

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B or equivalent) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5. If the Power of Attorney by Applicant form is not accompanied by this transmittal form or an equivalent, the Power of Attorney will not be recognized in the application.

Application Number	Not Yet Assigned
Filing Date	April 22, 2015
First Named Inventor	Hyoung-Gon Lee
Title	SCHEMES FOR CONNECTING TO WIRELESS NETWORK
Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned
Attorney Docket Number	2582-2.737BS

SIGNATURE of Applicant or Patent Practitioner

Signature	/Daniel J. Stanger/	Date	April 22, 2015
Name	Daniel J. Stanger	Telephone	703-684-1470
Registration Number	32,846		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications.

☐ *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.

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter.

- ☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

86636

OR

- ☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

Name	Registration Number	Name	Registration Number

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

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

OR

- ☒ The address associated with Customer Number:

86636

OR

☐ Firm or Individual Name

Address

City

State

Zip

Country

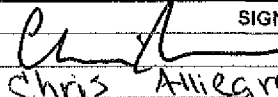
Telephone

Email

I am the Applicant:

- ☐ Inventor or Joint Inventor
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor
- ☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document)

SIGNATURE of Applicant for Patent

Signature		Date	7/2/2013
Name	Chris Allegro	Telephone	
Title and Company	Authorized Representative - Empire Technology Development, LLC		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms for more than one signature, 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.

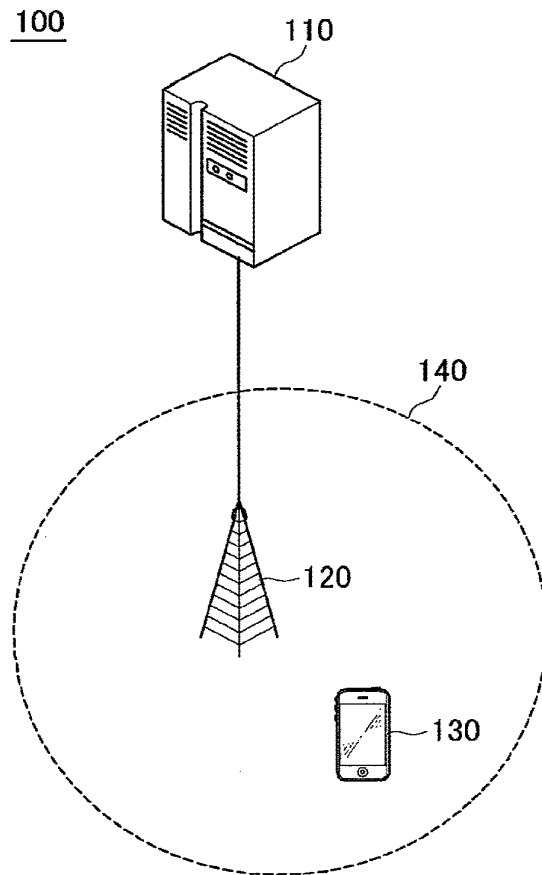
FIG. 1

*FIG. 2*200

ACCESS POINT	MAC ADDRESS	SSID
AUTHENTICATED ACCESS POINT 1	xxx111yyy	zzz
AUTHENTICATED ACCESS POINT 2	zzz222xxx	yyy
...	...	...

