters are communicated, STA12 can return to its real identity). GN21 communicates the parameters to STA11 (and perhaps to TN41), and thus, STA11 does no longer need to perform the connection process, and once it reaches the perimeter of the coverage (we will later discuss how to identify this situation) it can immediately use the new parameters and continue communications without any delay. STA11 (or GN21) can alert TN41 *before* the handover, so it can start and send information packets to the new location. TN41 may send the information in parallel to the old and the new location, and cease transmitting to the old location once the handover is complete (e.g., when it receives information from STA11 with its address from the new AP). STA12 may even open a TCP (Transmission Control Protocol, as used in the Internet) connection or send a UDP (User Datagram Protocol) packet on behalf of STA11, if required. This connection may wait for STA11 until it reaches AP32. If there is a timeout on these connections (either due to protocol, or due to firewalls), STA12 or other bypassing STAs can send and receive "keep-alive" messages on behalf of STA11 (as is instructed by GN21). The timeout for each AP

can be discovered over time by trial and error (or by discovering the APs type), and storing this information in GN21 for future use. GN21 can notify the STAs on the value of the timeout.

How STA12 can impersonate STA11:

To understand how STA12 can impersonate STA11 towards AP32, we must understand how identity is established in the network. The basic identity in the network is the physical address which is known as MAC Address (Media Access Control Address), which is globally unique. Each manufacturer is allocated a portion of the address space and allocates a unique MAC address to every network card (including WiFi network card) that it manufactures. Then, the manufacturer burns the allocated address into the network card. However, in most network cards, an application can (temporarily) change the MAC address of the card to another MAC address.

The MAC address is not used for end-to-end communications over the internet, but usually only for communications within the same physical network.

For example, STA12 communicates with AP32 using MAC address, but GN21 is not usually aware of the MAC address of STA12. The MAC address is universally unique.

We use the feature of temporarily changing the MAC address in the network cards in a novel way, allowing STA12 to impersonate STA11. Therefore, in the instructions that GN21 gives to STA12, it mentions the MAC address of STA11, so STA12 can assume the MAC identity of STA11. Then, STA12 can complete the association with AP32 (using the MAC address of STA11)), in which it receives the Association ID (AID), and completes a DHCP protocol in which it receives an IP address to be used with the MAC of STA11 while it is using AP32. STA12 can also perform a second authentication and log-in on behalf of STA11. STA12 sends the connection information back to GN21, which forwards it to STA11. STA12 can return to its original MAC address, but the allocated resources at AP32 remain allocated, as from the point of view of AP32, STA11 is already connected and in coverage. In order to avoid losing messages that are sent to STA12 during its impersonation to STA11, it can either continue and listen using both its own MAC address and STA11's MAC address, or it can issue a "power-save" mode command to its serving AP. The power

save mode indicates the AP that the STA is sleeping for a while, in which time the AP is buffering the incoming data packets. Therefore, even if STA12 is connected to the internet using another AP, it can issue a power-save mode command, possibly change the frequency, and perform the connection on behalf of STA12. It can return to its serving AP once the connection is established, or poll for incoming messages once in a while.

First Softening of the Assumption that STA12 is in the coverage of AP32: What if STA12 is not in the coverage of AP32, and there is no other station in AP32's coverage? The following process can be performed in advance, well before a handover is needed. GN21 can ask (in advance) stations that pass through AP32 to connect and receive an IP address from AP32 using some MAC address. The MAC address is not necessarily the MAC address of STA11, as the process is not specific to STA11. The stations send the connection details to GN21, which stores the AID, the MAC, the IP address and other connections details in a poll for future use. The poll may even contain UDP or TCP connections, which may be kept alive by bypassing STAs (against timeouts of firewalls, Network Address Translator devices (NAT), and protocol timeouts). UDP and TCP connections in the poll are targeted to some node in the network that can forward information for other nodes (for example TN41). When a connection is required by some STA, the pool is queried, and a resource can be allocated and applied by a STA. As a result, a station might change its MAC address and IP address every time it moves between APs. If the station moves very fast between these access points, GN21 can predict the direction in which the station is moving based on past movements, inform TN41 of the possible future addresses. In this way, TN41 can send data to the new address even before the station actually moved there. In some implementations of the APs and firewalls between AP32 and TN41 the STA must first send data before it can receive any data, otherwise, the firewall may block the incoming data, or a NAT (Network Address Translator) device might not know where to forward the data. The restriction, that the STA must be the first to send data, is usually required due to security policy that allows only outgoing connections, or due to NAT device that need to relate an internal IP address and port number with an external IP address and port number. For example, in most NAT implementations a connection must be established from within the NATed zone (e.g., the AP coverage) towards the internet. Many firewalls also require that the connection

is established from the private network towards the internet (rather than allowing incoming connections from the internet towards the private networks). In these cases, the data that TN41 sends is not transmitted by AP32 until the station reaches the access point and transmits information back to TN41. Depending on the type of firewalls and NAT devices, TN41 might be able to predict a port number to which it should send such messages before the first outgoing data packet is transmitted.

Another associated novel disclosure is that the same MAC address and IP address can actually be used by more than one STA. The differentiation between the STAs can be performed by using higher protocol identities such as different ports (for example TCP ports). Using the same MAC and IP address in more than one STA is not problematic for packets that are sent from the STA. However, while receiving an incoming packet, only one STA should send an acknowledgement. As each STA knows the ports that are in use, it only acknowledges messages that are designated to it. GN21 can coordinate between the STAs such that they do not use the same ports. For example, if there are at most n stations using the same MAC and IP address, station i will allocate port numbers that are equal to i modulo n. Another solution is to choose the port number at random. If each STA uses one port at random, according to the birthday paradox, port collisions occur with very low probability as long as the number of connections is smaller than about the square root of 65536 (i.e., when there are less than 256 connections using the same IP).

Another idea is to change the software at the AP such that it can communicate with GN21 and perform the connection procedure on behalf of STA11.

Knowing who are the adjacent APs and the location of a STA:

It is useful for a station STA11 to know the identity of the adjacent APs that the station might hand over to. The identity of an AP can be established in several ways: The SSID (Service Set ID) of the AP is usually broadcasted by the AP using periodical transmissions known as beacon. However, two adjacent AP may have the same SSID. In such a case, the MAC address of each AP is different, and APs can be differentiated based on their MAC address. Some APs do not transmit their SSID, but they still broadcast beacon messages with their MAC address. Even if the AP is locked and encrypted the MAC address is transmitted, and it is transmitted without

any encryption. In this way, STA11 can know the identity of adjacent APs, and infer its location.

Scanning by Idle STAs:

In a preferred embodiment, GN21 collects information about APs which are adjacent. Idle stations (i.e. stations which are not in an intensive data transfer) can perform a *scanning* operation once in a while. As a result they learn the MAC address (and possiblly the SSIDs) of the APs within radio reach. The STAs can then send this information to GN21 which collects it. The idle STAs can also perform tests to check what is the accessibility parameters of an AP (e.g., is it an open and free AP, is it a locked AP and the password is available from GN21, is it locked and there is no free access to the AP, is there a captive portal, does GN21 have a username/password available for the captive portal, etc.). All this discovered information is sent to GN21. When handovers are performed, GN21 takes note of the sequence of handovers that occur, and can learn common paths which are taken (for example, a road or a crosswalk might cause more likely paths than others).

It is very important that GN21 knows in advance the AP to which STA11 will be handed over to and when the handover will occur. Such a knowledge allows, for example, to alert TN41of the new location in advance. Gaining accuracy in the prediction of the handover (when and where) translates to better performance, as GN21 needs to allocate a MAC address and an IP address to STA11 in the new AP, and TN41 might start to send data to the new location. Therefore, knowing who the neighboring APs are, and their reception quality at STA11 is very important.

Scanning by a non-Idle STA.

In principle, STA11 can scan the surroundings once in a while and look for the beacons of adjacent APs, and thus measure the reception quality from each AP. However, such a scanning takes a lot of time (might even take couple of seconds for a full scan). Selective scanning for APs which are expected to be neighbors can reduce the scanning time, but it can still stay in the magnitude of a few hundred milliseconds. It is important to understand that during a contemporary scanning using current

technology, STA11 cannot receive or send messages from or to AP31, which means that the scanning time must be reduced to reduce this disconnection time.

The novel disclosed method is that STA11 will selectively scan for a neighboring AP in the following special way. Assume that STA11 scans to see if it can receive the beacon of AP33, where the scanning is performed exactly when the AP33 is expected to transmit its beacon. Therefore, the disconnection from AP31 will be minimal. The problem is, however, that although the beacons are transmitted periodically, STA11 does not know when a beacon is expected to be transmitted from AP33. As the beacons are transmitted about every 102.4ms (many variations are possible), STA11 might be forced to wait on average 51.2ms, which is a prohibitively long time to wait. STA11 may also transmit a *Probe* message to force a beacon to be sent especially for it– but a probe message requires a transmission that has implication on battery life. Furthermore, for the purpose of location finding, STA11 might wish to be able to receive beacons of APs that will not answer the probe (due to range, policies, etc.)

We can safely assume that other STAs visited the area of AP33 before STA11, and that they have reported the rate of the beacons of AP33 (e.g., a beacon every 102.4ms). A problem that remains is that the beacons are scheduled according to the internal clock of AP33, which might tick at a different rate than other clocks (and clocks tend to tick at different rates). Moreover, the clock of the visiting STAs is probably not exactly synchronized with the clock of STA11, which makes the process inaccurate. That is even if STA11 knows that at a specific time according to some STA's internal clock a beacon was transmitted, STA11 will not know how to translate this information to his clock, as the clocks are probably not synchronized to such great accuracy (network time synchronization services such as the network time protocol (NTP) cannot be more accurate than a couple of tens of milliseconds, where in this case we need an accuracy of around one millisecond). The following novel method allows accuracy of microseconds.

The novel approach for time synchronization is to rely on a relatively accurate clock already available to STA11: The 802.11 standard requires each AP to transmit in its beacon its clock (referred to in the 802.11 standard as *timestamp*). This clock must be the internal clock of the AP at the time of transmission in units of microseconds.

Therefore, STAs can specify the value of the clock of AP33 in terms of the value of the clock at the adjacent AP31. By measuring the timestamp of AP31 and AP33 at two different times T_{31}^{1} and T_{31}^{2} (based on the clock of AP31), in which the time value of AP33 T_{33}^{1} and T_{33}^{2}, respectively, it can be established with reasonable accuracy that AP33 clock ticks approximately $r_{33/31}=(T_{33}^{2}- T_{33}^{1})/(T_{31}^{2}-T_{31}^{1})$ times for every clock tick of AP31. At time T_{31}^{3} in the future, the clock of AP33 can be estimated as $T_{33}^{3}\approx T_{33}^{2}+r_{33/31}\cdot(T_{31}^{3}-T_{31}^{2})$. Similarly, at time T_{33}^{4} the clock of AP31 can be estimated as $T_{31}^{4}\approx T_{31}^{2}+(1/r_{33/31})\cdot(T_{33}^{4}-T_{33}^{2})$. Beacons are scheduled to transmission when the clock of the AP modulo the beacon interval is zero, where the beacon interval is measured in microseconds according to the clock of the AP, it is fixed for an AP, and the value of the beacon interval is transmitted in the beacon. Therefore, GN21 stores the relation $r_{33/31}$ together with T_{33}^{2} and T_{31}^{2} and the beacon interval of AP33 and AP31, and reports it to STA11 such that it can extrapolate the time at AP33 and infer the time of the beacon transmission. Once STA11 succeeds in receiving a beacon from AP33 it can report the times to GN21, so that GN21 can keep its time tracking accurate. Furthermore, the scanning allows GN21 and STA11 to make the best handover decisions based on the knowledge of the approximate location of STA11 with respect to the neighboring APs.

A technical problem that still has to be resolved is that a STA can know the value T_{31}^{1} but cannot measure the value of T_{33}^{1} in exactly the same time of T_{31}^{1} , as these values are carried on the beacons of APs, which are transmitted at different times. The solution is to measure the time of AP33 $T_{33}^{1'}$ at a time close to T_{33}^{1}, and note the time difference between the two measurements according to the STA's internal timer. As the measurements are very close to each other, the clock drift between the STA's timer and AP33's timer is negligible, and we can estimate that $T_{33}^{1}\approx T_{33}^{1'}+timediff$, where *timediff* is the time difference between the measurements of $T_{33}^{1}$and $T_{33}^{1'}$ according to the timer of the STA. If there is a large clock drift after all (although it is not expected), it can be corrected by calculating the r value between the clock at AP33 and the STA in a similar way to the way done for APs.

The location of STA11 can be deduced from the reception quality, the reception strength and the identity of the neighboring APs. This location information can be

taken into account while performing handover decisions, as well as for location based services or for other network applications.

It should also be noted that in Frequency Hopping, knowing the time of the AP has another special importance, as the frequency that the AP works in might depend on the time.

Preventing Exhaustion of Resources at the AP

As discussed under "Background Art", each AP has a limited number of Association IDs (AID) and usually, even a smaller pool of IP addresses (available through DHCP). Once this number of resources is exhausted, the AP might not be able to serve new STAs.

A situation where IP addresses are exhausted can happen very quickly: for example, consider an AP in a very busy location, where there are many STAs that connect to the AP only for a short period of time. Each STA performs the connection process and obtains an IP address using DHCP, but as it disconnects it might not release the IP address.

The pool of IP addresses in an unmanaged AP is usually limited to about 200 addresses, with many consumer APs supporting only tens of addresses. A device is assigned the IP address for a given period of time (known as the lease time). Many times, the lease time is set in a magnitude of days (although the granularity is seconds), and in many other instances the lease time is set to a magnitude of hours. In such a situation the pool of IP addresses runs empty very fast.

However, in this disclosure for fast handovers, GN21 keeps a pool of MAC addresses with associated IP address. Just before a STA enters the AP, GN21 can send it a MAC address and an IP address that are already associated with the AP. Therefore, the STA can connect even if the AP has no resources left for new STAs. Combined with the above disclosure that allows several STAs to share the same MAC address and IP address, an AP can serve more APs than its IP resources, even above its limit on the number of associated STAs.

Saving Battery Power by Reducing Location Updates

A novel disclosure of this invention is a method to reduce the number of location updates that are needed in WiFi, when a STA is idle. A location update is the process in which a STA informs an entity in the network of the current location of the STA (the notification can take many forms, including opening a TCP connection, or sending UDP packets). In prior art for WiFi networks (with for example mobile IP, or SIP – Session Initiation Protocol), a location update is required whenever the IP address of the STA changes (for example, when moving between APs of different subnets) – even if the STA is idle. The novel method allows defining a *location area* for WiFi, such that a STA needs to perform location update only when it moves between APs that belong to different location areas, but does not need to perform location update when it moves between APs of the same location area as long as it's idle.

We assume that the APs are divided into location areas, and for each location area there is a node in the network that is in charge of this location area. For example, assume GN21 is in charge of a location area composed of AP31, AP32, and AP33. How does a STA know which AP belongs to the location area? Either GN21 gives it a list of all the APs that belong to the location area, or GN21 transmits a *pseudo-beacon* in each AP.

A *pseudo-beacon* is a novel disclosure of this invention. It is a message that GN21 can periodically transmit in each AP. While some APs might permit a remote node to transmit a message in the AP, other APs might not allow it. In the novel method, a certain MAC address, IP address, and possibly port are allocated in each AP for the purpose of pseudo-beacon transmission. GN21 asks some STA to open a connection using these resources to GN21, and GN21 sends the pseudo-beacon messages using this transmission. Each pseudo-beacon contains the parameters needed to listen to the pseudo-beacons in the adjacent APs. A STA that lacks these parameters can contact GN21 and receive them. From that moment on, the STA can move between APs in the same location area, and receive the parameters that are needed to listen to the pseudo-beacon from other pseudo beacons. For example, assume that STA11 is located in AP31 and is moving to AP32. STA11 listens to the pseudo-beacon at AP31, and from the pseudo-beacon learns the parameters that are needed to listen to the pseudo-beacon of AP32. Thus, STA11 can move to AP32 without any transmission.

Which STAs of the stations in AP31 should acknowledge the pseudo-beacon? Preferably, none. However, some firewalls require minimum rate of outgoing packets to maintain an open connection. In such a case, once in a while GN21 sends on the pseudo-beacon a message that asks any station to send an acknowledgement with some probability *p*. The probability that GN21 states should be accommodated to the expected number of stations in AP31 (GN21 might not exactly know how many STAs are in the AP). If no STA acknowledges the pseudo-beacon for over the needed time, and the timeout of firewalls stop the incoming messages, then no pseudo-beacons are transmitted. In this case, a roaming STA will contact GN21 after a certain period of time of probing for the pseudo-beacon has passed (and no pseudo-beacon is seen). GN21 can request the STA to reopen the connection for the pseudo-beacon transmission.

If the STA is in a session with TN41 with many packets received (e.g., above a certain threshold), it is considered *non-idle* (which we also refer to as *in conversation*) and treated as described above in **fast handover**.
However, assume that STA11 is in idle mode (e.g., incoming packets below a threshold), it can move between APs of the same location area without performing location update. When a node TN41 wishes to send data to STA11, STA11 should change its state from *idle* to *in conversation*. TN41 contacts GN21 (TN41 might be forwarded to GN21 through a system such as dynamic DNS (Directory Name Service) or another method, such as a Distributed Hash Table – DHT, or a peer-to-peer network). GN21 sends a *paging* message for STA11 on the pseudo-beacon of all the APs in the location area. As STA11 listens to one of the pseudo-beacons, STA11 will receive the paging message. Then, STA11 responds preferably to GN21 (or to TN41, depending on what is written in the paging message) by initiating an outgoing connection as described below. It should be noted that GN21 can first page for STA11 in the APs that have a higher chance covering STA11, and the paging can repeat several times until STA11 replies.

When a STA is required to initiate an outgoing connection it can use a resource (MAC, IP, or TCP/UDP with port, user/password) that is listed as available on the pseudo-beacon or on the paging message, or it can request its own resources from the

AP. If two (or more) STAs use the same resources for a connection at the same time, GN21 will detect it, and in the acknowledge message (or second message of the TCP handshake) will announce the identity of the STA that it answers to. The other STA is required to initiate an outgoing connection again. Once a connection with GN21 is established, GN21 can allocate resources to the STA such that it moves to be in conversation status. One of the resources that are allocated is GN21 attention to accompany the STA as it might need to perform handover to another AP.

It should be noted that the location areas can overlap, meaning a single AP can belong to more than one location area. Upon the policy of the network, STA11 might be required to perform location update when it reaches such a APs, or it may just give helpful information. If possible, a STA might prefer to *park* on an AP that is within the same location area as its current AP, such that a location update is avoided.

It should also be noted that there is a tradeoff between the overhead that is spent during paging and establishing the connection, and the overhead that is being spent to keep a steady connection for each AP. The optimal point on the tradeoff depends on the rate that the AP switches APs as well as on the number of packets it receives and sends.

Easy Configuration of STA

When purchasing a new STA, it is required to configure the STA with the security settings of the existing network (in case the network is secure). If the network is not secure, the new owner usually only needs to select his network from the list of available networks that is received by the wireless network card.

Configuring the security might be a tedious job, as the security (authentication/encryption) code might be very long as known in the art, which the user might need to punch in. A novel solution for easy configuration is disclosed. Unlike previous solutions, the novel method does not require changing the existing AP of the customer. In one embodiment, software is run on a personal computer of the user (that is already configured to access the WiFi). Then, the software establishes a

secure channel with the STA, and copies the security information from the personal computer to the STA. In this way, the STA learns the security parameters.

In another embodiment, the customer first connects the STA by wire to its network (or alternatively, the STA first connects using a connection it establishes through an already connected device, such as a personal computer). As the STA can receive and transmit signals on the wireless network and it is connected to the internet (through the other connection) at the same time, it tries to locate the web configuration of the AP on the wired network (most APs have a web interface). In most cases, it is an easy job for the STA, as either the STA can locate the AP as it is the default gateway of the wired network, or it can try to find its IP by performing RARP (Reverse Address Resolution Protocol) using the wireless MAC address of the AP (which it can see off-the-air).

If none succeeds the STA can perform exhaustive search on commonly used IP addresses, or on very probable addresses, like all the IP addresses of the same subnet. Once the AP web interface is found, the STA tries to log into the AP. It can guess the default address or find it on a database that can be built on the web, with common default passwords for each manufacturer (the manufacturer and model will be usually sent by the AP during the web login process, or can be found out using the MAC address, which is unique per manufacturer). If the password for the AP cannot be guessed, the user is prompted for its password to complete the log-in. Then, the STA navigates to the security settings page and retrieves the password needed for the wireless network.

In the event that the procedure fails, the user is prompted for the security settings (which would happen without using the above method). For most common users and setups, the method succeeds (and for unsophisticated customers, who do not change the passwords – it succeeds in the majority of the cases). Thus, in the majority of cases, the setup is made much simpler.

Once the STA has access to the setup of the AP, it can (with permission from the user), open holes or forward certain port to some IP address. This IP address and port can serve as way that GN21 can send and broadcast the pseudo-beacon, without a STA first opening a connection from the AP, and without worrying about timeouts

(provided that there are no other firewall between the AP and GN21). Opened ports can also help during the fast handover, such that TN41 can directly send packets to the new location without a need for STA12 to open the connection.

In corporate settings, the company can set a special server which gives the configuration to the phone, over the network.

Gaining Access to Locked Networks

While performing the above easy setup (or at any other time), the user is prompted if he wishes to join a swapping service. The swapping service allows the user to gain access to many locked networks (the locked networks of the other users that joined the swapping service), in return that he allows users to use his network for the purpose of connecting to the internet. If the user agrees, the access parameters to his network (encryption key, MAC address, default gateway, etc.) are securely stored in the network (for example in GN21, and a backup server). The security information is securely sent directly into the hardware (or network card) of other STAs, when they need to connect using his AP. As the security parameters are sent directly to the STA's network hardware, it can make sure that the communication that is established is designated outside the user's network, and will not jeopardize the computers on the user's network. Furthermore, GN21 can monitor the amount of bandwidth that is consumed by visiting users, and to make sure their hardware limits the amount of used bandwidth such that the user does not experience a degradation of quality of his connection. Alternatively, the security information can be sent to the other STAs using other security measures, as known in the art.

The secrecy of the security parameters (such as the encryption key) can be cryptographically protected while on transit and storage, as known in the art.

Some APs limit the access of the subscribers by making sure that only specific MAC addresses connect to the network. As our methods as described above allow to use the same MAC address for several users, this specific MAC address can be used when using the network that restricts the use with specific MAC address.

In case a STA tries to connect to an AP with a captive portal, a special application on the STA is running and performs the authentication and log-in automatically. GN21 can store typical portal appearances, such that it can guide the STA on how to perform the authentication/log-in process. If the STA comes across a captive portal which is unknown or unexpected, it can locally store the web pages that it received from the captive portal and later transfer them to GN21. GN21 accumulates the reports and guides STAs how to log-in to the captive portal in the future. As part of the swapping service, GN21 can store username/passwords to enable connection through the captive portal automatically.

Special care for data

The above description works well for both voice and data.
TN41 might be a mobile node as well, or a fixed node in the network.
The transferred information between STA11 and GN21 can be voice, data, or their combination.

In case STA11 wishes to communicate with a node that is not aware of the novel network, it can do so through a node that is aware of the network. For example, TN41 can serve as a proxy for STA11 (in a similar way to mobile IP). The node that is not aware of the network communicates with TN41. TN41 forward the information to STA11. TN41 can allocate an IP address (perhaps using NAT, or allocate ports using its own IP address) that will serve STA11. To balance the communication load, STA11 can have several network nodes such as TN41, TN42 (not shown), etc, to be its proxies in parallel.
In fact, the resulting connection between STA11 and TN41 can be seen as a layer 2 (MAC) connection, on top of which the communication is performed. In this setup, TN41 serves as the default gateway of STA11, and optionally can run a DHCP server and a NAT server.

Executing the Invention over a Peer-to-peer network

Another novel aspect of the above novel methods takes advantage of the fact that the wireless network is local in nature, as the APs are geographically adjacent. The system and method as described in this disclosure allows GN21 to be responsible over

a small geographical area with little interaction with its neighbors. As a result, the methods that are disclosed can be implemented by many small devices forming a peer-to-peer network that implements the methods, without the need to rely heavily on large servers.

Many nodes GN21, GN22 (not shown), can each control a group of APs. To make the system grow "automatically", it is possible to give users a "base" that will act as their point of presence in the network. For example, the base can assume the role of TN41 as a Mobile IP proxy. The base can connect to the wired network at the premises of the customer. Some bases will assume the role of a GN, where the GNs can be managed by either a network control center, or through peer-to-peer protocols.

In early stages of deployment of the system, when there is still a small number of GNs, each GN might need to cover a large number APs. A general server can back-up all information that the GNs hold. To avoid the situation, where a single GN needs to cover a huge number of APs with pseudo-beacons, the system might not use the pseudo-beacon mechanism (although, it should be noted that with moderate computing power and network resources, a GN might be able to cover a few thousands of APs). In the worst case scenario of a peer-to-peer network, there is one base (GN) for each STA, and this GN act as the GN for the APs in the proximity of the STA. When the STA moves, the coverage area in the responsibility of the GN moves with it. In this case, the GN can fetch information on neighboring APs from the general server. When GN abandons an AP, it can store the information it gathered about it in the general server, for later use by possibly other GNs. In a system which is not based on many small GNs, a large GN can assume the role of the smaller GNs.

It should be noted that it takes some time to gather the information on the APs (such as timing, default gateways, etc). However, once a single STA passes in an area, it obtains the needed information. This information is later stored in the GNs and general server, for the benefit of all STAs in the future.

If a STA needs to handover into an AP which has no STAs currently in it, it might not have the needed resources pre-allocated (such as an associated MAC address and IP address), and might therefore need to gain it by itself. However, in many cases the

STA can obtain resources at one pass in the area, and these resources (such as IP address) will stay for the next pass in the area (which can be hours later).

An Alternate Fast Method for Connecting to an AP – Removing the Assumption on the Existence of STA12 in the Coverage of the new AP

The drawback of the above method of fast handover is that it requires that the pool of resources that GN21 holds should contain a valid IP address of the AP that STA is handing over to. If the DHCP lease time is long enough, having a valid IP might not be a problem, but on short lease times with only a few STAs roaming it is desirable to perform handovers even if there is no valid IP available in the pool. Unfortunately, a typical execution of the DHCP protocol can take several seconds to complete, which might be too long for a fast handover. Interestingly, we observe that many APs will forward information even if the IP that is being used was not allocated by DHCP.

Therefore, we disclose the following method:
Choose a MAC and associate it with the AP (or use an Associated MAC without an associated IP address), choose a random (but valid) IP address, and use it. The STA must use the correct default gateway settings of the AP (these settings can be stored in GN21). If the STA wishes to use DNS, it must have the DNS settings of the AP (which can be received from GN21), or DNS services are provided through GN21.

Choosing a valid IP at random results in a very low probability of colliding with another IP address that is used in the AP.
Note, however, that the STA still needs to authenticate/log-in through the captive portal in case such portal exists.

Another method that can be used to quickly obtain an IP address, such that the IP address is not already allocated by the DHCP of the AP is disclosed. Most DHCP implementations of AP send an ICMP (Internet Control Message Protocol) Echo Request (ping) before allocating an IP address, to make sure that it is unused. Therefore, STA can begin the DHCP protocol, then, wait for the ICMP echo request that the AP sends, and understand the IP that is going to be allocated to it. Therefore, STA can start using the IP address and respond to the ICMP echo request. It can then

prematurely terminate the DHCP protocol (as it already got an IP). Alternatively, STA can use the IP address from the ICMP echo request without responding to it, and complete the DHCP process. If the IP address that is allocated during the DHCP is identical to the IP address (vast majority of cases), then STA simply saved time. Otherwise, it can move from the IP address of the ICMP echo request to the IP address that was allocated.

If no connection to GN21 is available, the default gateway address can be guessed, as in the majority of the cases the default gateway address is one out of only a few addresses. Common addresses are: 192.168.1.1, 192.168.2.1, 10.0.0.1, etc. Moreover, the default gateway is usually the AP itself. Its MAC address is known (as it is broadcasted in the beacon). Therefore, in most cases it is enough to forward packets to this MAC address (without knowing its IP address).

A STA with a Capability to Connect on Two Channels in Parallel

We disclose a STA which has a capability of communicating in two or more channels in parallel (for example, by using two wireless network cards). This capability can enable a STA to be connected to two APs in parallel without the need to implement sophisticated mechanisms that actually simulate this situation. Thus, a STA can connect with future AP while maintaining a connection through its serving APs. Being connected to two APs simultaneously allows greater bandwidth by utilizing two connections instead of one, and soft-handovers, i.e., the STA stays connected through one AP, while disconnecting from the second AP in the process of handover.

We Claim:

1. A system and method for fast handovers in unmanaged wireless networks where the process of the handover is almost completed before the handover actually started.

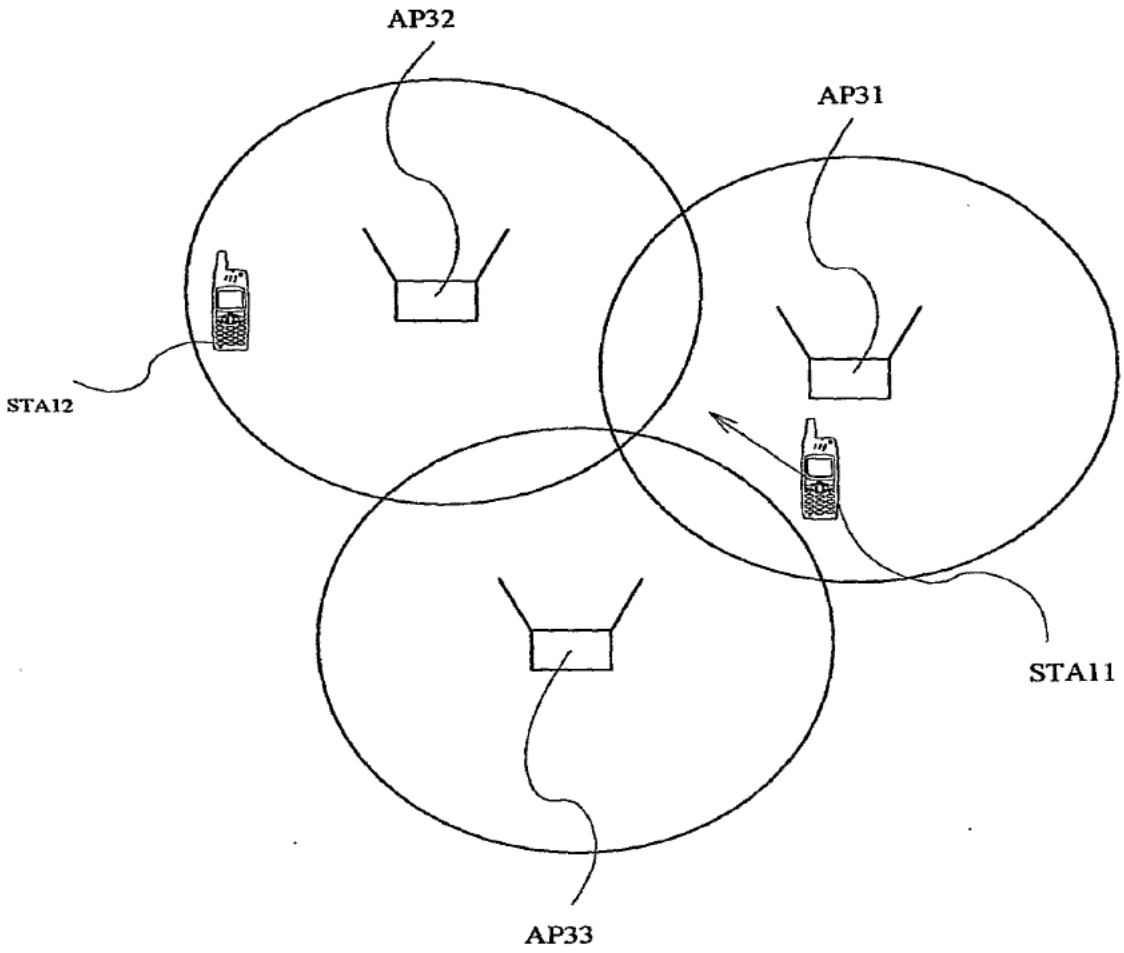


FIG.1

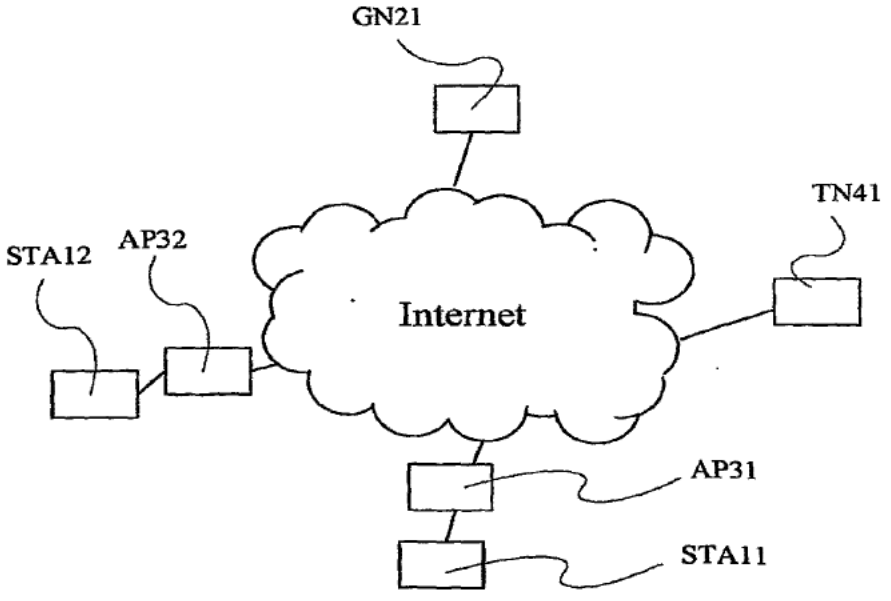


FIG.2

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/IL2007/000244

International filing date: 22 February 2007 (22.02.2007)

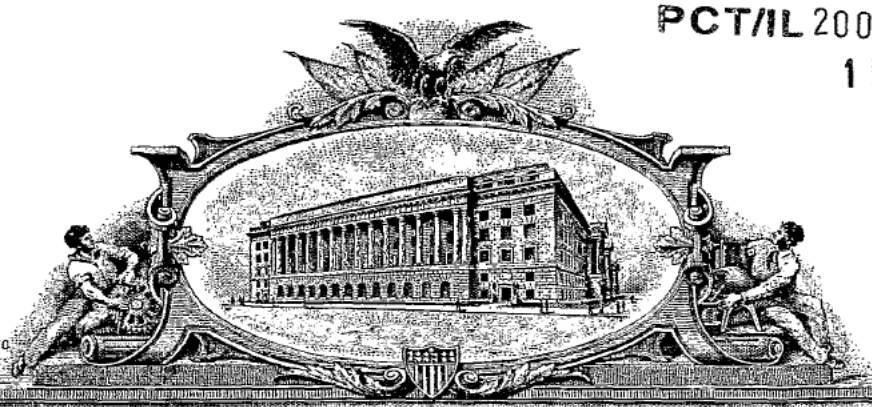
Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/794,135
Filing date: 24 April 2006 (24.04.2006)

Date of receipt at the International Bureau: 23 May 2007 (23.05.2007)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse



PA 1600860

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

April 23, 2007

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/794,135***
FILING DATE: ***April 24, 2006***

THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS ***US60/794,135***

By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office

L. Edelen

L. EDELEN
Certifying Officer

PTO/SB/16 (10-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 1 of 2

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. FEDEX 8547 7694 7226

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
ELAD	BARKAN	KFAR-SIRKIN, ISRAEL

Additional inventors are being named on the _____ *separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max):

WIRELESS INTERNET SYSTEM AND METHOD

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ The address corresponding to Customer Number:

OR

☑ Firm or Individual Name ELAD BARKAN

Address 12 HABANIM St

City	KFAR SIRKIN	State		Zip	49935
Country	ISRAEL	Telephone	972-54-520-4121	Email	MOTI@BARKAN.ORG

ENCLOSED APPLICATION PARTS ***(check all that apply)***

☐ Application Data Sheet. See 37 CFR 1.76
☐ CD(s), Number of CDs _____
☐ Specification *Number of Pages* _____
☐ Other (specify) _____
☐ Drawing(s) *Number of Sheets* _____

Fees Due: Filing Fee of $200 ($100 for small entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

METHOD OF PAYMENT OF THE FILING FEE AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT

☑ Applicant claims small entity status. See 37 CFR 1.27.
☐ A check or money order is enclosed to cover the filing fee and application size fee (if applicable).
☑ Payment by credit card. Form PTO-2038 is attached

100.00
TOTAL FEE AMOUNT ($)

☐ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: _____. A duplicative copy of this form is enclosed for fee processing.

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/16 (10-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☑ No.
☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

SIGNATURE E. Barkan Date APRIL 20, 2006

TYPED or PRINTED NAME ELAD BARKAN REGISTRATION NO. _____ *(if appropriate)*

TELEPHONE +(972)-54-520-4121 Docket Number: _____

Provisional Application For Paten

Title: Wireless Internet System and Method

Date: April 20, 2006

Inventor: **Elad Barkan**

12 Habanim St.
Kfar Sirkin 49935
Israel

Tel: +(972)-54-520-4121
Fax: +(972)-3-933-2284
Email: moti@barkan.org

Wireless Internet System and Method

Technical Field

This invention concerns a method and a system for wireless communications. In particular, it concerns systems for providing wireless internet connection to roaming devices, such as Portable Computers, laptops, PDAs, and phones, and the deployment of such a wireless connection in a viral method, in such a way that the existing access points are not changed.

Background Art

Currently, there is a growing number of WiFi public hot-spots (or Access Points – "AP"). These APs allow WiFi enabled devices (which we refer to as STA) that are in their coverage area to connect to the internet.

Some of the APs are operated as a business, service, or as part of a community, either with or without a charge to the STA's user. Other APs are placed by individuals in their premises, but are not "locked", i.e., they are "open", allowing bypassing STAs to utilize them. Other APs placed by individuals are "locked" (or "closed"), thus not allowing passing STAs to utilize them.

As APs are being deployed in larger numbers, many individuals lock their APs due to fear of unfair use of their network resources, and due to security concerns. For instance, there have been cases where a person places an open AP, and his neighbor uses this AP as its internet connection on a full-time basis without the consent of the first person, thus abusing and degrading the service of the first individual. In other cases, the neighbor hacked into the computer of the first person through the network. Thus, as time passes, most APs are either locked, or a payment is required to use them. Although the total number of APs and their area of coverage is growing fast, an even larger number of APs are becoming locked and inaccessible to roaming STAs.

An interesting recent approach for allowing roaming customers to access the internet is taken by Fon (www.fon.com). It allows individuals to download a new software into their APs, which makes their APs a pay for use APs, and in addition, they receive a username and password for free access to other APs which are operated by Fon or

utilize their software. It also allows users to enjoy from a portion of some of the payments made by other users to use the network.

Roaming STAs are forced either to find an open AP, find an AP for which they have an account, or pay for access in case there is a pay-for AP.

It is an aim of the current disclosure to provide a system and a method for deployment of APs for the purpose of connecting STAs to the Internet.

Roaming customers that connect to an AP are often far from the AP and have borderline reception conditions. As a result, the connection quality is very poor, and the user may experience a slow service or no service at all.
It is another aim of the current disclosure to provide a system and a method for improving the connection quality for roaming STAs.

Brief Summary of Invention

The invention is described by way of example, but it should be obvious to those skilled in the art that many variations follow.

One of the novel methods behind the deployment of APs is that devices function at the same time as STAs and as APs. For example see Figures 1 and 2, a laptop 11 is connected to the Internet through access point AP 10, and at the same time, laptop 11 shares its connection for other STAs by operating as an AP. Thus, other STAs 12 and 13 see laptop 11 as an AP, and can connect through it to the Internet.

Another novel method in the current disclosure is that the laptop 11 limits the set of addresses or internet sites that STAs 12 and 13 can access, but the set of addresses includes a special web site 30 from which STAs 12 and 13 can download software 31, where software 31 is a software that includes the functionality of the software of laptop 11. Once STAs 12 and 13 download and execute the software 31, laptop 11 allows them a wider access to the internet. As a result, STAs 12 and 13 must download and run the software 31 to get wide access to the internet. As STAs 12 and 13 run software 31, they become APs in their own right, and allow other STAs to

download and connect through them to the internet in the current location of STA 12 and STA 13, as well as in any other location they go.

Another novel method of the present disclosure allows STA 14 (Fig. 2) to connect through two or more APs simultaneously. For example, STA 14 connects through both laptop 11 and laptop 21 to the internet. Thus, STA 14 can enjoy a more stable connection even if both connections (through laptop 11 and 21) are in borderline quality. Furthermore, even in case the connections are not borderline, they can be used to provide STA 14 a broader connection to the internet, or balance its traffic such that laptop 11 and laptop 21 carry a lighter burden per laptop with regards to the extra bandwidth they carry due to STA 14.

Multiple connections also allow handovers, as if a STA is moving from one place to the other it can first establish a new connection and then the old connection is terminated, practically leaving the STA connected.

In a further development of the novel method, laptop 21 can connect with laptop 11 directly or through STA 14, such that both enjoy the internet connection of the other. As the internet connection is not used all the time (typical laptop uses on average a few percents of its maximum bandwidth), both laptops will experience a much faster connection to the internet.

Another important issue is the security of the system. Laptop 11 might agree to act as an APs, but it does not agree to allow STA 13 and STA 14 (Fig. 2) to access its inner network (i.e., it allows STA 13 and STA 14 to access the internet *through* its network but does not allow them to access *into* its network. For example, a private server 40 [Fig. 2]) should not be accessible to STA 13 and STA 14. On the other hand, STA 13 wish to use laptop 11 network, but might not wish laptop 11 to be able to tap into its communications. The current disclosure provides novel method to deals with these two problems.

First, external STAs are not allowed access to the inner network by not allowing access to local IP addresses. Second, STA 13's privacy is protected by tunneling his

sensitive traffic to a trusted network site 50 (Fig. 2), and STA 13 accesses the internet through his tunnel to the trusted network site 50, which acts as a proxy of STA 13.

An important issue is to prevent STAs from using other laptops for their primary network connection for a long period of time. A novel method detects that a STA is connected to the internet through the same laptop for a long period of time, and disconnects the STA. Alternatively, the STA needs to pay to continue and use the network, thus encouraging the STA's user to purchase his own connection.

In yet another novel method, the software 31 running on laptop 11 can replace the commercial banners that appear in the web pages that laptop 11 surfs into, as well as the web pages that STA13 surfs into. The banners can be stopped, replaced, and made specially targeted to the user, for example based on his location.

A further novel method is that the wireless internet coverage that is obtained using laptops can be used by devices such as wireless IP phones to make phone calls using the wireless internet coverage, cellular phones that have built-in WiFi connection, or digital cameras with WiFi that wish to upload the data stored in them. Other devices might include for example, radio or TV broadcast capabilities.

Another novel method relates to the configuration of the wireless network. The configuration, and especially the security configuration of a wireless internet connection such as WiFi is cumbersome and annoying to most users. Assume STA 12 belongs to the same user (or user group) of the owner of laptop 11. Then, by a special logging into website 30, the configuration of laptop 11 can be copied to STA 12, thus configuring it to use AP 10 (i.e., allowing a connection without laptop 11).

Another novel method allows devices with a trusted hardware to receive information that instructs them how to directly connect to AP, by providing them with the needed settings and security information.

Brief Description of the Drawings

The invention will now be described by way of example and with reference to the accompanying drawings in which:

Fig. 1 illustrates access point AP 10 connected to the internet, a laptop 11 is connected to AP 10, and two other stations STA 12 and STA 13 are connected through laptop 11 to the internet. A special web site 30 is also depicted.

Fig. 2. includes Fig.1., and in addition it illustrates another access point AP 20, with laptop 21 connected to it. STA 14 is connected to both laptop 21 and laptop 11, STA 15 is connected to laptop 11, and also depicted is a trusted site 50 connected to the internet.

Mode of Carrying out the Invention

A preferred embodiment of the present invention will now be described by way of example and with reference to the accompanying drawings.

Having a single laptop connected to the internet and serve as an AP in the same time

One of the novel methods performing the deployment of APs is that devices function at the same time as STAs and as APs. For example, a laptop 11 is connected to the Internet through access point AP 10, and at the same time, laptop 11 shares its connection for other STAs by operating as an AP. Thus, other STAs 12 and 13 look at laptop 11 as an AP, and can connect through it to the Internet.

When laptop 11 is connected to AP 10 through a wired connection, it can simply set its wireless connection as an AP (Infrastructure mode). However, when laptop 11 is connected to AP 10 through a wireless connection, the situation is more complex. We disclose a novel method that laptop 11 can be connected to AP 10 and serve as an AP using only a single wireless network card. Laptop 11 connects to AP 10 just like any other STA, and at the same time runs the protocol stack of an AP. AP 10 use the same channel as AP 10, and transmits a beacon message such that the beacon of AP 10 and

the beacon of laptop 11 are expected not to collide in time. AP 10 derives and updates its internal clock from AP 10, but adds a constant delay (to make his beacon appear with a delay after AP 10). In another embodiment, laptop 10 does not add a delay to the time of AP 10, but sets the beacon period to a value, such that the greatest common denominator (GCD) between its beacon period and the beacon period of AP 10 is the smallest that is possible. Such a choice of beacon period ensures minimal collisions between the beacons.

Viral Spreading

Many networks suffer from the network effect, in which the initial users have no incentive to join the network. However, the network is of great value once many users are in the network.

The following method and system attracts the initial users, and provide an increasing value as the network grows. The first very few laptops with the software are installed and deployed in key areas by the network initiator. The software running on the laptop 11 has functionality 31 as follows (explained through an example):

Laptop 11 acts as an AP and allows other STAs to connect to it. To further lure STAs, the SSID (Service Set Identification – this is the name of the network that users see when looking for an available network) can be set to "Free Internet" or another name that will attract roaming laptop users to log-into it while searching for wireless networks.

Assume a user using a laptop called STA 12 connects as described above. Once STA 12 is connected to the laptop 11 (as an AP), no matter which web site the user tries to enter, the software on laptop 11 forwards the connection to a special web site 30. The web site 30 informs the user (STA 12) that in order to use the free connection it must install a software with functionality 31. The deal is that the user is allowed the free access at this location, but it is requested to share his own connection when such a connection is available. The user then downloads and installs the software with functionality 31. Once laptop 11 identifies that STA 12 has functionality 31 running, it allows it a wider access to the internet (or a full access to the public internet).

Thus STA 12, which originally did not have functionality 31 running, but its user wished to connect to the internet, ended up with functionality 31 installed and running on STA 12, and the user received a working internet connection. When the user moves STA 12 to another area in which it connects directly to an AP (which might be locked), it shares its connection with other STAs, which are also motivated to install functionality 31. Thus, functionality 31 can spread quickly among STAs, and the total area that is served grows larger, where each additional STA spreads the network further.

Connection through multiple access points

Another novel method of the present disclosure allows STA 14 to connect simultaneously through two or more APs. For example, STA 14 connects through both laptop 11 and laptop 21 to the internet. Thus, STA 14 can enjoy a more stable connection even if both connections (through laptop 11 and 21) are in borderline quality. Furthermore, even in case the connections are not in borderline quality, they can be used to provide STA 14 a broader connection to the internet, or balance his traffic such that laptop 11 and laptop 21 carry a lighter burden per laptop with regards to the extra bandwidth they carry due to STA 14.

Multiple connections also allow handovers. When a STA is moving from one place to another, it can first establish a new connection and then the old connection is terminated, practically leaving the STA connected.

When laptop 11 and laptop 21 use the same channel, STA 14 connects to both laptops by creating two protocol stacks on the MAC (Media Access Control) layer. When laptop 11 and laptop 21 operate on different channels, STA 14 agrees with laptop 11 and laptop 21 on period of times in which laptop 11 sends packets to STA 14, and periods of time in which laptop 21 sends packets to STA 14. STA 14 makes sure that these periods of times do not overlap, thus, STA 14 sets the channel according to the period, such that it listens on the channel of the laptop that might transmit to it. If the laptop has packets pending for STA 14 it queues them for transmission in the transmission period.

In order to have a faster connection through the two (or more) connections, STA 14 downloads/uploads some of the information through one connection, and the rest through the other connection. For example, when downloading a web page, STA 14 can download the text through one connection, and download the images through the other connection.

In another embodiment a remote site 50 with a fast internet connection acts as a proxy of STA 14. Incoming and outgoing packets are forwarded between STA 14and remote site 50. The packets are sent using error-correction codes that allow reconstructing the data even if some packets are lost on one connection, but reach the destination using the other connections. The role of remote site 50 can be assumed by a service provider, by computer with a software that the user installs in his premise, or by another user with high bandwidth.

When the STA moves from one location to another, new connections are being established, while others are being disconnected. However, as long as there is at least one active connection, the STA will stay connected to the internet continuously and seamlessly.

Sharing Internet Connection between Laptops

When laptops 21 and 11 are within radio (wireless) contact (or through the mitigation of other STAs), each laptop can treat the other as another connection at his disposal. Thus, the data rate can be significantly extended, much like the case with a STA connected to two laptops.

Security

Another important issue is the security of the system. Consider a situation in which laptop 11 agrees to act as an APs, but it does not agree to allow STA 13 and STA 14 to access his inner network (i.e., it allows STA 13 and STA 14 to access the internet *through* his network but does not allow them to access *into* his network. For example, a private server 40 should not be accessible to them). On the other hand, STA 13 wishes to use laptop's 11 network, but might not wish laptop 11 to be able to tap into his communications. The current disclosure deals with these two problems in a novel method. First, external STAs are not allowed to access to the inner network by not

allowing them to access to local IP addresses. Second, STA 13's privacy is protected by tunneling its sensitive traffic to a trusted network site 50, and STA 13 accesses the internet through its tunnel to the trusted network site 50, which acts as a proxy of STA 13.

To prevent STAs from accessing the inner network, laptop 11 blocks all traffic from the STAs to internal addresses (i.e., addresses that appear only in local networks and not in the public internet, such as 192.168.*.*, or 10.*.*.*, and 172.16.0.0 - 172.31.255.255). Another method, which can be applied independently, is to allow the connection if it is at least x hops into the internet, where x is the maximum number of hops in the local network (which can be discovered by performing a traceroute command). Another method is to allow access to addresses which have an IP address with a different prefix, as internal networks typically have the same prefix on the IP address.

To protect the privacy of STA while it is surfing, its traffic can be tunneled to a trusted network site 50, which acts as its proxy. The network site can be replaced by simply tunneling the connection to another node in the network, and switching the network node once in a while. The access to the remote nodes is made without identifying the STA, but only proving that it belongs to the group of STAs, thus, its privacy is preserved. The frequent switching of remote nodes eliminates the possibility that a remote node can gather a significant amount of private information from peeking into the communication. The list of available remote nodes can be kept by a directory service, which can be distributed in a peer-to-peer fashion.

In another embodiment, the remote node is a trusted computer installed by the user. Such a configuration has the added benefit that the user can access internal nodes in his own private network, effectively having a Virtual Private Network (VPN) with his home network.

Maintaining Fairness

It is desirable to avoid an unfair situation in which one user exploits the network by continuously using a connection without ever sharing a connection. If many users

follow these lines, the network experience will degrade as there will be only a small number of laptops connected directly to APs.

A novel mechanism detects that a STA is connected to the internet by noting that the same STA (using the same laptop) connects from the same small area (or through the same AP) for a long period of time (i.e., beyond a threshold). For example, this threshold can be set to two weeks. Once a STA passes the threshold, the functionality 31 notes the user that the threshold is reached. The user is then required to move to another area or pay a small fee to continue and access the AP.

Functionality 31 may note the user when the threshold is being approached, even before it actually reaches it. It can then give a pre-warning to the user.

The laptop is identified through his account information, through the MAC address of his network card, and other machine-specific information, such as the serial number of the hard-disk.

Control over advertisements

A novel method disclosed is that the functionality 31can scan the web pages that passes through it and block or replace the advertisements on the page depending on various data such as the user name, the user location, etc. The advertisements can be performed in collaboration with the web site that is being surfed into, or without.

The site 30 can instruct functionality 31 as to which advertisements should be removed or changed, and which advertisements should be placed. New advertisements can also be added in places that there were no advertisements to begin with.

Configuration of Wireless Networks

An annoying task associated with wireless networks is the configuration of a STA to work with a network. The security settings are especially annoying, and currently, most of the people avoid securing their network due to the cumbersome setting procedure.

A novel method is disclosed to perform easy configuration of a wireless settings. The method is composed of two parts, the first is establishing the settings for the first

device, and the second part is establishing the settings for the rest of the devices. First part: Assume a user on laptop 11 is connected to his wireless AP 10. If AP 10 is not set to use encryption, the user can ask (or be offered) to secure his network. Functionality 31 automatically accesses the interface of AP 10 and configures it with security settings. Laptop 11 is also set with the security settings. The settings are also stored in an account in web site 30, for future use. Site 30 can also provide functionality 31 with the information on how to set the security setting on the specific model of AP 10.

Second part: When the user uses another device STA 12, he connects to the network through functionality 31 on laptop 11, which redirects him to web site 30. On the site, he can log-in using his account details. Web site 30, through functionality 31 which is running on laptop 11, discovers that the two devices (laptop 11 and STA 12) are both connected through AP 10, and both belong to the same user account. As a result, web site 30 offers the user to reconfigure STA 12 to work directly with AP 10. The user is advised to download functionality 31 to STA 12, and run it. Once functionality 31 is running on STA 12, it configures STA 12 with the settings of the network (which are retrieved from web site 30).

Many variations can follow to the above procedure, and should be clear to those skilled in the art. For example, the settings may be stored on laptop 11 instead on web site 30, the settings may be encrypted, and the sequence of events can be changed. The result is an easy configuration of the network by the user.

A network infrastructure for other devices

Functionality 31 may allow devices that do not have the functionality 31 to access the network. Such a device receives a capability to be identified as eligible to access the network towards functionality 31, and it identifies as eligible to access towards functionality 31 on the laptop in order to gain access to the network. Such identification may include cryptographic means, such as a digital certificate signed by an appropriate certification authority (CA) which gives the device the capability to be identified.

Configuration of secure devices

It might be desirable to allow a device to directly connect to an AP, rather than connect through a laptop. When devices have a secure sub-system, i.e., a sub-system that is trusted by web site 30, web site 30 may allow it to retrieve the settings of the network (assuming that they are stored on web site 30), and configure the device to use the network.

As the device has a trusted sub-system, the settings can be stored in the sub-system, such that they do not leak outside.

Alternatively, functionality 31 can reconfigure the AP to allow access to a roaming device.

Displaying the coverage map

A problem often faced by users that wish to connect through wireless internet is that they cannot connect to the internet in their current location because the coverage in their area is locked, and they do not have access rights. A novel method and system helps users find the nearest location from which they can connect. Web site 30 holds a list of all access points from which users can successfully connect, together with all the list of APs from which are closed. The list includes the MAC address of each AP. Parts or all of this list can be downloaded in advance to a device, such as into laptop 11. Then, laptop 11 uses the beacons of the APs which might be locked to determine its position (for example, www.SkyHookWireless.com uses beacons to determine the location of a STA). Then, laptop 11 can display on a map the location of the user, and the locations of near by access point in which it can connect to the internet. The user can then go to the nearby locations and connect to the internet. The list in site 30 can be constantly updated by information that STAs receive.

In another embodiment, the list of APs in site 30 can also hold the probability that the AP is accessible. The probability can change if the access is provided by a laptop rather than an AP, and the laptop may be present or not. An area covered by several independent APs, each with low probability, results in an area with higher probability of accessibility in the intersection of these areas. The probability of accessibility can be depicted in the map shown to the user, for example, by different colors representing the different probabilities.

Claims

1. In wireless internet system, a device that operates as a STA and as an AP in the same time.
2. The device in claim 1, where the device contains a functionality that:
   a. connects stations on its AP interface to the internet on its STA interface;
   b. limits the scope of the internet that can be accessed by stations on its AP interface, and broadens this scope for a specific station if the station proves to be running the functionality;
   c. the limited score of internet includes access to a special site;
   d. a software with the functionality can be retrieved from the special site;
3. The device in claim 2, where the device can connect to more than one other such device in the same time.
4. The device in claim 2, where the device does not allow access of stations to its inner network.
5. The device in claim 2, where the device is also capable to connect to another laptop.
6. The device in claim 2, where the special site or functionality detect the fact that a device uses an AP beyond a certain threshold, and limit the scope of the internet connection once the threshold is met.
7. The device in claim 2, where the functionality can remove or replace the advertisements from the traffic.
8. The device in claim 2, where the functionality allows devices that lack the functionality to have a broader access to the internet.
9. The device in claim 8, where the functionality allows the broader access to device that lack the functionality only if they perform identification, which might include cryptographic means.
10. The device in claim 2, where the functionality includes the ability to reconfigure the settings of the wireless network in the AP or on the machine that it runs on.
11. The device in claim 9, where devices that do not have the functionality can receive network settings and connect directly to the AP.

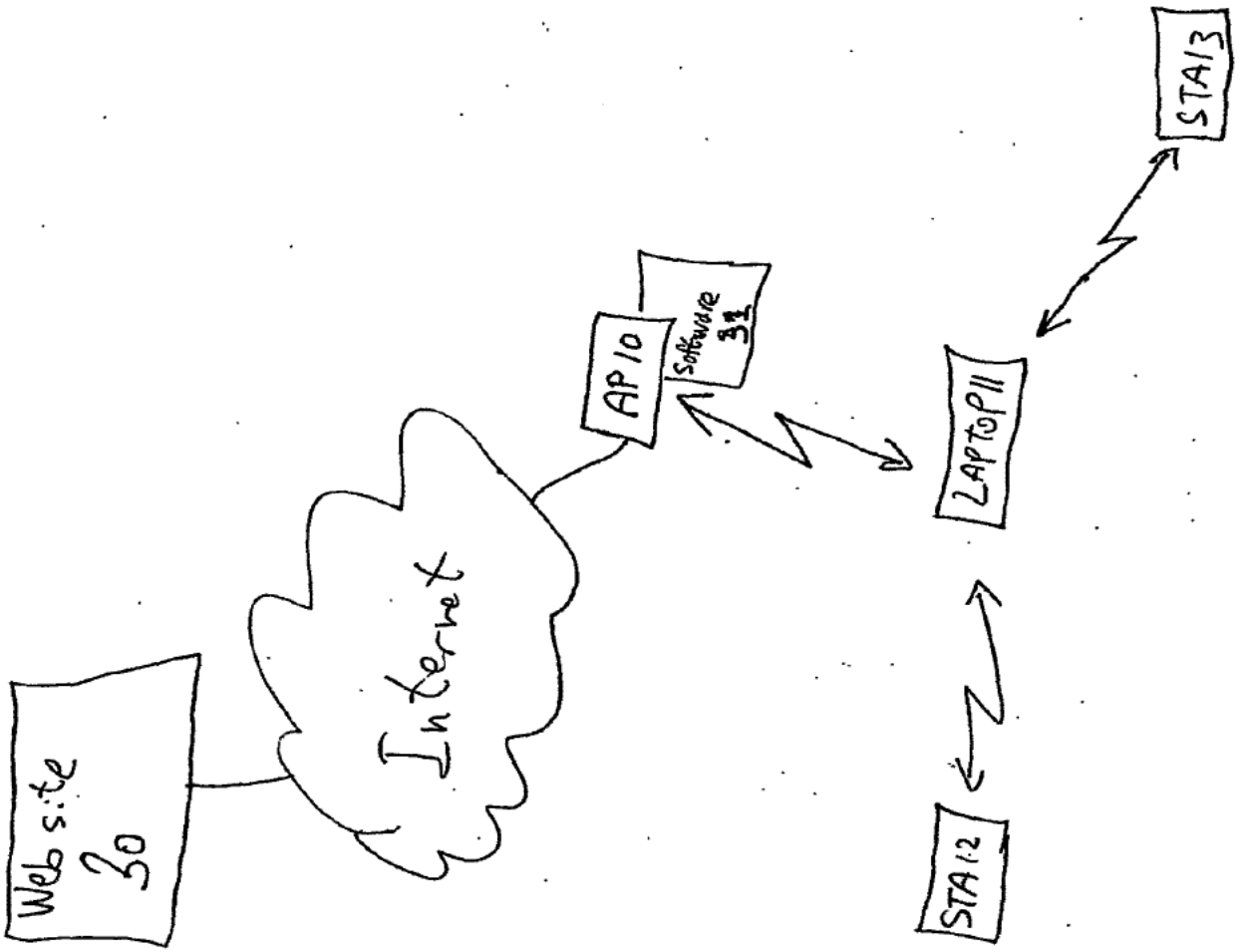


FIG 1

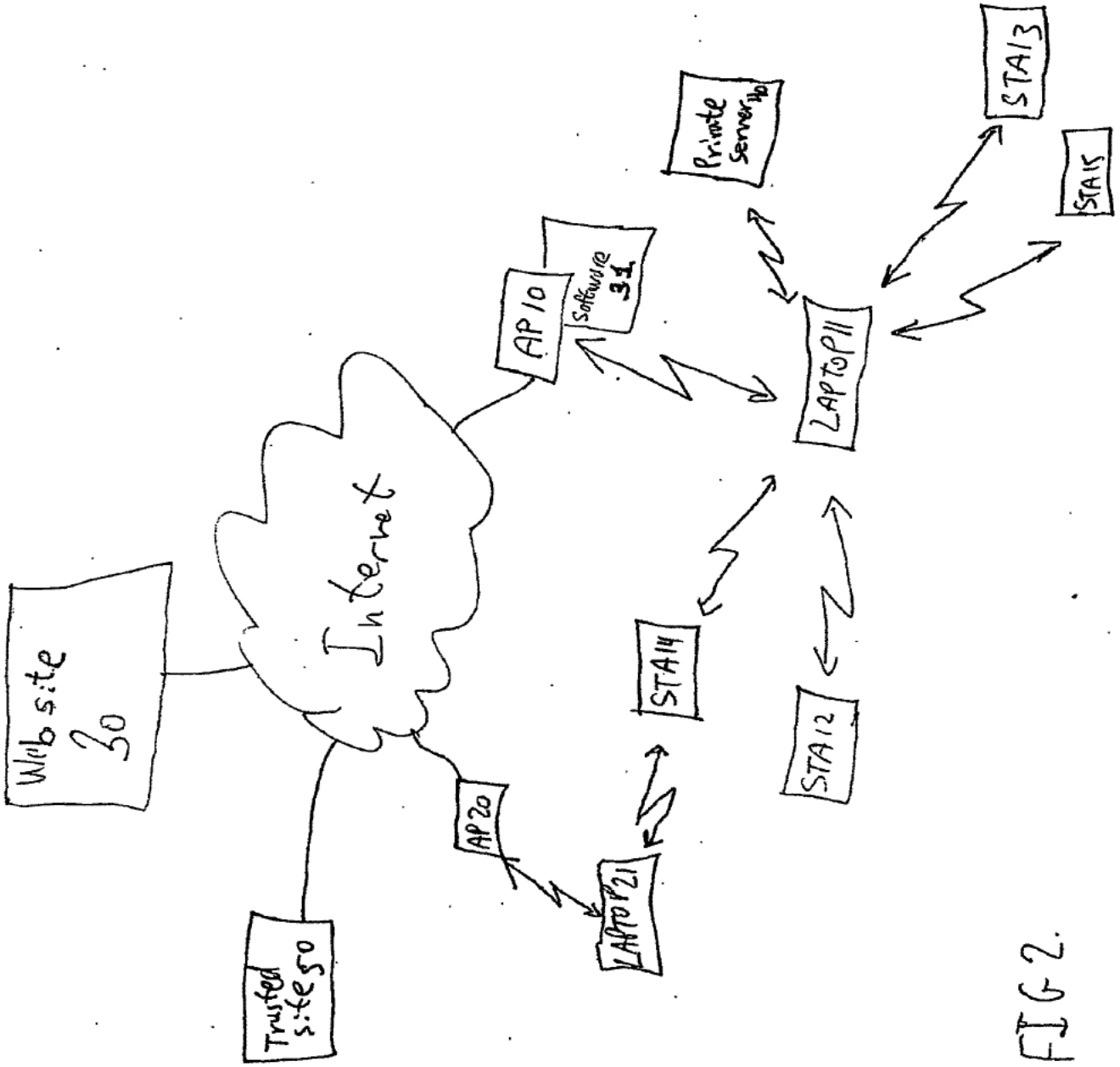


FIG 2.

BEST AVAILABLE COPY

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/IL2007/000244

International filing date: 22 February 2007 (22.02.2007)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/775,321
Filing date: 22 February 2006 (22.02.2006)

Date of receipt at the International Bureau: 23 May 2007 (23.05.2007)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PA 1600860

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

April 23, 2007

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/775,321***
FILING DATE: ***February 22, 2006***

THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS ***US60/775,321***

By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office

L. Edelen

L. EDELEN
Certifying Officer

PTO/SB/16 (10-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 1 of 2

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. FEDEX 8547 7688 0082

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
ELAD	BARKAN	KFAR-SIRKIN, ISRAEL

Additional inventors are being named on the _____ *separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max):

FAST HANDOVER IN WIRELESS NETWORKS

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ The address corresponding to Customer Number: _____

OR

☑ Firm or Individual Name ELAD BARKAN

Address 12 HABANIM St.

City KFAR-SIRKIN | State | Zip 44935

Country ISRAEL | Telephone +972-54-5204n | Email MCTIP@BARKAN.ORG

ENCLOSED APPLICATION PARTS ***(check all that apply)***

☐ Application Data Sheet. See 37 CFR 1.76
☐ CD(s), Number of CDs _____
☐ Specification *Number of Pages* 27
☐ Other (specify) _____
☐ Drawing(s) *Number of Sheets* 1

Fees Due: Filing Fee of $200 ($100 for small entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

METHOD OF PAYMENT OF THE FILING FEE AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT

☑ Applicant claims small entity status. See 37 CFR 1.27.
☐ A check or money order is enclosed to cover the filing fee and application size fee (if applicable).
☑ Payment by credit card. Form PTO-2038 is attached
☐ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: _____. A duplicative copy of this form is enclosed for fee processing.

100.00
TOTAL FEE AMOUNT ($)

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PROVISIONAL APPLICATION COVER SHEET
Page 2 of 2

PTO/SB/16 (10-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☑ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

SIGNATURE E. Barkan Date Feb 20, 2006

TYPED or PRINTED NAME ELAD BARKAN REGISTRATION NO. _____ *(if appropriate)*

TELEPHONE +(972)-54-520-4121 Docket Number: _____

Provisional Application For Paten

Title: Fast Handover in Wireless Networks

Date: February 20, 2006

Inventor: **Elad Barkan**

12 Habanim St.
Kfar Sirkin 49935
Israel

Tel: +(972)-54-520-4121
Fax: +(972)-3-933-2284
Email: moti@barkan.org

Fast Handover in Wireless Networks

Technical Field

This invention concerns systems and methods for fast handovers in wireless networks such as 802.11 networks, specifically in un-managed wireless networks, and more particularly such systems and methods which allow extremely fast handovers in these networks without any changes to existing 802.11 base stations. The invention also concerns efficient performance with regards to power consumption, coverage, security, installation, capacity and availability of wireless networks such as 802.11. The invention can achieve these goals without any change to the WiFi access point.

Background Art

Currently, there is a growing number of WiFi public hot-spots (or Access Points – "AP"). These APs allow WiFi enabled devices (which we refer to as STA) that are in their coverage area to connect to the internet.

Some of the APs are operated as a business, service, or as part of a community, either with or without a charge to the STA's user. Other APs are placed by individuals in their premises, but are not "locked", i.e., they allow bypassing STAs to utilize them. The cumulative connectivity provided by the APs is enormous and growing fast, thus, it is tempting to use this cumulative connectivity to compete with other wireless technologies. For example, it would be tempting to have a STA that looks like a cellular handset, where the WiFi handset uses the free connectivity to provide a "free" service that competes with or complements the cellular service.

One of the major difficulties of achieving this vision is that the coverage of a single WiFi AP is very small (about a few hundreds meters). When a user goes out of this area, his connectivity is lost. A natural approach to solve this problem is performing a *handover* (sometimes also called *handoff*) to another AP with a better radio connection to the user. Another approach is to have a handset which supports both WiFi and Cellular, and handover the conversation from WiFi to Cellular [See: WO 2004/036770], this way, WiFi extends the coverage of cellular, and conversation is handed over from WiFi to cellular, when there is no WiFi coverage. However, the

problem of performing handover between one WiFi AP to another WiFi AP remains when appropriate cellular coverage is not available (or there is no cooperation from the cellular company). The same idea applies when cellular is replaced by other access technology, such as satellite communications.

The concept of handover is taken from cellular networks. Handovers usually work well in *managed* networks, such as cellular networks, campuses, or office environment., where the entire network is usually owned by the same operator. The network operator in many cases chooses to add cells where coverage or capacity are needed. In managed networks, the APs (or the cellular cells) are synchronized and communicate with each other, and are usually controlled by some other network entity. For examples, the APs can communicate with each other, for example using the IEEE 802.11F protocol – the Inter-AP protocol, which involves a RADIUS (Remote Authentication Dial In User Service, see RFC 2138, 2865, and 2866) server. The APs can also employ a radio resource management such as IEEE 802.11K, or fast roaming using IEEE 802.11R, etc. However, in *unmanaged* networks, the APs can be deployed by many unrelated entities, such as by private individuals. There is usually no entity that synchronizes the APs. The APs can be manufactured by various manufacturers, use various security mechanisms etc. In unmanaged networks, the handovers are typically very slow, as in the process of handover, it takes time for the STA to re-connect to the internet in the new AP (and it must disconnect from the previous AP). In such a handover in an unmanaged network, the IP address often changes, therefore, a mechanism such as mobile IP must be used (as described later). This mechanism is limited with respect to the frequency in which the IP address can change, and a large latency (disconnection time) may result during the handover process. During the latency, the STA cannot receive any incoming messages.

A handover process is typically composed of the station STA connecting to a new AP, and disconnecting from the old AP. If STA is connected in parallel to both AP the handover is called *soft-handover*, and if STA first abandons the old AP and then connects to the new AP, the handover is called a *hard-handover*. Soft handovers require the ability of STA to communicate in parallel with at least two APs.

The process of connecting to a new AP is usually composed of the following steps.

1. STA performs a scanning process to discover neighboring APs.
2. STA chooses a new AP, and performs *authentication* with the AP, in which the AP verifies that STA is allowed to access the AP.
3. If the authentication is successful, STA performs an *association* process, in which the AP acknowledges that STA is connected to it (association requires the AP to allocate resources to the STA, and the 802.11 standard allows up to 2007 STAs to be associated with an AP).
4. Once STA is associated with the AP, the STA makes sure that it has all the information that it requires to communicate over the internet, for example, it must have an IP address, and it must update servers that govern its location (such as Mobile IP, as discussed later). In some cases, the user should go through a second authentication procedure (usually with a RADIUS server). Many times, this procedure is performed over a web interface, which is called a *Captive Portal*.

When a captive portal is used by the AP, the user needs to surf into the captive portal and perform a log-in to connect his IP address to the internet. In some implementations, the user's web browser is forwarded to the captive portal regardless of the internet site that it tries to surf into. Some APs allow the STA to surf in some limited number of internet sites before they complete the second authentication procedure (for example, if the AP is in an hotel, it might allow surfing into the hotel's website, or affiliated news web sites). The procedure at the captive portal typically includes authentication, payment, or agreeing to terms of usage. Once the authentication is complete, the IP address of the STA is connected to the internet (usually by reconfiguring the firewall that controls the communications of the AP). Each sub process takes time to complete, resulting in a total of over several seconds to complete the entire process.

It is important to note that in managed networks, Step 4 can be performed once in a certain amount or time (or for a certain area), as moving between APs of the managed network does not necessarily change the parameters of the STA such as IP address etc. However, in un-managed networks (and sometimes also in managed networks), the STA must gain a new IP address and other parameters, usually through DHCP

(Dynamic Host Configuration Protocol, see RFC 1541). Completing the DHCP protocol can take up to several seconds. Sometimes, obtaining an IP is not enough, and a second authentication is needed. In other cases, a proxy server or a Socks server should be set for the communication. The whole process can consume a few seconds, which are intolerable in a streaming two-way application such as a voice conversation.

Many protocols that are used in the Internet require that the IP address of the user would remain fixed during communications (for example, TCP – Transport Control Protocol, see RFC 793). However, a handover might result in the change of the IP.

One solution to this problem is provided by the Mobile IP standard (see RFC 2002): in this solution the STA updates a server with its current IP address, every time that the IP address changes. As a preparation for roaming, the server allocates to the STA (in addition to the STA's current IP address) an IP address that remains fixed, even when the real IP address of the STA changes. This fixed IP address is also known as a "care of" address. From this moment on, the STA keeps the server posted of the real IP address of the STA, and the STA can use (in its communications with the rest of the internet) the care of address (or its home address) as if it was its own fixed address. Any IP data packet that is sent to the care of IP address is tunneled by the server to the current IP address of the STA. For packets originating from the STA to the Internet, the STA can tunnel the packets to the server, which replaces the IP address with the care of address. However, many times the STA can simply write its care of IP address as the source address of the IP data packet, as many times, this address is not checked what-so-ever in the course of routing the IP data packet in the Internet.

This solution can be applied as long as the handovers are not performed too often. However, it incurs the punishment of routing all incoming packets through a server, causing both an increased travel time for the data packets, as well as latency (or disconnection) for the time that the real IP address changed, but the server is not informed yet. If the round-trip-time of the packets between the STA and the server is longer than the time a STA stays with the same IP, this method fails, as by the time packets reach the reported location of the STA, the STA is already in another location.

For many applications, such as voice, it is of utmost importance to minimize the time spent on the handover process. The time consumed by the handover process is usually dominated by the scanning step (Step 1 as mentioned above), and by Step 4 (specifically in case of an unmanaged network). There are many solutions that address fast handovers in cellular networks, and a few solutions that address fast handovers in managed WiFi networks (for example, see: WO2004/054283, which reduces Step 1 (mentioned above) by selective scanning but requires modifying the AP). None of these solutions deal with the delay due to Step 4.

It is an object of this invention to provide very fast handovers even in unmanaged networks.

Another barrier for wireless applications is that WiFi coverage might exists, and security policy might allow the STA to connect, but the AP might be out of resources (for example, there are 2007 associated STAs, and therefore it has no resources left, or that it has a limited IP address space which was already allocated through DHCP, and it has no IP address to allocate). It is an object of this invention to provide a system and method that allows STAs to use the services of the AP even when some of its resources are exhausted.

Another barrier for many wireless applications is the complex configuration of STA, especially the security parameters. A user that purchases a new STA and has an existing AP, might wish to configure his new STA to work with his AP. This configuration includes entering into the STA the encryption key and authentication key that would allow it to use the AP. Existing solutions require a change in the AP and STA, such that a special key can be pressed simultaneously at both ends to perform automatic configuration (like Buffalo INC's AirStation OneTouch Secure System – AOSS, or Broadcom's SecureEasySetup). Without such a solution, the user is usually forced to punch into his STA the security codes (which are typically long). The problem worsens when the STA moves between APs that use different security settings.

It is an object of this invention to provide easy configuration on both levels: at the initial setup and while roaming.

Another barrier for many wireless applications is that WiFi coverage might exist, but it is locked and unavailable for use for the STA.It is an object of this invention to provide a solution for (legally) accessing locked APs.

Another problem with WiFi is that the WiFi protocol is not optimized for low battery consumption (compared to cellular protocols such as GSM). In current solutions, if the STA moves between APs and changes its IP, it must use mobile IP and inform an entity (server) in the network of its current IP (we refer this process *location update*, as the STA updates the network entity of its location). Frequent location updates exhaust the STA's battery. Another problem with frequent location updates is that they create a heavy load on the network and on the network entities that manage and keep track of the STA's location.

The situation in WiFi is very different from the situation in cellular networks in two ways. Both of the ways cause increase on the number of location updates in WiFi: First, in cellular network, the cells are typically much larger than a "cell" that is created by a WiFi AP. Therefore, in cellular there are fewer transitions between cells, and hence less location updates. Second, cellular protocols allow defining a "location area" that encompasses several cells, and the STA is required to perform location update only when moving between location areas, and thus reducing the number of location updates. Current WiFi protocols are not built to support location areas.

It is an object of this invention to provide a method that reduces the number of location updates required for STAs while moving between APs.

It is an object of the current invention to provide the solutions to the above mentioned problems, using both a centralized (server based) approach, and also by providing a method for performing the solutions using a distributed peer-to-peer network. Therefore, no huge servers and no large investments are required.

Disclosure of Invention

The invention is described by way of example, but it should be obvious to those skilled in the art that many variations follow.

One of the novel ideas behind very fast handover is to practically almost complete the process of the handover before it even started, possibly with the assistance of another STA that is already in the new AP's coverage (further details are described later).

Another associated novel idea is that the same MAC address and IP address can actually be used by more than one STA. The differentiation between the STAs can be performed by using higher protocol identification, such as different port numbers (for example TCP ports), as detailed later.

It is useful for a station STA11 to know the identity of the adjacent APs that the STA might hand over to. The identity of an AP can be established in several ways, as disclosed herein. The SSID (Service Set ID) of the AP is usually broadcasted by the AP using periodical transmissions known as beacon. However, two adjacent AP may have the same SSID. In such a case, the MAC address of each AP is different, and APs can be differentiated based on their MAC address (which serves as a globally unique identification parameter). Some APs do not transmit beacon, and only respond when they are addressed using their SSID. In this case, a pre-knowledge is needed, as described later.

Another novel idea is that STA11 will selectively scan for a neighboring AP in the following novel way. Assume that STA11 scans to see if it can receive the beacon of AP33, where the scanning will be performed exactly when the AP33 is expected to transmit its beacon, therefore, the disconnection from AP31 will be minimal. The novel method consists of scanning and storing (in network entities) information about the relative time between adjacent APs, and their relative clock drift. This information is retrieved in the appropriate time such that the STA knows to wait for the beacon just before it is transmitted. The details are disclosed in the sequel..

Another aspect of this invention is to prevent exhaustion of resources at the APs. GN21 keeps a pool of MAC addresses with associated IP address. Just before a STA enters the AP, GN21 sends it a MAC address and an IP address that are already associated with the AP. Therefore, the STA can connect even if the AP has no resources left for new STAs. See a detailed description later.

Another novel idea in this disclosure is to save Battery Power and reduce network load by reducing the number of Location Updates in WiFi. A location update is the process in which a STA informs an entity in the network on its current location (the notification can take many forms, including opening a TCP connection, or sending UDP packets). In prior art for 802.11 networks, a location update is required whenever the IP address of the STA changes (for example, when moving between APs of different subnets) – even if the STA is idle (not transmitting or receiving data). The novel method allows to define a *location area* for WiFi, such that an idle STA needs to perform location update only when it moves between APs that belong to different location areas, but does not need to perform location update when it moves between APs of the same location area. See further details later.

A *pseudo-beacon* is another novel idea of this invention which allows reducing the number of Location Updates. It is a message that GN21 can periodically transmit in each AP. While some APs might permit a remote node to transmit a message in the AP, other APs might not allow it. In the novel method, a certain MAC address, IP address, and possibly a port number, are allocated in each AP for the purpose of pseudo-beacon transmission. Further details are described later.

Configuring the security might be a tedious job, as the security (authentication/encryption) code might be very long as known in the art, which the user might need to punch in. A novel solution for easy configuration is disclosed. Unlike previous solutions, the novel method does not require changing the existing AP of the customer. In one embodiment, software is run on a personal computer of the user (that is already configured to access the WiFi). Then, the software establishes a secure channel with the STA, and copies the security information from the personal computer to the STA. In this way, the STA learns the security parameters.
In another embodiment, the customer first connects the STA by wire to its network (or alternatively, the STA first connects using a connection it establishes through an already connected device, such as a personal computer). As the STA can receive and transmit signals on the wireless network and it is connected to the internet (through the other connection) at the same time, it tries to locate the web configuration of the AP on the wired network (most APs have a web interface). In most cases, it is an easy

job for the STA, as either the STA can locate the AP as it is the default gateway of the wired network, or it can try to find its IP by performing RARP (Reverse Address Resolution Protocol) using the wireless MAC address of the AP (which it can see off-the-air). Further details are described later.

Another novel method for gaining access to locked networks is disclosed. While performing the above described easy setup (or at any other time), the user is prompted, if he wishes, to join a swapping service. The swapping service allows the user to gain access to many locked networks (the locked networks of the other users that joined the swapping service), in return he allows users to use his network for the purpose of connecting to the internet. If the user agrees, the access parameters to his network (encryption key, MAC address, default gateway, etc.) are securely stored in the network (for example in GN21, and a backup server). The security information will be securely sent directly into the hardware of other STAs, when they need to connect using his AP. Further details are described later.

Another novel aspect of the invention takes advantage of the fact that the wireless network is local in nature, as the APs are geographically adjacent. As a result, the methods that are disclosed can be implemented by many small devices on the internet, each responsible for a geographic area. The devices form a peer-to-peer network that implement the methods, without the need to rely heavily on large servers.

Another novel idea in the invention is to have a STA which has a capability of communicating in two or more channels in parallel. This capability can enable a STA to be connected to two APs in parallel without the need to implement sophisticated mechanisms that actually simulate this situation. Thus, a STA can connect with future AP while maintaining a connection through its serving APs. Being connected to two APs simultaneously allows greater bandwidth by utilizing two connections instead of one, and soft-handovers, i.e., the STA stays connected through one AP, while disconnecting from the second AP in the process of handover.

Brief Description of the Drawings

The invention will now be described by way of example and with reference to the accompanying drawings in which:

Fig. 1 illustrates the mobile stations (STA) in the covering cell performed by the "Access Point" (AP)

Fig. 2. illustrates the connection among STA11, a Governing Node (GN) and another user – Termination Node (TN).

Mode of Carrying out the Invention

A preferred embodiment of the present invention will now be described by way of example and with reference to the accompanying drawings.

It is understood that the method and system in the present disclosure may be used for the transmission of voice, data, multimedia or a combination thereof.

Fast Handover

One of the novel ideas behind very fast handover is to practically almost complete the process of the handover before it even started.

Consider an example depicted in Figure 1 and Figure 2, in which STA11 is in conversation with TN41 (TN – Termination node, the node with which STA11 communicates, shown in Fig. 2), and STA11 is moving from AP31 towards AP32. Also assume that a node GN21 (GN – Governing Node, a node that is non-exclusively responsible for the mobility management in a certain geographic area for a given time, shown in Fig. 2) is in contact with STA11, and it is assisting STA11 during the handover process. STA11 currently has an IP address, which was allocated to it by AP31. To complete the handover, STA11 should be associated with AP32, have an IP address assigned by AP32, complete any second authentication that is required, and have TN41 be aware of the new IP address, so it can forward the conversation to the new location. Note that in some scenarios (in some cases when there are firewalls or

NAT devices between AP32 and TN41, the connection between STA11 and TN41 must be started from within AP32 towards TN41).

According to prior art, it appears that STA11 cannot begin the handover process until it reaches the coverage of AP32, since it cannot start the connection process. One novel solution (that requires changing the software of the AP) is to allow STA11 to perform the connection process through the Internet, instead of performing it wirelessly. In this way, once STA11 reaches radio connection with AP32, it can start working immediately.

However, we are more interested in solutions where there is no need to change the AP. To achieve this goal, assume the existence of a non-moving STA12 in the coverage of AP32 (we will somewhat soften this assumption later). According to the present invention STA12 is in contact with GN21, and receives instructions to *impersonate* STA11 towards AP32 (we will later discuss how to make it possible), and complete a connection process with AP32 on behalf of STA11 (including authentication, association, receiving an IP address, performing any second authentication/log-in procedure, and perhaps even opening connections or "punching holes" in the firewall). Then, STA12 communicates this parameters to GN21 (once the parameters are communicated, STA12 can return to its real identity). GN21 communicates the parameters to STA11 (and perhaps to TN41), and thus, STA11 does no longer need to perform the connection process, and once it reaches the perimeter of the coverage (we will later discuss how to identify this situation) it can immediately use the new parameters and continue communications without any delay. STA11 (or GN21) can alert TN41 *before* the handover, so it can start and send information packets to the new location. TN41 may send the information in parallel to the old and the new location, and cease transmitting to the old location once the handover is complete (e.g., when it receives information from STA11 with its address from the new AP). STA12 may even open a TCP (Transmission Control Protocol, as used in the Internet) connection or send a UDP (User Datagram Protocol) packet on behalf of STA11, if required. This connection may wait for STA11 until it reaches AP32. If there is a timeout on these connections (either due to protocol, or due to firewalls), STA12 or other bypassing STAs can send and receive "keep-alive" messages on behalf of STA11 (as is instructed by GN21). The timeout for each AP

can be discovered over time by trial and error (or by discovering the APs type), and storing this information in GN21 for future use. GN21 can notify the STAs on the value of the timeout.

How STA12 can impersonate STA11:

To understand how STA12 can impersonate STA11 towards AP32, we must understand how identity is established in the network. The basic identity in the network is the physical address which is known as MAC Address (Media Access Control Address), which is globally unique. Each manufacturer is allocated a portion of the address space and allocates a unique MAC address to every network card (including WiFi network card) that it manufactures. Then, the manufacturer burns the allocated address into the network card. However, in most network cards, an application can (temporarily) change the MAC address of the card to another MAC address.

The MAC address is not used for end-to-end communications over the internet, but usually only for communications within the same physical network.

For example, STA12 communicates with AP32 using MAC address, but GN21 is not usually aware of the MAC address of STA12. The MAC address is universally unique.

We use the feature of temporarily changing the MAC address in the network cards in a novel way, allowing STA12 to impersonate STA11. Therefore, in the instructions that GN21 gives to STA12, it mentions the MAC address of STA11, so STA12 can assume the MAC identity of STA11. Then, STA12 can complete the association with AP32 (using the MAC address of STA11)), in which it receives the Association ID (AID), and completes a DHCP protocol in which it receives an IP address to be used with the MAC of STA11 while it is using AP32. STA12 can also perform a second authentication and log-in on behalf of STA11. STA12 sends the connection information back to GN21, which forwards it to STA11. STA12 can return to its original MAC address, but the allocated resources at AP32 remain allocated, as from the point of view of AP32, STA11 is already connected and in coverage. In order to avoid losing messages that are sent to STA12 during its impersonation to STA11, it can either continue and listen using both its own MAC address and STA11's MAC address, or it can issue a "power-save" mode command to its serving AP. The power

save mode indicates the AP that the STA is sleeping for a while, in which time the AP is buffering the incoming data packets. Therefore, even if STA12 is connected to the internet using another AP, it can issue a power-save mode command, possibly change the frequency, and perform the connection on behalf of STA12. It can return to its serving AP once the connection is established, or poll for incoming messages once in a while.

First Softening of the Assumption that STA12 is in the coverage of AP32:
What if STA12 is not in the coverage of AP32, and there is no other station in AP32's coverage? The following process can be performed in advance, well before a handover is needed. GN21 can ask (in advance) stations that pass through AP32 to connect and receive an IP address from AP32 using some MAC address. The MAC address is not necessarily the MAC address of STA11, as the process is not specific to STA11. The stations send the connection details to GN21, which stores the AID, the MAC, the IP address and other connections details in a poll for future use. The poll may even contain UDP or TCP connections, which may be kept alive by bypassing STAs (against timeouts of firewalls, Network Address Translator devices (NAT), and protocol timeouts). UDP and TCP connections in the poll are targeted to some node in the network that can forward information for other nodes (for example TN41). When a connection is required by some STA, the pool is queried, and a resource can be allocated and applied by a STA. As a result, a station might change its MAC address and IP address every time it moves between APs. If the station moves very fast between these access points, GN21 can predict the direction in which the station is moving based on past movements, inform TN41 of the possible future addresses. In this way, TN41 can send data to the new address even before the station actually moved there. In some implementations of the APs and firewalls between AP32 and TN41 the STA must first send data before it can receive any data, otherwise, the firewall may block the incoming data, or a NAT (Network Address Translator) device might not know where to forward the data. The restriction, that the STA must be the first to send data, is usually required due to security policy that allows only outgoing connections, or due to NAT device that need to relate an internal IP address and port number with an external IP address and port number. For example, in most NAT implementations a connection must be established from within the NATed zone (e.g., the AP coverage) towards the internet. Many firewalls also require that the connection

is established from the private network towards the internet (rather than allowing incoming connections from the internet towards the private networks). In these cases, the data that TN41 sends is not transmitted by AP32 until the station reaches the access point and transmits information back to TN41. Depending on the type of firewalls and NAT devices, TN41 might be able to predict a port number to which it should send such messages before the first outgoing data packet is transmitted.

Another associated novel disclosure is that the same MAC address and IP address can actually be used by more than one STA. The differentiation between the STAs can be performed by using higher protocol identities such as different ports (for example TCP ports). Using the same MAC and IP address in more than one STA is not problematic for packets that are sent from the STA. However, while receiving an incoming packet, only one STA should send an acknowledgement. As each STA knows the ports that are in use, it only acknowledges messages that are designated to it. GN21 can coordinate between the STAs such that they do not use the same ports. For example, if there are at most n stations using the same MAC and IP address, station i will allocate port numbers that are equal to i modulo n. Another solution is to choose the port number at random. If each STA uses one port at random, according to the birthday paradox, port collisions occur with very low probability as long as the number of connections is smaller than about the square root of 65536 (i.e., when there are less than 256 connections using the same IP).

Another idea is to change the software at the AP such that it can communicate with GN21 and perform the connection procedure on behalf of STA11.

Knowing who are the adjacent APs and the location of a STA:

It is useful for a station STA11 to know the identity of the adjacent APs that the station might hand over to. The identity of an AP can be established in several ways: The SSID (Service Set ID) of the AP is usually broadcasted by the AP using periodical transmissions known as beacon. However, two adjacent AP may have the same SSID. In such a case, the MAC address of each AP is different, and APs can be differentiated based on their MAC address. Some APs do not transmit their SSID, but they still broadcast beacon messages with their MAC address. Even if the AP is locked and encrypted the MAC address is transmitted, and it is transmitted without

any encryption. In this way, STA11 can know the identity of adjacent APs, and infer its location.

Scanning by Idle STAs:

In a preferred embodiment, GN21 collects information about APs which are adjacent. Idle stations (i.e. stations which are not in an intensive data transfer) can perform a *scanning* operation once in a while. As a result they learn the MAC address (and possiblly the SSIDs) of the APs within radio reach. The STAs can then send this information to GN21 which collects it. The idle STAs can also perform tests to check what is the accessibility parameters of an AP (e.g., is it an open and free AP, is it a locked AP and the password is available from GN21, is it locked and there is no free access to the AP, is there a captive portal, does GN21 have a username/password available for the captive portal, etc.). All this discovered information is sent to GN21. When handovers are performed, GN21 takes note of the sequence of handovers that occur, and can learn common paths which are taken (for example, a road or a crosswalk might cause more likely paths than others).

It is very important that GN21 knows in advance the AP to which STA11 will be handed over to and when the handover will occur. Such a knowledge allows, for example, to alert TN41of the new location in advance. Gaining accuracy in the prediction of the handover (when and where) translates to better performance, as GN21 needs to allocate a MAC address and an IP address to STA11 in the new AP, and TN41 might start to send data to the new location. Therefore, knowing who the neighboring APs are, and their reception quality at STA11 is very important.

Scanning by a non-Idle STA.

In principle, STA11 can scan the surroundings once in a while and look for the beacons of adjacent APs, and thus measure the reception quality from each AP. However, such a scanning takes a lot of time (might even take couple of seconds for a full scan). Selective scanning for APs which are expected to be neighbors can reduce the scanning time, but it can still stay in the magnitude of a few hundred milliseconds. It is important to understand that during a contemporary scanning using current

technology, STA11 cannot receive or send messages from or to AP31, which means that the scanning time must be reduced to reduce this disconnection time.

The novel disclosed method is that STA11 will selectively scan for a neighboring AP in the following special way. Assume that STA11 scans to see if it can receive the beacon of AP33, where the scanning is performed exactly when the AP33 is expected to transmit its beacon. Therefore, the disconnection from AP31 will be minimal. The problem is, however, that although the beacons are transmitted periodically, STA11 does not know when a beacon is expected to be transmitted from AP33. As the beacons are transmitted about every 102.4ms (many variations are possible), STA11 might be forced to wait on average 51.2ms, which is a prohibitively long time to wait. STA11 may also transmit a *Probe* message to force a beacon to be sent especially for it– but a probe message requires a transmission that has implication on battery life. Furthermore, for the purpose of location finding, STA11 might wish to be able to receive beacons of APs that will not answer the probe (due to range, policies, etc.)

We can safely assume that other STAs visited the area of AP33 before STA11, and that they have reported the rate of the beacons of AP33 (e.g., a beacon every 102.4ms). A problem that remains is that the beacons are scheduled according to the internal clock of AP33, which might tick at a different rate than other clocks (and clocks tend to tick at different rates). Moreover, the clock of the visiting STAs is probably not exactly synchronized with the clock of STA11, which makes the process inaccurate. That is even if STA11 knows that at a specific time according to some STA's internal clock a beacon was transmitted, STA11 will not know how to translate this information to his clock, as the clocks are probably not synchronized to such great accuracy (network time synchronization services such as the network time protocol (NTP) cannot be more accurate than a couple of tens of milliseconds, where in this case we need an accuracy of around one millisecond). The following novel method allows accuracy of microseconds.

The novel approach for time synchronization is to rely on a relatively accurate clock already available to STA11: The 802.11 standard requires each AP to transmit in its beacon its clock (referred to in the 802.11 standard as *timestamp*). This clock must be the internal clock of the AP at the time of transmission in units of microseconds.

Therefore, STAs can specify the value of the clock of AP33 in terms of the value of the clock at the adjacent AP31. By measuring the timestamp of AP31 and AP33 at two different times T_{31}^{1} and T_{31}^{2} (based on the clock of AP31), in which the time value of AP33 T_{33}^{1} and T_{33}^{2}, respectively, it can be established with reasonable accuracy that AP33 clock ticks approximately $r_{33/31}=(T_{33}^{2}- T_{33}^{1})/(T_{31}^{2}-T_{31}^{1})$ times for every clock tick of AP31. At time T_{31}^{3} in the future, the clock of AP33 can be estimated as $T_{33}^{3}\approx T_{33}^{2}+r_{33/31}\cdot(T_{31}^{3}-T_{31}^{2})$. Similarly, at time T_{33}^{4} the clock of AP31 can be estimated as $T_{31}^{4}\approx T_{31}^{2}+(1/r_{33/31})\cdot(T_{33}^{4}-T_{33}^{2})$. Beacons are scheduled to transmission when the clock of the AP modulo the beacon interval is zero, where the beacon interval is measured in microseconds according to the clock of the AP, it is fixed for an AP, and the value of the beacon interval is transmitted in the beacon. Therefore, GN21 stores the relation $r_{33/31}$ together with T_{33}^{2} and T_{31}^{2} and the beacon interval of AP33 and AP31, and reports it to STA11 such that it can extrapolate the time at AP33 and infer the time of the beacon transmission. Once STA11 succeeds in receiving a beacon from AP33 it can report the times to GN21, so that GN21 can keep its time tracking accurate. Furthermore, the scanning allows GN21 and STA11 to make the best handover decisions based on the knowledge of the approximate location of STA11 with respect to the neighboring APs.

A technical problem that still has to be resolved is that a STA can know the value T_{31}^{1} but cannot measure the value of T_{33}^{1} in exactly the same time of T_{31}^{1} , as these values are carried on the beacons of APs, which are transmitted at different times. The solution is to measure the time of AP33 $T_{33}^{1'}$ at a time close to T_{33}^{1}, and note the time difference between the two measurements according to the STA's internal timer. As the measurements are very close to each other, the clock drift between the STA's timer and AP33's timer is negligible, and we can estimate that $T_{33}^{1}\approx T_{33}^{1'}+timediff$, where *timediff* is the time difference between the measurements of $T_{33}^{1}$and $T_{33}^{1'}$ according to the timer of the STA. If there is a large clock drift after all (although it is not expected), it can be corrected by calculating the r value between the clock at AP33 and the STA in a similar way to the way done for APs.

The location of STA11 can be deduced from the reception quality, the reception strength and the identity of the neighboring APs. This location information can be

taken into account while performing handover decisions, as well as for location based services or for other network applications.

It should also be noted that in Frequency Hopping, knowing the time of the AP has another special importance, as the frequency that the AP works in might depend on the time.

Preventing Exhaustion of Resources at the AP

As discussed under "Background Art", each AP has a limited number of Association IDs (AID) and usually, even a smaller pool of IP addresses (available through DHCP). Once this number of resources is exhausted, the AP might not be able to serve new STAs.

A situation where IP addresses are exhausted can happen very quickly: for example, consider an AP in a very busy location, where there are many STAs that connect to the AP only for a short period of time. Each STA performs the connection process and obtains an IP address using DHCP, but as it disconnects it might not release the IP address.

The pool of IP addresses in an unmanaged AP is usually limited to about 200 addresses, with many consumer APs supporting only tens of addresses. A device is assigned the IP address for a given period of time (known as the lease time). Many times, the lease time is set in a magnitude of days (although the granularity is seconds), and in many other instances the lease time is set to a magnitude of hours. In such a situation the pool of IP addresses runs empty very fast.

However, in this disclosure for fast handovers, GN21 keeps a pool of MAC addresses with associated IP address. Just before a STA enters the AP, GN21 can send it a MAC address and an IP address that are already associated with the AP. Therefore, the STA can connect even if the AP has no resources left for new STAs. Combined with the above disclosure that allows several STAs to share the same MAC address and IP address, an AP can serve more APs than its IP resources, even above its limit on the number of associated STAs.

Saving Battery Power by Reducing Location Updates

A novel disclosure of this invention is a method to reduce the number of location updates that are needed in WiFi, when a STA is idle. A location update is the process in which a STA informs an entity in the network of the current location of the STA (the notification can take many forms, including opening a TCP connection, or sending UDP packets). In prior art for WiFi networks (with for example mobile IP, or SIP – Session Initiation Protocol), a location update is required whenever the IP address of the STA changes (for example, when moving between APs of different subnets) – even if the STA is idle. The novel method allows defining a *location area* for WiFi, such that a STA needs to perform location update only when it moves between APs that belong to different location areas, but does not need to perform location update when it moves between APs of the same location area as long as it's idle.

We assume that the APs are divided into location areas, and for each location area there is a node in the network that is in charge of this location area. For example, assume GN21 is in charge of a location area composed of AP31, AP32, and AP33. How does a STA know which AP belongs to the location area? Either GN21 gives it a list of all the APs that belong to the location area, or GN21 transmits a *pseudo-beacon* in each AP.

A *pseudo-beacon* is a novel disclosure of this invention. It is a message that GN21 can periodically transmit in each AP. While some APs might permit a remote node to transmit a message in the AP, other APs might not allow it. In the novel method, a certain MAC address, IP address, and possibly port are allocated in each AP for the purpose of pseudo-beacon transmission. GN21 asks some STA to open a connection using these resources to GN21, and GN21 sends the pseudo-beacon messages using this transmission. Each pseudo-beacon contains the parameters needed to listen to the pseudo-beacons in the adjacent APs. A STA that lacks these parameters can contact GN21 and receive them. From that moment on, the STA can move between APs in the same location area, and receive the parameters that are needed to listen to the pseudo-beacon from other pseudo beacons. For example, assume that STA11 is located in AP31 and is moving to AP32. STA11 listens to the pseudo-beacon at AP31, and from the pseudo-beacon learns the parameters that are needed to listen to the pseudo-beacon of AP32. Thus, STA11 can move to AP32 without any transmission.

Which STAs of the stations in AP31 should acknowledge the pseudo-beacon? Preferably, none. However, some firewalls require minimum rate of outgoing packets to maintain an open connection. In such a case, once in a while GN21 sends on the pseudo-beacon a message that asks any station to send an acknowledgement with some probability *p*. The probability that GN21 states should be accommodated to the expected number of stations in AP31 (GN21 might not exactly know how many STAs are in the AP). If no STA acknowledges the pseudo-beacon for over the needed time, and the timeout of firewalls stop the incoming messages, then no pseudo-beacons are transmitted. In this case, a roaming STA will contact GN21 after a certain period of time of probing for the pseudo-beacon has passed (and no pseudo-beacon is seen). GN21 can request the STA to reopen the connection for the pseudo-beacon transmission.

If the STA is in a session with TN41 with many packets received (e.g., above a certain threshold), it is considered *non-idle* (which we also refer to as *in conversation*) and treated as described above in **fast handover**.
However, assume that STA11 is in idle mode (e.g., incoming packets below a threshold), it can move between APs of the same location area without performing location update. When a node TN41 wishes to send data to STA11, STA11 should change its state from *idle* to *in conversation*. TN41 contacts GN21 (TN41 might be forwarded to GN21 through a system such as dynamic DNS (Directory Name Service) or another method, such as a Distributed Hash Table – DHT, or a peer-to-peer network). GN21 sends a *paging* message for STA11 on the pseudo-beacon of all the APs in the location area. As STA11 listens to one of the pseudo-beacons, STA11 will receive the paging message. Then, STA11 responds preferably to GN21 (or to TN41, depending on what is written in the paging message) by initiating an outgoing connection as described below. It should be noted that GN21 can first page for STA11 in the APs that have a higher chance covering STA11, and the paging can repeat several times until STA11 replies.

When a STA is required to initiate an outgoing connection it can use a resource (MAC, IP, or TCP/UDP with port, user/password) that is listed as available on the pseudo-beacon or on the paging message, or it can request its own resources from the

AP. If two (or more) STAs use the same resources for a connection at the same time, GN21 will detect it, and in the acknowledge message (or second message of the TCP handshake) will announce the identity of the STA that it answers to. The other STA is required to initiate an outgoing connection again. Once a connection with GN21 is established, GN21 can allocate resources to the STA such that it moves to be in conversation status. One of the resources that are allocated is GN21 attention to accompany the STA as it might need to perform handover to another AP.

It should be noted that the location areas can overlap, meaning a single AP can belong to more than one location area. Upon the policy of the network, STA11 might be required to perform location update when it reaches such a APs, or it may just give helpful information. If possible, a STA might prefer to *park* on an AP that is within the same location area as its current AP, such that a location update is avoided.

It should also be noted that there is a tradeoff between the overhead that is spent during paging and establishing the connection, and the overhead that is being spent to keep a steady connection for each AP. The optimal point on the tradeoff depends on the rate that the AP switches APs as well as on the number of packets it receives and sends.

Easy Configuration of STA

When purchasing a new STA, it is required to configure the STA with the security settings of the existing network (in case the network is secure). If the network is not secure, the new owner usually only needs to select his network from the list of available networks that is received by the wireless network card.

Configuring the security might be a tedious job, as the security (authentication/encryption) code might be very long as known in the art, which the user might need to punch in. A novel solution for easy configuration is disclosed. Unlike previous solutions, the novel method does not require changing the existing AP of the customer. In one embodiment, software is run on a personal computer of the user (that is already configured to access the WiFi). Then, the software establishes a

secure channel with the STA, and copies the security information from the personal computer to the STA. In this way, the STA learns the security parameters.

In another embodiment, the customer first connects the STA by wire to its network (or alternatively, the STA first connects using a connection it establishes through an already connected device, such as a personal computer). As the STA can receive and transmit signals on the wireless network and it is connected to the internet (through the other connection) at the same time, it tries to locate the web configuration of the AP on the wired network (most APs have a web interface). In most cases, it is an easy job for the STA, as either the STA can locate the AP as it is the default gateway of the wired network, or it can try to find its IP by performing RARP (Reverse Address Resolution Protocol) using the wireless MAC address of the AP (which it can see off-the-air).

If none succeeds the STA can perform exhaustive search on commonly used IP addresses, or on very probable addresses, like all the IP addresses of the same subnet. Once the AP web interface is found, the STA tries to log into the AP. It can guess the default address or find it on a database that can be built on the web, with common default passwords for each manufacturer (the manufacturer and model will be usually sent by the AP during the web login process, or can be found out using the MAC address, which is unique per manufacturer). If the password for the AP cannot be guessed, the user is prompted for its password to complete the log-in. Then, the STA navigates to the security settings page and retrieves the password needed for the wireless network.

In the event that the procedure fails, the user is prompted for the security settings (which would happen without using the above method). For most common users and setups, the method succeeds (and for unsophisticated customers, who do not change the passwords – it succeeds in the majority of the cases). Thus, in the majority of cases, the setup is made much simpler.

Once the STA has access to the setup of the AP, it can (with permission from the user), open holes or forward certain port to some IP address. This IP address and port can serve as way that GN21 can send and broadcast the pseudo-beacon, without a STA first opening a connection from the AP, and without worrying about timeouts

(provided that there are no other firewall between the AP and GN21). Opened ports can also help during the fast handover, such that TN41 can directly send packets to the new location without a need for STA12 to open the connection.

In corporate settings, the company can set a special server which gives the configuration to the phone, over the network.

Gaining Access to Locked Networks

While performing the above easy setup (or at any other time), the user is prompted if he wishes to join a swapping service. The swapping service allows the user to gain access to many locked networks (the locked networks of the other users that joined the swapping service), in return that he allows users to use his network for the purpose of connecting to the internet. If the user agrees, the access parameters to his network (encryption key, MAC address, default gateway, etc.) are securely stored in the network (for example in GN21, and a backup server). The security information is securely sent directly into the hardware (or network card) of other STAs, when they need to connect using his AP. As the security parameters are sent directly to the STA's network hardware, it can make sure that the communication that is established is designated outside the user's network, and will not jeopardize the computers on the user's network. Furthermore, GN21 can monitor the amount of bandwidth that is consumed by visiting users, and to make sure their hardware limits the amount of used bandwidth such that the user does not experience a degradation of quality of his connection. Alternatively, the security information can be sent to the other STAs using other security measures, as known in the art.