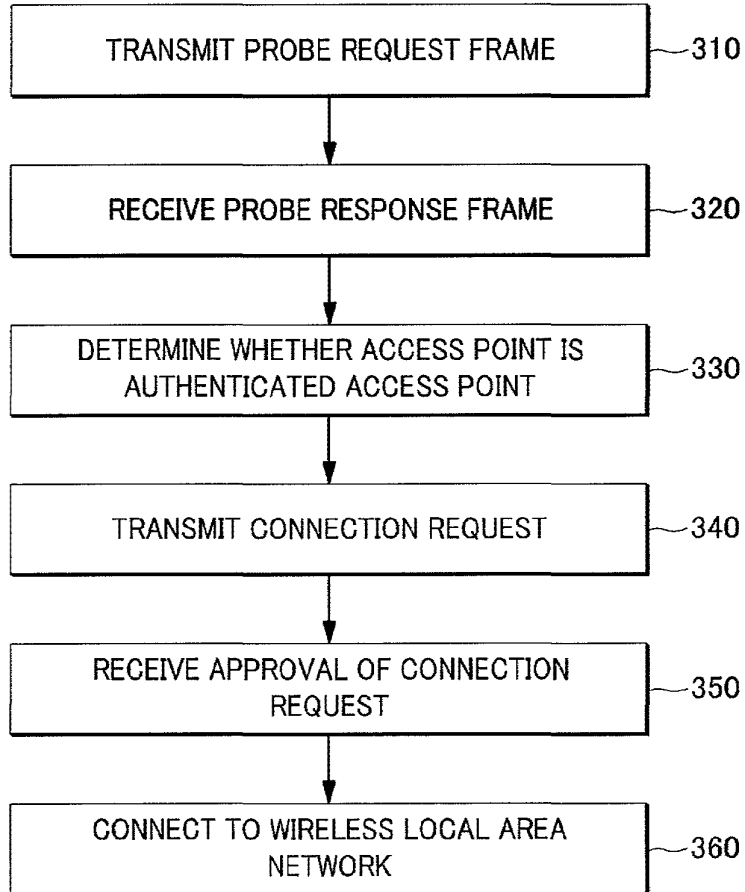
*FIG. 3*300