The secrecy of the security parameters (such as the encryption key) can be cryptographically protected while on transit and storage, as known in the art.

Some APs limit the access of the subscribers by making sure that only specific MAC addresses connect to the network. As our methods as described above allow to use the same MAC address for several users, this specific MAC address can be used when using the network that restricts the use with specific MAC address.

In case a STA tries to connect to an AP with a captive portal, a special application on the STA is running and performs the authentication and log-in automatically. GN21 can store typical portal appearances, such that it can guide the STA on how to perform the authentication/log-in process. If the STA comes across a captive portal which is unknown or unexpected, it can locally store the web pages that it received from the captive portal and later transfer them to GN21. GN21 accumulates the reports and guides STAs how to log-in to the captive portal in the future. As part of the swapping service, GN21 can store username/passwords to enable connection through the captive portal automatically.

Special care for data

The above description works well for both voice and data.
TN41 might be a mobile node as well, or a fixed node in the network.
The transferred information between STA11 and GN21 can be voice, data, or their combination.

In case STA11 wishes to communicate with a node that is not aware of the novel network, it can do so through a node that is aware of the network. For example, TN41 can serve as a proxy for STA11 (in a similar way to mobile IP). The node that is not aware of the network communicates with TN41. TN41 forward the information to STA11. TN41 can allocate an IP address (perhaps using NAT, or allocate ports using its own IP address) that will serve STA11. To balance the communication load, STA11 can have several network nodes such as TN41, TN42 (not shown), etc, to be its proxies in parallel.
In fact, the resulting connection between STA11 and TN41 can be seen as a layer 2 (MAC) connection, on top of which the communication is performed. In this setup, TN41 serves as the default gateway of STA11, and optionally can run a DHCP server and a NAT server.

Executing the Invention over a Peer-to-peer network

Another novel aspect of the above novel methods takes advantage of the fact that the wireless network is local in nature, as the APs are geographically adjacent. The system and method as described in this disclosure allows GN21 to be responsible over

a small geographical area with little interaction with its neighbors. As a result, the methods that are disclosed can be implemented by many small devices forming a peer-to-peer network that implements the methods, without the need to rely heavily on large servers.

Many nodes GN21, GN22 (not shown), can each control a group of APs. To make the system grow "automatically", it is possible to give users a "base" that will act as their point of presence in the network. For example, the base can assume the role of TN41 as a Mobile IP proxy. The base can connect to the wired network at the premises of the customer. Some bases will assume the role of a GN, where the GNs can be managed by either a network control center, or through peer-to-peer protocols.

In early stages of deployment of the system, when there is still a small number of GNs, each GN might need to cover a large number APs. A general server can back-up all information that the GNs hold. To avoid the situation, where a single GN needs to cover a huge number of APs with pseudo-beacons, the system might not use the pseudo-beacon mechanism (although, it should be noted that with moderate computing power and network resources, a GN might be able to cover a few thousands of APs). In the worst case scenario of a peer-to-peer network, there is one base (GN) for each STA, and this GN act as the GN for the APs in the proximity of the STA. When the STA moves, the coverage area in the responsibility of the GN moves with it. In this case, the GN can fetch information on neighboring APs from the general server. When GN abandons an AP, it can store the information it gathered about it in the general server, for later use by possibly other GNs. In a system which is not based on many small GNs, a large GN can assume the role of the smaller GNs.

It should be noted that it takes some time to gather the information on the APs (such as timing, default gateways, etc). However, once a single STA passes in an area, it obtains the needed information. This information is later stored in the GNs and general server, for the benefit of all STAs in the future.

If a STA needs to handover into an AP which has no STAs currently in it, it might not have the needed resources pre-allocated (such as an associated MAC address and IP address), and might therefore need to gain it by itself. However, in many cases the

STA can obtain resources at one pass in the area, and these resources (such as IP address) will stay for the next pass in the area (which can be hours later).

An Alternate Fast Method for Connecting to an AP – Removing the Assumption on the Existence of STA12 in the Coverage of the new AP

The drawback of the above method of fast handover is that it requires that the pool of resources that GN21 holds should contain a valid IP address of the AP that STA is handing over to. If the DHCP lease time is long enough, having a valid IP might not be a problem, but on short lease times with only a few STAs roaming it is desirable to perform handovers even if there is no valid IP available in the pool. Unfortunately, a typical execution of the DHCP protocol can take several seconds to complete, which might be too long for a fast handover. Interestingly, we observe that many APs will forward information even if the IP that is being used was not allocated by DHCP.

Therefore, we disclose the following method:
Choose a MAC and associate it with the AP (or use an Associated MAC without an associated IP address), choose a random (but valid) IP address, and use it. The STA must use the correct default gateway settings of the AP (these settings can be stored in GN21). If the STA wishes to use DNS, it must have the DNS settings of the AP (which can be received from GN21), or DNS services are provided through GN21.

Choosing a valid IP at random results in a very low probability of colliding with another IP address that is used in the AP.
Note, however, that the STA still needs to authenticate/log-in through the captive portal in case such portal exists.

Another method that can be used to quickly obtain an IP address, such that the IP address is not already allocated by the DHCP of the AP is disclosed. Most DHCP implementations of AP send an ICMP (Internet Control Message Protocol) Echo Request (ping) before allocating an IP address, to make sure that it is unused. Therefore, STA can begin the DHCP protocol, then, wait for the ICMP echo request that the AP sends, and understand the IP that is going to be allocated to it. Therefore, STA can start using the IP address and respond to the ICMP echo request. It can then

prematurely terminate the DHCP protocol (as it already got an IP). Alternatively, STA can use the IP address from the ICMP echo request without responding to it, and complete the DHCP process. If the IP address that is allocated during the DHCP is identical to the IP address (vast majority of cases), then STA simply saved time. Otherwise, it can move from the IP address of the ICMP echo request to the IP address that was allocated.

If no connection to GN21 is available, the default gateway address can be guessed, as in the majority of the cases the default gateway address is one out of only a few addresses. Common addresses are: 192.168.1.1, 192.168.2.1, 10.0.0.1, etc. Moreover, the default gateway is usually the AP itself. Its MAC address is known (as it is broadcasted in the beacon). Therefore, in most cases it is enough to forward packets to this MAC address (without knowing its IP address).

A STA with a Capability to Connect on Two Channels in Parallel

We disclose a STA which has a capability of communicating in two or more channels in parallel (for example, by using two wireless network cards). This capability can enable a STA to be connected to two APs in parallel without the need to implement sophisticated mechanisms that actually simulate this situation. Thus, a STA can connect with future AP while maintaining a connection through its serving APs. Being connected to two APs simultaneously allows greater bandwidth by utilizing two connections instead of one, and soft-handovers, i.e., the STA stays connected through one AP, while disconnecting from the second AP in the process of handover.

We Claim:

1. A system and method for fast handovers in unmanaged wireless networks where the process of the handover is almost completed before the handover actually started.

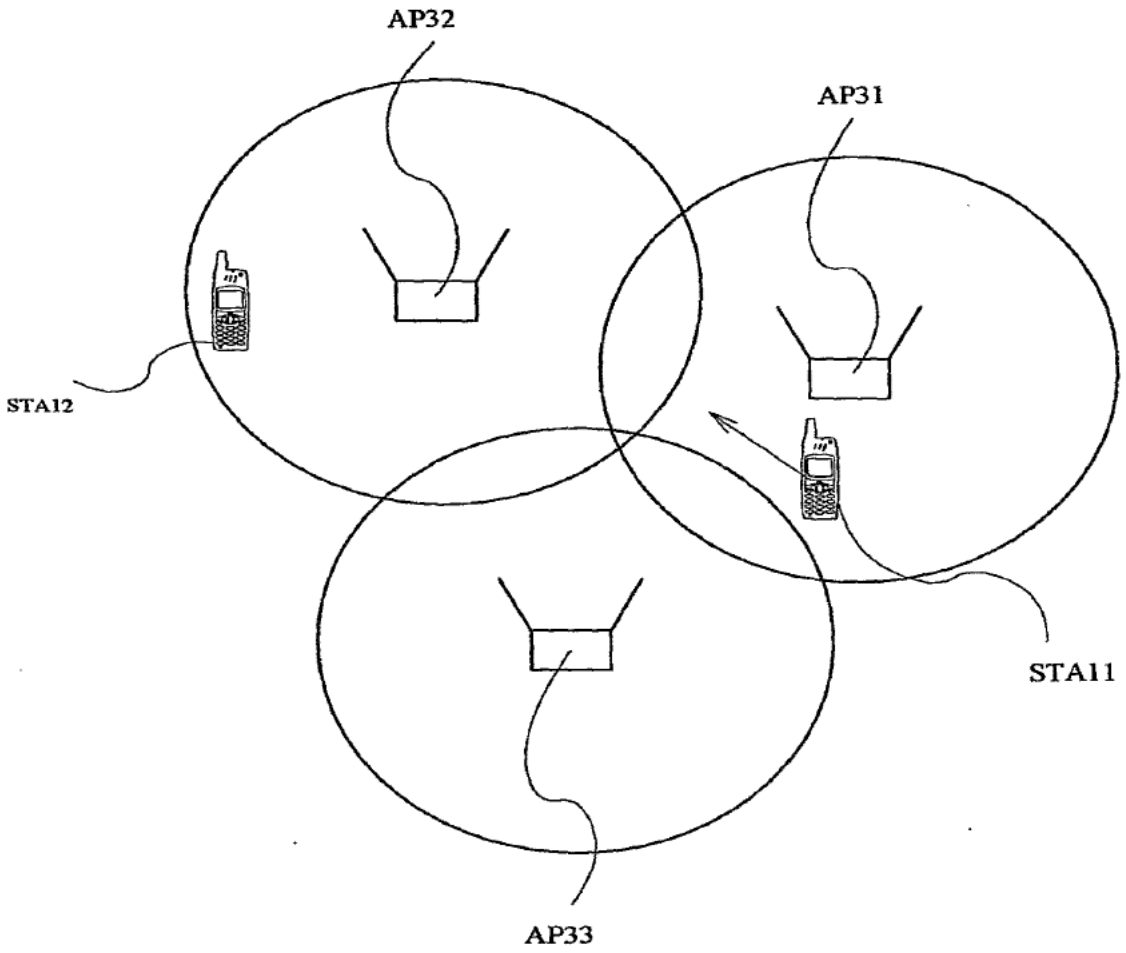


FIG.1

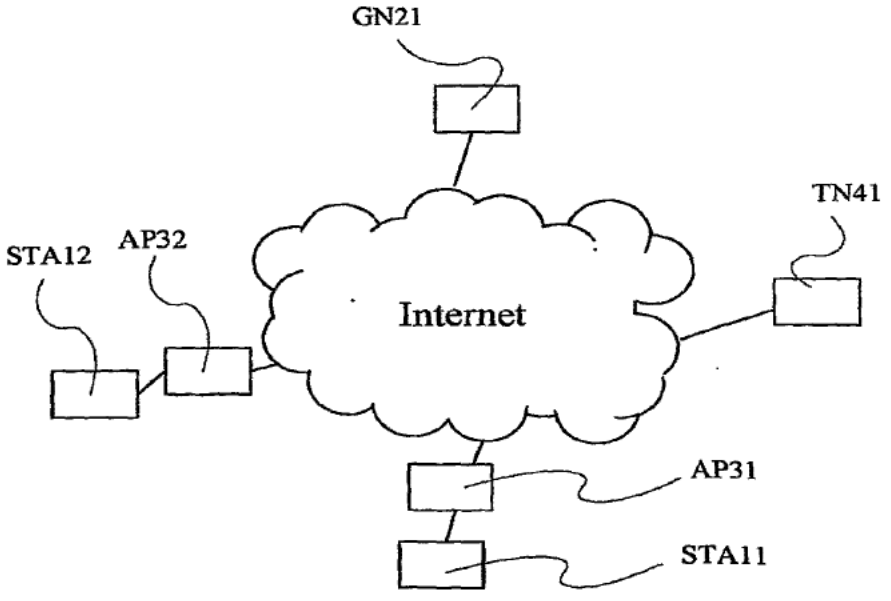


FIG.2

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/IL2007/000244

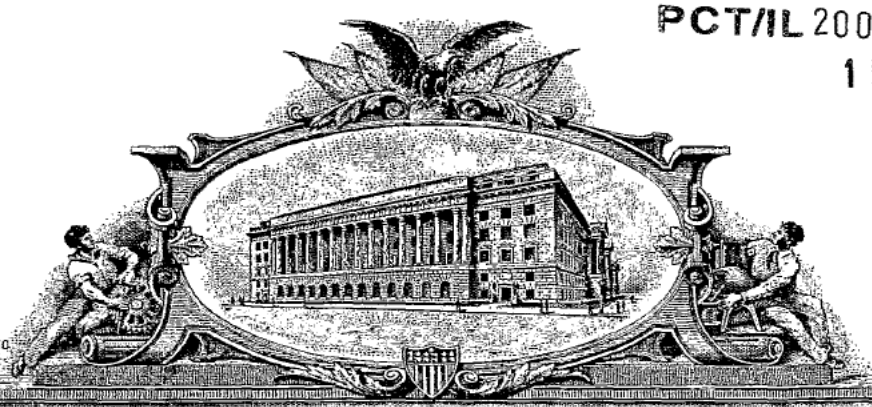
International filing date: 22 February 2007 (22.02.2007)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/794,135
Filing date: 24 April 2006 (24.04.2006)

Date of receipt at the International Bureau: 23 May 2007 (23.05.2007)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



PA 1600860

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

April 23, 2007

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/794,135***
FILING DATE: ***April 24, 2006***

THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS ***US60/794,135***

By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office

L. Edelen

L. EDELEN
Certifying Officer

PTO/SB/16 (10-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 1 of 2

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. FEDEX 8547 7694 7226

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
ELAD	BARKAN	KFAR-SIRKIN, ISRAEL

Additional inventors are being named on the _____ *separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max):

WIRELESS INTERNET SYSTEM AND METHOD

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ The address corresponding to Customer Number:

OR

☑ Firm or Individual Name ELAD BARKAN

Address 12 HABANIM St

City	KFAR SIRKIN	State		Zip	49935
Country	ISRAEL	Telephone	972-54-520-4121	Email	MOTI@BARKAN.ORG

ENCLOSED APPLICATION PARTS ***(check all that apply)***

☐ Application Data Sheet. See 37 CFR 1.76
☐ CD(s), Number of CDs _____
☐ Specification *Number of Pages* _____
☐ Other (specify) _____
☐ Drawing(s) *Number of Sheets* _____

Fees Due: Filing Fee of $200 ($100 for small entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

METHOD OF PAYMENT OF THE FILING FEE AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT

☑ Applicant claims small entity status. See 37 CFR 1.27.
☐ A check or money order is enclosed to cover the filing fee and application size fee (if applicable).
☑ Payment by credit card. Form PTO-2038 is attached

100.00
TOTAL FEE AMOUNT ($)

☐ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: _____. A duplicative copy of this form is enclosed for fee processing.

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/16 (10-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☑ No.
☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

SIGNATURE E. Barkan Date APRIL 20, 2006

TYPED or PRINTED NAME ELAD BARKAN REGISTRATION NO. _____ *(if appropriate)*

TELEPHONE +(972)-54-520-4121 Docket Number: _____

Provisional Application For Paten

Title: Wireless Internet System and Method

Date: April 20, 2006

Inventor: **Elad Barkan**

12 Habanim St.
Kfar Sirkin 49935
Israel

Tel: +(972)-54-520-4121
Fax: +(972)-3-933-2284
Email: moti@barkan.org

Wireless Internet System and Method

Technical Field

This invention concerns a method and a system for wireless communications. In particular, it concerns systems for providing wireless internet connection to roaming devices, such as Portable Computers, laptops, PDAs, and phones, and the deployment of such a wireless connection in a viral method, in such a way that the existing access points are not changed.

Background Art

Currently, there is a growing number of WiFi public hot-spots (or Access Points – "AP"). These APs allow WiFi enabled devices (which we refer to as STA) that are in their coverage area to connect to the internet.

Some of the APs are operated as a business, service, or as part of a community, either with or without a charge to the STA's user. Other APs are placed by individuals in their premises, but are not "locked", i.e., they are "open", allowing bypassing STAs to utilize them. Other APs placed by individuals are "locked" (or "closed"), thus not allowing passing STAs to utilize them.

As APs are being deployed in larger numbers, many individuals lock their APs due to fear of unfair use of their network resources, and due to security concerns. For instance, there have been cases where a person places an open AP, and his neighbor uses this AP as its internet connection on a full-time basis without the consent of the first person, thus abusing and degrading the service of the first individual. In other cases, the neighbor hacked into the computer of the first person through the network. Thus, as time passes, most APs are either locked, or a payment is required to use them. Although the total number of APs and their area of coverage is growing fast, an even larger number of APs are becoming locked and inaccessible to roaming STAs.

An interesting recent approach for allowing roaming customers to access the internet is taken by Fon (www.fon.com). It allows individuals to download a new software into their APs, which makes their APs a pay for use APs, and in addition, they receive a username and password for free access to other APs which are operated by Fon or

utilize their software. It also allows users to enjoy from a portion of some of the payments made by other users to use the network.

Roaming STAs are forced either to find an open AP, find an AP for which they have an account, or pay for access in case there is a pay-for AP.

It is an aim of the current disclosure to provide a system and a method for deployment of APs for the purpose of connecting STAs to the Internet.

Roaming customers that connect to an AP are often far from the AP and have borderline reception conditions. As a result, the connection quality is very poor, and the user may experience a slow service or no service at all.
It is another aim of the current disclosure to provide a system and a method for improving the connection quality for roaming STAs.

Brief Summary of Invention

The invention is described by way of example, but it should be obvious to those skilled in the art that many variations follow.

One of the novel methods behind the deployment of APs is that devices function at the same time as STAs and as APs. For example see Figures 1 and 2, a laptop 11 is connected to the Internet through access point AP 10, and at the same time, laptop 11 shares its connection for other STAs by operating as an AP. Thus, other STAs 12 and 13 see laptop 11 as an AP, and can connect through it to the Internet.

Another novel method in the current disclosure is that the laptop 11 limits the set of addresses or internet sites that STAs 12 and 13 can access, but the set of addresses includes a special web site 30 from which STAs 12 and 13 can download software 31, where software 31 is a software that includes the functionality of the software of laptop 11. Once STAs 12 and 13 download and execute the software 31, laptop 11 allows them a wider access to the internet. As a result, STAs 12 and 13 must download and run the software 31 to get wide access to the internet. As STAs 12 and 13 run software 31, they become APs in their own right, and allow other STAs to

download and connect through them to the internet in the current location of STA 12 and STA 13, as well as in any other location they go.

Another novel method of the present disclosure allows STA 14 (Fig. 2) to connect through two or more APs simultaneously. For example, STA 14 connects through both laptop 11 and laptop 21 to the internet. Thus, STA 14 can enjoy a more stable connection even if both connections (through laptop 11 and 21) are in borderline quality. Furthermore, even in case the connections are not borderline, they can be used to provide STA 14 a broader connection to the internet, or balance its traffic such that laptop 11 and laptop 21 carry a lighter burden per laptop with regards to the extra bandwidth they carry due to STA 14.

Multiple connections also allow handovers, as if a STA is moving from one place to the other it can first establish a new connection and then the old connection is terminated, practically leaving the STA connected.

In a further development of the novel method, laptop 21 can connect with laptop 11 directly or through STA 14, such that both enjoy the internet connection of the other. As the internet connection is not used all the time (typical laptop uses on average a few percents of its maximum bandwidth), both laptops will experience a much faster connection to the internet.

Another important issue is the security of the system. Laptop 11 might agree to act as an APs, but it does not agree to allow STA 13 and STA 14 (Fig. 2) to access its inner network (i.e., it allows STA 13 and STA 14 to access the internet *through* its network but does not allow them to access *into* its network. For example, a private server 40 [Fig. 2]) should not be accessible to STA 13 and STA 14. On the other hand, STA 13 wish to use laptop 11 network, but might not wish laptop 11 to be able to tap into its communications. The current disclosure provides novel method to deals with these two problems.

First, external STAs are not allowed access to the inner network by not allowing access to local IP addresses. Second, STA 13's privacy is protected by tunneling his

sensitive traffic to a trusted network site 50 (Fig. 2), and STA 13 accesses the internet through his tunnel to the trusted network site 50, which acts as a proxy of STA 13.

An important issue is to prevent STAs from using other laptops for their primary network connection for a long period of time. A novel method detects that a STA is connected to the internet through the same laptop for a long period of time, and disconnects the STA. Alternatively, the STA needs to pay to continue and use the network, thus encouraging the STA's user to purchase his own connection.

In yet another novel method, the software 31 running on laptop 11 can replace the commercial banners that appear in the web pages that laptop 11 surfs into, as well as the web pages that STA13 surfs into. The banners can be stopped, replaced, and made specially targeted to the user, for example based on his location.

A further novel method is that the wireless internet coverage that is obtained using laptops can be used by devices such as wireless IP phones to make phone calls using the wireless internet coverage, cellular phones that have built-in WiFi connection, or digital cameras with WiFi that wish to upload the data stored in them. Other devices might include for example, radio or TV broadcast capabilities.

Another novel method relates to the configuration of the wireless network. The configuration, and especially the security configuration of a wireless internet connection such as WiFi is cumbersome and annoying to most users. Assume STA 12 belongs to the same user (or user group) of the owner of laptop 11. Then, by a special logging into website 30, the configuration of laptop 11 can be copied to STA 12, thus configuring it to use AP 10 (i.e., allowing a connection without laptop 11).

Another novel method allows devices with a trusted hardware to receive information that instructs them how to directly connect to AP, by providing them with the needed settings and security information.

Brief Description of the Drawings

The invention will now be described by way of example and with reference to the accompanying drawings in which:

Fig. 1 illustrates access point AP 10 connected to the internet, a laptop 11 is connected to AP 10, and two other stations STA 12 and STA 13 are connected through laptop 11 to the internet. A special web site 30 is also depicted.

Fig. 2. includes Fig.1., and in addition it illustrates another access point AP 20, with laptop 21 connected to it. STA 14 is connected to both laptop 21 and laptop 11, STA 15 is connected to laptop 11, and also depicted is a trusted site 50 connected to the internet.

Mode of Carrying out the Invention

A preferred embodiment of the present invention will now be described by way of example and with reference to the accompanying drawings.

Having a single laptop connected to the internet and serve as an AP in the same time

One of the novel methods performing the deployment of APs is that devices function at the same time as STAs and as APs. For example, a laptop 11 is connected to the Internet through access point AP 10, and at the same time, laptop 11 shares its connection for other STAs by operating as an AP. Thus, other STAs 12 and 13 look at laptop 11 as an AP, and can connect through it to the Internet.

When laptop 11 is connected to AP 10 through a wired connection, it can simply set its wireless connection as an AP (Infrastructure mode). However, when laptop 11 is connected to AP 10 through a wireless connection, the situation is more complex. We disclose a novel method that laptop 11 can be connected to AP 10 and serve as an AP using only a single wireless network card. Laptop 11 connects to AP 10 just like any other STA, and at the same time runs the protocol stack of an AP. AP 10 use the same channel as AP 10, and transmits a beacon message such that the beacon of AP 10 and

the beacon of laptop 11 are expected not to collide in time. AP 10 derives and updates its internal clock from AP 10, but adds a constant delay (to make his beacon appear with a delay after AP 10). In another embodiment, laptop 10 does not add a delay to the time of AP 10, but sets the beacon period to a value, such that the greatest common denominator (GCD) between its beacon period and the beacon period of AP 10 is the smallest that is possible. Such a choice of beacon period ensures minimal collisions between the beacons.

Viral Spreading

Many networks suffer from the network effect, in which the initial users have no incentive to join the network. However, the network is of great value once many users are in the network.

The following method and system attracts the initial users, and provide an increasing value as the network grows. The first very few laptops with the software are installed and deployed in key areas by the network initiator. The software running on the laptop 11 has functionality 31 as follows (explained through an example):

Laptop 11 acts as an AP and allows other STAs to connect to it. To further lure STAs, the SSID (Service Set Identification – this is the name of the network that users see when looking for an available network) can be set to "Free Internet" or another name that will attract roaming laptop users to log-into it while searching for wireless networks.

Assume a user using a laptop called STA 12 connects as described above. Once STA 12 is connected to the laptop 11 (as an AP), no matter which web site the user tries to enter, the software on laptop 11 forwards the connection to a special web site 30. The web site 30 informs the user (STA 12) that in order to use the free connection it must install a software with functionality 31. The deal is that the user is allowed the free access at this location, but it is requested to share his own connection when such a connection is available. The user then downloads and installs the software with functionality 31. Once laptop 11 identifies that STA 12 has functionality 31 running, it allows it a wider access to the internet (or a full access to the public internet).

Thus STA 12, which originally did not have functionality 31 running, but its user wished to connect to the internet, ended up with functionality 31 installed and running on STA 12, and the user received a working internet connection. When the user moves STA 12 to another area in which it connects directly to an AP (which might be locked), it shares its connection with other STAs, which are also motivated to install functionality 31. Thus, functionality 31 can spread quickly among STAs, and the total area that is served grows larger, where each additional STA spreads the network further.

Connection through multiple access points

Another novel method of the present disclosure allows STA 14 to connect simultaneously through two or more APs. For example, STA 14 connects through both laptop 11 and laptop 21 to the internet. Thus, STA 14 can enjoy a more stable connection even if both connections (through laptop 11 and 21) are in borderline quality. Furthermore, even in case the connections are not in borderline quality, they can be used to provide STA 14 a broader connection to the internet, or balance his traffic such that laptop 11 and laptop 21 carry a lighter burden per laptop with regards to the extra bandwidth they carry due to STA 14.

Multiple connections also allow handovers. When a STA is moving from one place to another, it can first establish a new connection and then the old connection is terminated, practically leaving the STA connected.

When laptop 11 and laptop 21 use the same channel, STA 14 connects to both laptops by creating two protocol stacks on the MAC (Media Access Control) layer. When laptop 11 and laptop 21 operate on different channels, STA 14 agrees with laptop 11 and laptop 21 on period of times in which laptop 11 sends packets to STA 14, and periods of time in which laptop 21 sends packets to STA 14. STA 14 makes sure that these periods of times do not overlap, thus, STA 14 sets the channel according to the period, such that it listens on the channel of the laptop that might transmit to it. If the laptop has packets pending for STA 14 it queues them for transmission in the transmission period.

In order to have a faster connection through the two (or more) connections, STA 14 downloads/uploads some of the information through one connection, and the rest through the other connection. For example, when downloading a web page, STA 14 can download the text through one connection, and download the images through the other connection.

In another embodiment a remote site 50 with a fast internet connection acts as a proxy of STA 14. Incoming and outgoing packets are forwarded between STA 14and remote site 50. The packets are sent using error-correction codes that allow reconstructing the data even if some packets are lost on one connection, but reach the destination using the other connections. The role of remote site 50 can be assumed by a service provider, by computer with a software that the user installs in his premise, or by another user with high bandwidth.

When the STA moves from one location to another, new connections are being established, while others are being disconnected. However, as long as there is at least one active connection, the STA will stay connected to the internet continuously and seamlessly.

Sharing Internet Connection between Laptops

When laptops 21 and 11 are within radio (wireless) contact (or through the mitigation of other STAs), each laptop can treat the other as another connection at his disposal. Thus, the data rate can be significantly extended, much like the case with a STA connected to two laptops.

Security

Another important issue is the security of the system. Consider a situation in which laptop 11 agrees to act as an APs, but it does not agree to allow STA 13 and STA 14 to access his inner network (i.e., it allows STA 13 and STA 14 to access the internet *through* his network but does not allow them to access *into* his network. For example, a private server 40 should not be accessible to them). On the other hand, STA 13 wishes to use laptop's 11 network, but might not wish laptop 11 to be able to tap into his communications. The current disclosure deals with these two problems in a novel method. First, external STAs are not allowed to access to the inner network by not

allowing them to access to local IP addresses. Second, STA 13's privacy is protected by tunneling its sensitive traffic to a trusted network site 50, and STA 13 accesses the internet through its tunnel to the trusted network site 50, which acts as a proxy of STA 13.

To prevent STAs from accessing the inner network, laptop 11 blocks all traffic from the STAs to internal addresses (i.e., addresses that appear only in local networks and not in the public internet, such as 192.168.*.*, or 10.*.*.*, and 172.16.0.0 - 172.31.255.255). Another method, which can be applied independently, is to allow the connection if it is at least x hops into the internet, where x is the maximum number of hops in the local network (which can be discovered by performing a traceroute command). Another method is to allow access to addresses which have an IP address with a different prefix, as internal networks typically have the same prefix on the IP address.

To protect the privacy of STA while it is surfing, its traffic can be tunneled to a trusted network site 50, which acts as its proxy. The network site can be replaced by simply tunneling the connection to another node in the network, and switching the network node once in a while. The access to the remote nodes is made without identifying the STA, but only proving that it belongs to the group of STAs, thus, its privacy is preserved. The frequent switching of remote nodes eliminates the possibility that a remote node can gather a significant amount of private information from peeking into the communication. The list of available remote nodes can be kept by a directory service, which can be distributed in a peer-to-peer fashion.

In another embodiment, the remote node is a trusted computer installed by the user. Such a configuration has the added benefit that the user can access internal nodes in his own private network, effectively having a Virtual Private Network (VPN) with his home network.

Maintaining Fairness

It is desirable to avoid an unfair situation in which one user exploits the network by continuously using a connection without ever sharing a connection. If many users

follow these lines, the network experience will degrade as there will be only a small number of laptops connected directly to APs.

A novel mechanism detects that a STA is connected to the internet by noting that the same STA (using the same laptop) connects from the same small area (or through the same AP) for a long period of time (i.e., beyond a threshold). For example, this threshold can be set to two weeks. Once a STA passes the threshold, the functionality 31 notes the user that the threshold is reached. The user is then required to move to another area or pay a small fee to continue and access the AP.

Functionality 31 may note the user when the threshold is being approached, even before it actually reaches it. It can then give a pre-warning to the user.

The laptop is identified through his account information, through the MAC address of his network card, and other machine-specific information, such as the serial number of the hard-disk.

Control over advertisements

A novel method disclosed is that the functionality 31can scan the web pages that passes through it and block or replace the advertisements on the page depending on various data such as the user name, the user location, etc. The advertisements can be performed in collaboration with the web site that is being surfed into, or without.

The site 30 can instruct functionality 31 as to which advertisements should be removed or changed, and which advertisements should be placed. New advertisements can also be added in places that there were no advertisements to begin with.

Configuration of Wireless Networks

An annoying task associated with wireless networks is the configuration of a STA to work with a network. The security settings are especially annoying, and currently, most of the people avoid securing their network due to the cumbersome setting procedure.

A novel method is disclosed to perform easy configuration of a wireless settings. The method is composed of two parts, the first is establishing the settings for the first

device, and the second part is establishing the settings for the rest of the devices. First part: Assume a user on laptop 11 is connected to his wireless AP 10. If AP 10 is not set to use encryption, the user can ask (or be offered) to secure his network. Functionality 31 automatically accesses the interface of AP 10 and configures it with security settings. Laptop 11 is also set with the security settings. The settings are also stored in an account in web site 30, for future use. Site 30 can also provide functionality 31 with the information on how to set the security setting on the specific model of AP 10.

Second part: When the user uses another device STA 12, he connects to the network through functionality 31 on laptop 11, which redirects him to web site 30. On the site, he can log-in using his account details. Web site 30, through functionality 31 which is running on laptop 11, discovers that the two devices (laptop 11 and STA 12) are both connected through AP 10, and both belong to the same user account. As a result, web site 30 offers the user to reconfigure STA 12 to work directly with AP 10. The user is advised to download functionality 31 to STA 12, and run it. Once functionality 31 is running on STA 12, it configures STA 12 with the settings of the network (which are retrieved from web site 30).

Many variations can follow to the above procedure, and should be clear to those skilled in the art. For example, the settings may be stored on laptop 11 instead on web site 30, the settings may be encrypted, and the sequence of events can be changed. The result is an easy configuration of the network by the user.

A network infrastructure for other devices

Functionality 31 may allow devices that do not have the functionality 31 to access the network. Such a device receives a capability to be identified as eligible to access the network towards functionality 31, and it identifies as eligible to access towards functionality 31 on the laptop in order to gain access to the network. Such identification may include cryptographic means, such as a digital certificate signed by an appropriate certification authority (CA) which gives the device the capability to be identified.

Configuration of secure devices

It might be desirable to allow a device to directly connect to an AP, rather than connect through a laptop. When devices have a secure sub-system, i.e., a sub-system that is trusted by web site 30, web site 30 may allow it to retrieve the settings of the network (assuming that they are stored on web site 30), and configure the device to use the network.

As the device has a trusted sub-system, the settings can be stored in the sub-system, such that they do not leak outside.

Alternatively, functionality 31 can reconfigure the AP to allow access to a roaming device.

Displaying the coverage map

A problem often faced by users that wish to connect through wireless internet is that they cannot connect to the internet in their current location because the coverage in their area is locked, and they do not have access rights. A novel method and system helps users find the nearest location from which they can connect. Web site 30 holds a list of all access points from which users can successfully connect, together with all the list of APs from which are closed. The list includes the MAC address of each AP. Parts or all of this list can be downloaded in advance to a device, such as into laptop 11. Then, laptop 11 uses the beacons of the APs which might be locked to determine its position (for example, www.SkyHookWireless.com uses beacons to determine the location of a STA). Then, laptop 11 can display on a map the location of the user, and the locations of near by access point in which it can connect to the internet. The user can then go to the nearby locations and connect to the internet. The list in site 30 can be constantly updated by information that STAs receive.

In another embodiment, the list of APs in site 30 can also hold the probability that the AP is accessible. The probability can change if the access is provided by a laptop rather than an AP, and the laptop may be present or not. An area covered by several independent APs, each with low probability, results in an area with higher probability of accessibility in the intersection of these areas. The probability of accessibility can be depicted in the map shown to the user, for example, by different colors representing the different probabilities.

Claims

1. In wireless internet system, a device that operates as a STA and as an AP in the same time.
2. The device in claim 1, where the device contains a functionality that:
   a. connects stations on its AP interface to the internet on its STA interface;
   b. limits the scope of the internet that can be accessed by stations on its AP interface, and broadens this scope for a specific station if the station proves to be running the functionality;
   c. the limited score of internet includes access to a special site;
   d. a software with the functionality can be retrieved from the special site;
3. The device in claim 2, where the device can connect to more than one other such device in the same time.
4. The device in claim 2, where the device does not allow access of stations to its inner network.
5. The device in claim 2, where the device is also capable to connect to another laptop.
6. The device in claim 2, where the special site or functionality detect the fact that a device uses an AP beyond a certain threshold, and limit the scope of the internet connection once the threshold is met.
7. The device in claim 2, where the functionality can remove or replace the advertisements from the traffic.
8. The device in claim 2, where the functionality allows devices that lack the functionality to have a broader access to the internet.
9. The device in claim 8, where the functionality allows the broader access to device that lack the functionality only if they perform identification, which might include cryptographic means.
10. The device in claim 2, where the functionality includes the ability to reconfigure the settings of the wireless network in the AP or on the machine that it runs on.
11. The device in claim 9, where devices that do not have the functionality can receive network settings and connect directly to the AP.

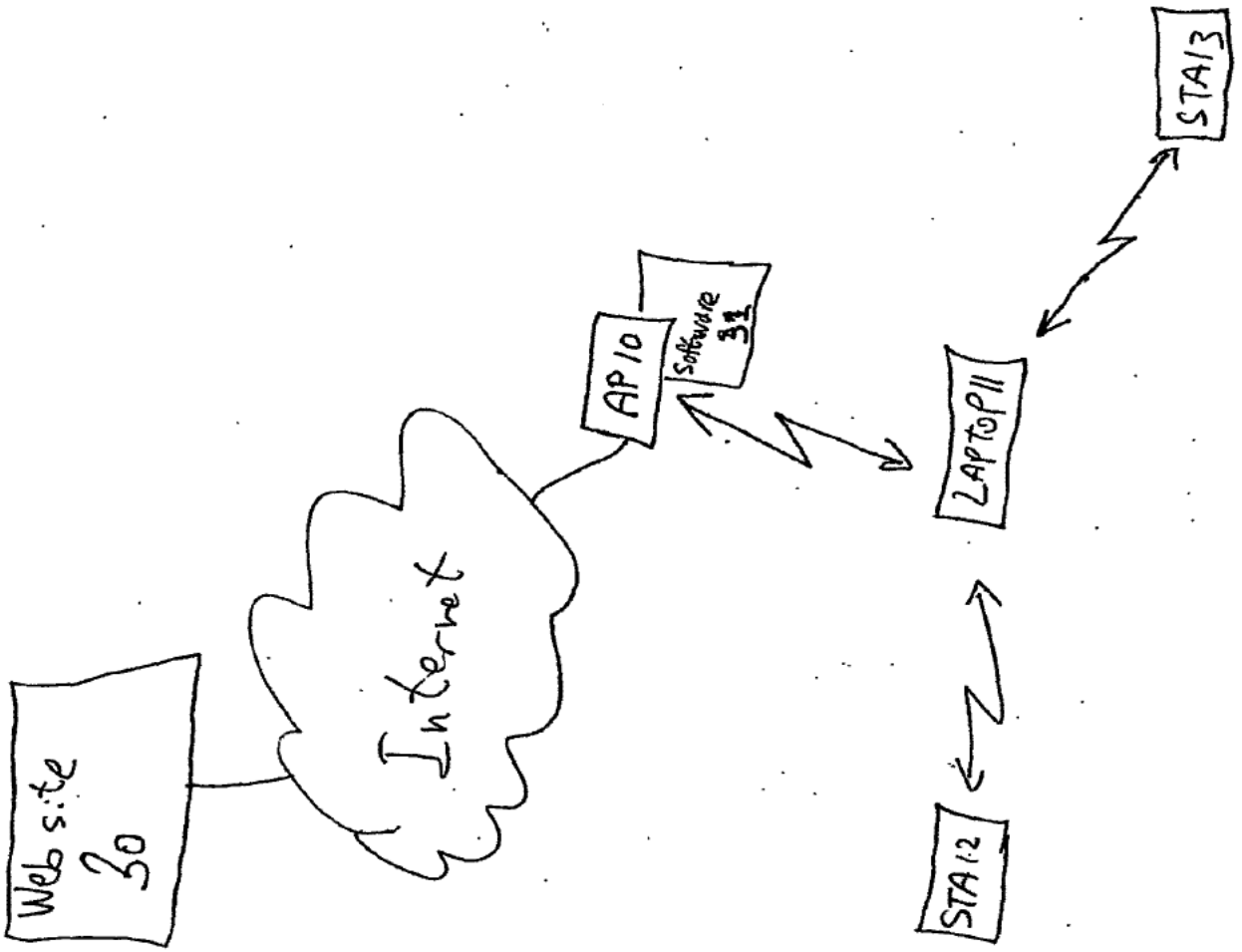


FIG. 1

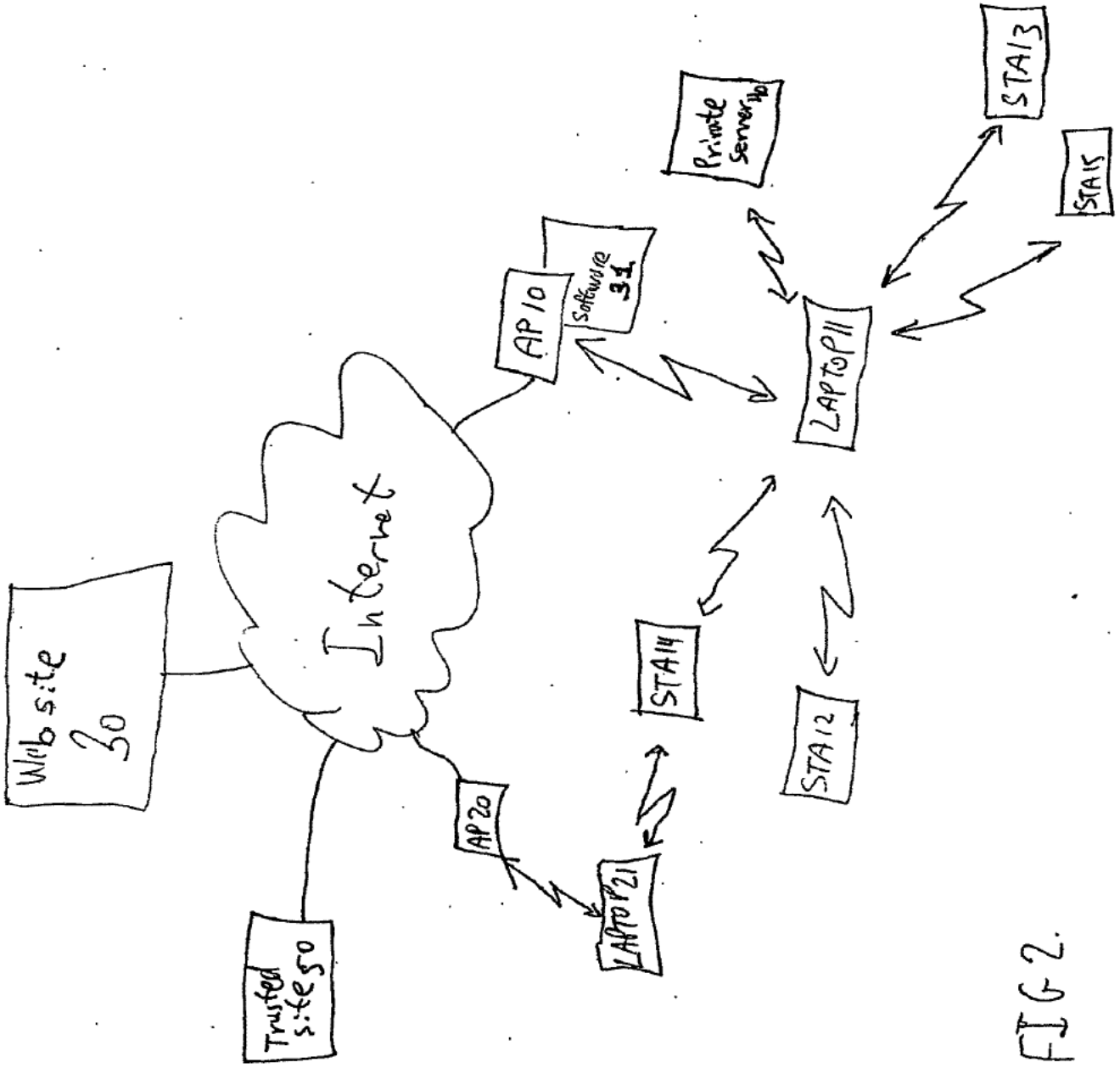


FIG 2.

BEST AVAILABLE COPY

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2007 (30.08.2007)

PCT

(10) International Publication Number
WO 2007/096884 A2

(51) International Patent Classification:
H04J 13/00 (2006.01)

(21) International Application Number:
PCT/IL2007/000244

(22) International Filing Date:
22 February 2007 (22.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/775,321 22 February 2006 (22.02.2006) US
60/794,135 24 April 2006 (24.04.2006) US

(71) Applicant and
(72) Inventor: **BARKAN, Elad** [IL/IL]; C/O Marc Zuta, Patent Attorney, P.O. Box 2162, 49120 Petah-Tikva (IL).

(74) Agent: **ZUTA, Marc**; Marc Zuta, Patent Attorney, P.O. Box 2162, 49120 Petah-Tikva (IL).

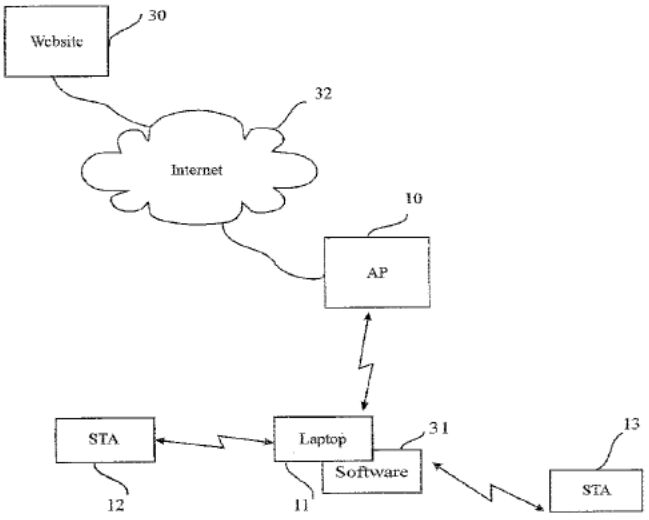
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: WIRELESS INTERNET SYSTEM AND METHOD



(57) Abstract: A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising: wirelessly connecting a first STA to the Internet through a first AP with a first SSID; remaining connected to the first Access Point (AP), the first STA creates a software-based wireless AP with a second SSID for wirelessly connecting other STAs to the Internet through the first STA. A software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein. A method for configuring STAs to connect to a wireless network, comprising: a customer first connects a STA by wire to its network; a software on the STA copies to the STA the security information gained through the wired connection, thus setting the security parameters for the STA.

WO 2007/096884 A2

Wireless Internet system and method

Cross-Reference to Related Applications

The present application is related to, and claims priority from, the provisional patent applications filed by the present applicant in U.S.A.: Application US 60/775,321 filed on 22 February 2006, and Application US 60/794,135 filed on 24 April 2006.

Technical Field

The present invention relates to a wireless Internet system and method, and more particularly to such systems for providing wireless Internet connection to roaming devices such as Portable computers, Laptops, PDAs and phones, and the deployment of such a system in a fast spreading manner (a viral-like method), in a client software-only manner such that the existing access points are not changed at all.

Background Art

Currently, there is a growing number of WiFi public hot-spots (or Access Points - "AP"). These APs allow WiFi-enabled devices (which we refer to as STA) that are in their coverage area to Connect to the internet.

Some of the APs are operated as a business, service, or as part of a community, either with or without a charge to the STA's owner. Other APs are placed by individuals in their premises, but are not "locked", i.e., they are "open", allowing bypassing STAs to utilize them. Other APs placed by individuals are "locked" (or "closed"), thus not allowing passing STAs to utilize them.

As APs are being deployed in growing numbers, many individuals lock their APs for fear of unfair use of their network resources, and due to security concerns. For instance, there have been cases where a person places an open AP, and his neighbor uses this AP as its internet connection on a full-time basis without the consent of the first person, thus abusing and degrading the service of the first individual. In other cases, the neighbor hacked into the computer of the first person through the network. Thus, as time passes, most APs are either locked, or a payment is required to use them. Although the total number of APs and their area of coverage is growing fast, a larger percent of the APs are becoming locked and inaccessible to roaming STAs.

A prior art approach for allowing roaming customers to access the Internet is taken by Fon (www.fon.com). It allows individuals to download a new software into their APs, which makes their APs a pay-for-use APs for STAs that roam in their vicinity, and in addition, they receive a username and password for free access to other APs which are operated by Fon or utilize their software. It also allows users to enjoy part of some of the payments made by other users to use the network. However, roaming STAs are forced either to find an open AP, find an AP for which they have an account, or pay for access in case there is a pay-for AP.

It is an aim of the current disclosure to provide a system and a method for deployment of APs for the purpose of connecting STAs to the Internet.

Roaming customers that connect to an AP are often far from the AP and have borderline reception conditions. As a result, the connection quality is very poor, and the user may experience a slow service or no service at all. It is another aim of the current disclosure to provide a system and a method for improving the connection quality for roaming STAs.

Another aspect of this invention refers to systems and methods for fast handovers in wireless networks such as 802.11 networks, specifically in un-managed wireless networks, and more particularly such systems and methods which allow extremely fast handovers in these networks without any changes to existing 802.11 base stations. The invention also

concerns efficient performance with regards to power consumption, coverage, security, installation, capacity and availability of wireless networks such as 802.11.
The invention can achieve these goals without any change to the WiFi access point.

Currently, there is a growing number of WiFi public hot-spots (or Access Points - "AP"). These APs allow WiFi enabled devices (which we refer to as STA) that are in their coverage area to connect to the internet.

Some of the APs are operated as a business, service, or as part of a community, either with or without a charge to the STA's owner. Other APs are placed by individuals in their premises, but are not "locked", i.e., they allow bypassing STAs to utilize them. The cumulative connectivity provided by the APs is enormous and growing fast, thus, it is tempting to use this cumulative connectivity to compete with other wireless technologies. For example, it would be tempting to have a STA that looks like a cellular handset (i.e., a WiFi Handset, or WiFi Phone), where the WiFi handset uses the free connectivity to provide a "free" service that competes with or complements the cellular service.

One of the major difficulties of achieving this vision is that the coverage of a single WiFi AP is very small (about a few hundreds to a few thousands of square meters). When a user goes out of this area, his connectivity is lost. A natural naive approach to solve this problem is performing a handover (sometimes also called handoff) to another AP with a better radio connection to the user. Another approach is to have a handset which supports both WiFi and Cellular, and handover the conversation from WiFi to Cellular [See: WO 2004/036770], this way, WiFi extends the coverage of cellular, and conversation is handed over from WiFi to cellular, when there is no WiFi coverage. However, the problem of performing handover between one WiFi AP to another WiFi AP remains when appropriate cellular coverage is not available (or there is no cooperation from the cellular company). The same idea applies when cellular is replaced by other access technology, such as satellite communications.

The concept of handover is taken from cellular networks. Handovers usually work well in

managed networks, such as cellular networks, campuses, or office environment., where the entire network is usually owned by the same operator.
The network operator in many cases chooses to add cells where coverage or capacity are needed. In managed networks, the APs (or the cellular cells) are synchronized and communicate with each other through a backbone, and are usually controlled by some other network entity (e.g., BSC - base station controller in cellular systems). For example, the APs can communicate with each other, for example using the IEEE 802.11F protocol - the Inter-AP protocol, which involves a RADIUS (Remote Authentication Dial In User Service, see RFC 2138, 2865, and 2866) server.

The APs can also employ a radio resource management such as IEEE 802.11K, or fast roaming using IEEE 802.11R, etc. However, in unmanaged networks, the APs can be deployed by many unrelated entities, such as by private individuals.

There is usually no entity that synchronizes the APs. The APs can be manufactured by various manufacturers, use various security mechanisms etc. In unmanaged networks, the handovers are typically very slow, as in the process of handover, it takes time for the STA to re-connect to the internet in the new AP (and it must disconnect from the previous AP). In such a handover in an unmanaged network, the IP address often changes. Therefore, a mechanism such as mobile IP must be used (as described later). This mechanism is limited with respect to the frequency in which the IP address can change, and a large latency (disconnection time) may result during the handover process. During the latency, the STA cannot receive any incoming messages.

A handover process is typically composed of the station STA connecting to a new AP, and disconnecting from the old AP. If STA is connected in parallel to both AP the handover is called soft-handover, and if STA first abandons the old AP and then connects to the new AP, the handover is called a hard-handover. Soft handovers require the ability of STA to communicate in parallel with at least two APs.

The process of connecting to a new AP is usually composed of the following steps:

1. STA performs a scanning process to discover neighboring APs.
2. STA chooses a new AP, and performs authentication with the AP, in which the AP verifies that STA is allowed to access the AP.
3. If the authentication is successful, STA performs an association process, in which the AP acknowledges that STA is connected to it (association requires the AP to allocate resources to the STA, and the 802.11 standard allows up to 2007 STAs to be associated with an AP).
4. Once STA is associated with the AP, the STA makes sure that it has all the information that it requires to communicate over the internet, for example, it must have an IP address, and it must update servers that govern its location (such as Mobile IP, as discussed later). In some cases, the user should go through a second authentication procedure (usually with a RADIUS server). Many times, this procedure is performed over a web interface, which is called a Captive Portal.

When a captive portal is used by the AP, the user needs to surf into the captive portal and perform a log-in to connect his IP address to the Internet. In some implementations, the user's web browser is forwarded to the captive portal regardless of the internet site that it tries to surf into. Some APs allow the STA to surf in some limited number of internet sites before they complete the second authentication procedure (for example, if the AP is in an hotel, it might allow surfing into the hotel's website, or affiliated news web sites). The procedure at the captive portal typically includes authentication, payment, or agreeing to terms of usage. Once the authentication is completed, the IP address of the STA is connected to the Internet (usually by reconfiguring the firewall that controls the communications of the AP). Each sub-process takes time to complete, resulting in a total delay of over several seconds to complete the entire process.

In managed networks, Step 4 can be performed once in a certain amount or time (or for a certain area), as moving between APs of the managed network does not necessarily change the parameters of the STA such as IP address etc. However, in un-managed networks (and sometimes also in managed networks), the STA must gain a new IP address and other parameters, usually through DHCP (Dynamic Host

Configuration Protocol, see RFC 1541). Completing the DHCP protocol can take up to several seconds. Sometimes, obtaining an IP is not enough, and a second authentication is needed. In other cases, a proxy server or a Socks server should be set for the communication. The entire process can consume a few seconds, which are intolerable in a streaming two-way application such as a voice conversation.