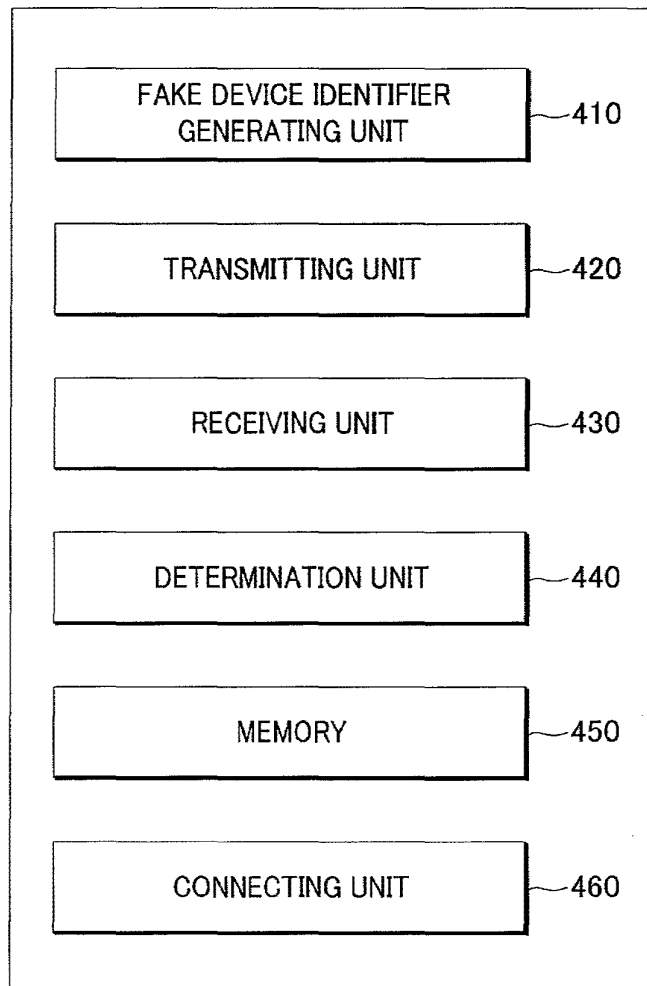
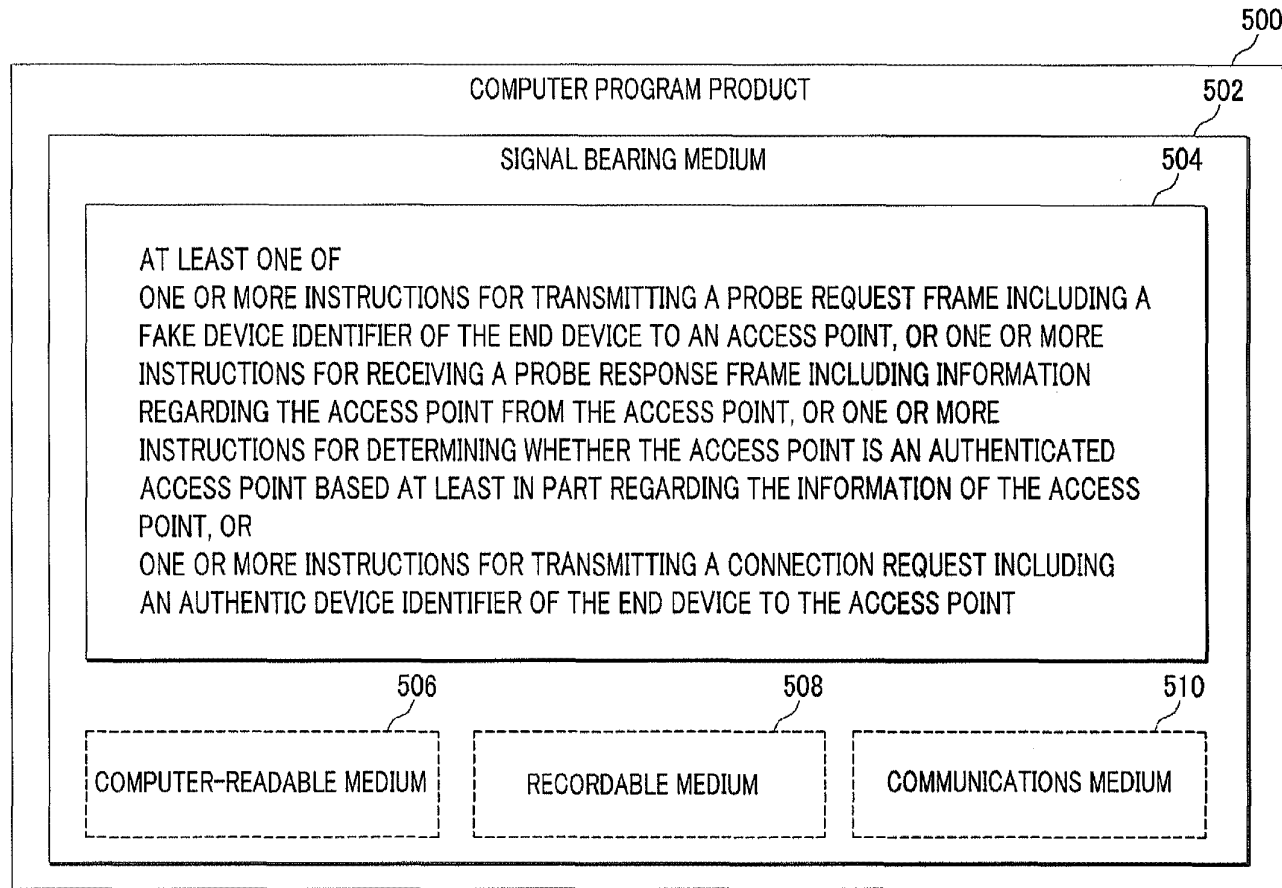