Many protocols that are used in the Internet require that the IP address of the STA would remain fixed during communications (for example, TCP - Transport Control Protocol, see RFC 793). However, a handover might result in the change of the IP address. This change of IP address causes a break in the communication as the communication needs to be restarted.

One solution to this problem is provided by the Mobile IP standard (see RFC 2002): in this solution the STA updates a server with its current IP address, every time that the IP address changes. As a preparation for roaming, the server allocates to the STA (in addition to the STA's current IP address) an IP address that remains fixed, even when the real IP address of the STA changes. This fixed IP address is also known as a "care of" address. From this moment on, the STA keeps the server posted of the real IP address of the STA, and the STA can use (in its communications with the rest of the Internet) the "care of" address (or its home address) as if it was its own fixed address.

Any IP data packet that is sent to the care-of IP address is tunneled by the Mobile-IP server to the current IP address of the STA. For packets originating from the STA to the Internet, the STA can tunnel the packets to the Mobile-IP server, which replaces the IP address with the care-of address. However, many times the STA can simply write its care-of IP address as the source address of the IP data packet, as many times, the source address of IP packets is not checked what-so-ever in the course of routing the IP data packet in the Internet.

The Mobile-IP solution can be applied as long as the handovers are not

performed too often. However, it incurs the punishment of routing all incoming packets through a server, causing both an increased travel time for the data packets, as well as latency (or disconnection) for the time that the real IP address changed, but the server is not informed yet. If the round-trip-time of the packets between the STA and the server is longer than the time a STA stays with the same IP, this method fails, as by the time packets reach the reported location of the STA, the STA is already in another location.

For many applications, such as voice, it is of utmost importance to minimize the time spent on the handover process. The time consumed by the handover process is usually dominated by the scanning step (Step 1 as mentioned above), and by Step 4 (specifically in case of an unmanaged network). There are many solutions that address fast handovers in cellular networks, and a few solutions that address fast handovers in managed WiFi networks (for example, see: WO2004/054283, which reduces Step 1 (mentioned above) by selective scanning but requires modifying the AP). None of these solutions deal with the delay due to Step 4.

It is an object of this invention to provide very fast handovers even in unmanaged networks.

Another barrier for wireless applications is that WiFi coverage might exists, and security policy might allow the STA to connect, but the AP might be out of resources (for example, there are 2007 associated STAs, and therefore it has no resources left, or that it has a limited IP address space which was already allocated through DHCP, and it has no IP address to allocate). It is an object of this invention to provide a system and method that allows STAs to use the services of the AP even when some of its resources are exhausted.

Another barrier for many wireless applications is the complex configuration of wireless parameters of STA, especially the security parameters. A user that purchases a new STA and has an existing AP, might wish to configure his new STA to work with his AP. This configuration includes entering into the STA the

encryption key and authentication key that would allow it to use the AP. Existing solutions require a change in the AP and STA, such that a special key can be pressed simultaneously at both ends to perform automatic configuration (like Buffalo INC's AirStation OneTouch Secure System - AOSS, or Broadcom's SecureEasySetup). Without such a solution, the user is usually forced to punch into his STA the security codes (which are typically long). The problem worsens when the STA moves between APs that use different security settings.

It is an object of this invention to provide for easy configuration on both levels: at the initial setup and while roaming.

Another barrier for many wireless applications is that WiFi coverage might exist, but it is locked and unavailable for use for the STA.It is an object of this invention to provide a solution for (legally) accessing locked APs.

Another problem with WiFi is that the WiFi protocol is not optimized for low battery consumption (compared to cellular protocols such as GSM). In current solutions, if the STA moves between APs and changes its IP, it must use mobile IP and inform an entity (server) in the network of its current IP (we refer to this process as "location update", as the STA updates the network entity of its location). Frequent location updates exhaust the STA's battery. Another problem with frequent location updates is that they create a heavy load on the network and on the network entities that manage and keep track of the STA's location.

The situation in WiFi is very different from the situation in cellular networks in two ways. Both of the ways cause an increase in the number of location updates in WiFi: First, in cellular network, the cells are typically much larger than a "cell" that is created by a WiFi AP. Therefore, in cellular networks, there are fewer transitions between cells, and hence less location updates. Second, cellular protocols allow defining a "location area" that encompasses several cells, and the STA is required to perform location update

only when moving between location areas, and thus reducing the number of location updates. Current WiFi protocols are not built to support location areas.

It is an object of this invention to provide a method that reduces the number of location updates required for STAs while moving between APs.

It is an object of the current invention to provide solutions to the above mentioned problems, using both a centralized (server based) approach, and also by providing a method for performing the solutions using a distributed peer-to-peer network. Therefore, no huge servers and no large investments are required.

Disclosure of Invention

The invention is described by way of example, but it should be obvious to persons skilled in the art that many variations thereof may be implemented.

A novel aspect of the invention relating to the deployment of APs is that devices function at the same time as STAs and as APs. This allows a STA to also create a new AP for connecting other STAs to the Internet therethrough. It is known in the art that a STA wireless card can operate in one of two modes, STA or AP. The present inventor has found a way to activate a device simultaneously in both modes.

According to another novel aspect, a connecting STA can limit the set of Internet addresses or internet sites that other STAs which connect through it can access, but the set of allowed addresses includes a special web site from which other STAs can download the Vagabee(TM) software. Vagabee software includes the functionality of the software of the first STA, to open new APs and further spread the Vagabee.

Once the new STAs download and execute the Vagabee software, the first STA

detects that the software is running on the new STAs, and allows them a wider access to the internet. Therefore, new STAs must download and run the Vagabee software to get wide access to the internet. As the new STAs run Vagabee, they become APs in their own right and allow other STAs to download and connect through them to the internet in the current location of these STAs, as well as in any other location they go.

Another novel method of the present invention allows a STA to connect through two or more APs simultaneously. Thus, a STA can enjoy a more stable connection even if part of the connections are of borderline quality. Furthermore, more connections may achieve a broader connection to the Internet, or may balance its traffic such that each STA carry a lighter burden with regards to the extra bandwidth they carry due to a new STA.

Multiple connections also allow faster handovers, as if a STA is moving from one place to the other it can first establish a new connection and then the old connection is terminated, practically leaving the STA connected.

In a further development of the novel method, a laptop (the terms STA and laptops are interchangeable, we use laptop rather than STA as in the preferred embodiment these cases the STA would be a laptop) can connect with another laptop directly or through a STA, such that both enjoy the Internet connection of the other. As the internet connection is not used all the time (typical laptop uses on average a few percents of its maximum bandwidth), both laptops will experience a much faster connection to the Internet.

Another important issue is the security of the system. A Laptop might agree to act as an APs, but it does not agree to allow other STAs to access its inner network (i.e., the laptop owner wishes to allows these STAs to access the internet through its private network but does not allow them to access computers on its private network. Another security concern is that the new

STAs may desire to prevent the first STA from tapping into their Communications, i.e., they do not want the first STA to be able to tap into communications that the first STA relays. The current disclosure provides novel method to deal with these two problems.

First, external STAs (new STAs) are not allowed access to computers in the inner network by having the first STA drop data packets from the external STAs that are designated to local IP addresses on the inner network. Second, a new STA's privacy is protected by tunneling its sensitive traffic to a trusted network site, and the new site accesses the Internet through his tunnel to the trusted network site which acts as a proxy for it.

An important issue is to prevent STAs from using other laptops for their primary network connection for a long period of time. A novel method detects that a STA is connected to the internet through the same laptop for a long period of time, and disconnects the STA. Alternatively, the STA has to pay to continue and use the network. The pricing can be such as to encourage the STA's user to purchase his own connection from an independent Internet Service Provider (ISP).

In yet another novel method, the software running on a laptop can replace the commercial banners that appear in the web pages the laptop surfs into, as well as the web pages that connected STAs surf into. The banners can be stopped, replaced, and made specially targeted to the user, for example based on his location.

A further novel method is that the wireless internet coverage that is obtained using laptops can be used by devices such as wireless IP phones to make phone calls using the wireless internet coverage, cellular phones that have built-in WiFi connection, or digital cameras with WiFi that wish to upload the data stored in them. Other devices might include for example, radio or TV broadcast capabilities.

For example, Digital cameras might be equipped with WiFi. The owner of such a

camera would like to upload his pictures from the camera to a server that stores the pictures on the Internet - the reasons for this may vary from being able to share the photos while on vacation with family members left at home, backup the pictures from the digital camera to the Internet server, or simply because the memory card on the camera is running out of space. A major problem is that to upload the pictures to the Internet may take a very long time, as pictures consume megabytes to store. In the novel method, the camera can send the photos to the laptop over WiFi (this connection is very fast), then disconnect and move on. Then, the laptop uploads the pictures to the Internet server (this process can take a long time as it involves uploading a lot of data), but the laptop owner would not feel it as a burden, since the pictures can be uploaded when his Internet connection is not used for other purposes.

Improvements to this method may include: The camera can encrypt the pictures so that the laptop owner cannot see them. The pictures can be still stored in the camera after being uploaded to the laptop, as the laptop might fail to upload them. The next time the camera connects to the Internet, it can check with the Internet server that the pictures arrived correctly to the server. If that is so, the pictures may be erased from the camera. Otherwise, the camera can re-transmit the pictures.

To have faster uploads, the camera can upload the pictures to several laptops that would upload the picture to the server.

Another novel method relates to configuring STAs to connect to a wireless network. The configuration, and especially the security configuration of STAs to connect to a wireless Internet connection such as WiFi is cumbersome and annoying to most users. Assume a STA belongs to the same user (or user group) of the owner of a laptop. Then, by a special logging into a website, the configuration of the laptop can be copied to the STA, thus configuring it to use the AP (i.e., allowing a connection without the laptop).

Another novel method allows devices with a trusted hardware to receive information that instructs them how to directly connect to AP, by providing them with the needed settings and security information.

One of the novel aspects of a very fast handover is to practically "almost complete" the process of the handover before it even started, possibly with the assistance of another STA that is already in the new AP's coverage (further details are described later).

Another novel aspect is that the same MAC address and IP address can actually be used by more than one STA. The differentiation between the STAs can be performed by using higher protocol identification, such as different port numbers (for example TCP ports), as detailed later.

It is useful for a station STA to know the identity of the adjacent APs that the STA might hand over to. The identity of an AP can be established in several ways, as disclosed herein. The SSID (Service Set ID) of the AP is usually broadcasted by the AP using periodical transmissions known as beacon. However, two adjacent AP may have the same SSID. In such a case, the MAC address of each AP is different, and APs can be differentiated based on their MAC address (which serves as a globally unique identification parameter). Some APs do not transmit beacon, and only respond when they are addressed using their SSID. In this case, a priory -knowledge is needed, see below.

Another aspect of the invention is for a STA to selectively scan for a neighboring AP in the following novel way. Assume that a STA scans to see if it can receive the beacon of a second AP, where the scanning will be performed exactly when the second AP is expected to transmit its beacon, therefore, the disconnection from the first AP will be minimal. The novel method consists of scanning and storing (in network entities) information about the relative time

between adjacent APs, and their relative clock drift. This information is retrieved at the appropriate time such that the STA knows to wait for the beacon just before it is transmitted.

Another aspect of the invention is to prevent exhaustion of resources at the APs. GN keeps a pool of MAC addresses with associated IP address. Just before a STA enters the AP, GN sends it a MAC address and an IP address that are already associated with the AP. Therefore, the STA can connect even if the AP has no resources left for new STAs.

Another novel aspect of the invention is to save Battery Power and reduce network load by reducing the number of Location Updates in WiFi. A location update is the process in which a STA informs an entity in the network on its current location (the notification can take many forms, including opening a TCP connection, or sending UDP packets). In prior art for 802.11 networks, a location update is required whenever the IP address of the STA changes (for example, when moving between APs of different subnets) - even if the STA is idle (not transmitting or receiving data). The novel method allows to define a location area for WiFi, such that an idle STA needs to perform location update only when it moves between APs that belong to different location areas, but does not need to perform location update when it moves between APs of the same location area, even if its IP address changes. See further details later.

A pseudo-beacon is another aspect of the invention which allows reducing the number of Location Updates. It is a message that GN can periodically transmit in each AP. While some APs might permit a remote node to transmit a message in the AP, other APs might not allow it. In the novel method, a certain MAC address, IP address, and possibly a port number, are allocated in each AP for the purpose of pseudo-beacon transmission. Further details are described later.

Configuring the security in new STAs to work with an existing AP might be a

tedious job, as the security (authentication/encryption) code might be very long as known in the art, and the user might need to punch it into the STA. A novel solution for easy configuration is disclosed. Unlike previous solutions, the novel method does not require changing the existing AP of the customer. In one embodiment, software is run on a personal computer of the user (that is already configured to access the WiFi). Then, the software establishes a secure channel with the STA, and copies the security information from the personal computer to the STA. In this way, the STA learns the security parameters. An authentication phase in which the STA is authenticated by the software or a remote server can be added before copying the security information.

In another embodiment, the customer first connects the STA by wire to its network (or alternatively, the STA first connects using a connection it establishes through an already connected device, such as a personal computer or laptop).

As the STA can receive and transmit signals on the wireless network and it is connected to the internet (through the other connection) at the same time, it tries to locate the web configuration of the AP on the wired network (most APs have a web interface). In most cases, it is an easy job for the STA, as either the STA can locate the AP as it is the default gateway of the wired network, or it can try to find its IP by performing RARP (Reverse Address Resolution Protocol) using the wireless MAC address of the AP (which it can see off-the-air). Further details are described later.

Another novel method for gaining access to locked networks is disclosed. While performing the above described easy setup (or at any other time), the user is prompted, if he wishes, to join a swapping service. The swapping service allows the user to gain access to many locked networks (the locked networks of the other users that joined the swapping service), in return he allows users to use his network for the purpose of connecting to the Internet. If the user agrees, the access parameters to his network (encryption key, MAC address,

default gateway, etc.) are securely stored in the network (for example in GN, and a backup server). The security information will be securely sent directly into the hardware of other STAs, when they need to connect using his AP. Further details are described later.

Another novel aspect of the invention takes advantage of the fact that the wireless network is local in nature, as the APs are geographically adjacent. As a result, the methods that are disclosed can be implemented by many small devices on the Internet, each responsible for a geographic area. The devices form a peer-to-peer network that implement the methods, without the need to rely heavily on large servers.

Another novel aspect of the invention is to have a STA which has a capability of communicating in two or more channels in parallel. This capability can enable a STA to be connected to two APs in parallel without the need to implement sophisticated mechanisms that actually simulate this situation. Thus, a STA can connect with future APs while maintaining a connection through its serving APs. Being connected to two APs simultaneously allows greater bandwidth by utilizing two connections instead of one, and soft-handovers, i.e., the STA stays connected through one AP, while disconnecting from the second AP in the process of handover.

The new system and method refers, among others, to the following innovative features:

1. A viral-like fast spread method for the Vagabee(tm) software:
- at the network level
- at the already connected PC
- at a connecting PC, already having the Vagabee software
- at a connecting PC, not yet having the Vagabee software
- details of the software package being loaded on a new computer: functions, operation, how installs, how spreads further away to other PCs.

2. Detail the viral spread method:
- use of existing standards; "as is" or with modifications
- method of reporting to user and getting a user's approval
- interaction with firewall and antivirus programs in the PC

3. Vagabee in use, with flow charts:
- manage communications with presently connected PCs
- add new PC
- remove a PC. Recover chain, reestablish communications when intermediary PC disconnects
- resolve conflicts where there are several Vagabee systems in one area.
Method of operation, so the networks will not interfere with each other,
rather they may assist each other and maybe provide backup functions.
- Knowing the identity of adjacent APs and the location of STAs.
- handoff to another local Vagabee network

4. Vagabee in use, system design:
- workload on the various PCs in the chain (the workload increases as one moves closer to the AP, the Internet connection)
- overhead, signaling and control, traffic control. Define signals, method of operation
- permission to access more sites on the Internet after a new PC downloads and activates Vagabee - how implemented.
- reliability issues

5. System design for various configurations
The basic assumptions greatly affect the performance of the network systems which may be formed:
- a PC connects to only one additional PC
- a PC may connect to one or two additional PCs
- a PC may connect to more than two additional PCs

6. Bandwidth control
Bandwidth request and allocation. For the various PCs in the chain.
Methods for improved channel use. How is implemented.

7. Privacy issues - how the inner/outer areas are implemented.
Protection from viruses and eavesdropping, passwords protection, etc.
Damage control, Recovery from a virus attack.
This is a vital aspect of the new technology.

8. User control and supervision
- the user of a PC decides whether to install Vagabee
- the user of a PC decides whether to allow additional users to connect, with what parameters (bandwidth allocation, etc.)
- incentives for a user to allow his computer to connect others.
- the user allows or forbids additional users, according to circumstances - how important his present activity is, what is the quality and bandwidth allocated to that user (how much spare bandwidth there is)

9. Details of implementation - software
- New software
- Modified existing software
- Method of use of existing software, standards

10. Functions, benefits to users - detail methods to implement them
- free internet connection
- enhanced bandwidth, reliability
- provide additional services - locate gas stations, Pizza Hut, restaurants.

Brief Description of Drawings

Figs. 1 and 2 illustrate a wireless system for connecting mobile devices to the Internet through an access point

Fig. 3 illustrates an expanded wireless system for connecting mobile devices to the internet through more than one access point

Fig. 4 details a method for fast spreading the Vagabee software by providing free wireless access to the Internet.

Fig. 5 details the dual mode connectivity of a STA also functioning as an AP with the Vagabee method and software

Figs. 6A to 6F detail stages in a wireless network evolvement and spreading of the Vagabee software

Fig. 7 details a method addressing control and security aspects of the Vagabee spreading method

Fig. 8 details a method addressing coordination and control aspects of the Vagabee spreading method for the first, connecting STA

Fig. 9 details multi-AP, fast configuration setting and handover aspects of the Vagabee spreading method for the second, to be connected STA

Fig. 10 details multi-AP, fast secure configuration setting and redirection aspects of the Vagabee spreading method for the first, connecting STA

Fig. 11 details multi-AP and fast configuration setting aspects of the Vagabee spreading method for the second, to be connected STA

Fig. 12 illustrates a system including mobile stations (STAs) and their Access Points (APs), with one STA moving from the coverage of one AP to the coverage of another

Fig. 13 illustrates a wireless system facilitating handover and including a STA, a Governing Node (GN) and another user, Termination Node (TN)

Fig. 14 details the handover method

Fig. 15 details a method for implementing two connections with a STA.

Fig. 16 details a method for connecting other STAs

Fig. 17 details another method for connecting other STAs

Fig. 18 details a method for configuring other STAs to directly connect to the AP

Fig. 19 details another method for configuring other STAs to directly connect to the AP

Fig. 20 details yet another method for configuring other STAs to directly connect to the AP

Best Mode for Carrying Out the Invention

A preferred embodiment of the present invention will now be described by way of example and with reference to the accompanying drawings.

Dual use laptop simultaneously connected to the internet and serving as AP

Figs. 1 and 2 illustrate a wireless system for connecting mobile devices to

the Internet through an access point. It may use a novel method for performing the deployment of APs, i.e., the method that allows devices to function at the same time as STAs and as APs. For example, a laptop 11 is connected to the Internet through access point AP 10, and at the same time, laptop 11 shares its connection for other STAs by operating as an AP. Thus, other STAs 12 and 13 look at laptop 11 as an AP, and can connect through it to the Internet.

When laptop 11 is connected to AP 10 through a wired connection, it can simply set its wireless connection as an AP (Infrastructure mode). However, when laptop 11 is connected to AP 10 through a wireless connection, the situation is more complex. Disclosed is a novel method in which laptop 11 can be connected to AP 10 and serve as an AP using only a single wireless network card. Laptop 11 connects to AP 10 just like any other STA, and at the same time runs the protocol stack of an AP.

Laptop 11 uses the same channel as AP 10, and transmits a beacon message such that the beacon of AP 10 and the beacon of laptop 11 are expected not to collide in time. Laptop 11 derives and updates its internal clock from AP 10, but adds a constant delay (to make his beacon appear with a delay after AP 10). In another embodiment, laptop 11 does not add a delay to the time of AP 10, but sets the beacon period to a value, such that the greatest common denominator (GCD) between its beacon period and the beacon period of AP 10 is the smallest that is possible. Such a choice of beacon period ensures minimal collisions between the beacons.

In the preferred embodiment, laptop 11 will run a Network Address Translation (NAT) and a DHCP server as part of his protocol stack. Running DHCP enables laptop 11 to provide an Internet address to STAs that connect to it. Running a NAT allows laptop 11 to connect other STAs through it, while keeping conformance with regards to AP 10 - To AP 10 all the communication appears to be originating form laptop 11.

The software package 31 may be contained in the laptop 11, or in the laptop 11

and the STA 12, for example.

Viral Spreading

Many networks suffer from the network effect in their infancy, in which the first users have no incentive to join the network. However, the network is of great value once many users are in the network.

The following method and system attracts the first users, and provide an increasing value as the network grows. The first very few laptops with the software are installed and deployed in key areas by the network initiator. The software running on the laptop 11 has functionality 31 as follows (explained through an example):

Laptop 11 acts as an AP and allows other STAs to connect to it. To further lure STAs, the SSID (Service Set Identification - this is the name of the network that users see when looking for an available network) can be set to "Free Internet" or another name that will attract roaming laptop users to log-into it while searching for wireless networks.

Assume a user using a laptop called STA 12 connects as described above. Once STA 12 is connected to the laptop 11 (laptop 11 serves as an AP), no matter which web site the user tries to enter, the software 31 on laptop 11 forwards

the connection to a special web site 30. The web site 30 informs the user (STA 12) that, in order to use the free connection, it must install a software with functionality 31. The deal is that the user is allowed the free access at this location, but it is requested to share his own connection when he has one at his disposal. The user then downloads and installs the software with functionality 31 (See Fig 1.B which shows software with functionality 31 running on STA 12. Once laptop 11 identifies that STA 12 has functionality 31

running, it allows it a wider access to the internet (or a full access to the public Internet).

Thus STA 12, which originally did not have functionality 31 running, but its user wished to connect to the internet, ended up with functionality 31 installed and running on STA 12, and the user received a working internet connection. When the user moves STA 12 to another area in which it connects directly to an AP (which might be locked), it shares its connection with other STAs, which are also motivated to install functionality 31. Thus, functionality 31 can spread quickly among STAs, and the total area that is served grows larger, where each additional STA spreads the network further.

Laptop 11 together with its software might need to use two different security parameters at the same time - one towards AP 10 (which might be locked), and open security towards other laptops - so they can connect with no security settings. Once functionality 31 is running, it can establish a secure connection with laptop 11 as a secure layer on top of the fundamental insecure wireless.

Connection through multiple access points

Another novel method of the present disclosure allows STA 14 to connect simultaneously through two or more APs, see Fig. 3. For example, STA 14 connects through both laptop 11 and laptop 21 to the internet. Thus, STA 14 can enjoy a more stable connection even if both connections (through laptop 11 and 21) are in borderline quality. Furthermore, even in case the connections are not in borderline quality, they can be used to provide STA 14 a broader connection to the internet, or balance his traffic such that laptop 11 and laptop 21 carry a lighter burden per laptop with regards to the extra bandwidth they carry due to STA 14.

Multiple connections also allow handovers. When a STA is moving from one place

to another, it can first establish a new connection and then the old connection is terminated, practically leaving the STA connected.

When laptop 11 and laptop 21 use the same WiFi channel, STA 14 connects to both laptops by creating two protocol stacks on the MAC (Media Access Control) layer. When laptop 11 and laptop 21 operate on different channels, STA 14 agrees with laptop 11 and laptop 21 on period of times in which laptop 11 sends packets to STA 14, and periods of time in which laptop 21 sends packets to STA 14. STA 14 makes sure that these periods of times do not overlap, thus, STA 14 sets the channel according to the period, such that it listens on the channel of the laptop that might transmit to it. If the laptop has packets pending for STA 14 it queues them for transmission in the transmission period.

In order to have a faster connection through the two (or more) connections, STA 14 downloads/uploads some of the information through one connection, and the rest through the other connection. For example, when downloading a web page, STA 14 can download the text through one connection, and download the images through the other connection.

In another embodiment a remote site 50 with a fast Internet connection acts as a proxy of STA 14. Incoming and outgoing packets are forwarded between STA 14 and remote site 50. The packets are sent using error-correction codes that allow reconstructing the data even if some packets are lost on one connection, but some packets reach the destination using the other connections. The role of remote site 50 can be assumed by a service provider, by computer with a software that the user installs in his premise, or by another user with high bandwidth.

When the STA moves from one location to another, new connections are being established, while other connections are being disconnected. However, as long as there is at least one active connection, the STA will stay connected to the Internet continuously and seamlessly.

Sharing Internet Connection between Laptops

When laptops 21 and 11 are within radio (wireless) contact (or through the mitigation of other STAs), each laptop can treat the other as another connection at his disposal. Thus, the maximum data rate available for each laptop can be significantly extended, much like the case with a STA connected to two laptops.

Fig. 4 details a method for fast spreading the Vagabee software by providing free wireless access to the Internet. The method includes:

a. First STA transmits "AP available" WIFI info 41
b. Info is presented to Guest 42
c. Guest chooses our AP? 43
d. Allow limited access to Guest including our Web site 44
e. Guest agrees to use our service? 45
f. Download connectivity software to Guest and activate it 46
g. Connect Guest to Internet and allow wider access 47
h. Guest transmits "AP available" info and further spreads our service 48
** End of method **

Note: It is not mandatory to perform all the above stages. The more important steps are 45 - 47 or any similar implementation.

Fig. 5 details the dual mode connectivity of a STA also functioning as an AP with the Vagabee method and software. The method includes:

a. First STA associates with an AP as a regular STA 411
b. First STA activates "AP" protocol stack with open security 412
c. Guest chooses our AP? 42
d Address translation to connect Guest to our Website 445

** End of method **

The above method has been implemented by the present inventor on a communication device using the Intel 2200 chipset, just as an example to show that it can be done. The present inventive approach and method may be used towards similar implementations with other communication devices.

Figs. 6A to 6F detail stages in a wireless network evolvement and spreading of the Vagabee software, including:

FIG. 6A: There is a Laptop 11 connected to the internet by wireless through the access point AP 10.

FIG. 6B: The Laptop 11 also functions as AP using the Vagabee software, thus allowing free access for STA 12 through Laptop 11.

FIG. 6C: STA 12 joined the Vagabee group, created a new AP to also connect Laptop 121. A long chain can thus be formed.

FIG. 6D: each AP can connect several new devices, as illustrated here with Laptop 122.

FIG. 6E: a multi-AP network may be configured, with a plurality of devices being connected through both AP 10 and AP 20. A device such as Laptop 122 can be simultaneously connected through more than one AP to the internet.

FIG. 6F: As the initiated device Laptop 124 moves to another location and connects to AP 24 (maybe it has a license or privileged access there, while Latop 125 and STA 126 cannot connect directly to AP 24 due to distance or lack of security parameters), the Vagabee software in device 124 opens a free AP at

that location, now being utilized by Laptop 125 and STA 126 to connect to the internet. At a separate location, AP 10 may still operate and connect STA 12, Laptop 121 etc.

Security

Another important issue is the security of the system. Consider a situation (shown in Fig.2) in which laptop 11 agrees to act as an APs, but it does not agree to allow STA 13 and STA 14 to access his inner network (i.e., it allows STA 13 and STA 14 to access the internet through his network but does not allow them to access computers in his network. For example, a private server 40 should not be accessible to them). On the other hand, STA 13 wishes to use laptop's 11 network, but might not wish laptop 11 to be able to tap into the data that STA 13 exchanges with Internet servers. The current disclosure addresses these two problems using a novel method. First, external STAs are not allowed to access to the inner network by not allowing them to access to local IP addresses. Second, STA 13's privacy is protected by tunneling its sensitive traffic to a trusted network site 50, and STA 13 accesses the internet through its tunnel to the trusted network site 50, which acts as a proxy of STA 13.

To prevent STAs from accessing the inner network, laptop 11 blocks all traffic from the guest STAs to internal addresses (i.e., addresses that appear only in local networks and not in the public internet, such as 192.168.*.*, or 10.*.*.*, and 172.16.0.0 - 172.31.255.255). Another method, which can be applied independently, is to allow the connection if it is at least x hops into the Internet, where x is the maximum number of hops in the local network (which can be discovered by performing a traceroute command). Another method is to allow access to addresses which have an IP address with a different prefix, as internal networks typically have the same prefix on the IP address. In another method, laptop 11 allow only packets to and from known servers such as trusted server 50 (i.e., white listing the allowed addresses).

To protect the privacy of STA while it is surfing, its traffic can be tunneled to a trusted network site 50, which acts as its proxy. The network site can be replaced by simply tunneling the connection to another node in the network, and switching the network node once in a while. The access to the remote nodes is made without identifying the STA, but only proving that it belongs to the group of STAs, thus, its privacy is preserved. The frequent switching of remote nodes eliminates the possibility that a remote node can gather a significant amount of private information from peeking into the communication. The list of available remote nodes can be kept by a directory service, which can be distributed in a peer-to-peer fashion.

In another embodiment, the remote node is a trusted computer installed by the user. Such a configuration has the added benefit that the user can access internal nodes in his own private network, effectively having a Virtual Private Network (VPN) with his home network.

Fig. 7 details control and security aspects of the Vagabee spreading method including:

a. First STA transmits "AP available" WIFI info 41
b. Info is presented to Guest 42
c. Guest has Vagabee software? 425
d. Guest agrees to use our service? 45
e. Download connectivity software to Guest and activate it 46
f. Connect Guest to Internet and allow wider access, excluding private servers/sites 472
g. Guest transmits "AP available" info and further spreads our service 48
h. Guest uses encryption and secure website to preserve privacy from connecting STA 481
i. Establish best route for all STAs 482
adaptive to changes in network.

Load balancing.
Connections thru multiple routes.

j. Connection time > Ts ? 483
k. Disconnect/change connection 485
** End of method **

Note: Not all the steps above are mandatory; a method may implement only part of the steps in the above method.

Maintaining Fairness

It is desirable to avoid an unfair situation in which one user exploits the network by continuously using a connection without ever sharing a connection. If many users follow these lines, the network experience will degrade as there will be only a small number of laptops connected directly to APs. A novel mechanism detects that a STA is connected to the internet by noting that the same STA (using the same laptop) connects from the same small area (or through the same AP) for a long period of time (i.e., beyond a threshold). For example, this threshold can be set to two weeks. Once a STA passes the threshold, the functionality 31 notes the user that the threshold is reached. The user is then required to move to another area or pay a small fee to continue and access the AP.

Functionality 31 may note the user when the threshold is being approached, even before it actually reaches it. It can then give a pre-warning to the user.

The laptop is identified through his account information, through the MAC address of his network card, and other machine-specific information, such as the serial number of the hard-disk.

Fig. 8 details coordination and control aspects of the Vagabee spreading method for the first, connecting STA, including:

a. First STA connects to AP in "AP" mode 412

b. Set wireless connection as "Ad-Hoc" using the same channel as the AP 413

c. Transmit beacon message at a delay after AP or set beacon period so as to minimize collisions 415

d. Act as AP for additional STAs, while preventing them access to its inner network 416

e. Replace commercial banners for own site and also for STAs connected to this STA 417

f. Security Option: Allow connection of connected STAs only if it is at least X hops into the Internet 418

g. Maintaining fairness: demand a connected STA to disconnect or move or pay after a predefined time 419
** End of method **

Fig. 9 details multi-AP, fast configuration setting and handover aspects of the Vagabee spreading method for the second, to be connected STA, including:

a. Connect through a first AP 481

b. Activate Vagabee to provide AP service to other STAs 482

c. Search for additional paths to 483
establish multiple simultaneous connections thru multiple APs

d. Copy configuration of connecting STA, 484
to gain direct access to the initial AP, or receive connecting instructions for STAs with trusted hardware

e. Preserve privacy using tunneling 485
to a trusted network site for sensitive traffic

f. Perform handover whenever necessary 486

g. When moving to a new location: 487
establishing a connection with available AP,
Activate Vagabee to provide AP service to other STAs

h. Maintaining fairness: demand a connected STA 419
to disconnect or move or pay after a predefined time

i. Control over advertisements (optional)
** End of method **

In a novel method hereby disclosed, the functionality 31 can scan the web pages that pass through it and block or replace the advertisements on the page depending on various data such as the user name, the user location, etc. The advertisements can be performed in collaboration with the web site that is being surfed into, or without.

Note: the functionality (or software module) 31 is an important part of the present method, a minimum requirement to allow Xiopea(tm) spreading. Moreover, module 31 need not include all the possible things that this

functionality can include, rather just the bare minimum directed toward allowing a connection to a STA in return to supporting the spreading of the this software.

The site 30 can instruct functionality 31 as to which advertisements should be removed or changed, and which advertisements should be placed. New advertisements can also be added in places that there were no advertisements to begin with.

The software 31 running on laptop 11 can replace the commercial banners that appear in the web pages that laptop 11 surfs into, as well as the web pages that STA 13 surfs into. The banners can be stopped, replaced, and made specially targeted to the user, for example based on his location.

Configuration of Wireless Networks

An annoying task associated with wireless networks is the configuration of a STA to work with a network. The security settings are especially annoying, and currently, many people avoid securing their network due to the cumbersome setting procedure.

A novel method is disclosed to perform easy configuration of a wireless settings. The method is composed of two parts, the first is establishing the settings for the first device, and the second part is establishing the settings for the rest of the devices. First part: Assume a user on laptop 11 is connected to his wireless AP 10. If AP 10 is not set to use encryption, the user can ask (or be offered) to secure his network. Functionality 31 automatically accesses the interface of AP 10 and configures it with security settings. Laptop 11 is also set with the security settings. The settings are also stored in an account in web site 30, for future use. Site 30 can also provide functionality 31 with the information on how to set the security setting on the specific model of AP 10.

Second part: When the user uses another device STA 12, he connects to the network through functionality 31 on laptop 11, which redirects him to web site 30. On the site, he can log-in using his account details. Web site 30, through functionality 31 which is running on laptop 11, discovers that the two devices (laptop 11 and STA 12) are both connected through AP 10, and both belong to the same user account. As a result, web site 30 offers the user to reconfigure STA 12 to work directly with AP 10. The user is advised to download functionality 31 to STA 12, and run it. Once functionality 31 is running on STA 12, it configures STA 12 with the settings of the network (which are retrieved from web site 30, or directly from laptop 11).

Fig. 10 details multi-AP, fast secure configuration setting and redirection aspects of the Vagabee spreading method for the first, connecting STA, including:

a. First STA connects to AP in "AP" mode 412

b. Establish settings for first STA: 511
configure AP with secure settings, set STA with secure settings.
Store settings in web site.

c. Redirect a connecting STA to the web site 512
to configure it with secure settings.
** End of method **

Fig. 11 details multi-AP and fast configuration setting aspects of the Vagabee spreading method for the second, to be connected STA, including:

a. Connect through a first/available AP 481

b. STA has secure sub-system trusted by the web site? 482

c. Web site allow it to retrieve the 483
settings of the network for direct connection

d. Both STAs use the same AP 484
and same user account?

e. Agrees to connect directly to AP? 485

f. Download functionality and activate it 486

g. Configure STA with the settings of the network 487
** End of method **

Many variations can follow to the above procedure, and should be clear to those skilled in the art. For example, the settings may be stored on laptop 11 instead on web site 30, the settings may be encrypted, and the sequence of events can be changed. The result is an easy configuration of the network by the user.

Fig. 12 illustrates the mobile stations (STA) with their covering Access Points (AP), where STA 11 is moving from the coverage of AP 31 to the coverage of AP 312. STA 12 is already in the coverage of AP 312, and another AP 313 has a coverage that intersects with both the coverage of AP 31 and AP 312.

A network infrastructure for other devices

Functionality 31 may allow devices that do not have the functionality 31 to access the network. Such a device receives a capability to be identified as eligible to access the network towards functionality 31, and it identifies as eligible to access towards functionality 31 on the laptop in order to gain access to the network. Such identification may include cryptographic means,

such as a digital certificate signed by an appropriate certification authority (CA) which gives the device the capability to be identified. Alternatively, the devices can be identified based on their MAC address. A username/password can be added for additional security.

Configuration of secure devices

It might be desirable to allow a device to directly connect to an AP, rather than connect through a laptop. When devices have a secure sub-system, i.e., a sub-system that is trusted by web site 30, web site 30 may allow it to retrieve the settings of the network (assuming that they are stored on web site 30), and configure the device to use the network.

As the device has a trusted sub-system, the settings can be stored in the sub-system, such that they do not leak outside.

Alternatively, functionality 31 can reconfigure the AP to allow access to a roaming device.

Displaying the coverage map

A problem often faced by users that wish to connect through wireless internet is that they cannot connect to the internet in their current location because the coverage in their area is locked, and they do not have access rights. A novel method and system helps users find the nearest location from which they can connect. Web site 30 holds a list of all access points from which users can successfully connect, together with all the list of APs from which are closed. The list includes the MAC address of each AP. Parts or all of this list can be downloaded in advance to a device, such as into laptop 11.

Then, laptop 11 uses the beacons of the APs which might be locked to determine its position (for example, www.SkyHookWireless.com uses beacons to determine

the location of a STA). Then, laptop 11 can display on a map the location of the user, and the locations of near by access point in which it can connect to the internet. The user can then go to the nearby locations and connect to the Internet. The list in site 30 can be constantly updated by information that STAs receive.

In another embodiment, the list of APs in site 30 can also hold the probability that the AP is accessible. The probability can change if the access is provided by a laptop rather than an AP, and the laptop may be present or not. An area covered by several independent APs, each with low probability, results in an area with higher probability of accessibility in the intersection of these areas. The probability of accessibility can be depicted in the map shown to the user, for example, by different colors representing the different probabilities.

It is understood that the method and system in the present disclosure may be used for the transmission of voice, data, multimedia or a combination thereof.

Gathering Physical Location

To display a map of coverage, the real-world physical location of STAs needs to be known. A novel idea is to use STAs that are equipped with both GPS (Global Positioning System) and WiFi to report back to a server (for example, web server 20), a scanning result and the physical location in which the scan was performed. The server can extract the physical location of the fixed APs and store it in a database. At a later time, when a WiFi-equipped STA that lacks a GPS receiver performs a WiFi AP scan, it can report the results to the server, which can use the database to determine the physical location of the STA. This physical location can be used to provide location-based services.

Fast Handover

A novel aspect of very fast handover is to practically almost complete the process of the handover before it even started.

Consider an example depicted in Figs 12 and 13, in which STA 11 is in conversation with TN 41 (TN - Termination node, the node with which STA 11 communicates, shown in Fig. 13), and STA 11 is moving from AP 31 towards AP 32. Also assume that a node GN 21 (GN - Governing Node, a node that is non-exclusively responsible for the mobility management in a certain geographic area for a given time, shown in Fig. 13) is in contact with STA 11, and it is assisting STA 11 during the handover process. STA 11 currently has an IP address, which was allocated to it by AP 31.

To complete the handover, STA 11 should be associated with AP 32, have an IP address assigned by AP 32, complete any second authentication that is required, and have TN 41 be aware of the new IP address, so it can forward the conversation to the new location. Note that in some scenarios (in some cases when there are firewalls or NAT devices between AP 32 and TN 41, the connection between STA 11 and TN 41 must be started from within AP 32 towards TN 41).

According to prior art, it appears that STA 11 cannot begin the handover process until it reaches the coverage of AP 32, since it cannot start the connection process. One novel solution (that requires changing the software of the AP) is to allow STA 11 to perform the connection process through the Internet, instead of performing it wirelessly. In this way, once STA 11 reaches radio connection with AP 32, it can start working immediately.

However, we are more interested in solutions where there is no need to change the AP. To achieve this goal, assume the existence of a non-moving STA 12 in

the coverage of AP 32 (we will somewhat soften this assumption later). According to the present invention STA 12 is in contact with GN 21, and receives instructions to impersonate STA 11 towards AP 32 (we will later discuss how to make it possible), and complete a connection process with AP 32 on behalf of STA 11 (including authentication, association, receiving an IP address, performing any second authentication/log-in procedure, and perhaps even opening connections or "punching holes" in the firewall).

Then, STA 12 communicates these parameters to GN 21 (once the parameters are communicated, STA 12 can return to its real identity). GN 21 communicates the parameters to STA 11 (and perhaps to TN 41), and thus, STA 11 does no longer need to perform the connection process, and once it reaches the perimeter of the coverage (we will later discuss how to identify this situation) it can immediately use the new parameters and continue communications without any delay. STA 11 (or GN 21) can alert TN 41 before the handover, so it can start and send information packets to the new location.

TN 41 may send the information in parallel to the old and the new location, and cease transmitting to the old location once the handover is complete (e.g., when it receives information from STA 11 with its address from the new AP). STA 12 may even open a TCP (Transmission Control Protocol, as used in the Internet) connection or send a UDP (User Datagram Protocol) packet on behalf of STA 11, if required.

This connection may wait for STA 11 until it reaches AP 32. If there is a timeout on these connections (either due to protocol, or due to firewalls), STA 12 or other bypassing STAs can send and receive -keep-alive- messages on behalf of STA 11 (as is instructed by GN 21). The timeout for each AP can be discovered over time by trial and error (or by discovering the APs type), and storing this information in GN 21 for future use. GN 21 can notify the STAs on the value of the timeout.

How STA 12 can impersonate STA 11:
To understand how STA 12 can impersonate STA 11 towards AP 32, we must understand how identity is established in the network. The basic identity in the network is the physical address which is known as MAC Address (Media Access Control Address), which is globally unique. Each manufacturer is allocated a portion of the address space and allocates a unique MAC address to every network card (including WiFi network card) that it manufactures. Then, the manufacturer burns the allocated address into the network card. However, in most network cards, an application can (temporarily) change the MAC address of the card to another MAC address.

The MAC address is not used for end-to-end communications over the internet, but usually only for communications within the same physical network. For example, STA 12 communicates with AP 32 using MAC address, but GN 21 is not usually aware of the MAC address of STA 12. The MAC address is universally unique. We use the feature of temporarily changing the MAC address in the network cards in a novel way, allowing STA 12 to impersonate STA 11.

Therefore, in the instructions that GN 21 gives to STA 12, it mentions the MAC address of STA 11, so STA 12 can assume the MAC identity of STA 11. Then, STA 12 can complete the association with AP 32 (using the MAC address of STA 11)), in which it receives the Association ID (AID), and completes a DHCP protocol in which it receives an IP address to be used with the MAC of STA 11 while it is using AP 32. STA 12 can also perform a second authentication and log-in on behalf of STA 11.

STA 12 sends the connection information back to GN 21, which forwards it to STA 11. STA 12 can return to its original MAC address, but the allocated resources at AP 32 remain allocated, as from the point of view of AP 32, STA 11 is already connected and in coverage. In order to avoid losing messages that are sent to STA 12 during its impersonation to STA 11, it can either

continue and listen using both its own MAC address and STA 11's MAC address, or it can issue a -power-save- mode command to its serving AP. The power save mode indicates the AP that the STA is sleeping for a while, in which time the AP is buffering the incoming data packets. Therefore, even if STA 12 is connected to the internet using another AP, it can issue a power-save mode command, possibly change the frequency, and perform the connection on behalf of STA 12. It can return to its serving AP once the connection is established, or pool for incoming messages once in a while.

First Softening of the Assumption that STA 12 is in the coverage of AP 32: What if STA 12 is not in the coverage of AP 32, and there is no other station in AP 32's coverage- The following process can be performed in advance, well before a handover is needed. GN 21 can ask (in advance) stations that pass through AP 32 to connect and receive an IP address from AP 32 using some MAC address. The MAC address is not necessarily the MAC address of STA 11, as the process is not specific to STA 11. The stations send the connection details to GN 21, which stores the AID, the MAC, the IP address and other connections details in a pool for future use.

The pool may even contain UDP or TCP connections, which may be kept alive by bypassing STAs (against timeouts of firewalls, Network Address Translator devices (NAT), and protocol timeouts). UDP and TCP connections in the pool are targeted to some node in the network that can forward information for other nodes (for example TN 41). When a connection is required by some STA, the pool is queried, and a resource can be allocated and applied by a STA. As a result, a station might change its MAC address and IP address every time it moves between APs. If the station moves very fast between these access points, GN 21 can predict the direction in which the station is moving based on past movements, inform TN 41 of the possible future addresses.

Using this method, TN 41 can send data to the new address even before the

station actually moved there. In some implementations of the APs and firewalls between AP 32 and TN 41 the STA must first send data before it can receive any data, otherwise, the firewall may block the incoming data, or a NAT (Network Address Translator) device might not know where to forward the data. The restriction, that the STA must be the first to send data, is usually required due to security policy that allows only outgoing connections, or due to NAT device that need to relate an internal IP address and port number with an external IP address and port number.

For example, in most NAT implementations a connection must be established from within the NATed zone (e.g., the AP coverage) towards the internet. Many firewalls also require that the connection is established from the private network towards the internet (rather than allowing incoming connections from the internet towards the private networks). In these cases, the data that TN 41 sends is not transmitted by AP 32 until the station reaches the access point and transmits information back to TN 41. Depending on the type of firewalls and NAT devices, TN 41 might be able to predict a port number to which it should send such messages before the first outgoing data packet is transmitted.

Another associated novel disclosure is that the same MAC address and IP address can actually be used by more than one STA. The differentiation between the STAs can be performed by using higher protocol identities such as different ports (for example TCP ports). Using the same MAC and IP address in more than one STA is not problematic for packets that are sent from the STA.

However, while receiving an incoming packet, only one STA should send an acknowledgement. As each STA knows the ports that are in use, it only acknowledges messages that are designated to it. GN 21 can coordinate between the STAs such that they do not use the same ports. For example, if there are at most n stations using the same MAC and IP address, station i will allocate port numbers that are equal to i modulo n. Another solution is to choose the

port number at random. If each STA uses one port at random, according to the birthday paradox, port collisions occur with very low probability as long as the number of connections is smaller than about the square root of 65536 (i.e., when there are less than 256 connections using the same IP).

Another idea is to change the software at the AP such that it can communicate with GN 21 and perform the connection procedure on behalf of STA 11.

Knowing who are the adjacent APs and the location of a STA:
It is useful for a station STA 11 to know the identity of the adjacent APs that the station might hand over to. The identity of an AP can be established in several ways: The SSID (Service Set ID) of the AP is usually broadcasted by the AP using periodical transmissions known as beacon. However, two adjacent AP may have the same SSID. In such a case, the MAC address of each AP is different, and APs can be differentiated based on their MAC address. Some APs do not transmit their SSID, but they still broadcast beacon messages with their MAC address. Even if the AP is locked and encrypted the MAC address is transmitted, and it is transmitted without any encryption. In this way, STA 11 can know the identity of adjacent APs, and infer its location.

Scanning by Idle STAs:

In a preferred embodiment, GN 21 collects information about APs which are adjacent. Idle stations (i.e. stations which are not in an intensive data transfer) can perform a scanning operation once in a while. As a result they learn the MAC address (and possibly the SSIDs) of the APs within radio reach. The STAs can then send this information to GN 21 which collects it. The idle STAs can also perform tests to check what is the accessibility parameters of an AP (e.g., is it an open and free AP, is it a locked AP and the password is available from GN 21, is it locked and there is no free access to the AP, is there a captive portal, does GN 21 have a username/password available for the

captive portal, etc.). All this discovered information is sent to GN 21.

When handovers are performed, GN 21 takes note of the sequence of handovers that occur, and can learn common paths which are taken (for example, a road or a crosswalk might cause more likely paths than others).

It is very important that GN 21 knows in advance the AP to which STA 11 will be handed over to and when the handover will occur. Such a knowledge allows, for example, to alert TN 41 of the new location in advance. Gaining accuracy in the prediction of the handover (when and where) translates to better performance, as GN 21 needs to allocate a MAC address and an IP address to STA 11 in the new AP, and TN 41 might start to send data to the new location.

Therefore, knowing who the neighboring APs are, and their reception quality at STA 11 is very important.

Scanning by a non-Idle STA

In principle, STA 11 can scan the surroundings once in a while and look for the beacons of adjacent APs, and thus measure the reception quality from each AP. However, such a scanning takes a lot of time (might even take couple of seconds for a full scan). Selective scanning for APs which are expected to be neighbors can reduce the scanning time, but it can still stay in the magnitude of a few hundred milliseconds. It is important to understand that during a contemporary scanning using current technology, STA 11 cannot receive or send messages from or to AP 31, which means that the scanning time must be reduced to reduce this disconnection time.

The novel disclosed method is that STA 11 will selectively scan for a neighboring AP in the following special way. Assume that STA 11 scans to see

if it can receive the beacon of AP 33, where the scanning is performed exactly when the AP 33 is expected to transmit its beacon. Therefore, the disconnection from AP 31 will be minimal. The problem is, however, that although the beacons are transmitted periodically, STA 11 does not know when a beacon is expected to be transmitted from AP 33. As the beacons are transmitted about every 102.4 ms (milliseconds); (many variations are possible)., STA 11 might be forced to wait on average 51.2 ms, which is a prohibitively long time to wait.

STA 11 may also transmit a Probe message to force a beacon to be sent especially for it- but a probe message requires a transmission that has implication on battery life. Furthermore, for the purpose of location finding, STA 11 might wish to be able to receive beacons of APs that will not answer the probe (due to range, policies, etc.)

We can safely assume that other STAs visited the area of AP 33 before STA 11, and that they have reported the rate of the beacons of AP 33 (e.g., a beacon every 102.4 ms). A problem that remains is that the beacons are scheduled according to the internal clock of AP 33, which might tick at a different rate than other clocks (and clocks tend to tick at different rates). Moreover, the clock of the visiting STAs is probably not exactly synchronized with the clock of STA 11, which makes the process inaccurate.

That is, even if STA 11 knows that at a specific time according to some STA's internal clock a beacon was transmitted, STA 11 will not know how to translate this information to his clock, as the clocks are probably not synchronized to such great accuracy (network time synchronization services such as the network time protocol (NTP) cannot be more accurate than a couple of tens of milliseconds, where in this case we need an accuracy of around one millisecond). The following novel method allows accuracy of microseconds.

The novel approach for time synchronization is to rely on a relatively accurate clock already available to STA 11: The 802.11 standard requires each AP to transmit in its beacon its clock (referred to in the 802.11 standard as timestamp). This clock must be the internal clock of the AP at the time of transmission in units of microseconds. Therefore, STAs can specify the value of the clock of AP 33 in terms of the value of the clock at the adjacent AP 31.

By measuring the timestamp of AP 31 and AP 33 at two different times T311 and T312 (based on the clock of AP 31), in which the time value of AP 33 T331 and T332, respectively, it can be established with reasonable accuracy that AP 33 clock ticks approximately r33/31=(T332- T331)/(T312-T311) times for every clock tick of AP 31. At time T313 in the future, the clock of AP 33 can be estimated as T333=T332+(r33/31)(T313-T312). Similarly, at time T334 the clock of AP 31 can be estimated as T314= T312+(1/r33/31)(T334-T332).

Beacons are scheduled to transmission when the clock of the AP modulo the beacon interval is zero, where the beacon interval is measured in microseconds according to the clock of the AP, it is fixed for an AP, and the value of the beacon interval is transmitted in the beacon. Therefore, GN 21 stores the relation r33/31 together with T332 and T312 and the beacon interval of AP 33 and AP 31, and reports it to STA 11 such that it can extrapolate the time at AP 33 and infer the time of the beacon transmission.

Once STA 11 succeeds in receiving a beacon from AP 33 it can report the times to GN 21, so that GN 21 can keep its time tracking accurate. Furthermore, the scanning allows GN 21 and STA 11 to make the best handover decisions based on the knowledge of the approximate location of STA 11 with respect to the neighboring APs.

A technical problem to be solved is that a STA can know the value T311 but cannot measure the value of T331 at exactly the same time of T311 , as these values are carried on the beacons of APs, which are transmitted at different times.

A solution is to measure the time of AP 33 T331' at a time close to T331, and note the time difference between the two measurements according to the STA's internal timer. As the measurements are very close to each other, the clock drift between the STA's timer and AP 33's timer is negligible, and we can estimate that T331= T331'+timediff, where timediff is the time difference between the measurements of T331 and T331' according to the timer of the STA. If there is a large clock drift after all (although it is not expected), it can be corrected by calculating the r value between the clock at AP 33 and the STA in a similar way to the way done for APs.

The location of STA 11 can be deduced from the reception quality, the reception strength and the identity of the neighboring APs. This location information can be taken into account while performing handover decisions, as well as for location based services or for other network applications.

It should also be noted that in Frequency Hopping, knowing the time of the AP has another special importance, as the frequency that the AP works in might depend on the time.