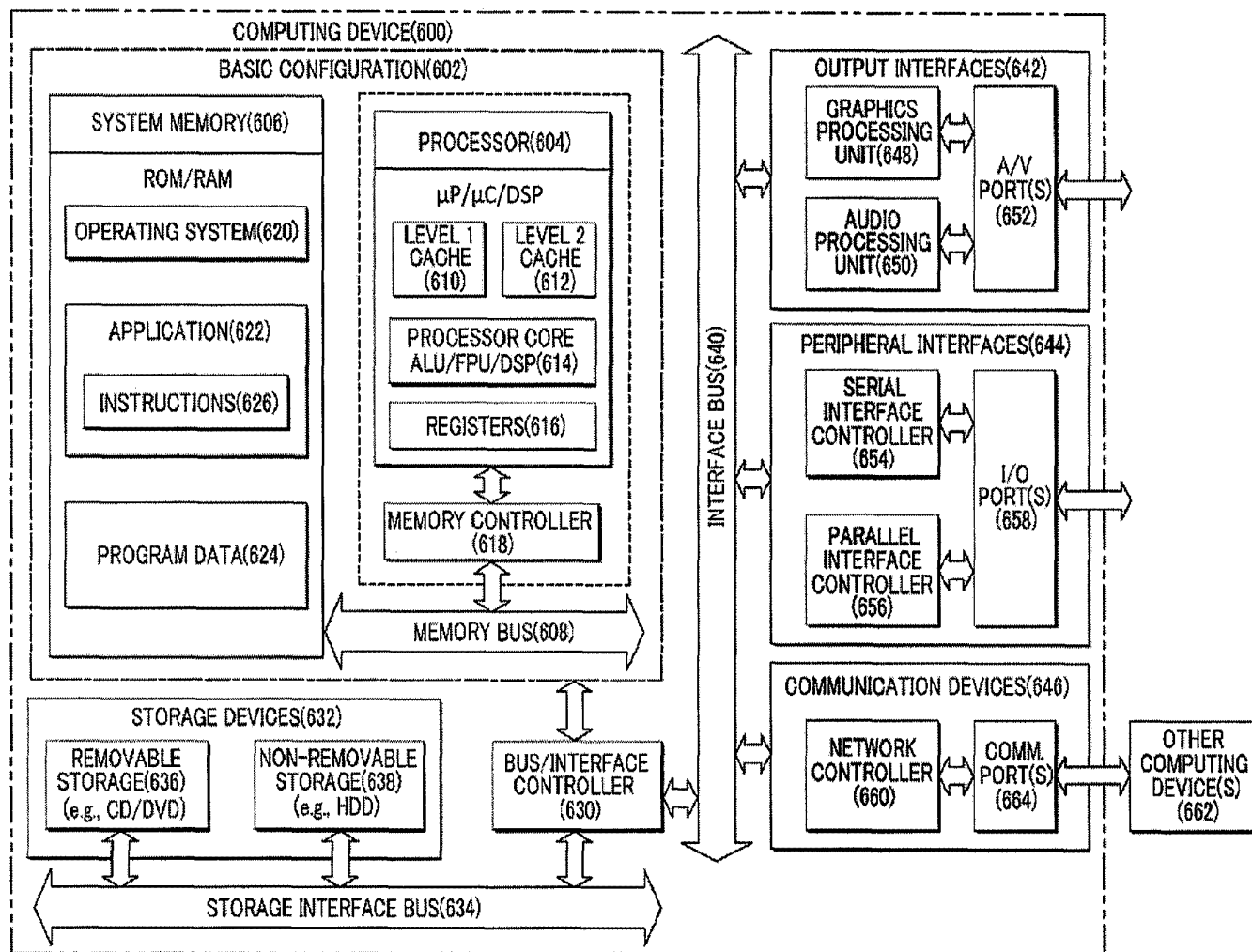
*FIG. 4*130