Fig. 14 details a preferred embodiment of the handover method, including:

a. STA prepares in advance for a handover: 541
* Assisted by another STA (or STAs)
* Optional: use the same MAC and IP addresses in more than one STA
* Learn the identity of adjacent APs
* Measure beacon strength from other APs

b. GN supports handover: 542
* GN keeps a pool of MAC and IP addresses
* GN sends the addresses to STA just before it enters the AP

c. STA reduces the number of Location Updates 543
by only updating when changing location area

d. GN transmits a pseudo-beacon including 544
MAC address, IP address, port number

e. Easy security configuration: 545
* The AP of the customer is not changed
* Establish secure channel with STA and Copy security information, or
* Connect the STA initially by wire

f. Gain access to locked networks 546
by joining the Vagabee service

g. Maintain simultaneous communication with 547
more than one AP.
Update net configuration responsive to changing circumstances
** End of method **

Fig. 15 details a method for implementing two connections with a STA.
The method includes:

a. Load BSS firmware to the NIC 415

b. Associate with AP using a first SSID 416

c. Load IBSS firmware to the NIC, but do not perform 417
dissociation from AP before loading the IBSS

d. Create an ad-hoc network using a second SSID 418

e. Communicate with AP and STA that connect to 419
the second SSID
** End of method **

Fig. 16 details a method for connecting other STAs, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs to connect to the Internet by 492
allowing them to connect to the second SSID.
The first STA decrypts and encrypts data packets as needed based on the security parameters of the first and second SSID (or APs), and performs address translations and forward packets between the second and first SSID to facilitate this connection for other STAs.
** End of method **

Fig. 17 details another method for connecting other STAs, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by 492
allowing them to connect to the second SSID. The limited access includes the ability to download a software that implements the current method.

The first STA decrypts and encrypts data packets as
needed based on the security parameters of the first and second SSID (or APs),
and performs address translations and forward packets between the second and

first SSID to facilitate this limited connection for other STAs.

c. When the first STA detects that another STA 493
has a software (which implements the current method) installed, the first STA allows the other STA a wider access to the Internet.
** End of method **

Fig. 18 details a method for configuring other STAs to directly connect to the AP, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by 492
allowing them to connect to the second SSID.
The limited access includes the ability to request an ability to access the first SSID directly, i.e. not through the second SSID and the first STA.

c. The first STA decrypts and encrypts data packets as needed based on the security parameters of the first and second SSID (or APs), and performs address translations and forward packets between the second and first SSID to facilitate this limited connection for other STAs.

d. Another STA requests an ability for direct access to 494
the first SSID

e. First STA prompts user: To 495
allow this access?

f. Security access parameters to access the first SSID are copied 496

from the first STA to the other STA

g. The other STA can access the first SSID directly 497
** End of method **

Fig. 19 details another method for configuring other STAs to directly connect to the AP, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by 492
allowing them to connect to the second SSID.

c. First STA's user can view a list of 498
connected STAs and can choose to allow access directly through the first SSID
to a chosen other STA

d. Security access parameters to access the first SSID are copied 496
from the first STA to the other STA

e. The other STA can access the first SSID directly 497
** End of method **

Fig. 20 details yet another method for configuring other STAs to directly connect to the AP, including:

a. First STA, using a single Wireless NIC, 491
connects to an AP using a first SSID, and creates a network using a second SSID

b. Allow other STAs limited access to the Internet by allowing them to connect to the second SSID. 492

c. Security access parameters to access the first SSID are copied to the other STA 496

d. The other STA can access the first SSID directly 497

** End of method **

Preventing Exhaustion of Resources at the AP

As discussed in the "Background" section, each AP has a limited number of Association IDs (AID) and usually, even a smaller pool of IP addresses (available through DHCP). Once this number of resources is exhausted, the AP might not be able to serve new STAs. A situation where IP addresses are exhausted can happen very quickly: for example, consider an AP in a very busy location, where there are many STAs that connect to the AP only for a short period of time. Each STA performs the connection process and obtains an IP address using DHCP, but as it disconnects it might not release the IP address.

The pool of IP addresses in an unmanaged AP is usually limited to about 200 addresses, with many consumer APs supporting only tens of addresses. A device is assigned the IP address for a given period of time (known as the lease time). Many times, the lease time is set in a magnitude of days (although the granularity is seconds), and in many other instances the lease time is set to a magnitude of hours. In such a situation the pool of IP addresses runs empty very fast.

However, in this disclosure for fast handovers, GN 21 keeps a pool of MAC addresses with associated IP address. Just before a STA enters the AP, GN 21 can send it a MAC address and an IP address that are already associated with

the AP. Therefore, the STA can connect even if the AP has no resources left for new STAs. Combined with the above disclosure that allows several STAs to share the same MAC address and IP address, an AP can serve more APs than its IP resources, even above its limit on the number of associated STAs.

Saving Battery Power by Reducing Location Updates

A novel disclosure of this invention is a method to reduce the number of location updates that are needed in WiFi, when a STA is idle. A location update is the process in which a STA informs an entity in the network of the current location of the STA (the notification can take many forms, including opening a TCP connection, or sending UDP packets). In prior art for WiFi networks (with for example mobile IP, or SIP - Session Initiation Protocol), a location update is required whenever the IP address of the STA changes (for example, when moving between APs of different subnets) - even if the STA is idle.

The novel method allows defining a location area for WiFi, such that a STA needs to perform location update only when it moves between APs that belong to different location areas, but does not need to perform location update when it moves between APs of the same location area as long as it's idle.

We assume that the APs are divided into location areas, and for each location area there is a node in the network that is in charge of this location area. For example, assume GN 21 is in charge of a location area composed of AP 31, AP 32, and AP 33.
How does a STA know which AP belongs to the location area- Either GN 21 gives it a list of all the APs that belong to the location area, or GN 21 transmits a pseudo-beacon in each AP.

A pseudo-beacon is a novel disclosure of this invention. It is a message that GN 21 can periodically transmit in each AP. While some APs might permit a remote node to transmit a message in the AP, other APs might not allow it. In

the novel method, a certain MAC address, IP address, and possibly port are allocated in each AP for the purpose of pseudo-beacon transmission. GN 21 asks some STA to open a connection using these resources to GN 21, and GN 21 sends the pseudo-beacon messages using this transmission. Each pseudo-beacon contains the parameters needed to listen to the pseudo-beacons in the adjacent APs. A STA that lacks these parameters can contact GN 21 and receive them.

From that moment on, the STA can move between APs in the same location area, and receive the parameters that are needed to listen to the pseudo-beacon from other pseudo beacons. For example, assume that STA 11 is located in AP 31 and is moving to AP 32. STA 11 listens to the pseudo-beacon at AP 31, and from the pseudo-beacon learns the parameters that are needed to listen to the pseudo-beacon of AP 32. Thus, STA 11 can move to AP 32 without any transmission.

Which STAs of the stations in AP 31 should acknowledge the pseudo-beacon- Preferably, none. However, some firewalls require minimum rate of outgoing packets to maintain an open connection. In such a case, once in a while GN 21 sends on the pseudo-beacon a message that asks any station to send an acknowledgement with some probability p. The probability that GN 21 states should be accommodated to the expected number of stations in AP 31 (GN 21 might not exactly know how many STAs are in the AP). If no STA acknowledges the pseudo-beacon for over the needed time, and the timeout of firewalls stop the incoming messages, then no pseudo-beacons are transmitted. In this case, a roaming STA will contact GN 21 after a certain period of time of probing for the pseudo-beacon has passed (and no pseudo-beacon is seen). GN 21 can request the STA to reopen the connection for the pseudo-beacon transmission.

If the STA is in a session with TN 41 with many packets received (e.g., above a certain threshold), it is considered non-idle (which we also refer to as "In conversation") and is treated as described above in "Fast handover".

However, assume that STA 11 is in idle mode (e.g., incoming packets below a threshold), it can move between APs of the same location area without performing location update. When a node TN 41 wishes to send data to STA 11, STA 11 should change its state from idle to in conversation. TN 41 contacts GN 21 (TN 41 might be forwarded to GN 21 through a system such as dynamic DNS (Directory Name Service) or another method, such as a Distributed Hash Table - DHT, or a peer-to-peer network).

GN 21 sends a paging message for STA 11 on the pseudo-beacon of all the APs in the location area. As STA 11 listens to one of the pseudo-beacons, STA 11 will receive the paging message. Then, STA 11 responds preferably to GN 21 (or to TN 41, depending on what is written in the paging message) by initiating an outgoing connection as described below. It should be noted that GN 21 can first page for STA 11 in the APs that have a higher chance covering STA 11, and the paging can repeat several times until STA 11 replies.

When a STA is required to initiate an outgoing connection it can use a resource (MAC, IP, or TCP/UDP with port, user/password) that is listed as available on the pseudo-beacon or on the paging message, or it can request its own resources from the AP. If two (or more) STAs use the same resources for a connection at the same time, GN 21 will detect it, and in the acknowledge message (or second message of the TCP handshake) will announce the identity of the STA that it answers to. The other STA is required to initiate an outgoing connection again. Once a connection with GN 21 is established, GN 21 can allocate resources to the STA such that it moves to be in conversation status. One of the resources that are allocated is GN 21 attention to accompany the STA as it might need to perform handover to another AP.

It should be noted that the location areas can overlap, meaning a single AP can belong to more than one location area. Upon the policy of the network, STA 11 might be required to perform location update when it reaches such a APs, or it may just give helpful information. If possible, a STA might prefer

to park on an AP that is within the same location area as its current AP, such that a location update is avoided.

It should also be noted that there is a tradeoff between the overhead that is spent during paging and establishing the connection, and the overhead that is being spent to keep a steady connection for each AP. The optimal point on the tradeoff depends on the rate that the AP switches APs as well as on the number of packets it receives and sends.

Easy Configuration of STA

When purchasing a new STA, it is required to configure the STA with the security settings of the existing network (in case the network is secure). If the network is not secure, the new owner usually only needs to select his network from the list of available networks that is received by the wireless network card.

Configuring the security might be a tedious job, as the security (authentication/encryption) code might be very long as known in the art, which the user might need to punch in. A novel solution for easy configuration is disclosed. Unlike previous solutions, the novel method does not require changing the existing AP of the customer. In one embodiment, software is run on a personal computer of the user (that is already configured to access the WiFi). Then, the software establishes a secure channel with the STA, and copies the security information from the personal computer to the STA. In this way, the STA learns the security parameters.

In another embodiment, the customer first connects the STA by wire to its network (or alternatively, the STA first connects using a connection it establishes through an already connected device, such as a personal computer). As the STA can receive and transmit signals on the wireless network and it is connected to the internet (through the other connection) at the same time, it tries to locate the web configuration of the AP on the wired network (most APs

have a web interface). In most cases, it is an easy job for the STA, as either the STA can locate the AP as it is the default gateway of the wired network, or it can try to find its IP by performing RARP (Reverse Address Resolution Protocol) using the wireless MAC address of the AP (which it can see off-the-air).

If none succeeds the STA can perform exhaustive search on commonly used IP addresses, or on very probable addresses, like all the IP addresses of the same subnet. Once the AP web interface is found, the STA tries to log into the AP. It can guess the default address or find it on a database that can be built on the web, with common default passwords for each manufacturer (the manufacturer and model will be usually sent by the AP during the web login process, or can be found out using the MAC address, which is unique per manufacturer). If the password for the AP cannot be guessed, the user is prompted for its password to complete the log-in. Then, the STA navigates to the security settings page and retrieves the password needed for the wireless network.

In the event that the procedure fails, the user is prompted for the security settings (which would happen without using the above method). For most common users and setups, the method succeeds (and for unsophisticated customers, who do not change the passwords - it succeeds in the majority of the cases). Thus, in the majority of cases, the setup is made much simpler.

Once the STA has access to the setup of the AP, it can (with permission from the user), open holes or forward certain port to some IP address. This IP address and port can serve as way that GN 21 can send and broadcast the pseudo-beacon, without a STA first opening a connection from the AP, and without worrying about timeouts (provided that there are no other firewall between the AP and GN 21). Opened ports can also help during the fast handover, such that TN 41 can directly send packets to the new location without a need for STA 12 to open the connection.

In corporate settings, the company can set a special server which gives the configuration to the phone, over the network.

Gaining Access to Locked Networks

While performing the above easy setup (or at any other time), the user is prompted if he wishes to join a swapping service. The swapping service allows the user to gain access to many locked networks (the locked networks of the other users that joined the swapping service), in return that he allows users to use his network for the purpose of connecting to the internet. If the user agrees, the access parameters to his network (encryption key, MAC address, default gateway, etc.) are securely stored in the network (for example in GN 21, and a backup server). The security information is securely sent directly into the hardware (or network card) of other STAs, when they need to connect using his AP.

As the security parameters are sent directly to the STA's network hardware, it can make sure that the communication that is established is designated outside the user's network, and will not jeopardize the computers on the user's network. Furthermore, GN 21 can monitor the amount of bandwidth that is consumed by visiting users, and to make sure their hardware limits the amount of used bandwidth such that the user does not experience a degradation of quality of his connection. Alternatively, the security information can be sent to the other STAs using other security measures, as known in the art.

In many scenarios it is enough to trust the software that runs on the STA to make sure all communications are targeted outside the user's network, such that it does not jeopardize the computers on the user's network, and limit bandwidth used by the STA.

The secrecy of the security parameters (such as the encryption key) can be cryptographically protected while on transit and storage, as known in the art.

Some APs limit the access of the subscribers by making sure that only specific MAC addresses connect to the network. As our methods as described above allow

to use the same MAC address for several users, this specific MAC address can be used when using the network that restricts the use with specific MAC address.

In case a STA tries to connect to an AP with a captive portal, a special application on the STA is running and performs the authentication and log-in automatically. GN 21 can store typical portal appearances, such that it can guide the STA on how to perform the authentication/log-in process. If the STA comes across a captive portal which is unknown or unexpected, it can locally store the web pages that it received from the captive portal and later transfer them to GN 21. GN 21 accumulates the reports and guides STAs how to log-in to the captive portal in the future. As part of the swapping service, GN 21 can store username/passwords to enable connection through the captive portal automatically.

Special care for data

The above description works well for both voice and data. TN 41 might be a mobile node as well, or a fixed node in the network. The transferred information between STA 11 and GN 21 can be voice, data, or their combination.

In case STA 11 wishes to communicate with a node that is not aware of the novel network, it can do so through a node that is aware of the network. For example, TN 41 can serve as a proxy for STA 11 (in a similar way to mobile IP). The node that is not aware of the network communicates with TN 41. TN 41 forward the information to STA 11. TN 41 can allocate an IP address (perhaps using NAT, or allocate ports using its own IP address) that will serve STA 11.

To balance the communication load, STA 11 can have several network nodes such as TN 41, TN 42 (not shown), etc, to be its proxies in parallel. In fact, the resulting connection between STA 11 and TN 41 can be seen as a layer 2 (MAC) connection, on top of which the communication is performed. In this setup, TN 41 serves as the default gateway of STA 11, and optionally can run a DHCP server and a NAT server.

Executing the Invention over a Peer-to-peer network

Another novel aspect of the above novel methods takes advantage of the fact that the wireless network is local in nature, as the APs are geographically adjacent. The system and method as described in this disclosure allows GN 21 to be responsible over a small geographical area with little interaction with its neighbors. As a result, the methods that are disclosed can be implemented by many small devices forming a peer-to-peer network that implements the methods, without the need to rely heavily on large servers.

Many nodes GN 21, GN 22 (not shown), can each control a group of APs. To make the system grow "automatically", it is possible to give users a "base" that will act as their point of presence in the network. For example, the base can assume the role of TN 41 as a Mobile IP proxy. The base can connect to the wired network at the premises of the customer. Some bases will assume the role of a GN, where the GNs can be managed by either a network control center, or through peer-to-peer protocols.

In early stages of deployment of the system, when there is still a small number of GNs, each GN might need to cover a large number APs. A general server can back-up all information that the GNs hold. To avoid the situation, where a single GN needs to cover a huge number of APs with pseudo-beacons, the system might not use the pseudo-beacon mechanism (although, it should be noted that with moderate computing power and network resources, a GN might be able to cover a few thousands of APs). In the worst case scenario of a peer-to-peer network, there is one base (GN) for each STA, and this GN act as the GN for the APs in the proximity of the STA.

When the STA moves, the coverage area in the responsibility of the GN moves with it. In this case, the GN can fetch information on neighboring APs from

the general server. When GN abandons an AP, it can store the information it gathered about it in the general server, for later use by possibly other GNs. In a system which is not based on many small GNs, a large GN can assume the role of the smaller GNs.

It should be noted that it takes some time to gather the information on the APs (such as timing, default gateways, etc). However, once a single STA passes in an area, it obtains the needed information. This information is later stored in the GNs and general server, for the benefit of all STAs in the future.

If a STA needs to handover into an AP which has no STAs currently in it, it might not have the needed resources pre-allocated (such as an associated MAC address and IP address), and might therefore need to gain it by itself. However, in many cases the STA can obtain resources at one pass in the area, and these resources (such as IP address) will stay for the next pass in the area (which can be hours later).

An Alternate Fast Method for Connecting to an AP - Removing the Assumption on the Existence of STA 12 in the Coverage of the new AP

A possible drawback of the above method of fast handover is that it requires that the pool of resources that GN 21 holds should contain a valid IP address of the AP that STA is handing over to. If the DHCP lease time is long enough, having a valid IP might not be a problem, but on short lease times with only a few STAs roaming it is desirable to perform handovers even if there is no valid IP available in the pool. Unfortunately, a typical execution of the DHCP protocol can take several seconds to complete, which might be too long for a fast handover. Interestingly, we observe that many APs will forward information even if the IP that is being used was not allocated by DHCP.

Therefore, we disclose the following method:
Choose a MAC and associate it with the AP (or use an Associated MAC without an associated IP address), choose a random (but valid) IP address, and use it.
The STA must use the correct default gateway settings of the AP (these settings can be stored in GN 21). If the STA wishes to use DNS, it must have the DNS settings of the AP (which can be received from GN 21), or DNS services are provided through GN 21.

Choosing a valid IP at random results in a very low probability of colliding with another IP address that is used in the AP. Note, however, that the STA still needs to authenticate/log-in through the captive portal in case such portal exists.

Another method that can be used to quickly obtain an IP address, such that the IP address is not already allocated by the DHCP of the AP is disclosed. Most DHCP implementations of AP send an ICMP (Internet Control Message Protocol) Echo Request (ping) before allocating an IP address, to make sure that it is unused. Therefore, STA can begin the DHCP protocol, then, wait for the ICMP echo request that the AP sends, and understand the IP that is going to be allocated to it.

Therefore, a STA can start using the IP address and respond to the ICMP echo request. It can then prematurely terminate the DHCP protocol (as it already got an IP). Alternatively, STA can use the IP address from the ICMP echo request without responding to it, and complete the DHCP process. If the IP address that is allocated during the DHCP is identical to the IP address (vast majority of cases), then STA simply saved time. Otherwise, it can move from the IP address of the ICMP echo request to the IP address that was allocated.

If no connection to GN 21 is available, the default gateway address can be guessed, as in the majority of the cases the default gateway address is one out of only a few addresses. Common addresses are: 192.168.1.1, 192.168.2.1, 10.0.0.1, etc.

Moreover, the default gateway is usually the AP itself. Its MAC address is known (as it is broadcasted in the beacon). Therefore, in most cases it is enough to forward packets to this MAC address (without knowing its IP address).

A STA with a Capability to Connect on Two Channels in Parallel

The present application discloses a STA which has a capability of communicating in two or more channels in parallel (for example, by using two wireless network cards). This capability can enable a STA to be connected to two APs in parallel without the need to implement sophisticated mechanisms that actually simulate this situation. Thus, a STA can connect with future AP while maintaining a connection through its serving APs. Being connected to two or more APs simultaneously allows greater bandwidth by utilizing two connections instead of one, and the performance of soft-handovers, i.e., the STA stays connected through one AP, while disconnecting from the second AP in the process of handover.

Fast uploading of digital camera pictures

Digital cameras might be equipped with WiFi. The owner of such a camera would like to upload his pictures from the camera to a server that stores the pictures on the Internet - the reasons for this may vary from being able to share the photos while on vacation with family members left at home, back up the pictures from the digital camera to the Internet server, or simply because the memory card on the camera is running out of space. A major problem is that to upload the pictures to the Internet may take a very long time, as pictures consume megabytes to store.

Solution: The camera sends the photos to a laptop over WiFi (this connection is very fast), then disconnects and the camera's user may move on. Then, the laptop uploads the pictures to the Internet server (this process can take a long time as it involves uploading a lot of data), but the laptop owner would not feel it as a burden, since the pictures can be uploaded when his Internet connection is not used for other purposes.

Method for uploading data files

In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for fast uploading of information from STAs to the Internet, comprises:

a. a first STA, such as a laptop computer, connects to the Internet;

b. a second STA, such as a camera, wirelessly connects to the first STA, and uploads the information using the fast and direct-wireless connection between the STAs;

c. The first STA temporarily stores the information;

d. The first STA uploads the information to the Internet through its backhaul.

** End of method **

Notes:

1. In the above method, the first STA may include for example a laptop or a personal computer, the second STA may include a digital camera or a digital video camera, and the information may include digital pictures or digital clips.

2. The second STA preferably disconnects from the first STA after completing to upload the information to the first STA, but before the first STA completes the upload of information to the Internet; the first STA completes the upload of information from its temporary storage.

3. An additional step in the above method may include the following:

e. at a later time, the second STA connects to the Internet and verifies that the information was uploaded correctly.

4. The information may be encrypted by the second STA before being transmitted.

It will be recognized that the foregoing is but one example of an apparatus and method within the scope of the present invention and that various modifications will occur to those skilled in the art upon reading the disclosure set forth hereinbefore.

CLAIMS

1. A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising:

a. wirelessly connecting a first STA to the Internet through a first AP with a first SSID;

b. remaining connected to the first Access Point (AP), the first STA creates a software-based wireless AP with a second SSID for wirelessly connecting other STAs to the Internet through the first STA.

2. The method for providing a wireless Internet connections to STAs according to claim 1, further including the step of:

c. a software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein.

3. The method for providing a wireless Internet connection to STAs according to claim 1 or 2, wherein each STA can be a laptop computer, PDA, wireless camera, wireless phone or a wireless device.

4. The method for providing a wireless Internet connection to STAs according to claim 1, wherein the first STA includes means for simultaneously connecting to the first AP and for opening the second AP, and means for transferring Internet packets between the first and second APs, while decrypting and encrypting the packets as needed based on the security parameters of the first and second AP, in addition to any communications with the Internet as required by a user of that STA.

5. The method for providing a wireless Internet connection to STAs according to claim 1, wherein activating, in the first STA, a single wireless card so as to operate in two modes at the same time, a STA mode and an AP mode.

6. The method for providing a wireless Internet connection to STAs according to claim 1, wherein the first AP does not provide wide, unconditional access to all.

7. The method for providing a wireless Internet connection to STAs according to claim 6, wherein a remote database may be accessed to determine if a STA without the software module should be allowed access, and how wide that access should be.

8. The method for providing a wireless Internet connection to STAs according to claim 1, 2, 3, 4 or 5, wherein the software module, upon detecting that the other STA does not have the software module therein, allows to install and activate the software module in the other STA and then provides wide access to the other STA.

9. The method for providing a wireless Internet connection to STAs according to claim 6, wherein the software module, upon detecting that the other STA does not have the software module therein:

c1. presents to the user of the other STA a message indicating that wide Internet access is possible upon loading a copy of the software module;

c2. waiting for that user's permission;

c3. after receiving that user's permission, the other STA. STA downloads, installs and activates a copy of the software module to gain a wide Internet access to the other STA.

10. The method for providing a wireless Internet connection to STAs according to claim 1, 2, 3, 4 or 5 wherein the step of connecting another STA comprises:

c1. the first STA connects the other STA, while limiting the set of Internet addresses and/or Internet sites the other STA can access, and wherein the accessible sites include a special web site from which the other STA can download the software module;

c2. the other STA downloads, installs and activates the software module therein;

c3. the first STA, upon detecting the installed and active software module in the other STA, then removes the limitations on the set of Internet addresses

and/or Internet sites the other STA can access.

11. The method for providing a wireless Internet connection to STAs according to claim 1, 2, 3, 4 or 5 wherein the step of connecting another STA comprises:

c1. the first STA connects the other STA to the Internet, while limiting the set of Internet addresses and/or Internet sites the other STA can access, and wherein the accessible sites include a special web site from which the other STA can download the software module;

c2. if so instructed by the user of the other STA, the other STA downloads, installs and activates the software module therein;

c3. the first STA, upon detecting the installed and active software module in the other STA, then removes the limitations on the set of Internet addresses and/or Internet sites the other STA can access.

12. The method for providing a wireless Internet connection to STAs according to claim 10 or 11 wherein the first STA, upon detecting the installed and active software module in the other STA, then removes part of the limitations on the set of Internet addresses and/or Internet sites the other STA can access, so as to keep some sites and/or addresses private to the first STA.

13. A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising:

a. activate in a first STA a software module for connecting with other STAs and to the Internet;

b. when required by the user to connect to the Internet and upon connecting with another STA which is already connected to the Internet and has a copy of the software module active therein, signal to the other STA that the first STA has a copy of the software module, and request to connect to the Internet through the other STA;

c. connect the first STA to the Internet through the second STA;

d. the software module in the first STA opens a second, software-based

wireless Access Point (AP) at the first STA for connecting other STAs to the Internet through the first STA, and wherein the software module only provides wide Internet access to other STAs which each has a copy of the software module installed and active therein.

14. A method for providing a wireless Internet connection to WiFi-enabled devices (STAs), comprising:

a. activate in a first STA a software module for connecting with other STAs and to the Internet;

b. connect the first STA to the Internet and open a second, software-based wireless AP for connecting other STAs to the Internet through the first STA;

c. when another STA connects with the first STA through the second AP and requests access to the Internet:

1) check whether the other STA has a copy of the software module installed and active therein;

2) if the answer is positive, then connect the other STA to the Internet;

3) if the answer is negative, then support the other STA in loading, installing and activating a copy of the software module therein and, after the software module is active in the second STA, provide wide Internet access to the other STA.

15. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein each STA may include a Portable computer, a Laptop, a PDA or a wireless phone.

16. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein each STA includes means for simultaneously connecting to the first AP and for opening the second AP, and means for transferring Internet packets between the first and second APs, in addition to any communications with the Internet as require by a user of that STA.

17. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein activating, in the first STA, a wireless card so as

to operate in two modes at the same time, a STA mode and an AP mode.

18. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein a STA connects to the Internet through two or more STAs simultaneously.

19. The method for providing a wireless Internet connection to STAs according to claim 18, wherein a STA repeats the connecting stage two or more times to connect to the Internet through two or more APs simultaneously.

20. The method for providing a wireless Internet connection to STAs according to claim 18 or 19, wherein a STA performs a fast handover by continuously searching for new APs to connect therethrough and connecting to newly available APs as older APs may become inaccessible.

21. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein the first STA prevents other STAs from accessing its inner network by limiting the access rights of the other STAs.

22. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein the other STA prevents the first STA from eavesdropping on its communications by tunneling its sensitive traffic to a trusted network site, and accesses the Internet through its tunnel to the trusted network site which acts as a proxy for it.

23. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein preventing STAs from using other STAs for their primary network connection for a long period of time, by detecting that a STA is connected to the Internet through the same STA for a long period of time, and disconnecting that STA.

24. The method for providing a wireless Internet connection to STAs according to claim 13 or 14, wherein preventing STAs from using other STAs for their primary network connection for a long period of time, by detecting

that a STA is connected to the Internet through the same STA for a long period of time, and disconnecting that STA if it refuses to pay for the continued use of that connection.

25. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for configuring STAs to connect to a wireless network, comprising:

a. activating a software module in first STA, which is already configured to access an Access Point (AP);

b. the software module copies the security information from the personal computer to another STA, thus setting the security parameters for the other STA as to allow access to the AP.

26. The method for configuring STAs according to claim 25, further including an authentication phase in which the other STA is authenticated by the software module or by a remote server before copying the security information.

27. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for configuring STAs to connect to a wireless network, comprising:

a. a customer first connects a STA by wire to its network, (or the STA first connects using a connection it establishes through an already connected device, such as a personal computer or laptop);

b. a software on the STA copies to the STA the security information gained through the wired connection, thus setting the security parameters for the STA.

28. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for performing fast handover for a first STA, from being connected to a first Access Point (AP) to a second AP, comprising:

a. a first STA communicates with a Termination Node (TN) and is in contact with a

Governing Node (GN), wherein GN is non-exclusively responsible for the mobility management in a certain geographic area for a given time and wherein the GN is in contact with another STA in the coverage area of the second AP;

b. the other STA receives instructions from GN to impersonate the first STA towards the second AP and to complete a connection process with the second AP on behalf of the first STA;

c. the other STA communicates the connection parameters to the GN and, once the parameters are communicated, the other STA returns to its real identity;

d. the GN communicates the parameters to the first STA, thereby eliminating the need for the first STA to perform the connection process itself;

e. when the first STA reaches the perimeter of the coverage of the first AP, it can immediately use the new parameters and continue communications with the second AP, without any delay.

29. The fast handover method according to claim 28, wherein the first STA alerts the TN before the handover, so it can start sending information packets to the new location.

30. The fast handover method according to claim 28, wherein the TN sends information in parallel to the old and the new location, and ceases transmitting to the old location once the handover is complete.

31. The fast handover method according to claim 28, wherein the other STA further opens a Transmission Control Protocol (TCP) as used in the Internet or sends a User Datagram Protocol (UDP) packet on behalf of the first STA, if required.

32. The fast handover method according to claim 28, wherein the connection process performed by the other STA on behalf of the first STA includes authentication, association, receiving an IP address and performing any second authentication/log-in procedure.

33. The fast handover method according to claim 28, wherein the connection process performed by the other STA on behalf of the first STA further includes

opening connections or "punching holes" in the firewall.

34. The fast handover method according to claim 28, wherein the connection waits for the first STA until it reaches the second AP and, if there is a timeout on these connections (either due to protocol, or due to firewalls), the other STA or yet other bypassing STAs can send and receive -keep-alive-messages on behalf of the first STA.

35. The fast handover method according to claim 34, wherein the timeout for each AP is stored in the GN for future use.

36. The fast handover method according to claim 34, wherein the value of the timeout is transmitted by the GN to the first STA.

37. The first handover method according to claim 34, wherein the connections parameters are not limited in use for the first STA, but are also available for the use of other STAs.

38. In a system with means for providing a wireless Internet connection to WiFi-enabled devices (STAs), a method for fast uploading of information from STAs to the Internet, comprising:
a. a first STA connects to the Internet;
b. a second STA wirelessly connects to the first STA, and uploads the information using the fast and direct-wireless connection between the STAs;
c. The first STA temporarily stores the information;
d. The first STA uploads the information to the Internet through its backhaul.

39. The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the first STA includes a laptop or a personal computer, the second STA includes a digital camera or a digital video camera, and the information includes digital pictures or digital clips.

40. The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the second STA disconnects from the first STA after completing to upload the information to the first STA, but before the first STA completes the upload of information to the Internet; the first STA completes the upload of information from its temporary storage.

41. The method for fast uploading of information from STAs to the Internet according to Claim 38, further including the step:

e. at a later time, the second STA connects to the Internet and verifies that the information was uploaded correctly.

42. The method for fast uploading of information from STAs to the Internet according to Claim 38, wherein the information is encrypted by the second STA before being transmitted.

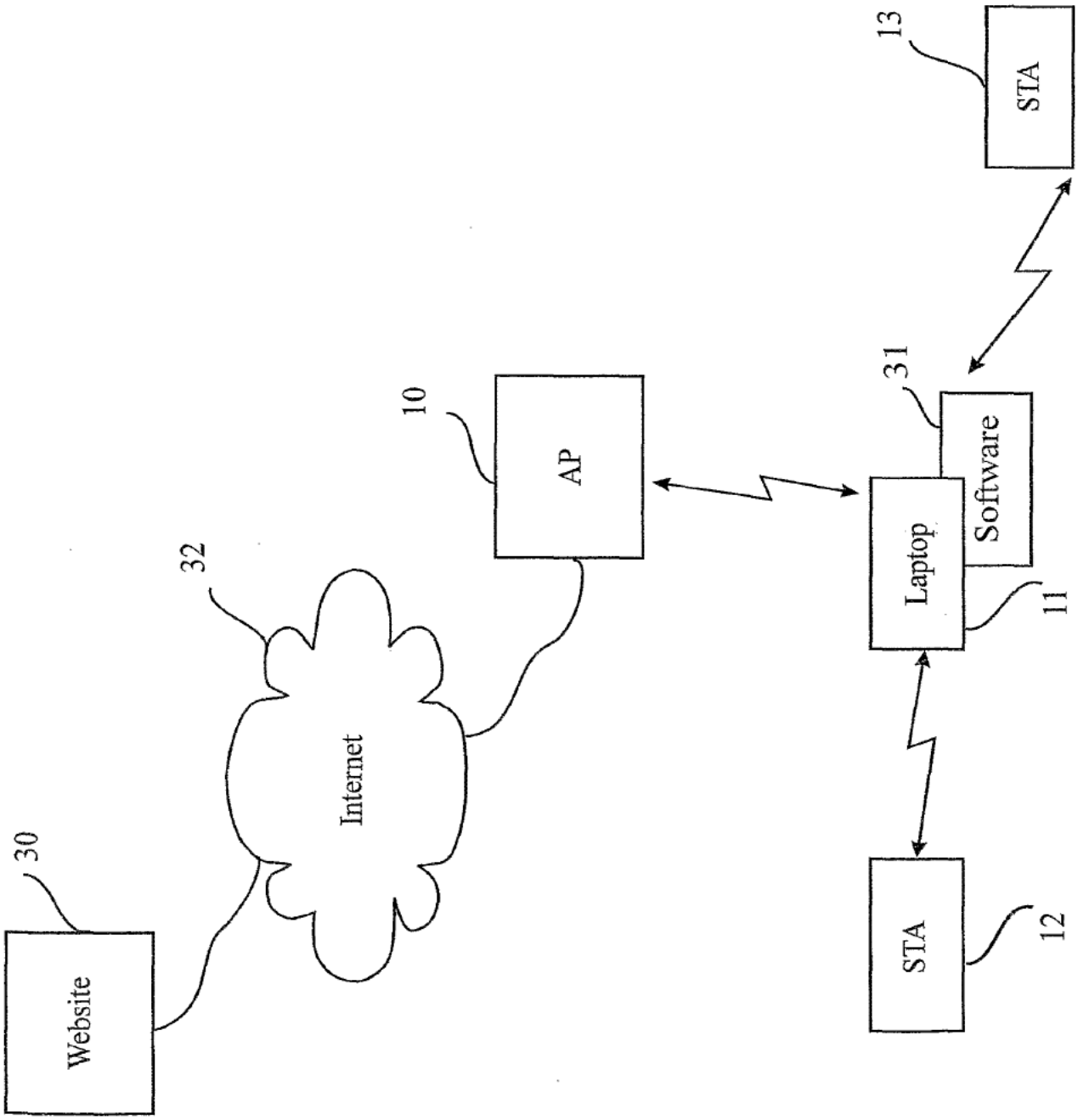

Website
30
Internet
32
AP
10
Laptop
Software
31
11
STA
12
STA
13

FIG. 1

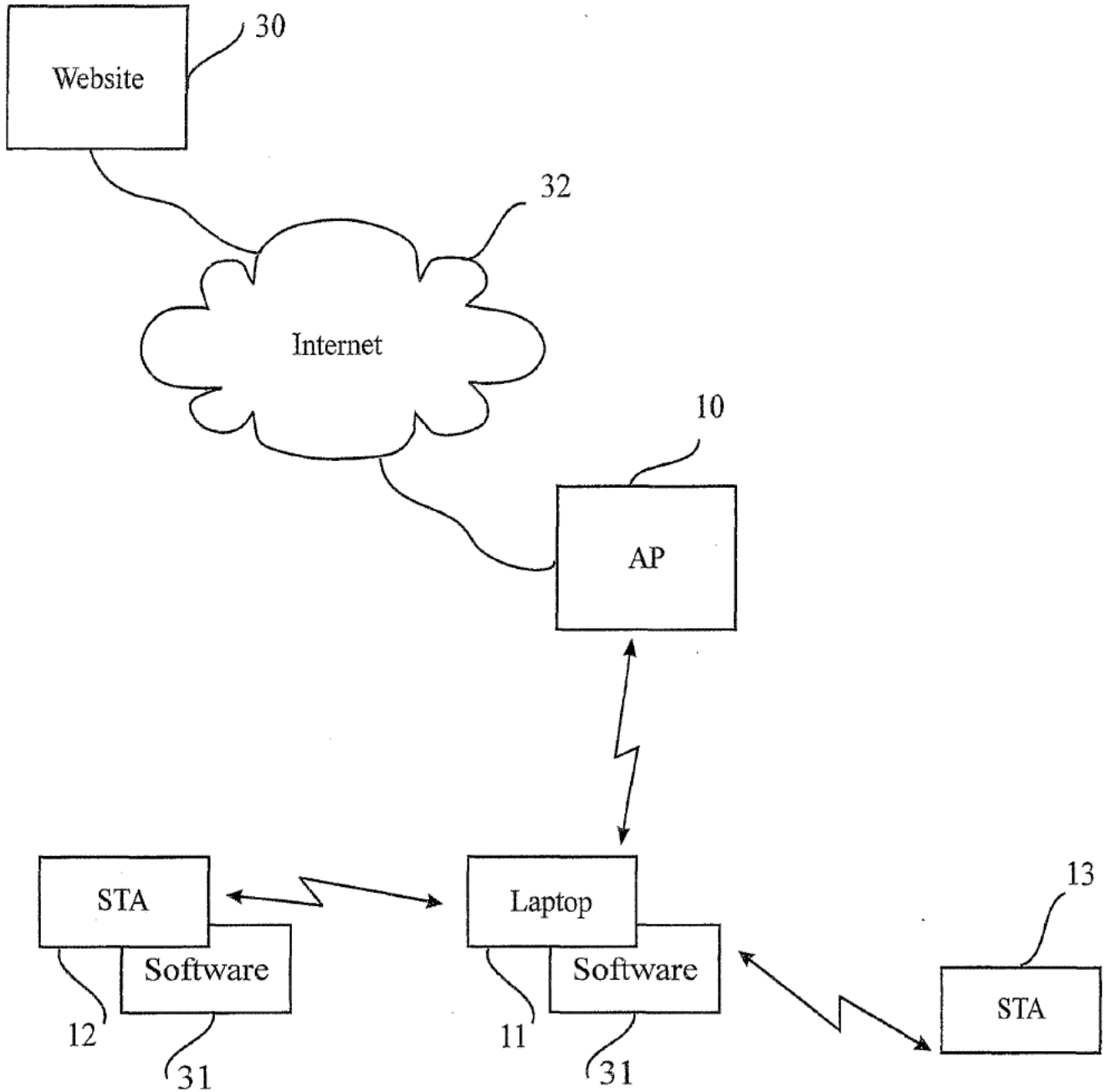

Website
30
32
Internet
10
AP
STA
Software
12
31
Laptop
Software
11
31
13
STA

FIG. 2

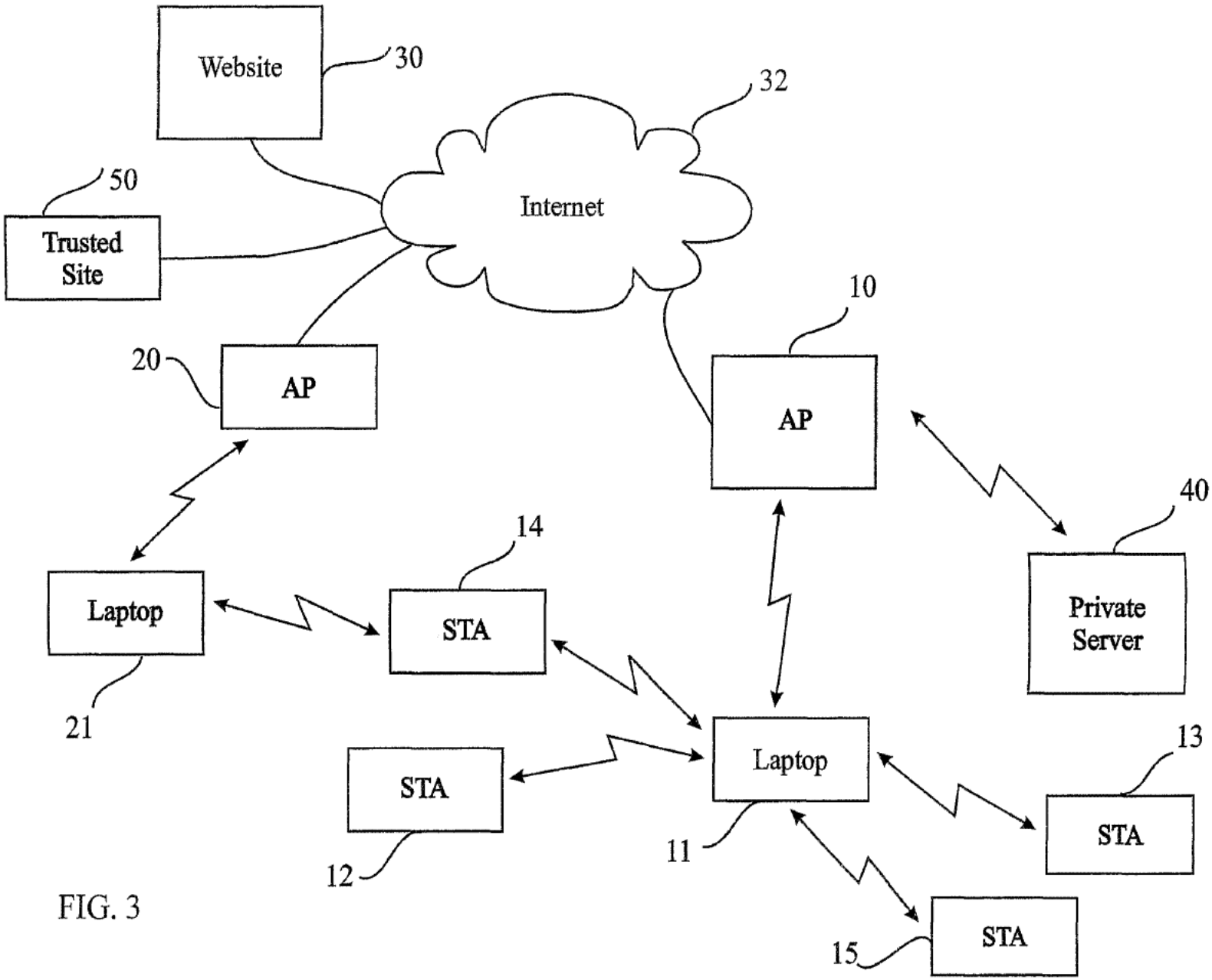

Website
30
32
Internet
50
Trusted Site
10
20
AP
AP
40
14
Laptop
STA
Private Server
21
13
STA
Laptop
STA
11
12
15
STA

FIG. 3

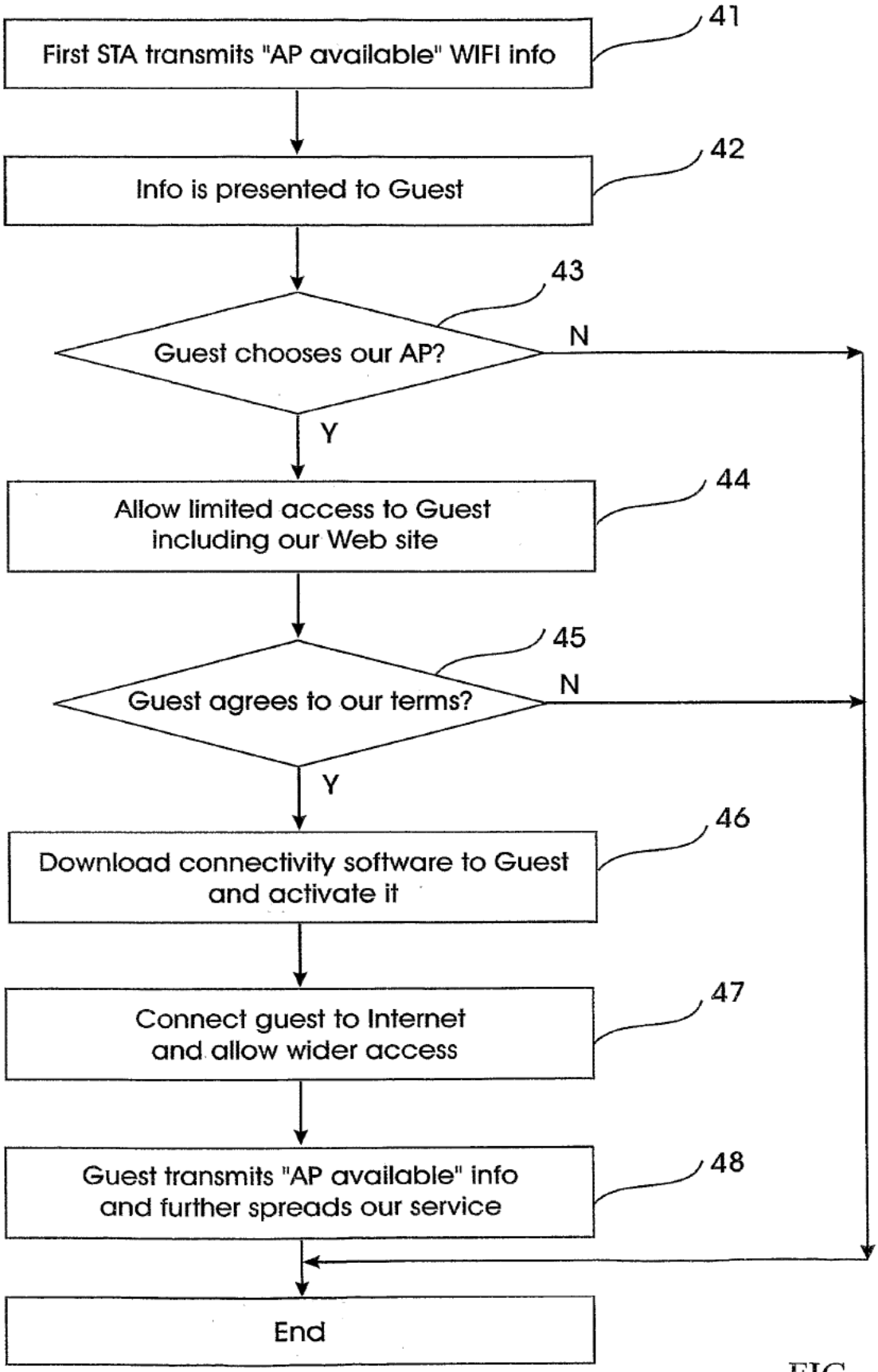

First STA transmits "AP available" WIFI info
41
Info is presented to Guest
42
Guest chooses our AP?
43
N
Y
Allow limited access to Guest including our Web site
44
Guest agrees to our terms?
45
N
Y
Download connectivity software to Guest and activate it
46
Connect guest to Internet and allow wider access
47
Guest transmits "AP available" info and further spreads our service
48
End

FIG. 4

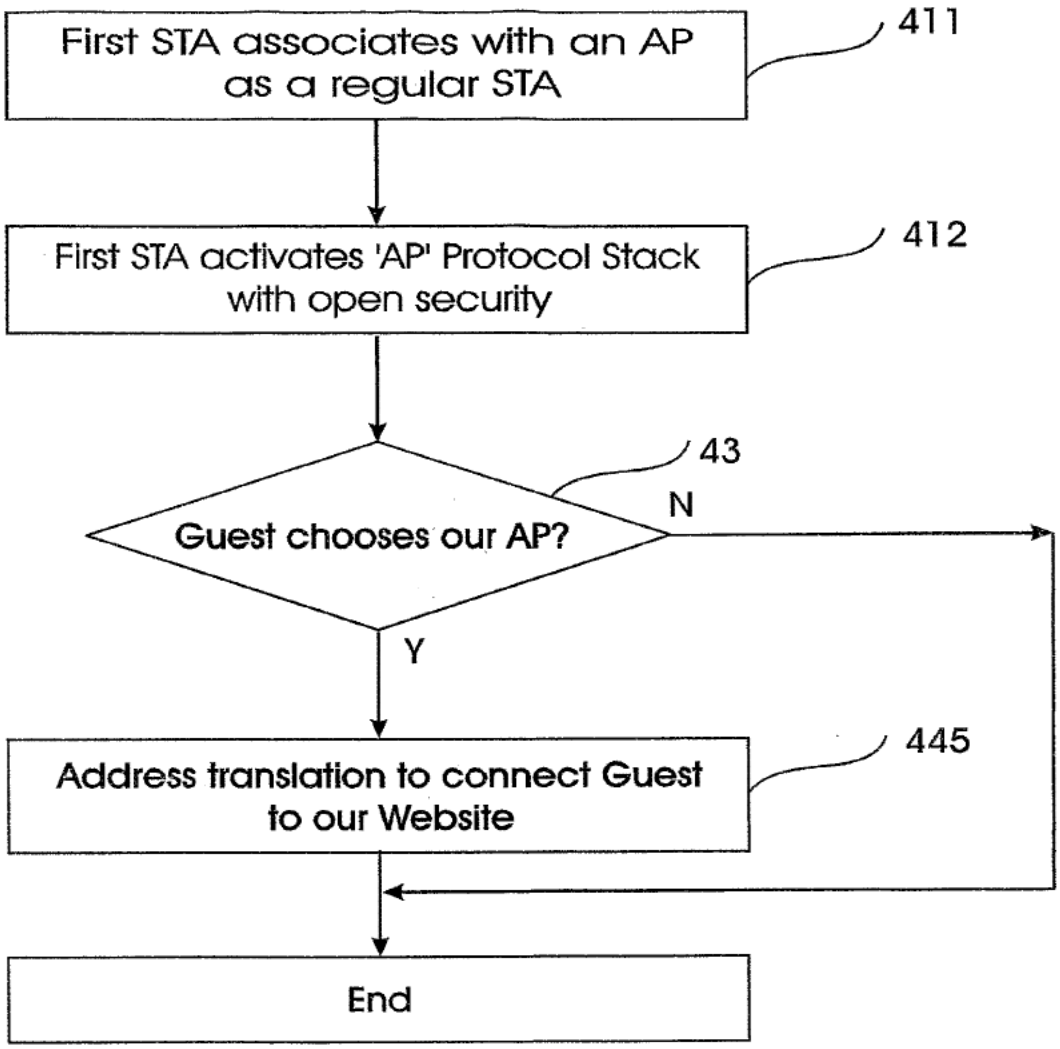

First STA associates with an AP as a regular STA
411
First STA activates 'AP' Protocol Stack with open security
412
43
Guest chooses our AP?
N
Y
Address translation to connect Guest to our Website
445
End

FIG. 5

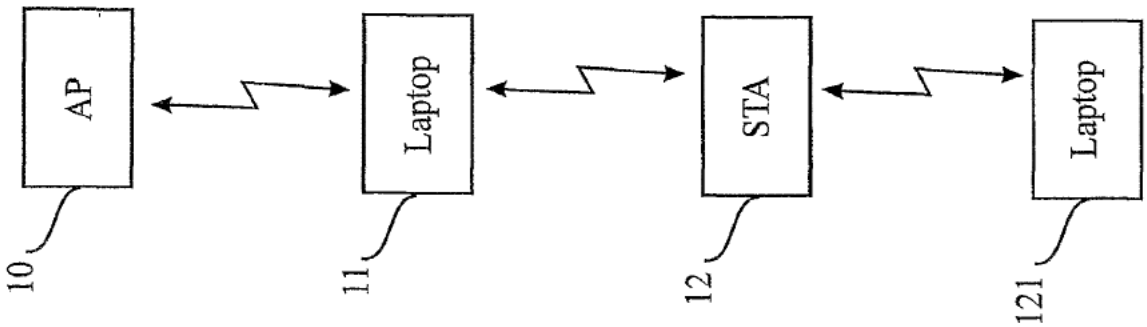


FIG. 6C

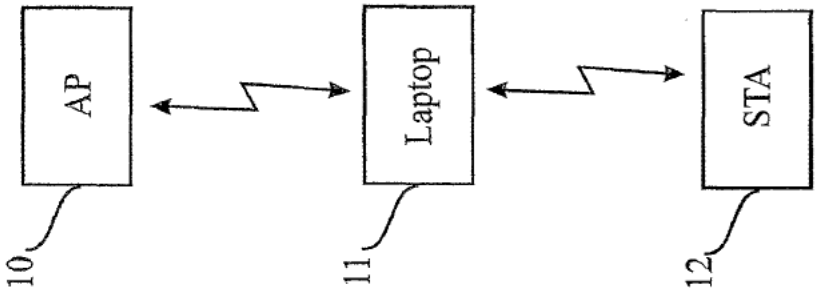


FIG. 6B

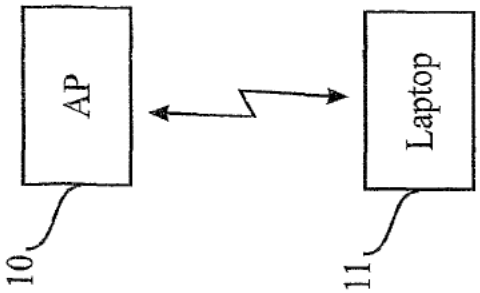


FIG. 6A

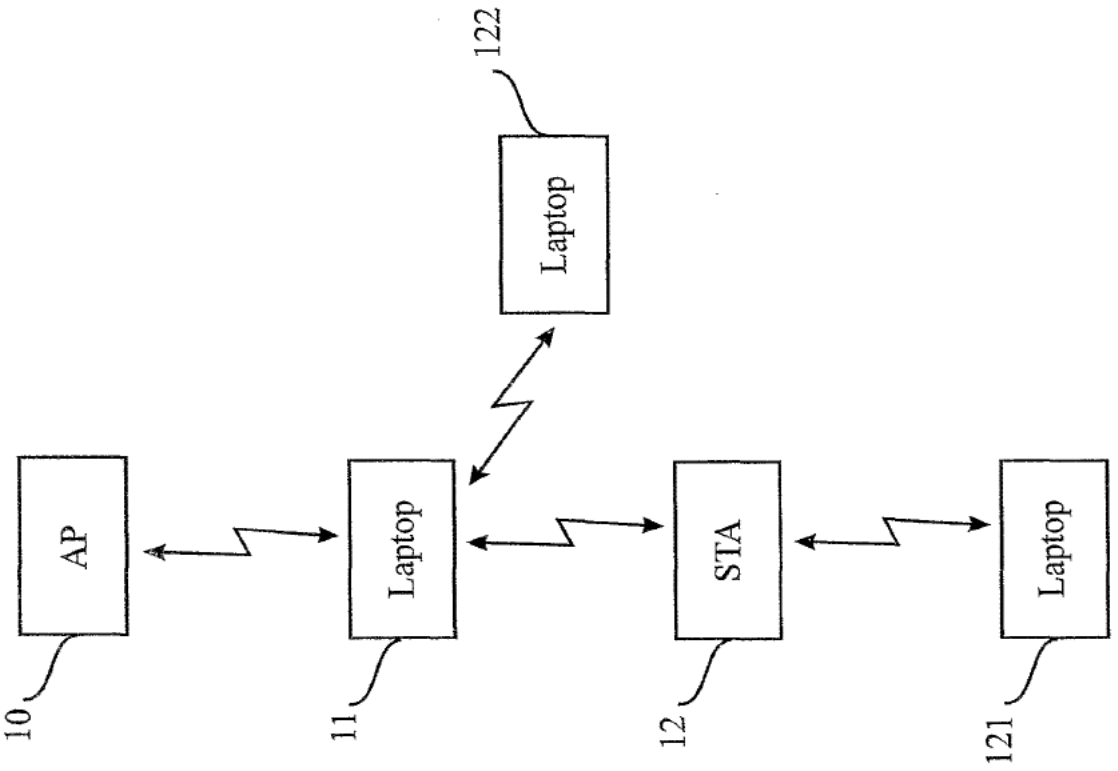


FIG. 6D

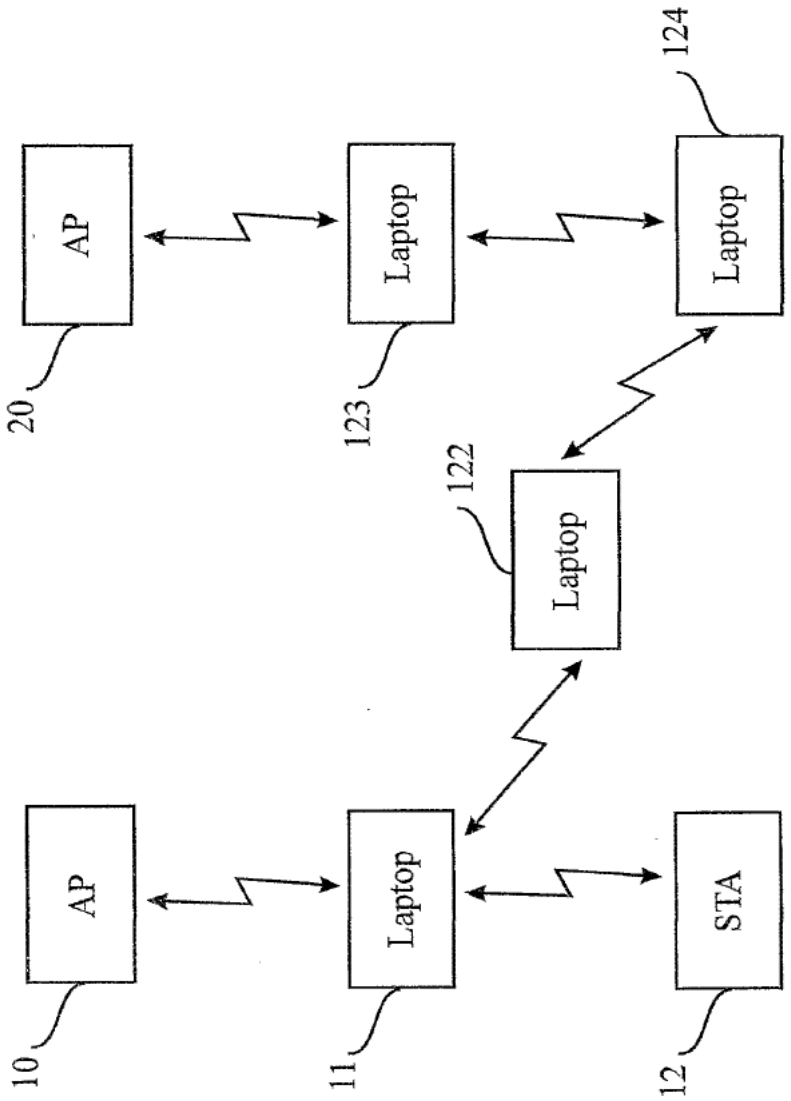


FIG. 6E

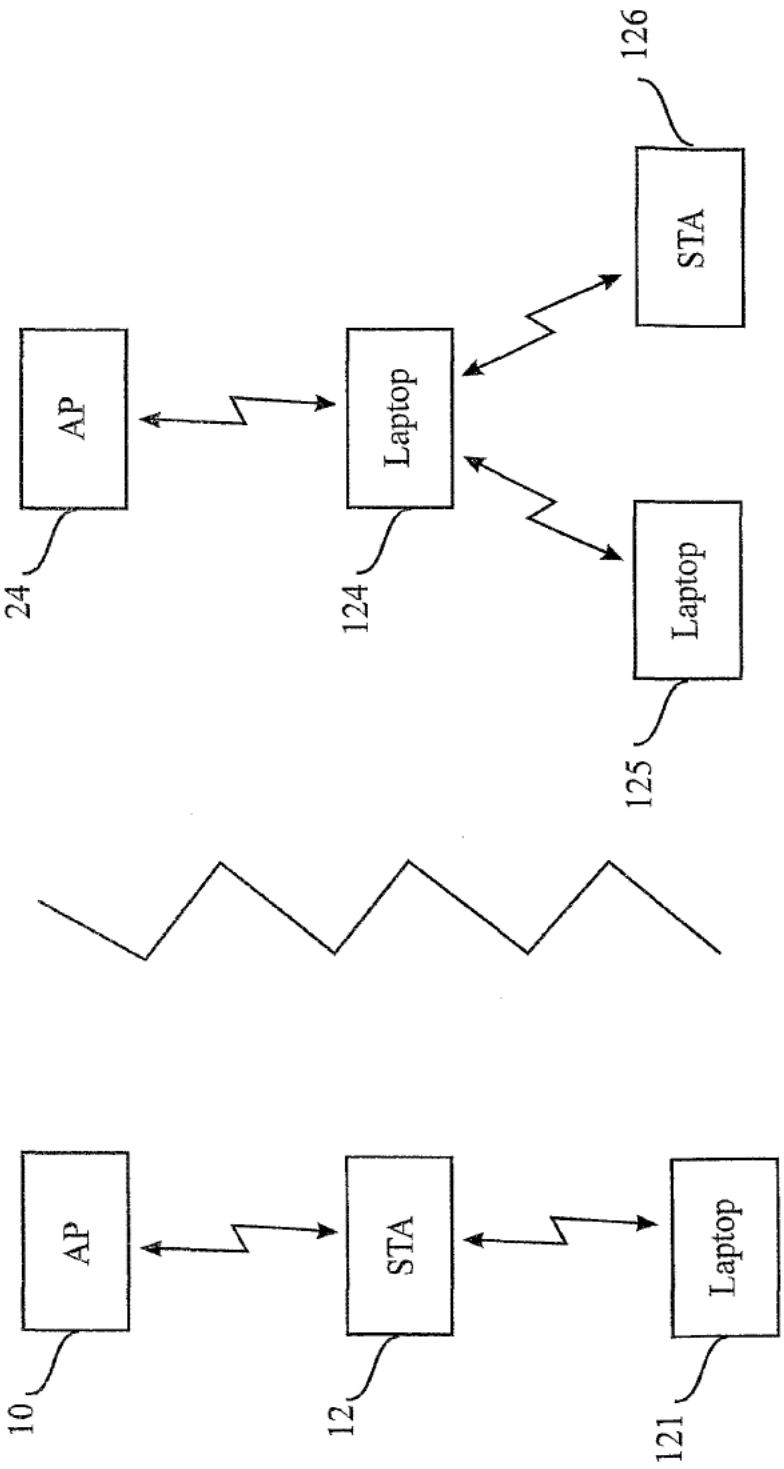


FIG. 6F

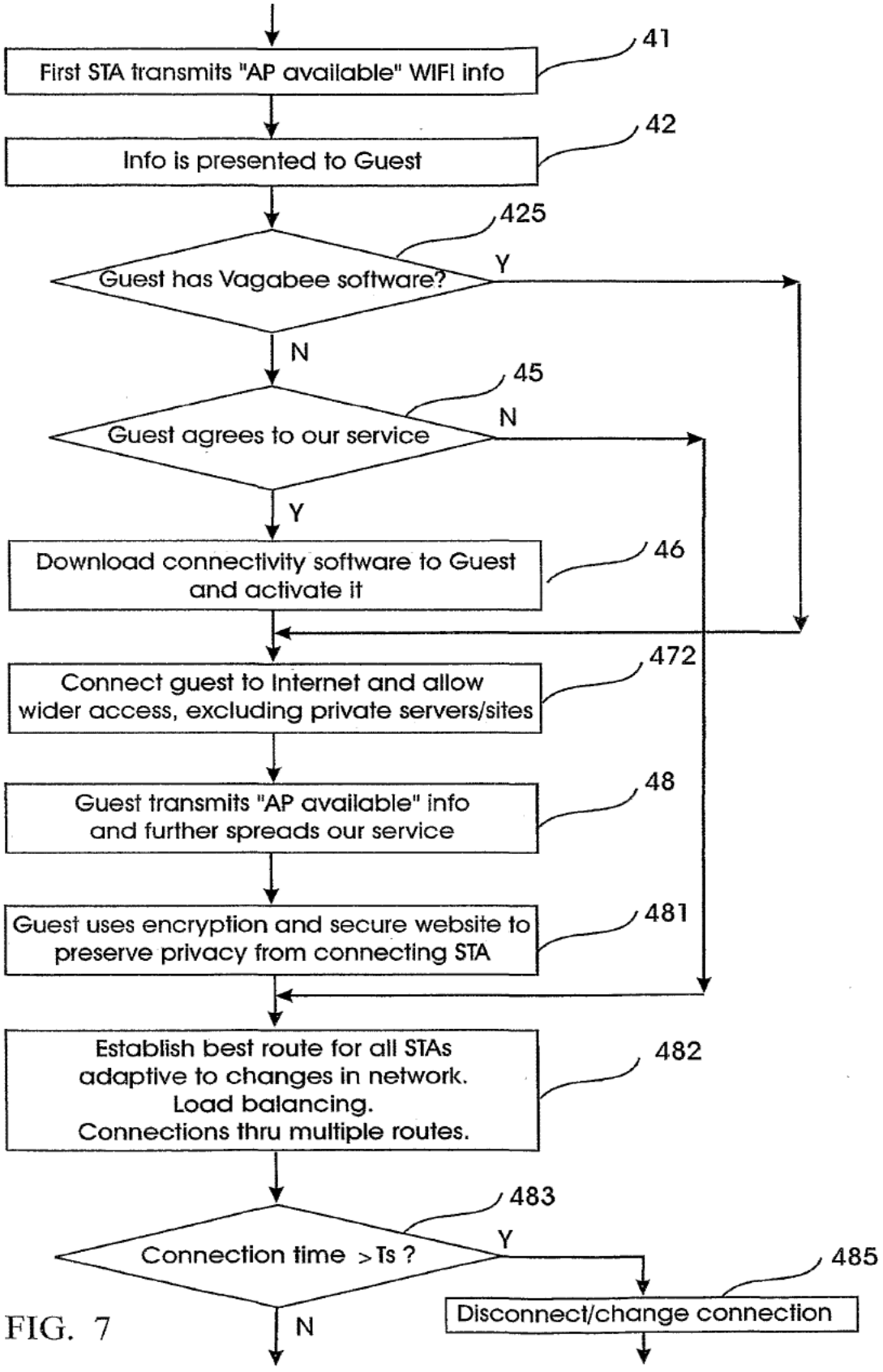

First STA transmits "AP available" WIFI info
41
Info is presented to Guest
42
425
Guest has Vagabee software?
Y
N
45
Guest agrees to our service
N
Y
Download connectivity software to Guest and activate it
46
Connect guest to Internet and allow wider access, excluding private servers/sites
472
Guest transmits "AP available" info and further spreads our service
48
Guest uses encryption and secure website to preserve privacy from connecting STA
481
Establish best route for all STAs adaptive to changes in network. Load balancing. Connections thru multiple routes.
482
483
Connection time >Ts ?
Y
N
485
Disconnect/change connection

FIG. 7

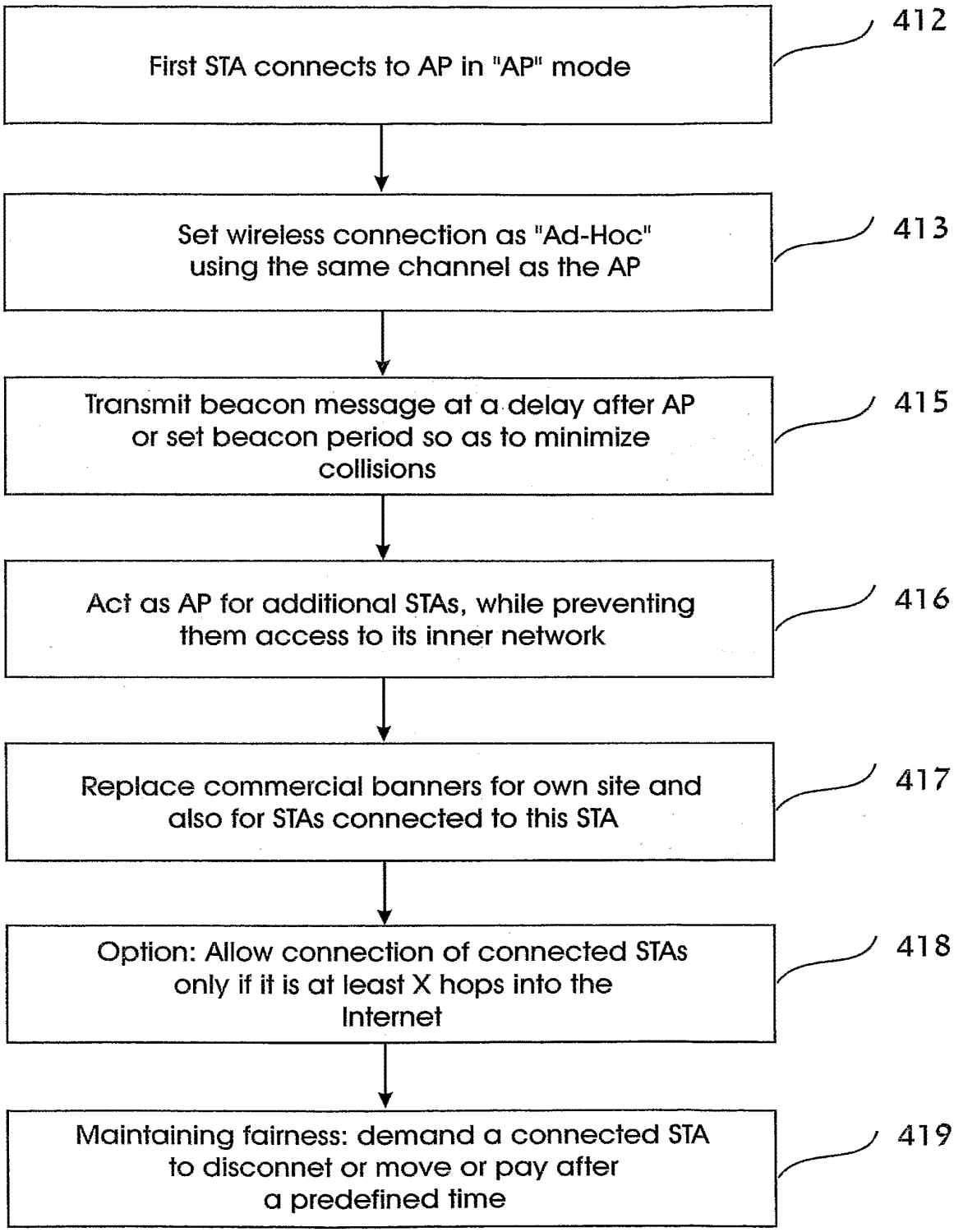

First STA connects to AP in "AP" mode
412
Set wireless connection as "Ad-Hoc" using the same channel as the AP
413
Transmit beacon message at a delay after AP or set beacon period so as to minimize collisions
415
Act as AP for additional STAs, while preventing them access to its inner network
416
Replace commercial banners for own site and also for STAs connected to this STA
417
Option: Allow connection of connected STAs only if it is at least X hops into the Internet
418
Maintaining fairness: demand a connected STA to disconnet or move or pay after a predefined time
419

FIG. 8

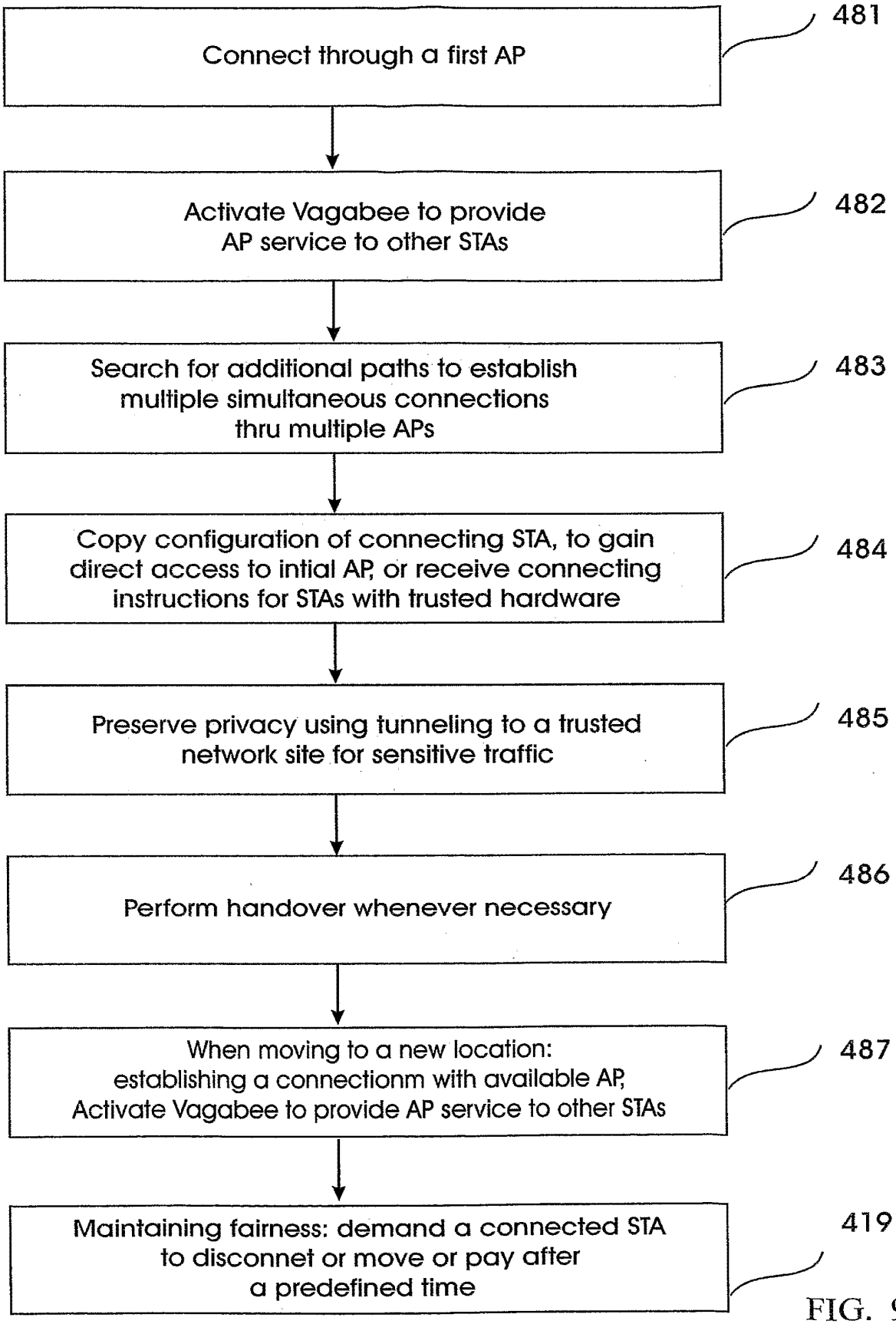

Connect through a first AP
481
Activate Vagabee to provide AP service to other STAs
482
Search for additional paths to establish multiple simultaneous connections thru multiple APs
483
Copy configuration of connecting STA, to gain direct access to intial AP, or receive connecting instructions for STAs with trusted hardware
484
Preserve privacy using tunneling to a trusted network site for sensitive traffic
485
Perform handover whenever necessary
486
When moving to a new location: establishing a connectionm with available AP, Activate Vagabee to provide AP service to other STAs
487
Maintaining fairness: demand a connected STA to disconnet or move or pay after a predefined time
419

FIG. 9

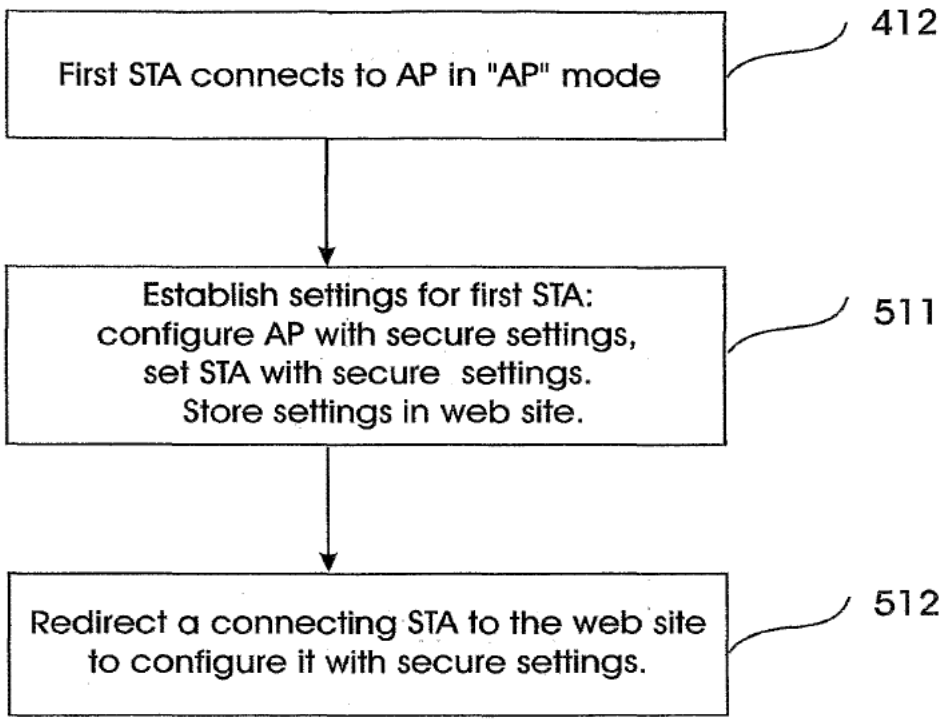

First STA connects to AP in "AP" mode
412
Establish settings for first STA:
configure AP with secure settings,
set STA with secure settings.
Store settings in web site.
511
Redirect a connecting STA to the web site
to configure it with secure settings.
512

FIG. 10

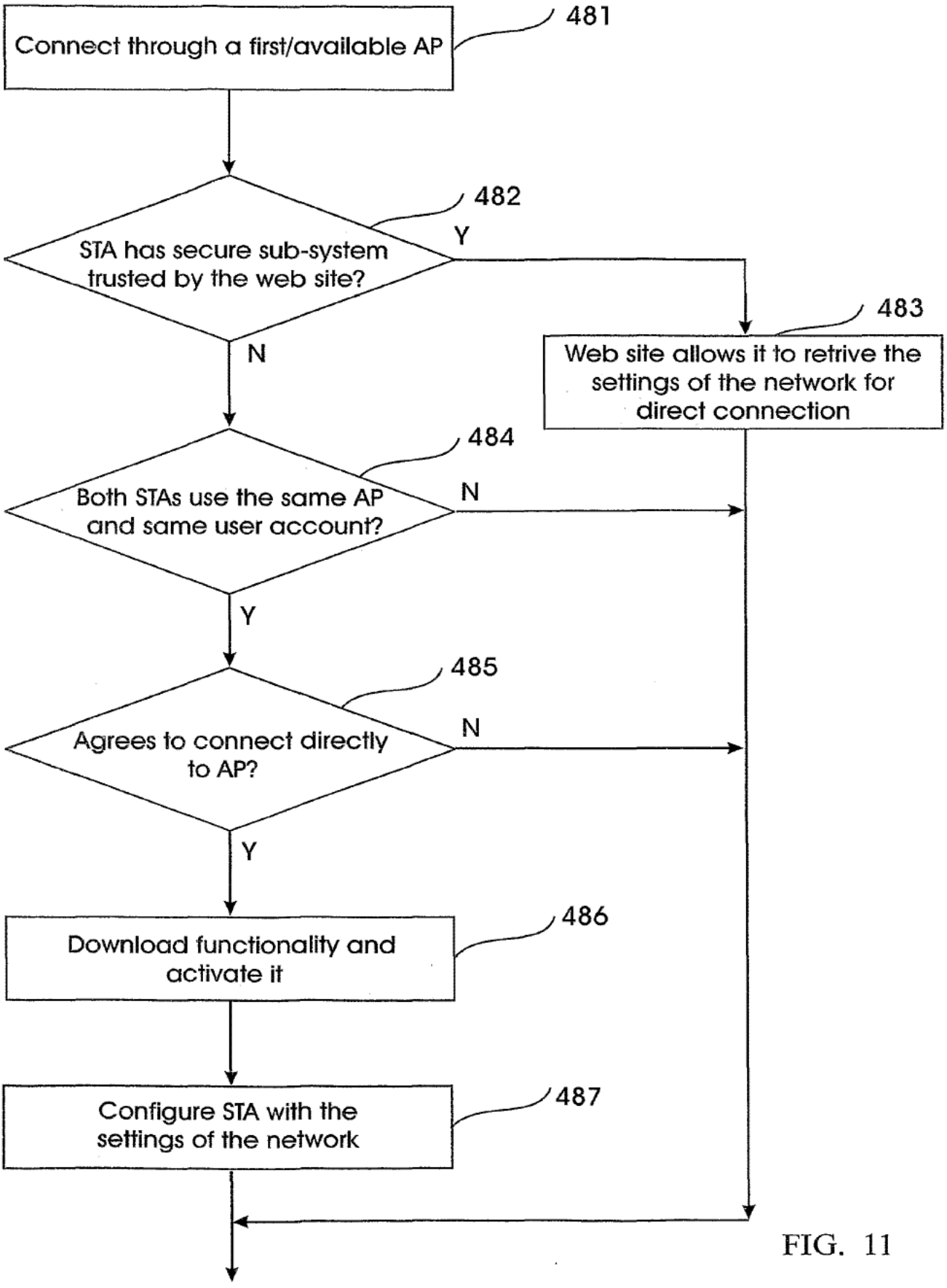

Connect through a first/available AP
481
STA has secure sub-system trusted by the web site?
482
Y
N
Web site allows it to retrive the settings of the network for direct connection
483
Both STAs use the same AP and same user account?
484
N
Y
Agrees to connect directly to AP?
485
N
Y
Download functionality and activate it
486
Configure STA with the settings of the network
487

FIG. 11

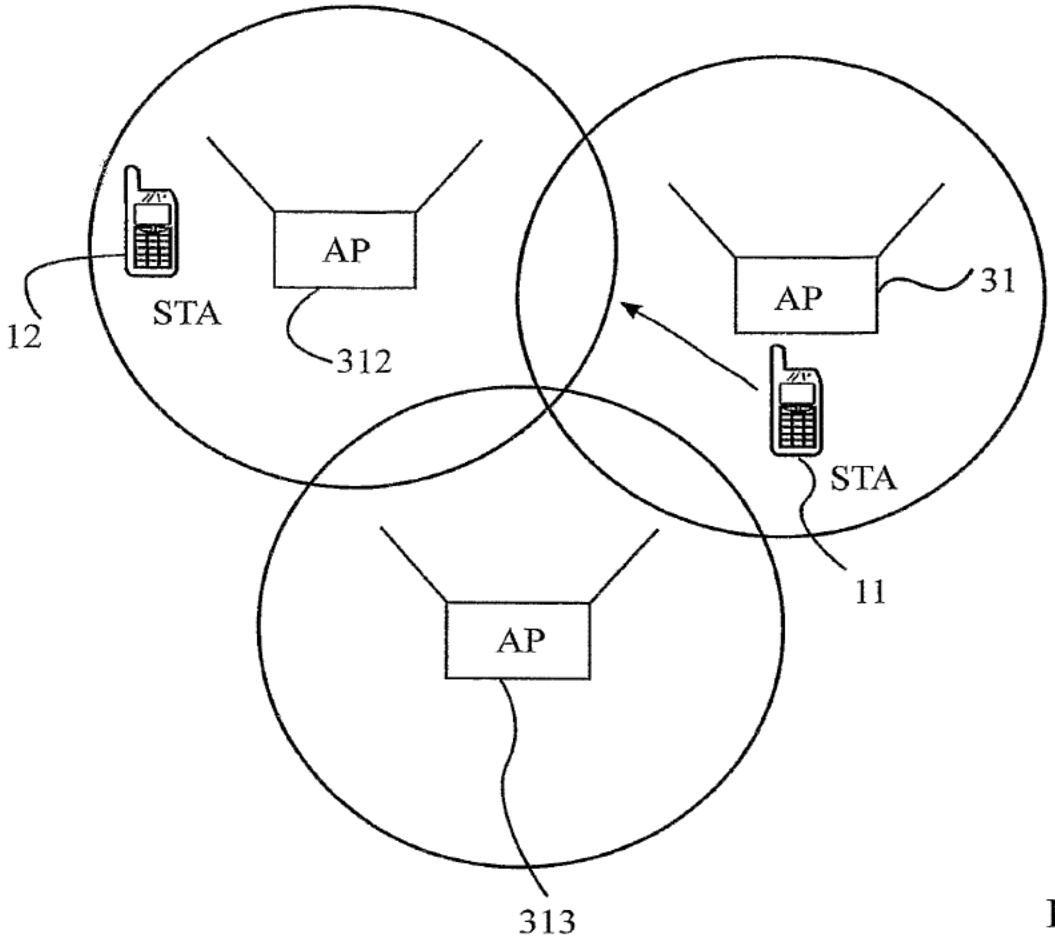

AP
STA
12
312
AP
31
STA
11
AP
313

FIG. 12

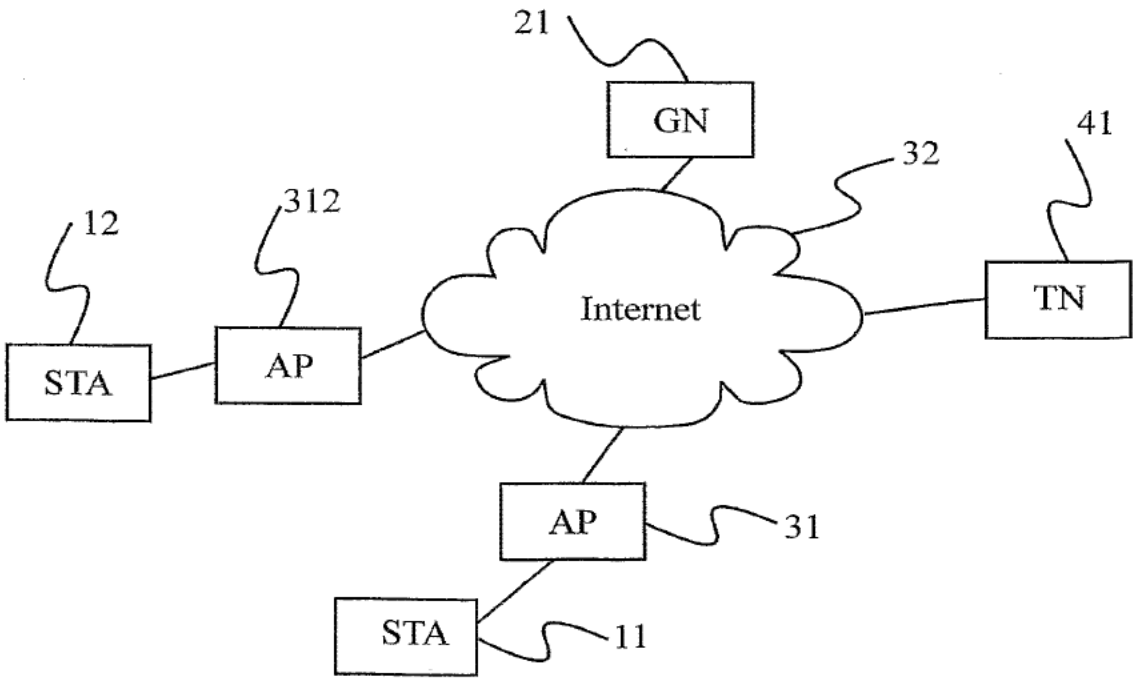

21
GN
41
32
312
12
Internet
TN
STA
AP
AP
31
STA
11

FIG. 13

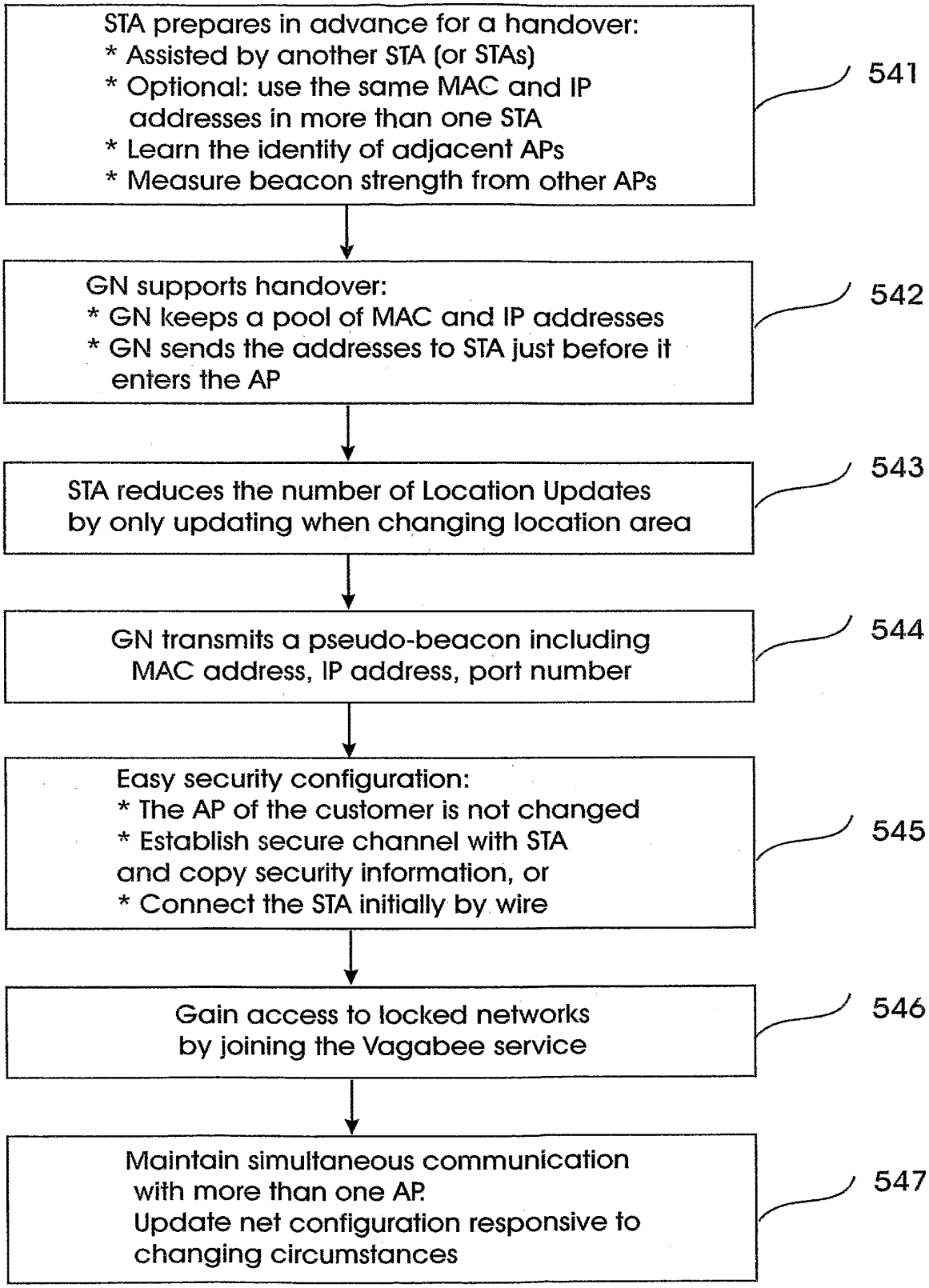

STA prepares in advance for a handover:
* Assisted by another STA (or STAs)
* Optional: use the same MAC and IP addresses in more than one STA
* Learn the identity of adjacent APs
* Measure beacon strength from other APs
541
GN supports handover:
* GN keeps a pool of MAC and IP addresses
* GN sends the addresses to STA just before it enters the AP
542
STA reduces the number of Location Updates by only updating when changing location area
543
GN transmits a pseudo-beacon including MAC address, IP address, port number
544
Easy security configuration:
* The AP of the customer is not changed
* Establish secure channel with STA and copy security information, or
* Connect the STA initially by wire
545
Gain access to locked networks by joining the Vagabee service
546
Maintain simultaneous communication with more than one AP.
Update net configuration responsive to changing circumstances
547

FIG. 14

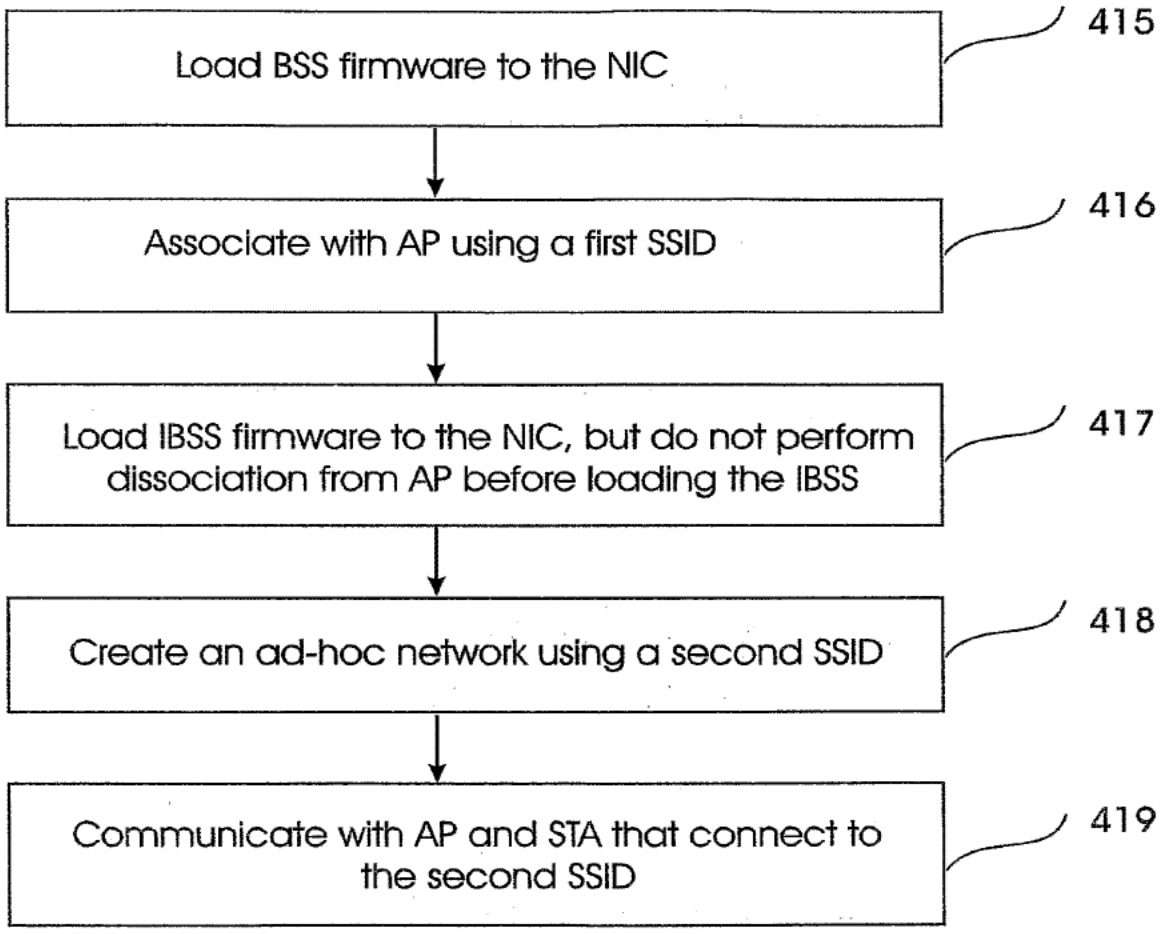

Load BSS firmware to the NIC
415
Associate with AP using a first SSID
416
Load IBSS firmware to the NIC, but do not perform dissociation from AP before loading the IBSS
417
Create an ad-hoc network using a second SSID
418
Communicate with AP and STA that connect to the second SSID
419

FIG. 15

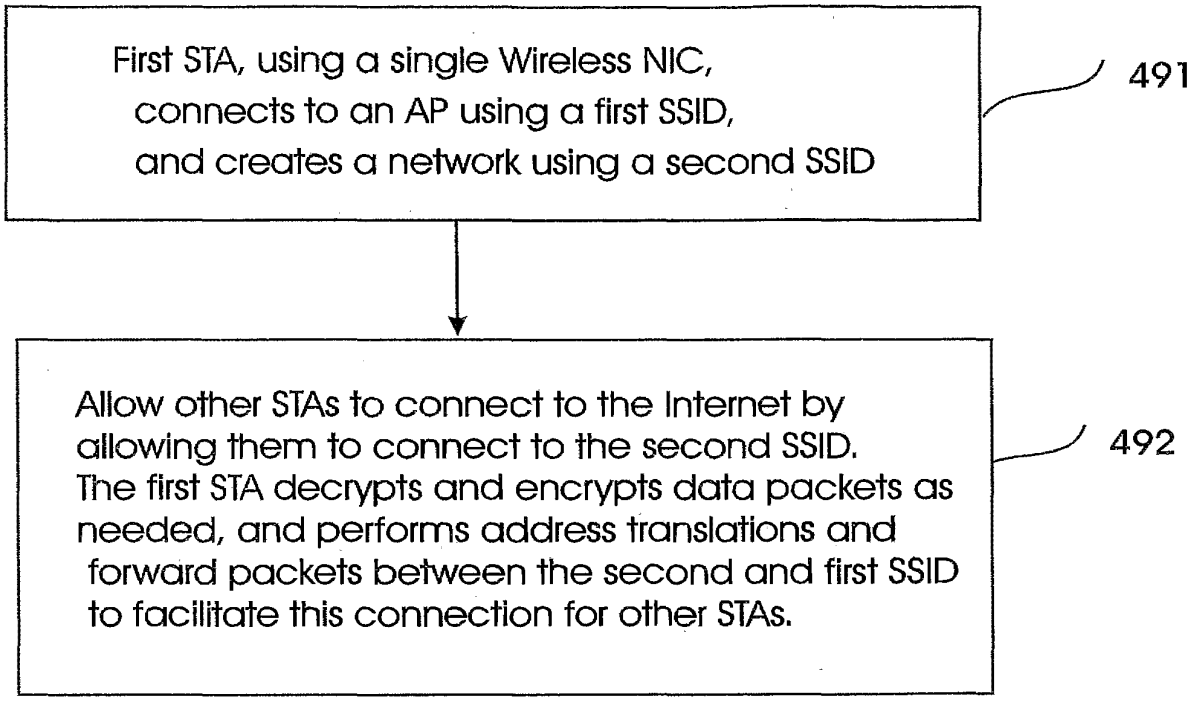

First STA, using a single Wireless NIC,
connects to an AP using a first SSID,
and creates a network using a second SSID
491
Allow other STAs to connect to the Internet by
allowing them to connect to the second SSID.
The first STA decrypts and encrypts data packets as
needed, and performs address translations and
forward packets between the second and first SSID
to facilitate this connection for other STAs.
492

FIG. 16

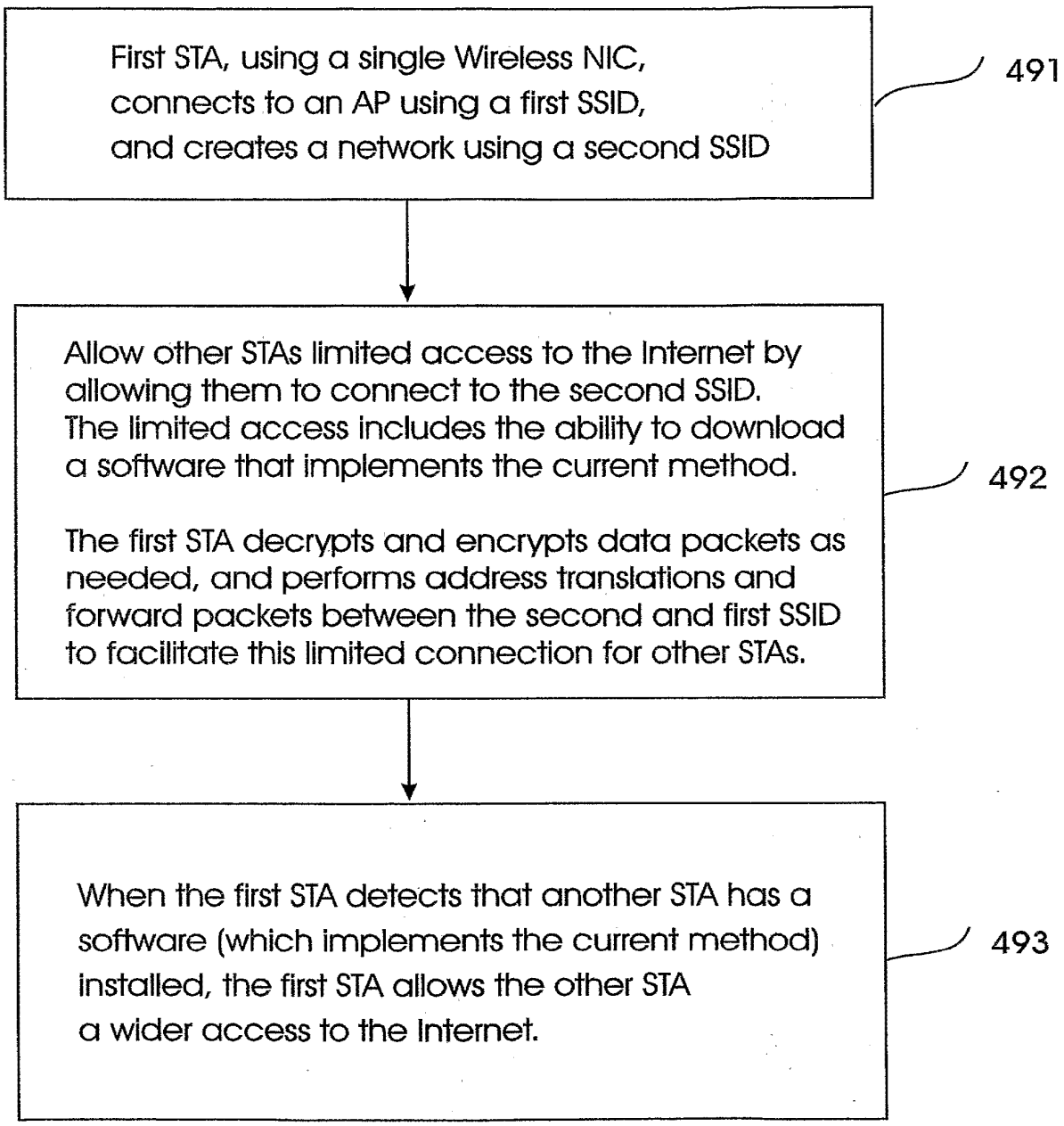

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID. The limited access includes the ability to download a software that implements the current method.
The first STA decrypts and encrypts data packets as needed, and performs address translations and forward packets between the second and first SSID to facilitate this limited connection for other STAs.
492
When the first STA detects that another STA has a software (which implements the current method) installed, the first STA allows the other STA a wider access to the Internet.
493

FIG. 17

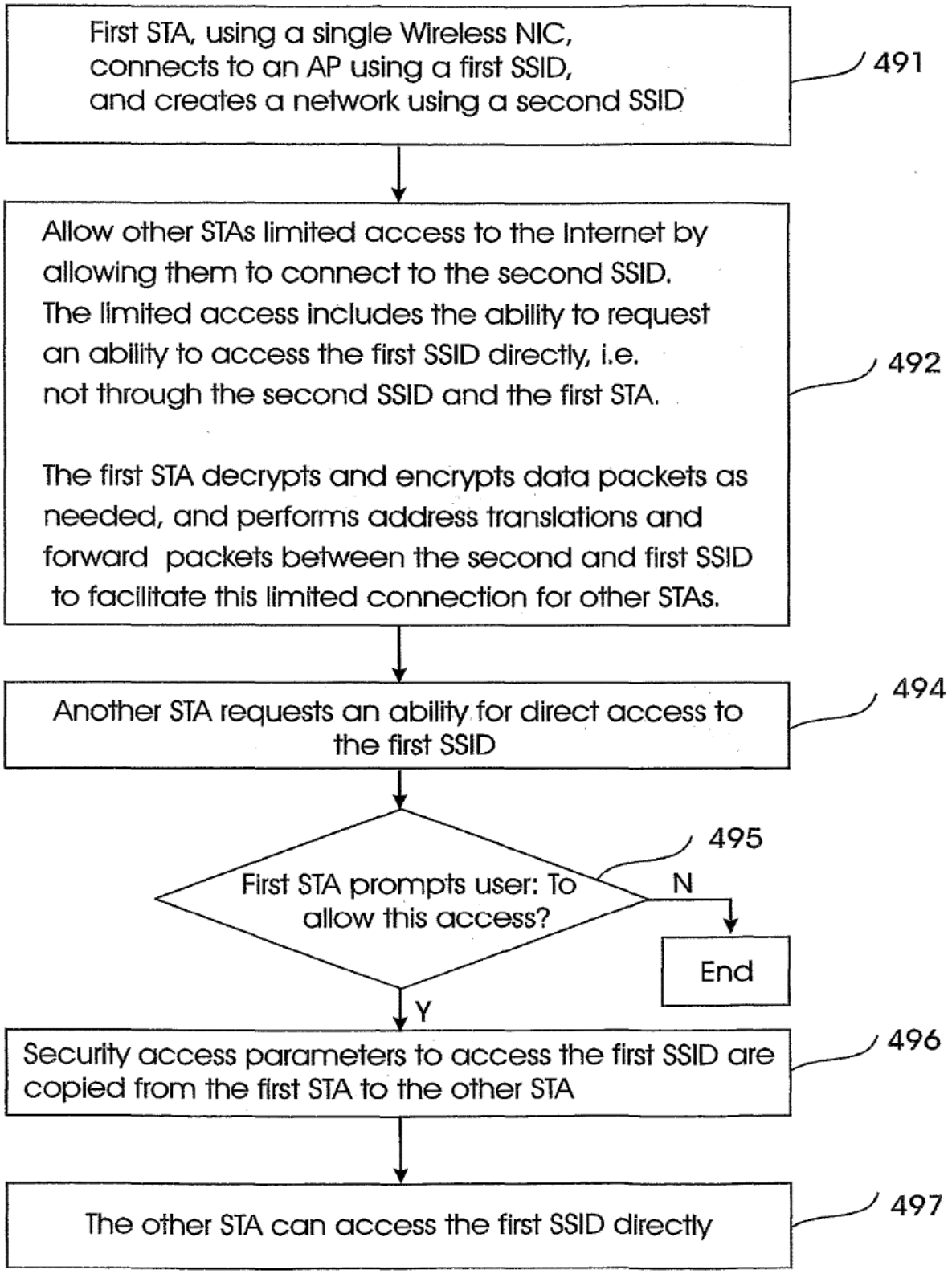

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID. The limited access includes the ability to request an ability to access the first SSID directly, i.e. not through the second SSID and the first STA.
The first STA decrypts and encrypts data packets as needed, and performs address translations and forward packets between the second and first SSID to facilitate this limited connection for other STAs.
492
Another STA requests an ability for direct access to the first SSID
494
First STA prompts user: To allow this access?
495
N
End
Y
Security access parameters to access the first SSID are copied from the first STA to the other STA
496
The other STA can access the first SSID directly
497