FIG. 5

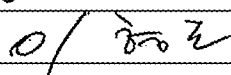


5/6

FIG. 6



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

Title of Invention	SCHEMES FOR CONNECTING TO WIRELESS NETWORK		
As the below named inventor, I hereby declare that: This declaration is directed to: ☐ The attached application, or ☒ United States application or PCT international application number <u>PCT/US12/66306</u> filed on <u>11/21/2012</u> The above-identified application was made or authorized to be made by me. I believe that I am the original inventor or an original joint inventor of a claimed invention in the application. I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both. 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.			
LEGAL NAME OF INVENTOR Inventor: <u>Hyoung-Gon Lee</u> Date (Optional): <u>APR. 26, 2013</u> Signature: <u></u>			
Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional PTO/AIA/01 form for each additional inventor.			

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1 minute 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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2015-04-22
	First Named Inventor	Lee, Hyoung-Gon	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	2582-2.737BS	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7808958	B1	2010-10-05	Hernacki et al	
	2	7185204	B2	2007-02-27	Narayanaswami et al	
	3	8005458	B2	2011-08-23	Baik et al	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20080052779	A1	2008-02-28	Sinha et al	
	2	20110083165	A1	2011-04-07	Gopinath et al	
	3	20110314147	A1	2011-12-22	Whelan et al	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		
Filing Date		2015-04-22
First Named Inventor	Lee, Hyoung-Gon	
Art Unit		
Examiner Name		
Attorney Docket Number	2582-2.737BS	

4	20080043686	A1	2008-02-21	Sperti et al	
5	20070286143	A1	2007-12-13	Olson et al	
6	20030221006	A1	2003-11-27	Kuan et al	
7	20120221955	A1	2012-08-30	Raleigh et al	
8	20090235077	A1	2009-09-17	Cam Winget et al.	
9	20120210395	A1	2012-08-16	Cam Winget et al.	
10	20120311328	A1	2012-12-06	Wang et al.	
11	20130179943	A1	2013-07-11	Sun et al.	
12	20130281056	A1	2013-10-24	Abraham et al	

If you wish to add additional U.S. Published Application citation information please click the Add button. **Add**

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² ;	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		
Filing Date		2015-04-22
First Named Inventor	Lee, Hyoung-Gon	
Art Unit		
Examiner Name		
Attorney Docket Number	2582-2.737BS	

	1							☐
--	---	--	--	--	--	--	--	--------------------------

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	International Search Report from International Application No.: PCT/US12/66306 mailed Feb. 8, 2013.	☐
	2	Singelee, et al., "Enabling Location Privacy in Wireless Personal Area Networks", 20 pages, Sept. 2006.	☐
	3	Gruteser, et al., "Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis", Sept. 19, 2003, 10 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	2015-04-22
First Named Inventor	Lee, Hyoung-Gon
Art Unit	
Examiner Name	
Attorney Docket Number	2582-2.737BS

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Daniel J. Stanger/	Date (YYYY-MM-DD)	2015-04-22
Name/Print	Daniel J. Stanger	Registration Number	32846

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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.

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	2582-2.737BS
		Application Number	
Title of Invention	SCHEMES FOR CONNECTING TO WIRELESS NETWORK		
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.)
--

Inventor Information:

Inventor 1 Remove				
Legal Name				
Prefix	Given Name	Middle Name	Family Name	Suffix
	Hyoung-Gon		LEE	
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service				
City	Seoul	Country of Residence i	KR	
Mailing Address of Inventor:				
Address 1	101-705, Daechi Hyundai APT. 974, Daechi-2-dong,			
Address 2	Gangnam-gu			
City	Seoul	State/Province		
Postal Code	135-850	Country i	KR	
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	86636		
Email Address	mail@brundidge-stanger.com	Add Email	Remove Email

Application Information:

Title of the Invention	SCHEMES FOR CONNECTING TO WIRELESS NETWORK		
Attorney Docket Number	2582-2.737BS	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	6	Suggested Figure for Publication (if any)	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	2582-2.737BS
		Application Number	
Title of Invention	SCHEMES FOR CONNECTING TO WIRELESS NETWORK		

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). Either enter 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)
Prefix	Given Name	Middle Name	Family Name	Suffix
	Daniel	J	Stanger	
Registration Number		32846		
Prefix	Given Name	Middle Name	Family Name	Suffix
	David	S	Lee	
Registration Number		38222		
Additional Representative Information blocks may be generated within this form by selecting the Add button.				

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.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13885754	2013-05-16
Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13885754	a 371 of international	PCT/US12/66306	2012-11-21
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			

Foreign Priority Information:

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	2582-2.737BS
		Application Number	
Title of Invention	SCHEMES FOR CONNECTING TO WIRELESS NETWORK		

This section allows for the applicant to claim priority to a foreign application. 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(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐	This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
--------------------------	--

Authorization to Permit Access:

☒	Authorization to Permit Access to the Instant Application by the Participating Offices
If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application. In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application. In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	2582-2.737BS
		Application Number	
Title of Invention	SCHEMES FOR CONNECTING TO WIRELESS NETWORK		