FIG. 18

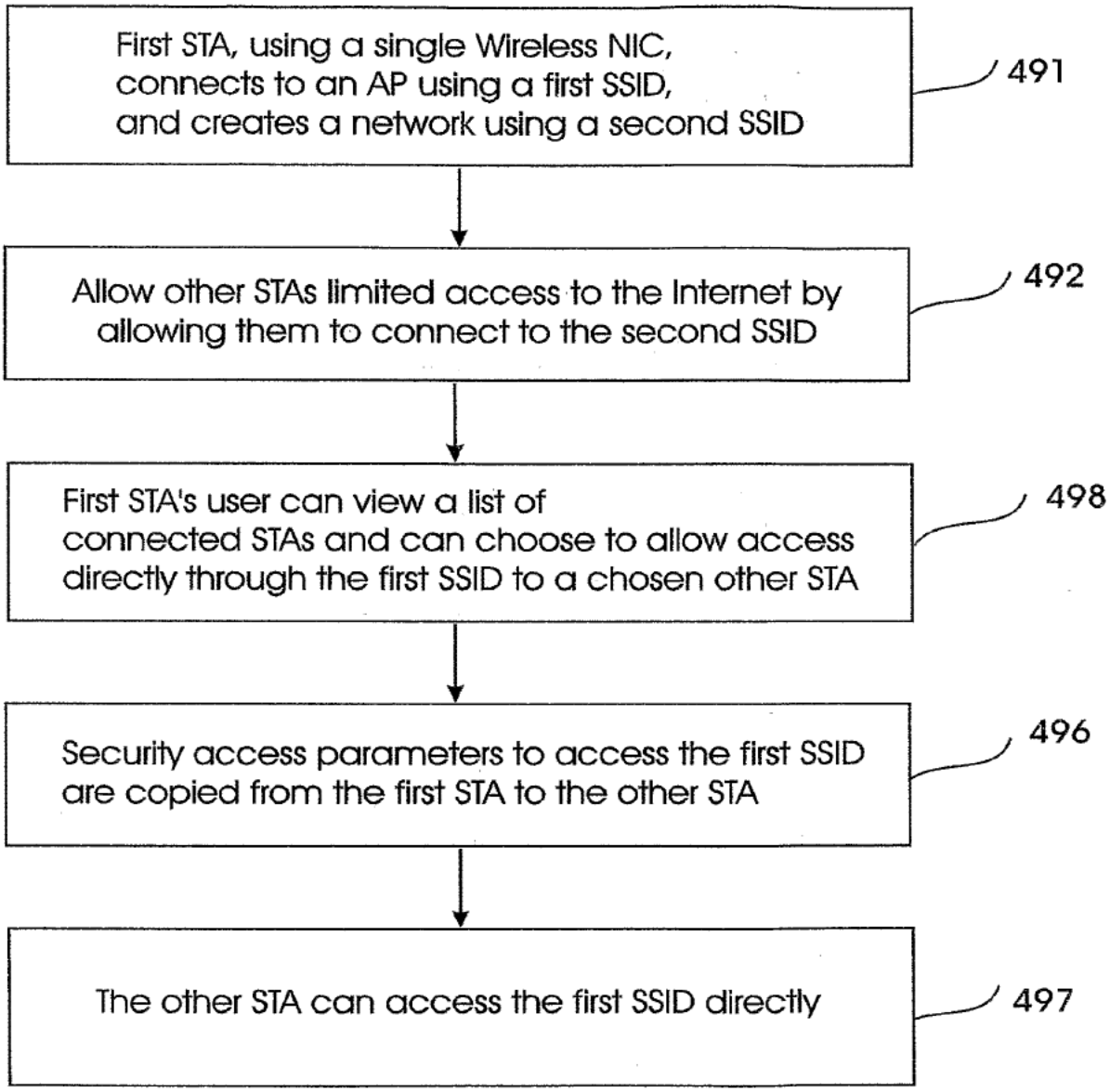

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID
492
First STA's user can view a list of connected STAs and can choose to allow access directly through the first SSID to a chosen other STA
498
Security access parameters to access the first SSID are copied from the first STA to the other STA
496
The other STA can access the first SSID directly
497

FIG. 19

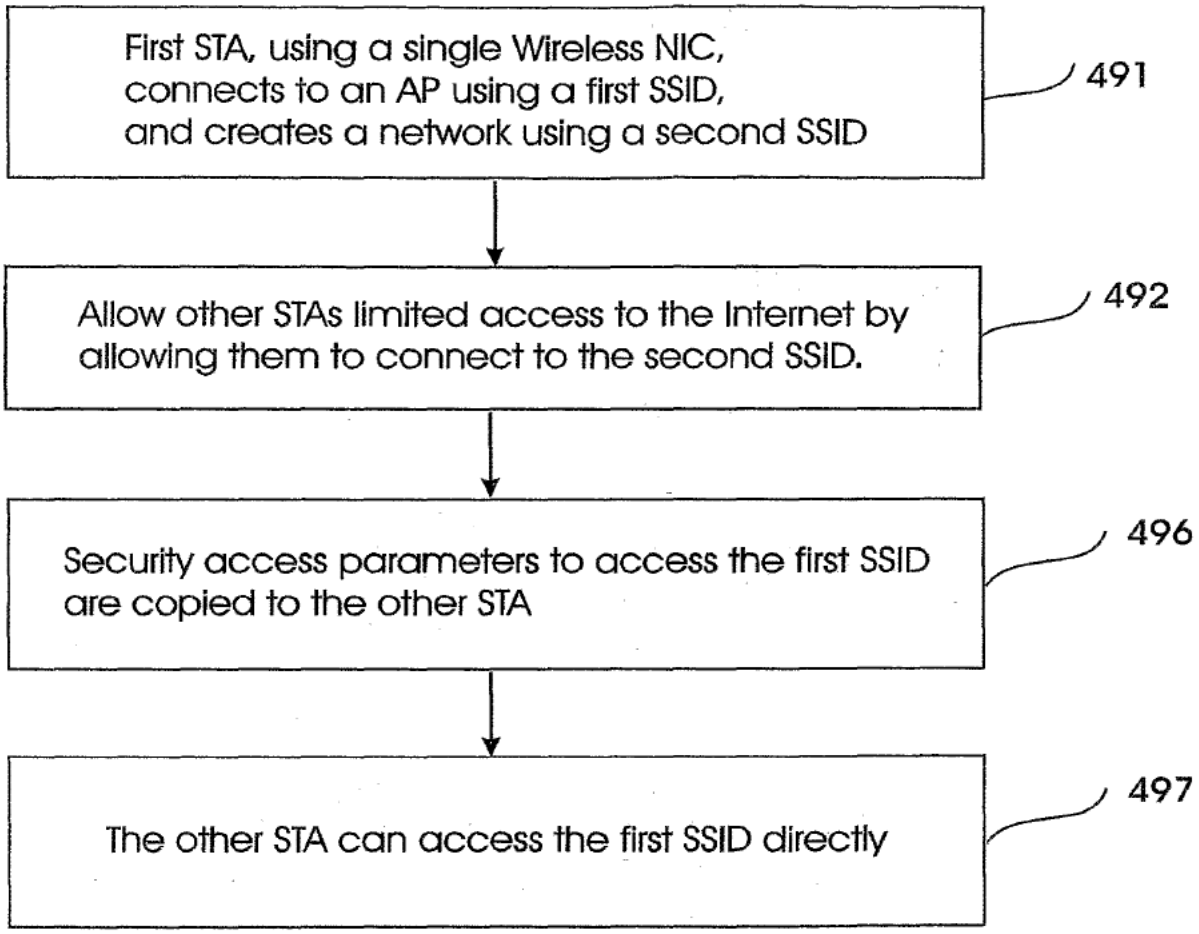

First STA, using a single Wireless NIC, connects to an AP using a first SSID, and creates a network using a second SSID
491
Allow other STAs limited access to the Internet by allowing them to connect to the second SSID.
492
Security access parameters to access the first SSID are copied to the other STA
496
The other STA can access the first SSID directly
497

FIG. 20

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2007 (30.08.2007)

PCT

(10) International Publication Number
WO 2007/096884 A3

(51) International Patent Classification:
H04Q 7/24 (2006.01)

(21) International Application Number:
PCT/IL2007/000244

(22) International Filing Date:
22 February 2007 (22.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/775,321 22 February 2006 (22.02.2006) US
60/794,135 24 April 2006 (24.04.2006) US

(71) Applicant and
(72) Inventor: **BARKAN, Elad** [IL/IL]; C/O Marc Zuta, Patent Attorney, P.O. Box 2162, 49120 Petah-Tikva (IL).

(74) Agent: **ZUTA, Marc**; Marc Zuta, Patent Attorney, P.O. Box 2162, 49120 Petah-Tikva (IL).

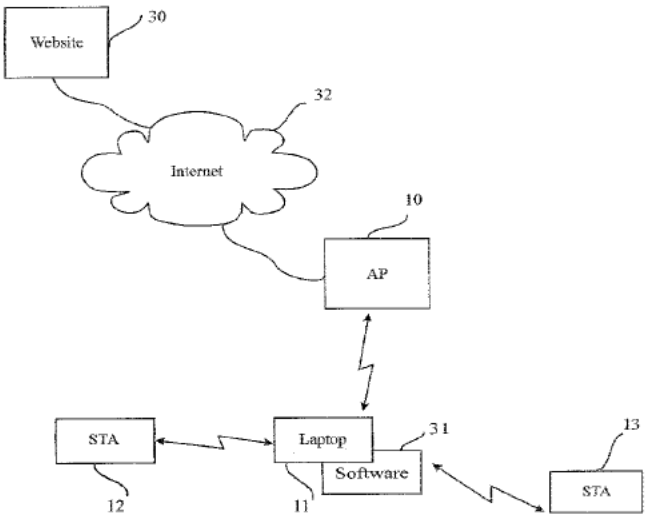
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
9 April 2009

(54) Title: WIRELESS INTERNET SYSTEM AND METHOD



(57) Abstract: A method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising: wirelessly connecting a first STA to the Internet through a first AP with a first SSID; remaining connected to the first Access Point (AP), the first STA creates a software-based wireless AP with a second SSID for wirelessly connecting other STAs to the Internet through the first STA. A software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein. A method for configuring STAs to connect to a wireless network, comprising: a customer first connects a STA by wire to its network; a software on the STA copies to the STA the security information gained through the wired connection, thus setting the security parameters for the STA.

WO 2007/096884 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL07/00244

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04Q 7/24**(2006.01)

USPC: 370/338
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 370/338

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/0097473 (Saitoh) 22 May 2003 (22.05.2003), [0038] and [0039]	1-9, 13-21 and 25-42
Y	US 2007/0066306 (Cheng) 22 March 2007 (22.03.2007),	[0014] and [0020]-[0024]
Y	US 2002/0077094 (Leppanen) 20 June 2002 (20.06.2002), [0014]	7, 8, 14-21, 26 and 28-37
Y	US 7,292,870 (Heredin et al.) 6 Nov 2007 (06.11.2007), column 16 lines 34-48	10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
01 September 2008 (01.09.2008)	24 NOV 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Vincent P Harper Telephone No. (571) 272-7375

Form PCT/ISA/210 (second sheet) (April 2007)

UNITED STATES PATENT AND TRADEMARK OFFICE

26 JUL 2010

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

PROFESSIONAL PATENT SOLUTIONS
P.O. BOX 654
HERZELIYA PITUACH 46105 IL
ISRAEL

In re Application of:
Elad Barkan
Application No.: 12/665,978
PCT No.: PCT/IL2007/000244
Int. Filing Date: 22 February, 2007
Priority Date: 22 February, 2006
Attorney Docket No.: BRK-PU-001-US1
For: WIRELESS INTERNET SYSTEM AND METHOD

DECISION ON PETITION UNDER 37 CFR 1.137(b)

This is a decision on the applicants' petition to revive under 37 CFR 1.137 (b) filed on 22 December 2009.

BACKGROUND

On 22 February 2007, applicants filed international application PCT/IL2007/000244 claiming a priority date of 22 February 2006. The deadline for entry into the United States National Stage was thirty months from the international filing date, which is 24 August 2009 (22 August 2009 is a Saturday).

On 22 December 2009, applicants filed a national stage application under 35 U.S.C. 371 of PCT/IL2007/000244, which was accompanied by, *inter alia*, a petition to revive under 37 CFR 1.137(b).

DISCUSSION

A petition under 37 CFR 1.137(b) must be accompanied by (1) a proper reply, (2) the petition fee required by law, (3) a statement that the "entire delay in filing the required reply from the due date for the reply until the filing of a grantable petition was unintentional," and (4) a terminal disclaimer and fee (if the international application was filed prior to June 8, 1995).

Here, the proper reply was the filing of the subject petition to revive along with a national stage application and fee. The petition fee of $810.00 was provided. The statement required by 37 CFR 1.137(b)(3) was provided. A terminal disclaimer is not required.

All requirements of 37 CFR1.137 (b) are satisfied.

CONCLUSION

The petition to revive the application abandoned under 37 CFR 1.137(b) is **GRANTED**.

A declaration in compliance with 37 CFR 1.497(a) and (b) was provided with the national stage papers.

This application is being forwarded to the United States Designated/Elected Office for further processing in accordance with this decision.

Richard Cole
PCT Legal Examiner
PCT Legal Administration

Layla Lauchman
Detailee
Telephone: (571) 272-2412

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
12/665,978	Elad Barkan	BRK-PU-001-US1

60956
Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

INTERNATIONAL APPLICATION NO.	
PCT/IL07/00244	
I.A. FILING DATE	PRIORITY DATE
02/22/2007	02/22/2006

CONFIRMATION NO. 5873
371 ACCEPTANCE LETTER

OC000000043055374

Date Mailed: 08/18/2010

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office in its capacity as a Designated / Elected Office (37 CFR 1.495), has determined that the above identified international application has met the requirements of 35 U.S.C. 371, and is ACCEPTED for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above and the relevant dates are:

12/22/2009	12/22/2009
DATE OF RECEIPT OF 35 U.S.C. 371(c)(1), (c)(2) and (c)(4) REQUIREMENTS	DATE OF COMPLETION OF ALL 35 U.S.C. 371 REQUIREMENTS

A Filing Receipt (PTO-103X) will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE " FILING DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1), (c)(2) and (c)(4) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN ABOVE.** *The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363).* Once the Filing Receipt has been received, send all correspondence to the Group Art Unit designated thereon.

The following items have been received:

- Indication of Small Entity Status
- Copy of the International Application filed on 12/22/2009
- Copy of the International Search Report filed on 12/22/2009
- Preliminary Amendments filed on 12/22/2009
- Oath or Declaration filed on 12/22/2009
- Small Entity Statement filed on 12/22/2009
- Request for Immediate Examination filed on 12/22/2009
- U.S. Basic National Fees filed on 12/22/2009
- Priority Documents filed on 12/22/2009
- Power of Attorney filed on 12/22/2009

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

WINSTON M ALVARADO

Telephone: (703) 756-1466

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/665,978	12/22/2009		325	BRK-PU-001-US1	20	3

CONFIRMATION NO. 5873

60956
Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

FILING RECEIPT

Date Mailed: 08/18/2010

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Elad Barkan, Kfar-Sirkin, ISRAEL;

Power of Attorney: The patent practitioners associated with Customer Number 60956

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/IL07/00244 02/22/2007
which claims benefit of 60/775,321 02/22/2006
and claims benefit of 60/794,135 04/24/2006

Foreign Applications

If Required, Foreign Filing License Granted: 08/13/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/665,978**

Projected Publication Date: 11/25/2010

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

Title

WIRELESS INTERNET SYSTEM AND METHOD

Preliminary Class

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier

license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

PATENT APPLICATION FEE DETERMINATION RECORD

Effective October 2, 2008*

Application or Docket Number: 12/665978

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)	SMALL ENTITY TYPE ☐ RATE	SMALL ENTITY FEE	OR	OTHER THAN SMALL ENTITY RATE	OTHER THAN SMALL ENTITY FEE
U.S. NATIONAL STAGE FEES							
BASIC FEE	SMALL ENT. = $ 165	LARGE ENT. = $ 330	BASIC FEE	165	OR	BASIC FEE	
EXAMINATION FEE	Satisfies PCT Article 33(1)-(4) = $ 0 / $0	All other situations = $ 110 / $ 220	EXAM. FEE	110		EXAM. FEE	
SEARCH FEE	U.S. is ISA = $ 50 / $ 100 ALL other countries = $ 215 /$ 430	ALL other situations = $ 270/ $ 540	SEARCH FEE	50		SEARCH FEE	
FEE FOR EXTRA SPEC. PGS.	minus 100 =	/ 50 =	X $ 135 =			X $ 270 =	
TOTAL CHARGEABLE CLAIMS	20 minus 20 =	* —	X $ 26 =		OR	X $ 52 =	
INDEPENDENT CLAIMS	3 minus 3 =	* —	X $ 110 =		OR	X $ 220 =	
MULTIPLE DEPENDENT CLAIM PRESENT		☐	+ $ 195 =		OR	+ $ 390 =	
* If the difference in column 1 is less than zero, enter "0" in column 2			TOTAL	325	OR	TOTAL	

CLAIMS AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE	SMALL ENTITY ADDITIONAL FEE	OR	OTHER THAN SMALL ENTITY RATE	OTHER THAN SMALL ENTITY ADDITIONAL FEE
AMENDMENT A	Total	*	Minus	**	=	X $ 26 =		OR	X $ 52 =	
	Independent	*	Minus	***	=	X $ 110 =		OR	X $ 220 =	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐					+ $ 195 =		OR	+ $ 390 =	
						TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
AMENDMENT B	Total	*	Minus	**	=	X $ 26 =		OR	X $ 52 =	
	Independent	*	Minus	***	=	X $ 115=		OR	X $ 220 =	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐					+ $ 195 =		OR	+ $ 390 =	
						TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than '20', enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than '3', enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET

(FOR USE WITH FORM PTO-875)

SERIAL NO. 12/665978 | FILING DATE

APPLICANT(S)

CLAIMS

	AS FILED		AFTER 1ST AMENDMENT		AFTER 2ND AMENDMENT	
	IND.	DEP.	IND.	DEP.	IND.	DEP.
1	/		/			
2		/		/		
3		2		/		
4		/		/		
5		/		/		
6		/		/		
7		/		/		
8		0		/		
9		/		/		
10		0		/		
11		0		/		
12		0		/		
13	/		/			
14	/		/			
15		2		/		
16		2		—		
17		2		—		
18		2		/		
19		1		—		
20		0		—		
21		2		/		
22		2		/		
23		2		/		
24		2		/		
25	/	/		—		
26		/		—		
27	/			—		
28	/			—		
29		/		—		
30		/		—		
31		/		—		
32		/		—		
33		/		—		
34		/		—		
35		/		—		
36		/		—		
37		/		—		
38	/			—		
39		/		—		
40		/		—		
41		/		—		
42		/		—		
43						
44						
45						
46						
47						
48						
49						
50						
TOTAL IND.	7	⬇	3	⬇		⬇
TOTAL DEP.	45		17			⬅
TOTAL CLAIMS	52		20			

	AS FILED		AFTER 1ST AMENDMENT		AFTER 2ND AMENDMENT	
	IND.	DEP.	IND.	DEP.	IND.	DEP.
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						
TOTAL IND.		⬇		⬇		⬇
TOTAL DEP.		⬅		⬅		⬅
TOTAL CLAIMS						

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/665,978	12/22/2009	Elad Barkan	BRK-PU-001-US1

CONFIRMATION NO. 5873

60956
Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

PUBLICATION NOTICE

OC000000044678123

Title:WIRELESS INTERNET SYSTEM AND METHOD

Publication No.US-2010-0296441-A1
Publication Date:11/25/2010

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/665,978	12/22/2009	Elad Barkan	BRK-PU-001-US1	5873

60956 7590 08/17/2012

Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

EXAMINER	
SHARMA, GAUTAM	
ART UNIT	PAPER NUMBER
2467	

NOTIFICATION DATE	DELIVERY MODE
08/17/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

office@propats.com
vsherman@propats.com
utalmi@propats.com

Office Action Summary	Application No.	Applicant(s)	
	12/665,978	BARKAN, ELAD	
	Examiner	Art Unit	
	GAUTAM SHARMA	2467	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-15,18 and 21-24* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-15,18 and 21-24* is/are rejected.

8)☒ Claim(s) *7-12* is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *12/22/2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-15, 18, 21-24 are pending.

Claim Objections

1. **Claims 3, 8, 10-12, 15, 18 and 21-24 are objected to** because of the following informalities: Improper use of brackets for deleting claim language. Claim 3 for example recites "*according to claim 1 [or 2]*". **To delete claim language with an amendment it must be have either as strikethrough the wording or the wording should be placed in double brackets instead of single brackets**. Appropriate correction is required.

2. **For the purpose of the correspondence, the examiner assumes the single brackets encapsulating the claim language delete the claim language**. Therefore claims 3, 8, 10, 11 only depend from claim 1, Claim 12 only depends from claim 10, and claims 15, 18, 21-24 only depend from claim 13.

1. **Claim 7 objected to** because of the following informalities: Lack of antecedent basis. Claim 7 refers "the software module" however there is no recitation of "a software module" in either parent claim 1 or parent claim 6. Appropriate correction is required.

2. **Claim 8 objected to** because of the following informalities: the claim recites "allows to install and activate the software module in the other STA...". However it is not clear who is allowed to install and active the software module in the other STA. Appropriate correction is required.

3. **Claim 9 is objected to** because of the following informalities: Lack of antecedent basis. Claim 7 refers "the user" however there is no recitation of "a user" in either parent claim 1 or parent claim 6. Appropriate correction is required.

4. **Claim 9 objected to** because of the following informalities: the claim recites "*after receiving the user's per permission, the other STA. STA downloads, installs and activates...*". However it is not clear if it's the first STA or the other STA downloads, installs and activates the software. Appropriate correction is required.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. **Claims 1, 3, 4, 5 and 6 are rejected** under 35 U.S.C. 103(a) as being unpatentable over Shu et al, application No. 2005/0078624 hereinafter known as Shu and further in view of Volpano et al application No. 2004/0141617, hereinafter known as Volpano.

4. **As to claim 1,** Shu discloses *a method for providing a wireless Internet connection to WiFi-enabled devices (STAs) comprising: a. wirelessly connecting a first STA to the Internet through a first AP with a first SSID; b. remaining connected to the first Access Point (AP), the first STA creates a software-based wireless AP for wirelessly connecting other STAs to the Internet through the first STA* (Shu, Figure 1- figure 4, station (i.e. PC0) device connecting to broadband while also running software AP for connecting other station). Shu does not disclose however Volpano discloses *the first STA creates a software-based wireless AP with a second SSID* (Volpano figure 3, [0025]-[0028], creating virtual AP's with associated Identifiers SSID for the AP's).

5. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu to include the limitations of *the first STA creates a software-*

based wireless AP with a second SSID as taught by Volpano. AP's in the art commonly comprise individual identifiers (SSID) for stations to associate with an AP.

6. As **to claim 3,** Shu discloses *wherein each STA can be a laptop computer, PDA, wireless camera, wireless phone or a wireless device* (Shu, [0029], PDA, LAPTOP, Cell phone embodiment of stations (PC)).

7. **As to claim 4,** Shu and Volpano disclose *the method for providing a wireless Internet connection to STAs according to claim 1.* Shu discloses *wherein the first STA includes means for simultaneously connecting to the first AP and for opening the second AP, and means for transferring Internet packets between the first and second APs, in addition to any communications with the Internet as required by a user of that STA* (Shu, figure 1-5, Station with soft AP connected to both a broadband or wired side and a providing wireless access to other similar stations, [0032]-[0034], exemplary relay functionality of station with soft AP running). Shu does not disclose however Volpano discloses *while decrypting and encrypting the packets as needed based on the security parameters of the first and second AP* (Volpano, [0059-[0063], encryption and decryption).

8. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu to include the limitations of *while decrypting and encrypting the packets as needed based on the security parameters of the first and second AP* as taught by

Volpano. Virtual LANs are commonly in the art to enable private and secure communication through encryption/decryption processes for a particular set of user or stations.

9. **As to claim 5,** Shu discloses *wherein activating, in the first STA, a single wireless card so as to operate in two modes at the same time, a STA mode and an AP mode* (Shu, [0021]-[0022] Dual mode communication and dual mode NIC's).

10. **As to claim 6,** Shu discloses *wherein the first AP does not provide wide, unconditional access to all* (Shu, [0047]-[0048] authenticated and authorized stations are allowed conditionally access the network).

11. **Claims 2, 7-15, 18 and 21-24 are rejected** under 35 U.S.C. 103(a) as being unpatentable over Shu in view of Volpano and further in view of Urera et al, application No. 2002/0078059, hereinafter known as Urera.

12. **As to claim 2,** Shu and Volpano disclose *the method for providing a wireless Internet connections to STAs according to claim 1.* Whereas Shu and Volpano disclose *wireless* access distributed from station to station, Shu and Volpano do not disclose stations have a shared software as an access control however Urera discloses *c. a software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein* (Urera, [0008], [0025]-[0027], free internet access allocated to user with relevant software).

13. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu and Volpano to include the limitations of *c. a software module running on the first STA allows a second STA a wide access to the Internet only if the second STA has a copy of the software module running installed and active therein* as taught by Urera. Free internet access offered for a user of software can be monetized with advertisements and other incentives to generate revenue.

14. **As to claim 7,** Shu, Volpano and Urera disclose *the method for providing a wireless Internet connection to STAs according to claim 7.* Shu discloses authenticating user to allow access to network (Shu, [0047]-[0048] authenticated and authorized stations are allowed conditionally access the network). **Shu and Volpano do not disclose authentication is based on installed software module** however Urera discloses *wherein a remote database may be accessed to determine if a STA without the software module should be allowed access, and how wide that access should be* (Urera, [0007], [0025], [0026], database and account information to determine if a user has access via the free internet software).

15. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu and Volpano to include the limitations of *wherein a remote database may be accessed to determine if a STA without the software module should be allowed access, and how wide that access should be* as taught by Urera. Free internet access offered for a user of software can be monetized with advertisements and other incentives to generate revenue.

16. **As to claim 8,** Shu and Volpano disclose *the method for providing a wireless Internet connection to STAs according to claim 1,* **Shu and Volpano do not disclose providing software to the user to be download and installed to connect to network however Urera discloses** *wherein the software module, upon detecting that the other STA does not have the software module therein, allows to install and activate the software module in the other STA and then provides wide access to the other STA* (Urera, [0007]-[0009], [0028]-[0029], software enabling access to network providing for user, software invariably requiring download and installation and activation as common in the art).

17. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu and Volpano to include the limitations of *wherein the software module, upon detecting that the other STA does not have the software module therein, allows to install and activate the software module in the other STA and then provides wide access to the other STA* as taught by Urera. Software for free internet access is invariably download, installed and activated to enable benefits of the software for particular user.

18. **As to claim 9,** Shu, Volpano and Urera disclose *the method for providing a wireless Internet connection to STAs according to claim 6.* Shu discloses the station capable of providing software or virtual AP functionality (Shu, [0021]-[0023], client station or soft AP functionality in stations) **Shu and Volpano do not disclose providing software to the user to be download**

and installed to connect to network however Urera discloses *wherein the software module, upon detecting that the other STA does not have the software module therein: c1. presents to the user of the other STA a message indicating that wide Internet access is possible upon loading a copy of the software module; c2. waiting for that user's permission; c3. after receiving that user's permission, the other STA. STA downloads, installs and activates a copy of the software module to gain a wide Internet access to the other STA* (Urera, [0007]-[0009], [0028]-[0029], software enabling access to network providing for user, software invariably requiring download and installation and activation as common in the art).

19. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu and Volpano to include the limitations of *wherein the software module, upon detecting that the other STA does not have the software module therein: c1. presents to the user of the other STA a message indicating that wide Internet access is possible upon loading a copy of the software module; c2. waiting for that user's permission; c3. after receiving that user's permission, the other STA. STA downloads, installs and activates a copy of the software module to gain a wide Internet access to the other STA* as taught by Urera. Software for free internet access is invariably download, installed and activated to enable benefits of the software for particular user.

20. **As to claim 10**, the claim is rejected as applied to claim 9 above by Shu in view of Volpano and further in view of Urera.

21. **As to claim 11**, the claim is rejected as applied to claim 9 above by Shu in view of Volpano and further in view of Urera.

22. **As to claim 12,** the claim is disclosed as applied to claim 4 and 8 above by Shu in view of Volpano further in view of Urera. Urera discloses in claim 8 above limited access (no access) to free network connectivity for user who do not have software and open network connectivity when user install the software. Shu and Volpano disclose in claim 4 above as is common in the art user of VLAN that are availably set of user that are authorized to use that network.

23. **As to claim 13,** the claim is rejected as applied by in claims 1, 2, 7 and 9 by Shu in view of Volpano and further in view of Urera. Shu disclose providing access to station that share the same AP. AP's have a software or virtual AP to access and distribute AP accessibility (Figure 1-5).

24. **As to claim 14,** the claim is rejected as applied by in claims 1, 2, 7 and 9 by Shu in view of Volpano and further in view of Urera.

25. **As to claim 15,** Shu discloses *wherein each STA may include a Portable computer, a Laptop, a PDA or a wireless phone* (Shu, [0029], PDA, LAPTOP, Cell phone embodiment of stations (PC)).

26. **As to claim 18,** Shu discloses *wherein a STA connects to the Internet through two or more STAs simultaneously* (Shu, figure 5, connecting via multiple stations (PC's)).

27. **As to claim 21,** Shu discloses *wherein the first STA prevents other STAs from accessing its inner network by limiting the access rights of the other STAs* . Free internet access offered for a user of software can be monetized with advertisements and other incentives to generate revenue.

28. **As to claim 22,** Shu, Volpano and Urera disclose *the method for providing a wireless Internet connection to STAs according to claim 13,* **Shu does not disclose however Volpano** *wherein the other STA prevents the first STA from eavesdropping on its communications by tunneling its sensitive traffic to a trusted network site, and accesses the Internet through its tunnel to the trusted network site which acts as a proxy for it* (Volpano, [0022], [0051-[0055], creating VLAN for private, secure communication as common in the art, [0059-[0063], encryption and decryption).

29. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu and Volpano to include the limitations of *wherein the other STA prevents the first STA from eavesdropping on its communications by tunneling its sensitive traffic to a trusted network site, and accesses the Internet through its tunnel to the trusted network site which acts as a proxy for it* as taught by Urera. Virtual LANs are commonly in the art to enable

private and secure communication through encryption/decryption processes for a particular set of user or stations.

30. **As to claim 23**, Shu, Volpano and Urera disclose *the method for providing a wireless Internet connection to STAs according to claim 13,* **Shu and Volpano do not disclose however Urera discloses** *wherein preventing STAs from using other STAs for their primary network connection for a long period of time, by detecting that a STA is connected to the Internet through the same STA for a long period of time, and disconnecting that STA* (Urera, [0025], time limited access to the network).

31. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu and Volpano to include the limitations of *wherein preventing STAs from using other STAs for their primary network connection for a long period of time, by detecting that a STA is connected to the Internet through the same STA for a long period of time, and disconnecting that STA* as taught by Urera. Internet access time-limited to provide incentive such as fee based internet access to monetize access to the network and to remove unfair use of free access by users.

32. **As to claim 24,** the claim is rejected as applied to claim 23 above Shu in view of Volpano and further in view of Urera. Urera further discloses fee based access as desired by user and common in the art (Urera, [0034]).

Art Made of Record

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Mondragon et al, application No. 2002/0078089
- Kalavade et al, application No. 2003/0051041
- Turanyi et al, application No. 2003/0228868
- Kim et al, application No. 2004/0042596
- Lee et al, application No. 2005/0220048
- Raverdy et al, application No. 2005/0223086
- Raverdy et al, application No. 2005/0223106
- Louks et al, application No. 2006/0135206
- Karaoguz et al, application No.2007/0121839
- Anton et al, application No. 2007/0124802
- Jones et al, application No. 2007/0215684
- Waisman-Diamond et al , application No. 2007/0242657

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GAUTAM SHARMA whose telephone number is (571)270-7182. The examiner can normally be reached on Monday thru Friday, 9:30 AM - 6:00 PM..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan A. Phillips can be reached on 571-272-3940. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/G. S./

Examiner, Art Unit 2467

/HASSAN PHILLIPS/

Supervisory Patent Examiner, Art Unit 2467

Notice of References Cited	Application/Control No. 12/665,978	Applicant(s)/Patent Under Reexamination BARKAN, ELAD	
	Examiner GAUTAM SHARMA	Art Unit 2467	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2002/0078059 A1	06-2002	Urera, Marco Antonio	707/100
*	B	US-2002/0103879 A1	08-2002	Mondragon, Oscar A.	709/218
*	C	US-2003/0051041 A1	03-2003	Kalavade et al.	709/229
*	D	US-2003/0228868 A1	12-2003	Turanyi et al.	455/432.1
*	E	US-2004/0042596 A1	03-2004	Kim et al.	379/112.01
*	F	US-2004/0103278 A1	05-2004	Abhishek et al.	713/160
*	G	US-2004/0141617 A1	07-2004	Volpano, Dennis Michael	380/270
*	H	US-2005/0078624 A1	04-2005	Shu et al.	370/328
*	I	US-2005/0220048 A1	10-2005	Lee et al.	370/328
*	J	US-2005/0223086 A1	10-2005	Raverdy et al.	709/220
*	K	US-2005/0220106 A1	10-2005	Raverdy et al.	370/392
*	L	US-2006/0135206 A1	06-2006	Louks et al.	455/557
*	M	US-2007/0121839 A1	05-2007	Karaoguz et al.	379/114.1

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 12/665,978	Applicant(s)/Patent Under Reexamination BARKAN, ELAD	
	Examiner GAUTAM SHARMA	Art Unit 2467	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2007/0124802 A1	05-2007	Anton et al.	726/003
*	B	US-2007/0215684 A1	09-2007	Jones, Adrian	235/375
*	C	US-2007/0242657 A1	10-2007	Waisman-Diamond, Martin Varsavsky	370/352
*	D	US-2010/0296441 A1	11-2010	Barkan, Elad	370/328
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	Art Unit
	GAUTAM SHARMA	2467

SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Classfication Search	8/9/2012	Gautam Sharma
EAST Search	8/9/2012	Gautam Sharma
Inventor Search	8/9/2012	Gautam Sharma

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 5873

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
12/665,978	12/22/2009	370	2467	BRK-PU-001-US1

APPLICANTS
Elad Barkan, Kfar-Sirkin, ISRAEL;

**** CONTINUING DATA ***************************
This application is a 371 of PCT/IL07/00244 02/22/2007
which claims benefit of 60/775,321 02/22/2006
and claims benefit of 60/794,135 04/24/2006

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
08/13/2010

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /GAUTAM SHARMA/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		ISRAEL	22	20	3

ADDRESS
Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

TITLE
WIRELESS INTERNET SYSTEM AND METHOD

FILING FEE RECEIVED		
325	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"20100296441"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/07/24 18:42
S2	3	"8000276"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/07/24 18:42
S3	1	"8000276".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/07/24 18:42
S5	9807	370/328.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/01 17:55
S6	0	"vagabee$4" or "fon.com"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/02 13:34
S7	0	"fon.com"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/03 13:28
S8	35486	(sta or "ue" or "ms" or "at" or mobile or equipment) with (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) with (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/03 14:13
S9	1401	(sta or "ue" or "ms" or "at" or mobile or equipment) near2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) near2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/03 14:13
S10	233	(sta or "ue" or "ms" or "at" or mobile or equipment) adj2 (acting or broadcast$4 or	US-PGPUB;	OR	ON	2012/08/03 15:15

		provid$4 or initiat$4 or implement$4) adj2 (wi$1fi or internet or hotspot)	USPAT; USOCR; EPO; JPO			
S11	1	(sta or "ue" or "ms" or "at" or mobile or equipment or "pda" or "laptop") adj2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) adj2 (hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/03 18:00
S12	7	(sta or "ue" or "ms" or "at" or mobile or equipment or "pda" or "laptop") adj2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) adj2 (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/03 18:00
S13	318	((distribut$4) near3 (wi$1fi or hotspot))	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/03 18:01
S14	2	((distribut$4) near3 (wi$1fi or hotspot)) with (software)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/03 18:01
S15	4	("20030119537" | "20040003133" | "7284062" | "20040133689").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/07 15:07
S16	2040	(peer$1to$1peer or "p2p" or "peer-peer") with (wi$1fi or "wifi" or bluetooth)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/07 15:22
S17	165	(peer$1to$1peer or "p2p" or "peer-peer") with (wi$1fi or "wifi" or bluetooth) same (shared or distributed)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/07 15:49
S18	165	((peer$1to$1peer or "p2p" or "peer-peer") with (wi$1fi or "wifi" or bluetooth)) same (shared or distributed)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/07 15:54
S19	165	(wi$1fi or "wifi" or bluetooth) near1 (shared or distributed)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/07 16:34
S20	13	Barkan-elad.in.	US-PGPUB;	OR	ON	2012/08/07 18:57

			USPAT; USOCR; EPO; JPO			
S21	0	("cell phone" or "user equipment" or "ue" or "sta" or "wtru") adj2 (provid$4 or implement$4 or broadcast$4 or advertis$6) adj2 ("wi$1fi" or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/07 19:00
S22	0	("pda" or laptop) adj2 (provid$4 or implement$4 or broadcast$4 or advertis$6) adj2 ("wi$1fi" or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/07 19:00
S23	4	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near3 (provid$4 or implement$4 or broadcast$4 or advertis$6) near3 ("wi$1fi" or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/07 19:01
S24	356	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near2 (relay) with (data or traffic or internet or wi$1fi)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 12:14
S25	492	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near5(relay) near5 (data or traffic or internet or wi$1fi)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 12:38
S26	288	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near3(relay) near3 (data or traffic or internet or wi$1fi)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 12:38
S27	49	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") adj2 ("as a" or serves or serving or provid$4) adj2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 12:57
S28	11258	(distribut$4) adj2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 13:21
S29	2625	(distribut$4) adj1 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 13:21
S30	46	(distribut$4) adj1 (wi$1fi or hotspot)	US-PGPUB;	OR	ON	2012/08/08 13:21

			USPAT; USOCR; EPO; JPO			
S31	97	(distribut$4) adj2 (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 13:21
S32	11447	"fon"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 17:12
S33	114	"fon" and (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 17:12
S34	114	("fon" or "fon.com." or "www.fon.com" or foneros) and (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 17:20
S35	7	("fon.com." or "www.fon.com" or foneros)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 17:20
S36	1363	ipass	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 17:26
S37	18	ipass and (wi$1fi and hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 17:26
S38	40	ipass and (wi$1fi OR hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 17:26
S39	11	jones-adrian.in.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 18:00
S40	1	("2007/0215684").URPN.	USPAT	OR	ON	2012/08/08 18:09

S41	6	("6934530" | "20040052223" | "20060041931" | "20040052223" | "20040141617" | "6991575" | "20050204037" | "20050223086" | "20050250448" | "20050021781" | "20030051041" | "20050260972" | "20030051041" | "20050050352" | "20060223527" | "6795700" | "6957069" | "20040133687" | "20050220106" | "20050232242" | "6950628" | "20050233740" | "20050232283" | "6957086" | "20010053683" | "20070008885").PN.	USPAT	OR	ON	2012/08/08 18:10
S42	2	("20040158618" | "20040042596" | "20040158618").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 18:11
S43	24	("6934530" | "20040052223" | "20060041931" | "20040052223" | "20040141617" | "6991575" | "20050204037" | "20050223086" | "20050250448" | "20050021781" | "20030051041" | "20050260972" | "20030051041" | "20050050352" | "20060223527" | "6795700" | "6957069" | "20040133687" | "20050220106" | "20050232242" | "6950628" | "20050233740" | "20050232283" | "6957086" | "20010053683" | "20070008885").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 18:11
S44	135	(shared or sharing) adj2 (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 18:47
S45	2242	(virtual or software or "software$1defined") near2 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 18:48
S46	812	(virtual or software$1based or "software$1defined") near2 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 18:54
S47	475	(virtual or software$1based or "software$1defined") near1 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 18:55
S48	82	fon.as.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 18:56

S49	387	(virtual or software$1based or "software$1defined") adj2 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 19:25
S50	265	(virtual or software$1based or "software$1defined") adj ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 19:26
S51	265	(virtual or software$1based or "software$1defined") adj1 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 19:26
S52	3	(wi$1fi or hotspot or internet) near1 Pyramid	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 19:30
S53	0	(wi$1fi or hotspot) near1 Pyramid	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 19:31
S54	2	(wi$1fi or hotspot) with Pyramid	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/08 19:31
S55	1213	(((timer or time) or (limit$4 or based)) with (wi$1fi or wireless or internet) with free) same (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/09 16:10
S56	175	(((timer or time) or (limit$4 or based)) near5 (wi$1fi or wireless or internet) near5 free) same (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/09 16:11
S57	69	(((timer or time) or (limit$4 or based)) near5 (wi$1fi or wireless) near5 free) same (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/09 17:10
S58	1200	(wi$1fi or wireless) with free with (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/09 17:21

S59	73	(wi$1fi or wireless) near3 free near3 (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/09 17:21
S60	23	free adj2 (wi$1fi or wireless) adj3 (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/09 17:24
S61	27	free adj2 (internet) adj2(software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/09 17:25
S62	27	free adj2 (internet) adj2 (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/09 17:25
S63	115	free adj2 (wi$1fi or wireless) adj2 (access)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2012/08/09 17:26

EAST Search History (Interference)

< This search history is empty>

8/ 9/ 2012 6:22:01 PM
C:\ Users\ gsharma\ Documents\ EAST\ Workspaces\ 12665978.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	**Art Unit**
	GAUTAM SHARMA	2467

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/01/2012								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	O								
	9	✓								
	10	O								
	11	O								
	12	O								
	13	✓								
	14	✓								
	15	✓								
	16	-								
	17	-								
	18	✓								
	19	-								
	20	-								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	-								
	26	-								
	27	-								
	28	-								
	29	-								
	30	-								
	31	-								
	32	-								
	33	-								
	34	-								
	35	-								
	36	-								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	**Art Unit**
	GAUTAM SHARMA	2467

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/01/2012								
	37	-								
	38	-								
	39	-								
	40	-								
	41	-								
	42	-								

Attorney Docket No.: BRK-PU-001-US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Barkan, Elad	Examiner:	Sharma, Gautam
Serial No.:	12/665,978	Group Art Unit:	2467
Filed:	12/22/2009		
Title:	WIRELESS INTERNET SYSTEM AND METHOD		

AMENDMENT

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

This communication is filed in response to the Non-Final Office Action dated August 17, 2012 issued by the United States Patent and Trademark Office in connection with the above-identified Application. A response to the August 17, 2012 Non-Final Office Action was due November 17, 2012. Applicant is concurrently filing a petition for a 2 month extension of time. Therefore the response is due January 17, 2013. Accordingly, this communication is being timely filed.

Kindly amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 5 of this paper.

AMENDMENTS TO THE CLAIMS

Please add or amend the claims to read as follows, and cancel without prejudice or disclaimer to resubmission in a divisional or continuation application, claims indicated as cancelled:

1 – 42. (cancelled)

43. (new) A computing device comprising:

a communication module adapted to:

(1) wirelessly connect said computing device to an IP based network via a first access point (AP) having a first AP Identification (APID); and

(2) wirelessly connect said computing device to other wireless enabled computing devices;

a user interface and display adapted to allow a user of the computing device to interact with other computing devices over the IP based network; and

an AP module adapted to:

(1) provide a given device of the other wireless enabled computing devices with access to the IP based network by causing said computing device to serve the given device as a second AP having a second APID, distinct from the first APID, and provide the given device access to the network via the first AP; and

(2) tunnel data traffic from the given device, through the IP network, to a proxy server, such that the proxy server acts as a proxy of the given device and the data traffic is secure from the first computing device and first AP.

44. (new) A computing device according to claim 43, wherein the second APID is associated with the proxy server.

45. (new) A computing device according to claim 44, wherein said AP module tunnels data traffic to the proxy server in response to the given device using the second APID.

46. (new) A computing device according to claim 43, wherein said computing device is a mobile device.

47. (new) A computing device according to claim 46, wherein said computing device is a cellular phone.

48. (new) A computing device according to claim 46, wherein said computing device is a laptop computer.

49. (new) A computing device according to claim 43, wherein said computing device prevents the other wireless enabled computing devices from accessing its inner network.

50. (new) A computing device comprising:

a first communication module adapted to communicate over an IP network;

a second communication module adapted to wirelessly communicate, as an access point (AP), with other wireless enabled computing devices;

data storage adapted to store data, addressed to a destination on the IP network, received from a given device of the other wireless enabled computing devices;

transmission logic adapted to transmit the stored data to the destination, over the IP network, after communications with the given device are disconnected, such that data may be uploaded from a client device to the AP and subsequently uploaded by the AP to a destination on the internet.

51. (new) A computing device according to claim 50, wherein said computing device is a mobile device.

52. (new) A computing device according to claim 51, wherein said computing device is a cellular phone.

53. (new) A computing device according to claim 51, wherein said computing device is a laptop computer.

54. (new) A computing device according to claim 50, wherein the computing device is further adapted to send to the given device, over the IP network, a confirmation once the data is completely transmitted to the destination.

55. (new) Communication circuitry adapted to:

(1) generate a second access point identification (APID) associated with an access point (AP) having a first APID:

(2) provide a tunnel for wireless devices connecting to said AP using the second APID.

REMARKS

The present response is intended to be fully responsive to all points of objection and/or rejection raised by the Examiner and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application is respectfully requested.

Status of Claims

Claims 1-15, 18 and 21-24 are pending in the application. Claims 1-15, 18 and 21-24 have been rejected and Claims 7-12 have been objected to.

Claims 1-15, 18 and 21-24 have been voluntarily cancelled herein by the Applicant, without prejudice or disclaimer. New claims 43-55 have been added herein by the Applicant.

Applicant respectfully submits that the current amendments do not add any new subject matter.

CLAIM OBJECTIONS

In the Office Action, the Examiner objected to claims 3, 8, 10-12, 15, 18 and 21-24 due to alleged informalities. Applicant respectfully traverses these objections, however, as the Applicant has cancelled the objected to claims herein, Applicant respectfully asserts that these objections are now moot.

CLAIM REJECTIONS

35 U.S.C. § 103 Rejections

In the Office Action, the Examiner rejected:

(1) Claims 1 and 3-6 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Shu et al, U.S. Patent Application No. 2005/0078624 (hereinafter: "**Shu**") in view of Volpano et al U.S. Patent Application No. 2004/0141617 (hereinafter: "**Volpano**"); and

(2) Claims 2, 7-15, 18 and 21-24 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Shu in view of Volpano and further in view of Urera et al, U.S. Patent Application No. 2002/0078059 (hereinafter: "**Urera**").

Applicant respectfully traverses these rejections, however, in the interest of expediting the prosecution of the present application, Applicant has voluntarily cancelled Claims 1-15, 18 and 21-24 and added new claims 43-55. Applicant respectfully asserts that the new claims, 43-55, are directed to novel subject matter for which Applicant is seeking patent protection neither present nor suggested in the currently cited prior art and accordingly, clearly recite limitations neither taught nor suggested by the cited prior art.

Namely, Applicant respectfully asserts that the limitations recited in the pending claims of:

(1) "*an AP module adapted to:*

(1) *provide a given device of the other wireless enabled computing devices with access to the IP based network by causing said computing device to serve the given device as a second AP having a second APID, distinct from the first APID, and provide the given device access to the network via the first AP; and*

(2) *tunnel data traffic from the given device, through the IP network, to a proxy server, such that the proxy server acts as a proxy of the given device and the data traffic is secure from the first computing device and first AP.*"

– As recited in pending independent claim 43;

(2) "*data storage adapted to store data addressed to a destination on the IP network received from a given device of the other wireless enabled computing devices;*

transmission logic adapted to transmit the stored data to the destination, over the IP network, after communications with the given device are disconnected, such that data may be uploaded from a client device to the AP and subsequently uploaded by the AP to a destination on the internet"

– As recited in pending independent claim 50; and

(3) "*provide a tunnel for wireless devices connecting to said AP using the second APID.*"

– As recited in pending independent claim 55;

are neither taught nor suggested by any of the cited references.

Applicant respectfully asserts that new claims 43-55 are directed to novel structures and features described in the pending application which are not present in the currently cited prior art, nor any other prior art known to the Applicant. Accordingly, Applicant respectfully requests allowance thereof.

CONCLUSION

In view of the foregoing amendments and remarks, all pending claims are considered to be allowable. Their favorable reconsideration and allowance is respectfully requested.

Should the Examiner have any question or comment as to the form, content or entry of this Amendment, the Examiner is requested to contact the undersigned at the telephone number below. Similarly, if there are any further issues yet to be resolved to advance the prosecution of this application to issue, the Examiner is requested to telephone the undersigned counsel.

Respectfully submitted,

/Vladimir Sherman/

Vladimir Sherman
Attorney for Applicant(s)
Registration No. 43,116

Dated: **January 17, 2013**

Professional Patent Solutions
P.O.Box 654
Herzeliya Pituach, 46105
ISRAEL

Tel: *+972 9 9541971*
Fax: *+972 9 9541975*
E-mail: office@propats.com

Electronic Patent Application Fee Transmittal

Application Number:	12665978
Filing Date:	22-Dec-2009
Title of Invention:	WIRELESS INTERNET SYSTEM AND METHOD
First Named Inventor/Applicant Name:	Elad Barkan
Filer:	Vladimir Sherman/Dina Cohen
Attorney Docket Number:	BRK-PU-001-US1

Filed as Small Entity

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with $0 paid	2252	1	285	285

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**285**

Electronic Acknowledgement Receipt

EFS ID:	14724991
Application Number:	12665978
International Application Number:	
Confirmation Number:	5873
Title of Invention:	WIRELESS INTERNET SYSTEM AND METHOD
First Named Inventor/Applicant Name:	Elad Barkan
Customer Number:	60956
Filer:	Vladimir Sherman/Dina Cohen
Filer Authorized By:	Vladimir Sherman
Attorney Docket Number:	BRK-PU-001-US1
Receipt Date:	17-JAN-2013
Filing Date:	22-DEC-2009
Time Stamp:	13:38:04
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$285
RAM confirmation Number	13177
Deposit Account	505880
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Amendment/Req. Reconsideration-After Non-Final Reject	BRK-PU-001-US1-RNFOA17AUG2012-Filed.pdf	140724 e7e1534a9813759ca4a7bbaf96009af67f3c6ee3	no	8
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30506 77f33cc67e96a6d899cec9ada76c3a805a9d86e8	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	171230		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
12/665,978	12/22/2009	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
			TOTAL			TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

AMENDMENT 01/17/2013	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 13	Minus	** 20	= 0	X $31 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $125 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/DELEACHES YOUNG/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/665,978	12/22/2009	Elad Barkan	BRK-PU-001-US1	5873

60956 7590 03/13/2013

Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

EXAMINER	
SHARMA, GAUTAM	
ART UNIT	PAPER NUMBER
2467	

NOTIFICATION DATE	DELIVERY MODE
03/13/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

office@propats.com
vsherman@propats.com
utalmi@propats.com

Office Action Summary	Application No.	Applicant(s)	
	12/665,978	BARKAN, ELAD	
	Examiner	Art Unit	
	GAUTAM SHARMA	2467	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2013*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *43-55* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *43-55* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Claims 43-55 are pending.

Claim Rejections - 35 USC § 112

1. Claim limitations "communication module" and "AP module" has been interpreted under 35 U.S.C. 112(f) or 35 U.S.C. 112 (pre-AIA), sixth paragraph, because it uses a non-structural term " module" coupled with functional language "adapted to" without reciting sufficient structure to achieve the function. Furthermore, the non-structural term is not preceded by a structural modifier.

Since this claim limitation invokes 35 U.S.C. 112(f) or 35 U.S.C. 112 (pre-AIA), sixth paragraph, claims 43,45 and 50 interpreted to cover the corresponding structure described in the specification that achieves the claimed function, and equivalents thereof.

A review of the specification shows that the following appears to be the corresponding structure described in the specification for the 35 U.S.C. 112(f) or 35 U.S.C. 112 (pre-AIA), sixth paragraph limitation: Software module in a STA or software module in laptop (specifications, [0235] , [0236] and abstract)

If applicant wishes to provide further explanation or dispute the examiner's interpretation of the corresponding structure, applicant must identify the corresponding structure with reference

to the specification by page and line number, and to the drawing, if any, by reference characters in response to this Office action.

If applicant does **not** wish to have the claim limitation treated under 35 U.S.C. 112(f) or 35 U.S.C. 112 (pre-AIA), sixth paragraph, applicant may amend the claim so that it will clearly not invoke 35 U.S.C. 112(f) or 35 U.S.C. 112 (pre-AIA), sixth paragraph, or present a sufficient showing that the claim recites sufficient structure, material, or acts for performing the claimed function to preclude application of 35 U.S.C. 112(f) or 35 U.S.C. 112 (pre-AIA), sixth paragraph.

For more information, see MPEP § 2173 et seq. and *Supplementary Examination Guidelines for Determining Compliance with 35 U.S.C. § 112 and for Treatment of Related Issues in Patent Applications*, 76 FR 7162, 7167 (Feb. 9, 2011).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. **Claim 43-55 are rejected** under 35 U.S.C. 103(a) as being unpatentable over Shu et al, application No. 2005/0078624 hereinafter known as Shu and further in view of Volpano et al application No. 2004/0141617, hereinafter known as Volpano and further in view of Meier et al, Patent No.6,950,628, hereinafter known as Meier.

1. **As to claim 43,** Shu discloses a *computing device comprising: a communication module adapted to: (1) wirelessly connect said computing device to an IP based network via a first access point (AP) having a first AP Identification (APID); and (2) wirelessly connect said computing device to other wireless enabled computing devices;* (Shu, Figure 1- figure 4, station (i.e. PC0) device connecting to broadband while also running software AP for connecting other stations). *a user interface and display adapted to allow a user of the computing device to interact with other computing devices over the IP based network* (Shu, [0029], PDA, LAPTOP, Cell phone embodiment of stations (PC), The devices commonly comprise display in the art with software access to connect to networks or other devices)*;* Shu discloses *and an AP module adapted to: (1) provide a given device of the other wireless enabled computing devices with access to the IP based network by causing said computing device to serve the given device as a second AP, distinct from the first APID, and provide the given device access to the network via the first AP*(Shu, Figure 1- figure 4, station (i.e. PC0) device connecting to broadband while also running software AP for connecting other stations)*;* **Shu does not expressly disclos**e the *a*

second AP having a second APID however Volpano disclose a *second AP having a second APID* (Volpano figure 3, [0025]-[0028], creating virtual AP's with associated Identifiers SSID for the AP's).

2. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu to include the limitations of *second AP having a second APID* as taught by Volpano. AP's in the art commonly comprise individual identifiers (SSID) for stations to associate with an AP.

3. **Further as to claim 43,** Shu does not disclose however Volpano discloses *and (2) tunnel data traffic from the given device, through the IP network and the data traffic is secure from the first computing device and first AP* (Volpano, [0022], [0051-[0055], creating VLAN for private, secure communication as common in the art, [0059-[0063], encryption and decryption).

4. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu to include the limitations of *and (2) tunnel data traffic from the given device, through the IP network, to a proxy server, such that the proxy server acts as a proxy of the given device and the data traffic is secure from the first computing device and first AP* as taught by Volpano. Virtual LANs are commonly in the art to enable private and secure communication through encryption/decryption processes for a particular set of user or stations.

5. **Also as to claim 43**, Shu and Volpano does not expressly disclose a proxy server for a given device however Meier disclose *a proxy server, such that the proxy server acts as a proxy of the given device* (Meier, Figure 1-5, setting tunnel traffic with proxy server and associated SSID).

6. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu and Volpano to include the limitations of *a proxy server, such that the proxy server acts as a proxy of the given device* as taught by Meier. Proxy server for VLAN traffic is commonly employed in the art for secure routing.

7. **As to claim 44,** Shu and Volpano disclose *computing device according to claim 43,* Shu and Volpano do not expressly disclose however Meier discloses *wherein the second APID is associated with the proxy server* (Meier, Figure 1-5, setting tunnel traffic with proxy server and associated SSID).

8. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu and Volpano to include the limitations of *wherein the second APID is associated with the proxy server* as taught by Meier. Proxy server for VLAN traffic is commonly employed in the art for secure routing.

4. **As to claim 45,** Shu and Volpano disclose *a computing device according to claim 44,* Shu and Volpano do not expressly disclose however Meier discloses *wherein said AP module*

tunnels data traffic to the proxy server in response to the given device using the second APID (Meier, Figure 1-5, setting tunnel traffic with proxy server and associated SSID).

5. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shu and Volpano to include the limitations of *wherein said AP module tunnels data traffic to the proxy server in response to the given device using the second APID* as taught by Meier. Proxy server for VLAN traffic is commonly employed in the art for secure routing.

6. **As to claim 46,** Shu discloses *computing device according to claim 43, wherein said computing device is a mobile device* (Shu, [0029], PDA, LAPTOP, Cell phone embodiment of stations (PC)).

7. **As to claim 47,** Shu discloses *a computing device according to claim 46, wherein said computing device is a cellular phone* (Shu, [0029], PDA, LAPTOP, Cell phone embodiment of stations (PC)).

8. **As to claim 48,** Shu discloses *a computing device according to claim 46, wherein said computing device is a laptop computer* (Shu, [0029], PDA, LAPTOP, Cell phone embodiment of stations (PC)).

9. **As to claim 49,** Shu discloses *wherein said computing device prevents the other wireless enabled computing devices from accessing its inner network.* (Shu, [0047]-[0048] authenticated and authorized stations are allowed conditionally access the network).

10. **As to claim 50,** the claim is rejected as applied to claim 43 above by Shu in view of Volpano and further in view of Meier.

11. **As to claim 51,** the claim is rejected as applied to claim 46 above by Shu in view of Volpano and further in view of Meier.

12. **As to claim 52,** the claim is rejected as applied to claim 47 above by Shu in view of Volpano and further in view of Meier.

13. **As to claim 53,** the claim is rejected as applied to claim 48 above by Shu in view of Volpano and further in view of Meier.

14. **As to claim 54,** *wherein the computing device is further adapted to send to the given device, over the IP network, a confirmation once the data is completely transmitted to the destination* (Use of Acknowledge messages such as ACK or NACK are common in the art to either acknowledge or not acknowledge respectively the transmission of data).

15. **As to claim 55,** the claim is rejected as applied to claim 43 above by Shu in view of Volpano and further in view of Meier.

Response to Arguments

1. Applicant's arguments with respect to claim 48-55 have been considered but are moot because the arguments do not apply to any of the references being used in the current rejection.

Conclusion

16. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GAUTAM SHARMA whose telephone number is (571)270-7182. The examiner can normally be reached on Monday thru Friday, 9:30 AM - 6:00 PM..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan A. Phillips can be reached on 571-272-3940. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/G. S./

Examiner, Art Unit 2467

/HASSAN PHILLIPS/

Supervisory Patent Examiner, Art Unit 2467

Notice of References Cited	Application/Control No. 12/665,978	Applicant(s)/Patent Under Reexamination BARKAN, ELAD	
	Examiner GAUTAM SHARMA	Art Unit 2467	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,950,628 B1	09-2005	Meier et al.	455/41.2
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	Art Unit
	GAUTAM SHARMA	2467

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Classfication Search(370/310,328)	8/9/2012	Gautam Sharma
EAST Search	8/9/2012	Gautam Sharma
Inventor Search	8/9/2012	Gautam Sharma
Classfication Search(370/310,328)	2/26/2013	Gautam Sharma
EAST Search	2/26/2013	Gautam Sharma
Inventor Search	2/26/2013	Gautam Sharma

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	**Art Unit**
	GAUTAM SHARMA	2467

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/01/2012	02/26/2013							
	1	✓	-							
	2	✓	-							
	3	✓	-							
	4	✓	-							
	5	✓	-							
	6	✓	-							
	7	✓	-							
	8	O	-							
	9	✓	-							
	10	O	-							
	11	O	-							
	12	O	-							
	13	✓	-							
	14	✓	-							
	15	✓	-							
	16	-	-							
	17	-	-							
	18	✓	-							
	19	-	-							
	20	-	-							
	21	✓	-							
	22	✓	-							
	23	✓	-							
	24	✓	-							
	25	-	-							
	26	-	-							
	27	-	-							
	28	-	-							
	29	-	-							
	30	-	-							
	31	-	-							
	32	-	-							
	33	-	-							
	34	-	-							
	35	-	-							
	36	-	-							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	**Art Unit**
	GAUTAM SHARMA	2467

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/01/2012	02/26/2013							
	37	-	-							
	38	-	-							
	39	-	-							
	40	-	-							
	41	-	-							
	42	-	-							
	43		✓							
	44		✓							
	45		✓							
	46		✓							
	47		✓							
	48		✓							
	49		✓							
	50		✓							
	51		✓							
	52		✓							
	53		✓							
	54		✓							
	55		✓							

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	26	(US-20100296441-$ or US-20030228868-$ or US-20060135206-$ or US-20070124802-$ or US-20080101290-$ or US-20050223086-$ or US-20070121839-$ or US-20070140163-$ or US-20070180136-$ or US-20070183383-$ or US-20050220106-$ or US-20070242657-$ or US-20060236378-$ or US-20070124490-$ or US-20070215684-$ or US-20070054654-$ or US-20040042596-$ or US-20030051041-$ or US-20040141617-$ or US-20040103278-$ or US-20050078624-$ or US-20050220048-$ or US-20030171989-$ or US-20020078059-$ or US-20020103879-$ or US-20050147084-$).did.	US-PGPUB	OR	ON	2013/02/26 17:12
L3	9	l2 and proxy	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:12
L4	7	l2 and proxy and (vlan or "virtual" or tunnel)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:37
L5	2	l2 and (proxy same (vlan or "virtual" or tunnel))	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:39
L6	9916	(proxy same (vlan or "virtual" or tunnel))	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:40
L7	5903	(proxy with (vlan or "virtual" or tunnel))	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:40
L8	11	(proxy with (vlan or tunnel)) with (apid or ssid)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:40

L9	24	("6934530" | "20040052223" | "20060041931" | "20040052223" | "20040141617" | "6991575" | "20050204037" | "20050223086" | "20050250448" | "20050021781" | "20030051041" | "20050260972" | "20030051041" | "20050050352" | "20060223527" | "6795700" | "6957069" | "20040133687" | "20050220106" | "20050232242" | "6950628" | "20050233740" | "20050232283" | "6957086" | "20010053683" | "20070008885").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:43
L10	1	l8 and l9	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:43
L11	27	(US-20100296441-$ or US-20030228868-$ or US-20060135206-$ or US-20070124802-$ or US-20080101290-$ or US-20050223086-$ or US-20070121839-$ or US-20070140163-$ or US-20070180136-$ or US-20070183383-$ or US-20050220106-$ or US-20070242657-$ or US-20060236378-$ or US-20070124490-$ or US-20070215684-$ or US-20070054654-$ or US-20040042596-$ or US-20030051041-$ or US-20040141617-$ or US-20040103278-$ or US-20050078624-$ or US-20050220048-$ or US-20030171989-$ or US-20020078059-$ or US-20020103879-$ or US-20050147084-$).did. or (US-6950628-$).did.	US-PGPUB; USPAT	OR	ON	2013/02/26 17:58
L12	14	l11 and ("user interface" or "ui" or "display")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:58
L13	6	l11 and (acknowledge or "ack/nack" or "ack" or "nack" or "nak")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:59
S1	1	"20100296441"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S2	5	"8000276"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S3	1	"8000276".pn.	US-PGPUB; USPAT; USOCR; EPO;	OR	ON	2013/02/22 17:10

			JPO			
S4	11293	370/328.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S5	0	"vagabee$4" or "fon.com"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S6	0	"fon.com"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S7	39532	(sta or "ue" or "ms" or "at" or mobile or equipment) with (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) with (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S8	1526	(sta or "ue" or "ms" or "at" or mobile or equipment) near2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) near2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S9	253	(sta or "ue" or "ms" or "at" or mobile or equipment) adj2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) adj2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S10	1	(sta or "ue" or "ms" or "at" or mobile or equipment or "pda" or "laptop") adj2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) adj2 (hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S11	8	(sta or "ue" or "ms" or "at" or mobile or equipment or "pda" or "laptop") adj2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) adj2 (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S12	393	((distribut$4) near3 (wi$1fi or hotspot))	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S13	2	((distribut$4) near3 (wi$1fi or hotspot)) with (software)	US-PGPUB; USPAT; USOCR; EPO;	OR	ON	2013/02/22 17:10

			JPO			
S14	4	("20030119537" | "20040003133" | "7284062" | "20040133689").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S15	2393	(peer$1to$1peer or "p2p" or "peer-peer") with (wi$1fi or "wifi" or bluetooth)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S16	191	(peer$1to$1peer or "p2p" or "peer-peer") with (wi$1fi or "wifi" or bluetooth) same (shared or distributed)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S17	191	((peer$1to$1peer or "p2p" or "peer-peer") with (wi$1fi or "wifi" or bluetooth)) same (shared or distributed)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S18	179	(wi$1fi or "wifi" or bluetooth) near1 (shared or distributed)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S19	15	Barkan-elad.in.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S20	0	("cell phone" or "user equipment" or "ue" or "sta" or "wtru") adj2 (provid$4 or implement$4 or broadcast$4 or advertis$6) adj2 ("wi$1fi" or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S21	0	("pda" or laptop) adj2 (provid$4 or implement$4 or broadcast$4 or advertis$6) adj2 ("wi$1fi" or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S22	5	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near3 (provid$4 or implement$4 or broadcast$4 or advertis$6) near3 ("wi$1fi" or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S23	441	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near2 (relay) with (data or traffic or internet or wi$1fi)	US-PGPUB; USPAT; USOCR; EPO;	OR	ON	2013/02/22 17:10

			JPO			
S24	594	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near5(relay) near5 (data or traffic or internet or wi$1fi)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S25	354	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near3(relay) near3 (data or traffic or internet or wi$1fi)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S26	55	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") adj2 ("as a" or serves or serving or provid$4) adj2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S27	11957	(distribut$4) adj2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S28	2775	(distribut$4) adj1 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S29	53	(distribut$4) adj1 (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S30	120	(distribut$4) adj2 (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S31	11505	"fon"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S32	122	"fon" and (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S33	122	("fon" or "fon.com." or "www.fon.com" or foneros) and (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO;	OR	ON	2013/02/22 17:10

			JPO			
S34	9	("fon.com." or "www.fon.com" or foneros)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S35	1379	ipass	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S36	20	ipass and (wi$1fi and hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S37	50	ipass and (wi$1fi OR hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S38	11	jones-adrian.in.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S39	1	("2007/0215684").URPN.	USPAT	OR	ON	2013/02/22 17:10
S40	6	("6934530" | "20040052223" | "20060041931" | "20040052223" | "20040141617" | "6991575" | "20050204037" | "20050223086" | "20050250448" | "20050021781" | "20030051041" | "20050260972" | "20030051041" | "20050050352" | "20060223527" | "6795700" | "6957069" | "20040133687" | "20050220106" | "20050232242" | "6950628" | "20050233740" | "20050232283" | "6957086" | "20010053683" | "20070008885").PN.	USPAT	OR	ON	2013/02/22 17:10
S41	2	("20040158618" | "20040042596" | "20040158618").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S42	24	("6934530" | "20040052223" | "20060041931" | "20040052223" | "20040141617" | "6991575" | "20050204037" | "20050223086" | "20050250448" | "20050021781" | "20030051041" | "20050260972" | "20030051041" | "20050050352" | "20060223527" | "6795700" | "6957069" | "20040133687" | "20050220106" |	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10

		"20050232242" | "6950628" | "20050233740" | "20050232283" | "6957086" | "20010053683" | "20070008885").PN.				
S43	159	(shared or sharing) adj2 (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S44	2455	(virtual or software or "software$1defined") near2 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S45	896	(virtual or software$1based or "software$1defined") near2 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S46	527	(virtual or software$1based or "software$1defined") near1 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S47	85	fon.as.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S48	434	(virtual or software$1based or "software$1defined") adj2 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S49	300	(virtual or software$1based or "software$1defined") adj ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S50	300	(virtual or software$1based or "software$1defined") adj1 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S51	3	(wi$1fi or hotspot or internet) near1 Pyramid	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S52	0	(wi$1fi or hotspot) near1 Pyramid	US-PGPUB;	OR	ON	2013/02/22 17:10

			USPAT; USOCR; EPO; JPO			
S53	3	(wi$1fi or hotspot) with Pyramid	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S54	1315	(((timer or time) or (limit$4 or based)) with (wi$1fi or wireless or internet) with free) same (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S55	188	(((timer or time) or (limit$4 or based)) near5 (wi$1fi or wireless or internet) near5 free) same (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S56	74	(((timer or time) or (limit$4 or based)) near5 (wi$1fi or wireless) near5 free) same (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S57	1314	(wi$1fi or wireless) with free with (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S58	75	(wi$1fi or wireless) near3 free near3 (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S59	24	free adj2 (wi$1fi or wireless) adj3 (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S60	28	free adj2 (internet) adj2(software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S61	28	free adj2 (internet) adj2 (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S62	131	free adj2 (wi$1fi or wireless) adj2 (access)	US-PGPUB;	OR	ON	2013/02/22 17:10

			USPAT; USOCR; EPO; JPO			
S63	3133	370/310.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10

EAST Search History (Interference)

< This search history is empty>

2/ 26/ 2013 6:13:16 PM
C:\ Users\ gsharma\ Documents\ EAST\ Workspaces\ 12665978_update_2013_feb_22.wsp

Doc Code: M865 or FAI.REQ.INTV

PTOL-413A (08-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 12/665,978 First Named Applicant: Elad Barkan
Examiner: Sharma, Guatam Art Unit: 2467 Status of Application: Final Rejection Mailed

Tentative Participants:
(1) Vladimir Sherman (Attorney for Applicant) **(2)** Uri Segal, adv (Associate)

(3)_____ **(4)**_____

Proposed Date of Interview: May 28-30, June 3-6 **Proposed Time:** 8 - 11 A.M. **(AM/PM)**

Type of Interview Requested:
(1) [✓] Telephonic (2) [ ] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [✓] NO
If yes, provide brief description:_____

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) Rej.	43 & 50		[ ]	[ ]	[ ]
(2)			[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached [ ] Proposed Amendment or Arguments Attached

Brief Description of Arguments to be Presented: Applicant would like to discuss the current rejections of the pending claims.

An interview was conducted on the above-identified application on _____

NOTE: This form should be completed and filed by applicant in advance of the interview (see MPEP § 713.01). If this form is signed by a registered practitioner not of record, the Office will accept this as an indication that he or she is authorized to conduct an interview on behalf of the principal (37 CFR 1.32(a)(3)) pursuant to 37 CFR 1.34. This is not a power of attorney to any above named practitioner. See the Instruction Sheet for this form, which is incorporated by reference. By signing this form, applicant or practitioner is certifying that he or she has read the Instruction Sheet. After the interview is conducted, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible. This application will not be delayed from issue because of applicant's failure to submit a written record of this interview.

/Vladimir Sherman/
Applicant/Applicant's Representative Signature

Examiner/SPE Signature

Vladimir Sherman
Typed/Printed Name of Applicant or Representative

43,116
Registration Number, if applicable

Electronic Acknowledgement Receipt

EFS ID:	15873467
Application Number:	12665978
International Application Number:	
Confirmation Number:	5873
Title of Invention:	WIRELESS INTERNET SYSTEM AND METHOD
First Named Inventor/Applicant Name:	Elad Barkan
Customer Number:	60956
Filer:	Vladimir Sherman/uri segal
Filer Authorized By:	Vladimir Sherman
Attorney Docket Number:	BRK-PU-001-US1
Receipt Date:	27-MAY-2013
Filing Date:	22-DEC-2009
Time Stamp:	10:49:11
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Letter Requesting Interview with Examiner	BRK-PU-001-US1-interviewrequestmay27.pdf	175051 b49723415bbd000a55560ef49fac17d7880f ebeb	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	175051

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/665,978	12/22/2009	Elad Barkan	BRK-PU-001-US1	5873

60956 7590 06/04/2013

Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

EXAMINER	
SHARMA, GAUTAM	
ART UNIT	PAPER NUMBER
2467	

NOTIFICATION DATE	DELIVERY MODE
06/04/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

office@propats.com
vsherman@propats.com
utalmi@propats.com

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	12/665,978	BARKAN, ELAD	
	Examiner	Art Unit	
	GAUTAM SHARMA	2467	

All participants (applicant, applicant's representative, PTO personnel):

(1) *GAUTAM SHARMA*.

(2) *Hassan Phillips*.

(3) *Uri Segal*.

(4) *Vladimir Sherman*.

Date of Interview: *30 May 2013*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *43 and 50*.

Identification of prior art discussed: *Yes*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiner and Applicants representative discussed the novel of aspects of the instant application, the claimed invention and the relevance of prior art used to reject the claims. Applicant asserted the claim 43 was not disclosed by the combined prior art and that the combination of prior art itself was not appropriate. Examiner asserted the combination of prior does read on claim 43 and is proper combination. No agreement was reached on claim 43. Applicant further asserted rejection of claim 50 is inappropriate in that claim 50 is an entirely different embodiment and that the same art and rejection of claim 43 cannot be applied to claim 50. Examiner asserted several of the limitations of claim 50 are similar to 43 and that the prior does apply partially while conceding the rejection of claim 50 is lacking in "storage of data from a given device at the computing for subsequent transmission even after disconnecting". No resolution was reached for claim 50. Applicant will provide amended claims for examiners consideration. Examiner will provide feedback to further prosecution of the application upon consideration of the amendments and updated search.
.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/G. S./ Examiner, Art Unit 2467	/HASSAN PHILLIPS/ Supervisory Patent Examiner, Art Unit 2467

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

60956 7590 06/19/2013

Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

EXAMINER
SHARMA, GAUTAM

ART UNIT	PAPER NUMBER
2467	

DATE MAILED: 06/19/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/665,978	12/22/2009	Elad Barkan	BRK-PU-001-US1	5873

TITLE OF INVENTION: WIRELESS INTERNET SYSTEM AND METHOD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	09/19/2013

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

60956 7590 06/19/2013
Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/665,978	12/22/2009	Elad Barkan	BRK-PU-001-US1	5873

TITLE OF INVENTION: WIRELESS INTERNET SYSTEM AND METHOD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	09/19/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHARMA, GAUTAM	2467	370-328000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/665,978	12/22/2009	Elad Barkan	BRK-PU-001-US1	5873

60956 7590 06/19/2013

Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

EXAMINER	
SHARMA, GAUTAM	
ART UNIT	PAPER NUMBER
2467	

DATE MAILED: 06/19/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 481 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 481 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 12/665,978	Applicant(s) BARKAN, ELAD	
	Examiner GAUTAM SHARMA	Art Unit 2467	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *01/17/2013*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *43-55*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☒ All b) ☐ Some *c) ☐ None of the:
   1. ☒ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

   Interim copies:

   a) ☐ All b) ☐ Some c) ☐ None of the: Interim copies of the priority documents have been received.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☒ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/G. S./ Examiner, Art Unit 2467	/HASSAN PHILLIPS/ Supervisory Patent Examiner, Art Unit 2467

Allowability Notice

Claims 43-55 are allowed.

EXAMINER'S AMENDMENT

1) An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Uri Segal on 06/06/2013.The application has been amended as follows:

1. In the claims:

In Claim 43,

"*43. A computing device comprising:*

a communication module adapted to:

(1) wirelessly connect said computing device to an IP based network via a first access point (AP) having a first AP Identification (APID); and

(2) wirelessly connect said computing device to other wireless enabled computing devices;

a user interface and display adapted to allow a user of the computing device to interact with other computing devices over the IP based network; and

an AP module adapted to:

(1) provide a given device of the other wireless enabled computing devices with access to the IP based network by causing said computing device to serve the given device as a second AP having a second APID, distinct from the first APID, and provide the given device access to the network via the first AP; and

(2) tunnel data traffic from the given device, through the IP network, to a proxy server, such that the proxy server acts as a proxy of the given device and the data traffic is secure from the first computing device and first AP."

Has been changed to

43. --- A computing device comprising:

a communication module adapted to:

(1) wirelessly connect said computing device to an IP based network via a first wireless access point (AP) having a first AP Identification (APID); and

(2) wirelessly communicate with other wireless enabled computing devices ;

a user interface and display adapted to allow a user of said computing device to interact with destinations over the IP based network, through the first wireless AP, using a first public IP address ; and

an AP module adapted to:

(1) provide a given device of the other wireless enabled computing devices with access to the IP based network by causing said computing device to serve the given device as a second AP having a second APID, distinct from the first APID, and provide the given device access to the network via the first AP; and

(2) *tunnel data traffic from the given device, through said computing device, through the first AP, through the IP network, to a proxy server, such that the proxy server acts as a proxy of the given device and the data traffic is secure from said computing device and first AP and the given device operates on the network with a public IP address distinct from the first public IP address.---*

In Claim 50,

"*50. A computing device comprising:*

a first communication module adapted to communicate over an IP network;

a second communication module adapted to wirelessly communicate, as an access point (AP), with other wireless enabled computing devices;

data storage adapted to store data, addressed to a destination on the IP network, received from a given device of the other wireless enabled computing devices;

transmission logic adapted to transmit the stored data to the destination, over the IP network, after communications with the given device are disconnected, such that data may be uploaded from a client device to the AP and subsequently uploaded by the AP to a destination on the internet."

Has been changed to

--- *A computing device comprising:*

a first communication module adapted to communicate over an IP network, using a first public IP address, via a first wireless access point (AP), the first wireless AP having a first AP Identification (APID);

a second communication module adapted to wirelessly communicate, as a second access point (AP) having a second APID, with other wireless enabled computing devices and provide the other wireless enabled computing devices access to the IP network via the first wireless AP, wherein data traffic from the other wireless enabled computing devices is tunneled by the second AP through the first AP to a proxy server such that the proxy server acts as a proxy of the other wireless enabled computing devices and the data traffic is secure from the first and second APs and the other wireless enabled computing devices operate on the IP network with a public IP address distinct from the first public IP address;

data storage adapted to store data, addressed to a destination on the IP network, received wirelessly via said second communication module, from a given device of the other wireless enabled computing devices;

transmission logic adapted to transmit the stored data to the destination, over the IP network, after communications between said computing device and the given device are disconnected, such that data may be uploaded from a client device to said computing device and subsequently uploaded by said computing device to a destination on the internet.---

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GAUTAM SHARMA whose telephone number is (571)270-7182. The examiner can normally be reached on Monday thru Friday, 9:30 AM - 6:00 PM..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan A. Phillips can be reached on 571-272-3940. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/G. S./

Examiner, Art Unit 2467

/HASSAN PHILLIPS/

Supervisory Patent Examiner, Art Unit 2467

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	**Art Unit**
	GAUTAM SHARMA	2467

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/01/2012	02/26/2013	06/06/2013						
	1	✓	-							
	2	✓	-							
	3	✓	-							
	4	✓	-							
	5	✓	-							
	6	✓	-							
	7	✓	-							
	8	O	-							
	9	✓	-							
	10	O	-							
	11	O	-							
	12	O	-							
	13	✓	-							
	14	✓	-							
	15	✓	-							
	16	-	-							
	17	-	-							
	18	✓	-							
	19	-	-							
	20	-	-							
	21	✓	-							
	22	✓	-							
	23	✓	-							
	24	✓	-							
	25	-	-							
	26	-	-							
	27	-	-							
	28	-	-							
	29	-	-							
	30	-	-							
	31	-	-							
	32	-	-							
	33	-	-							
	34	-	-							
	35	-	-							
	36	-	-							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	**Art Unit**
	GAUTAM SHARMA	2467

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/01/2012	02/26/2013	06/06/2013						
	37	-	-							
	38	-	-							
	39	-	-							
	40	-	-							
	41	-	-							
	42	-	-							
	43		✓	=						
	44		✓	=						
	45		✓	=						
	46		✓	=						
	47		✓	=						
	48		✓	=						
	49		✓	=						
	50		✓	=						
	51		✓	=						
	52		✓	=						
	53		✓	=						
	54		✓	=						
	55		✓	=						

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	**Art Unit**
	GAUTAM SHARMA	2467

CPC					
Symbol				**Type**	**Version**
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		
			/		

CPC Combination Sets							
Symbol				**Type**	**Set**	**Ranking**	**Version**
			/				
			/				

US ORIGINAL CLASSIFICATION					
CLASS			**SUBCLASS**		
370			328		
CROSS REFERENCE(S)					
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**				
370	351	389	392	395.1	395.2
370	395.4	396	397	398	399

INTERNATIONAL CLASSIFICATION					
CLAIMED					**NON-CLAIMED**
H	0	4	W	80 / 04 (2009.0)	
H	0	4	W	88 / 06 (2009.0)	
H	0	4	W	88 / 08 (2009.0)	
H	0	4	W	84 / 18 (2009.0)	
H	0	4	L	29 / 06 (2006.0)	

/GAUTAM SHARMA/ Examiner.Art Unit 2467 (Assistant Examiner)	06/06/2013 (Date)	**Total Claims Allowed:** 13	
/HASSAN PHILLIPS/ Supervisory Patent Examiner.Art Unit 2467 (Primary Examiner)	06/13/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

U.S. Patent and Trademark Office

Part of Paper No. 20130606

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	**Art Unit**
	GAUTAM SHARMA	2467

/GAUTAM SHARMA/ Examiner.Art Unit 2467	06/06/2013	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	13	
/HASSAN PHILLIPS/ Supervisory Patent Examiner.Art Unit 2467	06/13/2013	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

U.S. Patent and Trademark Office

Part of Paper No. 20130606

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	**Art Unit**
	GAUTAM SHARMA	2467

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	43														
2	44														
3	45														
4	46														
5	47														
6	48														
7	49														
8	50														
9	51														
10	52														
11	53														
12	54														
13	55														

/GAUTAM SHARMA/ Examiner.Art Unit 2467	06/06/2013	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	13	
/HASSAN PHILLIPS/ Supervisory Patent Examiner.Art Unit 2467	06/13/2013	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

U.S. Patent and Trademark Office

Part of Paper No. 20130606

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12665978	BARKAN, ELAD
	Examiner	Art Unit
	GAUTAM SHARMA	2467

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Classfication Search(370/310,328)	8/9/2012	Gautam Sharma
EAST Search	8/9/2012	Gautam Sharma
Inventor Search	8/9/2012	Gautam Sharma
Classfication Search(370/310,328)	2/26/2013	Gautam Sharma
EAST Search	2/26/2013	Gautam Sharma
Inventor Search	2/26/2013	Gautam Sharma
Classfication Search(370/310,328,351,389,392,395.1,395.2,395.4, 396,397,398,399)	6/6/2013	Gautam Sharma
EAST Search	6/6/2013	Gautam Sharma
Inventor Search	6/6/2013	Gautam Sharma
Consultation and approval for allowance provided by Hassan Phillips.	6/6/2013	Gautam Sharma

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
370	310,328,351,389,392,395.1,395.2,395.4, 396,397,398,399	6/6/2013	Gautam Sharma

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3281	370/310.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:10
L2	12016	370/328.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:10
L3	3290	370/351.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:10
L4	10084	370/389.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:10
L5	9754	370/392.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:10
L7	1775	370/395.1.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:11
L8	1345	370/395.2.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:11
L9	1233	370/395.4.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:11
L10	576	370/396.ccls.	US-PGPUB;	OR	ON	2013/06/06 14:11

			USPAT; USOCR; EPO; JPO			
L11	928	370/397.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:11
L12	365	370/398.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:11
L13	502	370/399.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:11
L15	16	barkan-elad.in.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:11
L16	263	(sta or "ue" or "ms" or "at" or mobile or equipment) adj2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) adj2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:12
L17	124	("fon" or "fon.com." or "www.fon.com" or foneros) and (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:12
L18	329	(virtual or software$1based or "software$1defined") adj1 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:12
L21	17378	(sta or "ue" or "ms" or "at" or mobile or equipment).clm. and (acting or broadcast$4 or provid$4 or initiat$4 or implement$4).clm. and (wi$1fi or internet or hotspot).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:14
L22	977	(sta or "ue" or "ms" or "at" or mobile or equipment).clm. and (acting or broadcast$4 or provid$4 or initiat$4 or implement$4).clm. and (wi$1fi or internet or hotspot).clm. and (proxy).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:14
L23	1365	(wi$1fi or wireless) with free with (software or application)	US-PGPUB;	OR	ON	2013/06/06 14:15

			USPAT; USOCR; EPO; JPO			
L24	9	l22 and l1	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:15
L25	66	l22 and l2	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:15
L26	3	l22 and l3	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:15
L27	23	l22 and l4	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:15
L28	12	l22 and l5	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:15
L29	0	l22 and l7	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:15
L30	0	l22 and l9	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:15
L31	7	l22 and l8	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:15
L32	0	l22 and l9	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L33	1	l22 and l10	US-PGPUB;	OR	ON	2013/06/06 14:16

			USPAT; USOCR; EPO; JPO			
L34	0	l22 and l11	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L35	0	l22 and l13	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L36	1	l22 and l15	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L37	12	l23 and 1	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L38	12	l23 and l1	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L39	37	l23 and l2	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L40	1	l23 and l3	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L41	9	l23 and l4	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L42	9	l23 and l5	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L43	0	l23 and l6	US-PGPUB;	OR	ON	2013/06/06 14:16

			USPAT; USOCR; EPO; JPO			
L44	0	l23 and l7	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L45	1	l23 and l8	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L46	4	l23 and l9	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L47	2	l23 and l10	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L48	0	l23 and l11	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L49	0	l23 and l12	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L50	0	l23 and l13	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L51	0	l23 and l14	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L52	1	l23 and l15	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:16
L53	134	l21 and l1	US-PGPUB;	OR	ON	2013/06/06 14:36

			USPAT; USOCR; EPO; JPO			
L54	718	l21 and l2	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L55	91	l21 and l3	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L56	236	l21 and l4	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L57	135	l21 and l5	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L58	28	l21 and l7	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L59	41	l21 and l8	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L60	6	l21 and l9	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L61	7	l21 and l10	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L62	7	l21 and l11	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L63	7	l21 and l12	US-PGPUB;	OR	ON	2013/06/06 14:36

			USPAT; USOCR; EPO; JPO			
L64	3	l21 and l13	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L65	0	l21 and l14	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L66	3	l21 and l15	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:36
L82	1324	(sta or "ue" or "ms" or "at" or mobile or equipment or station or wtru).clm. and (acting or broadcast$4 or provid$4 or initiat$4 or implement$4 or serv$4 or manag$4).clm. and (wi$1fi or internet or hotspot).clm. and (proxy).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:39
L83	10	l82 and l1	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L84	92	l82 and l2	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L85	7	l82 and l3	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L86	31	l82 and l4	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L87	22	l82 and l5	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L88	1	l82 and l7	US-PGPUB;	OR	ON	2013/06/06 14:41

			USPAT; USOCR; EPO; JPO			
L89	7	l82 and l8	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L90	0	l82 and l9	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L91	1	l82 and l10	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L92	2	l82 and l11	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L93	0	l82 and l12	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L94	0	l82 and l13	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L95	0	l82 and l14	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
L96	1	l82 and l15	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/06/06 14:41
S1	1	"20100296441"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S2	5	"8000276"	US-PGPUB;	OR	ON	2013/02/22 17:10

			USPAT; USOCR; EPO; JPO			
S3	1	"8000276".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S4	11293	370/328.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S5	0	"vagabee$4" or "fon.com"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S6	0	"fon.com"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S7	39532	(sta or "ue" or "ms" or "at" or mobile or equipment) with (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) with (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S8	1526	(sta or "ue" or "ms" or "at" or mobile or equipment) near2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) near2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S9	253	(sta or "ue" or "ms" or "at" or mobile or equipment) adj2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) adj2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S10	1	(sta or "ue" or "ms" or "at" or mobile or equipment or "pda" or "laptop") adj2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) adj2 (hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S11	8	(sta or "ue" or "ms" or "at" or mobile or equipment or "pda" or "laptop") adj2 (acting or broadcast$4 or provid$4 or initiat$4 or implement$4) adj2 (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S12	393	((distribut$4) near3 (wi$1fi or hotspot))	US-PGPUB;	OR	ON	2013/02/22 17:10

			USPAT; USOCR; EPO; JPO			
S13	2	((distribut$4) near3 (wi$1fi or hotspot)) with (software)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S14	4	("20030119537" | "20040003133" | "7284062" | "20040133689").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S15	2393	(peer$1to$1peer or "p2p" or "peer-peer") with (wi$1fi or "wifi" or bluetooth)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S16	191	(peer$1to$1peer or "p2p" or "peer-peer") with (wi$1fi or "wifi" or bluetooth) same (shared or distributed)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S17	191	((peer$1to$1peer or "p2p" or "peer-peer") with (wi$1fi or "wifi" or bluetooth)) same (shared or distributed)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S18	179	(wi$1fi or "wifi" or bluetooth) near1 (shared or distributed)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S19	15	Barkan-elad.in.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S20	0	("cell phone" or "user equipment" or "ue" or "sta" or "wtru") adj2 (provid$4 or implement$4 or broadcast$4 or advertis$6) adj2 ("wi$1fi" or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S21	0	("pda" or laptop) adj2 (provid$4 or implement$4 or broadcast$4 or advertis$6) adj2 ("wi$1fi" or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S22	5	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near3	US-PGPUB;	OR	ON	2013/02/22 17:10

		(provid$4 or implement$4 or broadcast$4 or advertis$6) near3 ("wi$1fi" or hotspot)	USPAT; USOCR; EPO; JPO			
S23	441	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near2 (relay) with (data or traffic or internet or wi$1fi)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S24	594	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near5(relay) near5 (data or traffic or internet or wi$1fi)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S25	354	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") near3(relay) near3 (data or traffic or internet or wi$1fi)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S26	55	("pda" or laptop or "cell phone" or "user equipment" or "ue" or "sta" or "wtru") adj2 ("as a" or serves or serving or provid$4) adj2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S27	11957	(distribut$4) adj2 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S28	2775	(distribut$4) adj1 (wi$1fi or internet or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S29	53	(distribut$4) adj1 (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S30	120	(distribut$4) adj2 (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S31	11505	"fon"	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S32	122	"fon" and (wi$1fi or hotspot)	US-PGPUB;	OR	ON	2013/02/22 17:10

			USPAT; USOCR; EPO; JPO			
S33	122	("fon" or "fon.com." or "www.fon.com" or foneros) and (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S34	9	("fon.com." or "www.fon.com" or foneros)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S35	1379	ipass	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S36	20	ipass and (wi$1fi and hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S37	50	ipass and (wi$1fi OR hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S38	11	jones-adrian.in.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S39	1	("2007/0215684").URPN.	USPAT	OR	ON	2013/02/22 17:10
S40	6	("6934530" | "20040052223" | "20060041931" | "20040052223" | "20040141617" | "6991575" | "20050204037" | "20050223086" | "20050250448" | "20050021781" | "20030051041" | "20050260972" | "20030051041" | "20050050352" | "20060223527" | "6795700" | "6957069" | "20040133687" | "20050220106" | "20050232242" | "6950628" | "20050233740" | "20050232283" | "6957086" | "20010053683" | "20070008885").PN.	USPAT	OR	ON	2013/02/22 17:10
S41	2	("20040158618" | "20040042596" | "20040158618").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10

S42	24	("6934530" | "20040052223" | "20060041931" | "20040052223" | "20040141617" | "6991575" | "20050204037" | "20050223086" | "20050250448" | "20050021781" | "20030051041" | "20050260972" | "20030051041" | "20050050352" | "20060223527" | "6795700" | "6957069" | "20040133687" | "20050220106" | "20050232242" | "6950628" | "20050233740" | "20050232283" | "6957086" | "20010053683" | "20070008885").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S43	159	(shared or sharing) adj2 (wi$1fi or hotspot)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S44	2455	(virtual or software or "software$1defined") near2 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S45	896	(virtual or software$1based or "software$1defined") near2 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S46	527	(virtual or software$1based or "software$1defined") near1 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S47	85	fon.as.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S48	434	(virtual or software$1based or "software$1defined") adj2 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S49	300	(virtual or software$1based or "software$1defined") adj ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S50	300	(virtual or software$1based or "software$1defined") adj1 ("bss" or "ap" or "access point")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10

S51	3	(wi$1fi or hotspot or internet) near1 Pyramid	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S52	0	(wi$1fi or hotspot) near1 Pyramid	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S53	3	(wi$1fi or hotspot) with Pyramid	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S54	1315	(((timer or time) or (limit$4 or based)) with (wi$1fi or wireless or internet) with free) same (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S55	188	(((timer or time) or (limit$4 or based)) near5 (wi$1fi or wireless or internet) near5 free) same (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S56	74	(((timer or time) or (limit$4 or based)) near5 (wi$1fi or wireless) near5 free) same (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S57	1314	(wi$1fi or wireless) with free with (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S58	75	(wi$1fi or wireless) near3 free near3 (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S59	24	free adj2 (wi$1fi or wireless) adj3 (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S60	28	free adj2 (internet) adj2(software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10

S61	28	free adj2 (internet) adj2 (software or application)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S62	131	free adj2 (wi$1fi or wireless) adj2 (access)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S63	3133	370/310.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/22 17:10
S64	26	(US-20100296441-$ or US-20030228868-$ or US-20060135206-$ or US-20070124802-$ or US-20080101290-$ or US-20050223086-$ or US-20070121839-$ or US-20070140163-$ or US-20070180136-$ or US-20070183383-$ or US-20050220106-$ or US-20070242657-$ or US-20060236378-$ or US-20070124490-$ or US-20070215684-$ or US-20070054654-$ or US-20040042596-$ or US-20030051041-$ or US-20040141617-$ or US-20040103278-$ or US-20050078624-$ or US-20050220048-$ or US-20030171989-$ or US-20020078059-$ or US-20020103879-$ or US-20050147084-$).did.	US-PGPUB	OR	ON	2013/02/26 17:12
S65	9	S64 and proxy	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:12
S66	7	S64 and proxy and (vlan or "virtual" or tunnel)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:37
S67	2	S64 and (proxy same (vlan or "virtual" or tunnel))	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:39
S68	9916	(proxy same (vlan or "virtual" or tunnel))	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:40
S69	5903	(proxy with (vlan or "virtual" or tunnel))	US-PGPUB; USPAT; USOCR; EPO;	OR	ON	2013/02/26 17:40

			JPO			
S70	11	(proxy with (vlan or tunnel)) with (apid or ssid)	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:40
S71	24	("6934530" | "20040052223" | "20060041931" | "20040052223" | "20040141617" | "6991575" | "20050204037" | "20050223086" | "20050250448" | "20050021781" | "20030051041" | "20050260972" | "20030051041" | "20050050352" | "20060223527" | "6795700" | "6957069" | "20040133687" | "20050220106" | "20050232242" | "6950628" | "20050233740" | "20050232283" | "6957086" | "20010053683" | "20070008885").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:43
S72	1	S70 and S71	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:43
S73	27	(US-20100296441-$ or US-20030228868-$ or US-20060135206-$ or US-20070124802-$ or US-20080101290-$ or US-20050223086-$ or US-20070121839-$ or US-20070140163-$ or US-20070180136-$ or US-20070183383-$ or US-20050220106-$ or US-20070242657-$ or US-20060236378-$ or US-20070124490-$ or US-20070215684-$ or US-20070054654-$ or US-20040042596-$ or US-20030051041-$ or US-20040141617-$ or US-20040103278-$ or US-20050078624-$ or US-20050220048-$ or US-20030171989-$ or US-20020078059-$ or US-20020103879-$ or US-20050147084-$).did. or (US-6950628-$).did.	US-PGPUB; USPAT	OR	ON	2013/02/26 17:58
S74	14	S73 and ("user interface" or "ui" or "display")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:58
S75	6	S73 and (acknowledge or "ack/nack" or "ack" or "nack" or "nak")	US-PGPUB; USPAT; USOCR; EPO; JPO	OR	ON	2013/02/26 17:59

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L19	1742	370/310.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:13
L20	5603	370/328.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:13

L67	2174	370/351.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:37
L68	1742	370/310.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:37
L69	5603	370/328.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:37
L70	5646	370/389.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:37
L71	4859	370/392.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:37
L72	1185	370/395.1.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:37
L73	909	370/395.2.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:37
L74	841	370/395.4.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:37
L75	473	370/396.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:37
L76	787	370/397.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:37
L77	310	370/398.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:38
L78	437	370/399.ccls.	USPAT; UPAD	OR	ON	2013/06/06 14:38
L79	5	barkan-elad.in.	USPAT; UPAD	OR	ON	2013/06/06 14:38
L80	379	(sta or "ue" or "ms" or "at" or mobile or equipment or station or wtru).clm. and (acting or broadcast$4 or provid$4 or initiat$4 or implement$4).clm. and (wi$1fi or internet or hotspot).clm. and (proxy).clm.	USPAT; UPAD	OR	ON	2013/06/06 14:38
L81	464	(sta or "ue" or "ms" or "at" or mobile or equipment or station or wtru).clm. and (acting or broadcast$4 or provid$4 or initiat$4 or implement$4 or serv$4 or manag$4).clm. and (wi$1fi or internet or hotspot).clm. and (proxy).clm.	USPAT; UPAD	OR	ON	2013/06/06 14:39
L97	5	l81 and l67	USPAT; UPAD	OR	ON	2013/06/06 14:42
L98	4	l81 and l68	USPAT; UPAD	OR	ON	2013/06/06 14:42
L99	38	l81 and l69	USPAT; UPAD	OR	ON	2013/06/06 14:42
L100	14	l81 and l70	USPAT; UPAD	OR	ON	2013/06/06 14:42
L101	12	l81 and l71	USPAT; UPAD	OR	ON	2013/06/06 14:42
L102	0	l81 and l72	USPAT; UPAD	OR	ON	2013/06/06 14:42
L103	4	l81 and l73	USPAT; UPAD	OR	ON	2013/06/06 14:42
L104	0	l81 and l74	USPAT; UPAD	OR	ON	2013/06/06 14:42
L105	1	l81 and l75	USPAT; UPAD	OR	ON	2013/06/06 14:42

L106	2	l81 and l76	USPAT; UPAD	OR	ON	2013/06/06 14:42
L107	0	l81 and l77	USPAT; UPAD	OR	ON	2013/06/06 14:42
L108	0	l81 and l78	USPAT; UPAD	OR	ON	2013/06/06 14:42
L109	0	l81 and l79	USPAT; UPAD	OR	ON	2013/06/06 14:42

6/6/2013 2:43:26 PM
C:\Users\gsharma\Documents\EAST\Workspaces\12665978_update_2013_June_6.wsp

dup

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

60956 7590 06/19/2013
Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

OPAP AKIMA-18 SEP 0 5 2013 PATENT & TRADEMARK OFFICE

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

12/665,978

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/665,978	12/22/2009	Elad Barkan	BRK-PU-001-US1	5873

TITLE OF INVENTION: WIRELESS INTERNET SYSTEM AND METHOD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	09/19/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHARMA, GAUTAM	2467	370-328000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 ELAD BARKAN
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)
PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.
(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☑ Issue Fee
☑ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)
☐ A check is enclosed.
☑ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

PTOL-85 (Rev. 02/11)

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature Elad Barkan Date Sep. 5, 2013

Typed or printed name ELAD BARKAN Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PTOL-85 (Rev. 02/11) Approved for use through 08/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

60956 7590 06/19/2013
Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

12/665,978

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/665,978	12/22/2009	Elad Barkan	BRK-FU-001-US1	5873

TITLE OF INVENTION: WIRELESS INTERNET SYSTEM AND METHOD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	09/19/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHARMA, GAUTAM	2467	370-328000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 ELAD BARKAN
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)
PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☑ Issue Fee
- ☑ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)
- ☐ A check is enclosed.
- ☑ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

09/06/2013 ZJUHAR2 00000010 12665978
01 FC:2501 890.00 OP
02 FC:1504 300.00 OP

PTOL-85 (Rev. 02/11)

b. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature Elad Barkan Date Sep. 5, 2013

Typed or printed name ELAD BARKAN Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PTOL-85 (Rev. 02/11) Approved for use through 08/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/665,978	10/15/2013	8559369	BRK-PU-001-US1	5873

60956 7590 09/25/2013

Professional Patent Solutions
P.O. BOX 654
HERZELIYA PITUACH, 46105
ISRAEL

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 905 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Elad Barkan, Kfar-Sirkin, ISRAEL;

Doc Code: PET.POA.WDRW
Document Description: Petition to withdraw attorney or agent (SB83)

PTO/SB/83 (04-13)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST FOR WITHDRAWAL AS ATTORNEY OR AGENT AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	12/665,978
Filing Date	12/22/2009
First Named Inventor	Elad Barkan
Art Unit	2467
Examiner Name	SHARMA, GAUTAM
Practitioner Docket Number	BRK-PU-001-US1

To: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Please withdraw me as attorney or agent for the above-identified patent application, and

- ☐ all the practitioners of record;
- ☐ the practitioners (with registration numbers) of record listed on the attached paper(s); or
- ☑ the practitioners of record associated with Customer Number: 60956

NOTE: The immediately preceding box should only be marked when the practitioners were appointed using the listed Customer Number.

The reason(s) for this request are those described in 37 CFR:

☐ 11.116(a)(1)	☐ 11.116(a)(2)	☐ 11.116(a)(3)
☑ 11.116(b)(1)	☐ 11.116(b)(2)	☐ 11.116(b)(3)
☐ 11.116(b)(4)	☑ 11.116(b)(5)	☐ 11.116(b)(6)

☐ 11. 116(b)(7) Please explain below:

Certifications

Check each box below that is factually correct. WARNING: If a box is left unchecked, the request will likely not be approved.

1. ☑ I/We have given reasonable notice to the client, prior to the expiration of the response period, that the practitioner(s) intend to withdraw from employment.
2. ☑ I/We have delivered to the client or a duly authorized representative of the client all papers and property (including funds) to which the client is entitled.
3. ☑ I/We have notified the client of any responses that may be due and the time frame within which the client must respond.

Please provide an explanation, if necessary:

PTO/SB/83 (04-13)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

REQUEST FOR WITHDRAWAL AS ATTORNEY OR AGENT AND CHANGE OF CORRESPONDENCE ADDRESS

Complete the following section only when the correspondence address will change. *Changes of address will only be accepted to the first named inventor or an assignee that has properly made itself of record pursuant to 37 CFR 3.71.*

Change the correspondence address and direct all future correspondence to:

A. ☐ The address of the first named inventor or assignee associated with Customer Number: _____

OR

B. ☑ First Named Inventor or Assignee Name

Address 12 Habanim Street			
City Kfar-Sirkin	State	Zip 49935	Country Israel
Telephone +972-54-5204123		Email elad.barkan@gmail.com	

I am authorized to sign on behalf of myself and all withdrawing practitioners.

Signature /Vladimir Sherman/

Name Vladimir Sherman — Registration No. 43116

Address Professional Patent Solutions, P.O. Box 654			
City Herzeliya Pituach	State	Zip 46105	Country Israel

Date 11/11/2013 — Telephone No. +972-9-954-1971

NOTE: Withdrawal is effective when approved rather than when received.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	17371446
Application Number:	12665978
International Application Number:	
Confirmation Number:	5873
Title of Invention:	WIRELESS INTERNET SYSTEM AND METHOD
First Named Inventor/Applicant Name:	Elad Barkan
Customer Number:	60956
Filer:	Vladimir Sherman/Dina Cohen
Filer Authorized By:	Vladimir Sherman
Attorney Docket Number:	BRK-PU-001-US1
Receipt Date:	12-NOV-2013
Filing Date:	22-DEC-2009
Time Stamp:	07:59:02
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition to withdraw attorney or agent (SB83)	BRK-PU-001-US1-RequestWithdrawalAsAttorney.pdf	304057 6fcb716cb6bdd558ccfcf62d14468697755c9f1b	no	3

Warnings:	
Information:	

Total Files Size (in bytes):	304057

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas (Marshall Division) on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:16-cv-00063	1/19/2016	for the Eastern District of Texas (Marshall Division)

PLAINTIFF	DEFENDANT
Barkan Wireless Technologies, L.P.	T-Mobile US, Inc. T-Mobile USA, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,042,306	5/26/2015	Barkan Wireless Technologies, L.P.
2	8,559,369	10/15/2013	Barkan Wireless Technologies, L.P.
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas (Marshall Division) on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:16-cv-00063	1/19/2016	for the Eastern District of Texas (Marshall Division)

PLAINTIFF	DEFENDANT
Barkan Wireless Technologies, L.P.	T-Mobile US, Inc. T-Mobile USA, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,042,306	5/26/2015	Barkan Wireless Technologies, L.P.
2	8,559,369	10/15/2013	Barkan Wireless Technologies, L.P.
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas (Marshall Division) on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:16-cv-00063	1/19/2016	for the Eastern District of Texas (Marshall Division)

PLAINTIFF	DEFENDANT
[AMENDED] Barkan Wireless Access Technologies, L.P.	T-Mobile US, Inc. T-Mobile USA, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,042,306	5/26/2015	Barkan Wireless Access Technologies, L.P.
2	8,559,369	10/15/2013	Barkan Wireless Access Technologies, L.P.
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**