Applicant Information:

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

Applicant 1	Remove		
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section. Clear			
☒ Assignee	☐ Legal Representative under 35 U.S.C. 117		
☐ Person to whom the inventor is obligated to assign.	☐ Person who shows sufficient proprietary interest		
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
Name of the Deceased or Legally Incapacitated Inventor :			
If the Applicant is an Organization check here. ☒			
Organization Name	Empire Technology Development LLC		
Mailing Address Information:			
Address 1	2711 Centerville Road		
Address 2	Suite 400		
City	Wilmington	State/Province	DE
Country ⁱ	US	Postal Code	19808
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button. Add			

Non-Applicant Assignee Information:

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	2582-2.737BS
		Application Number	
Title of Invention	SCHEMES FOR CONNECTING TO WIRELESS NETWORK		

Assignee 1				
Complete this section only if non-applicant assignee information is desired to be included on the patent application publication in accordance with 37 CFR 1.215(b). Do not include in this section an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest), as the patent application publication will include the name of the applicant(s).				
Remove				
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 i		Postal Code		
Phone Number		Fax Number		
Email Address				
Additional Assignee Data may be generated within this form by selecting the Add button. Add				

Signature: Remove				
NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications				
Signature	/Daniel J. Stanger/		Date (YYYY-MM-DD)	2015-04-22
First Name	Daniel	Last Name	Stanger	Registration Number
				32846
Additional Signature may be generated within this form by selecting the Add button. Add				

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.

SCHEMES FOR CONNECTING TO WIRELESS NETWORK

CROSS-REFERENCE

This Application is a Continuation Application of U.S. Ser. No. 13/885,754, filed on May 16, 2013, which is a National Stage filing under 35 U.S.C. § 371 of PCT Ser. No. PCT/US12/66306 filed on November 21, 2012. The disclosures of both applications are hereby incorporated herein by reference in their entireties.

BACKGROUND

[0001] The availability of third generation (3G) and fourth generation (4G) mobile telecommunications technologies, and Wi-Fi wireless access technologies make it possible to provide wireless data communications. It is generally preferable to use Wi-Fi networks for data transmission because Wi-Fi wireless access technologies are typically available at lower cost but with higher throughput than the third generation (3G) and/or fourth generation (4G) mobile telecommunications technologies. However, security for Wi-Fi wireless access technologies has drawn intense scrutiny.

SUMMARY

[0002] In an example, a method performed under control of an end device first device may include transmitting a probe request frame including a fake device identifier for the end device to an access point, receiving a probe response frame including information regarding the access point from the access point, determining whether the access point is an authenticated access point based at least in part on the information regarding the access point, and transmitting a connection request including an authentic device identifier for the end device to the access point.

[0003] In another example, an end device may include a transmitting unit configured to transmit a probe request frame including a fake device identifier to an access point, a receiving unit configured to receive a probe response frame including information regarding the access point from the access point, a memory configured to

store an authenticated access point list including information regarding at least one authenticated access point, a determination unit configured to determine whether the access point is an authenticated access point based at least in part on the information regarding the access point or the authenticated access point list, and a connecting unit configured to connect to a wireless local area network provided by the access point. The transmitting unit is further configured to transmit a connection request including an original device identifier to the access point, and the receiving unit is further configured to receive an approval of the connection request from the access point.

[0004] In yet another example, a computer-readable storage medium may store thereon computer-executable instructions that, in response to execution, cause an end device to perform operations, including transmitting a probe request frame including a fake device identifier of the end device to an access point, receiving a probe response frame including information regarding the access point from the access point, determining whether the access point is an authenticated access point based at least in part regarding the information regarding the access point, and transmitting a connection request including an original device identifier of the end device to the access point.

[0005] The foregoing summary is illustrative only and is not intended to be in any way limiting. In addition to the illustrative aspects, embodiments, and features described above, further aspects, embodiments, and features will become apparent by reference to the drawings and the following detailed description.

BRIEF DESCRIPTION OF THE FIGURES

[0006] The foregoing and other features of this disclosure will become more fully apparent from the following description and appended claims, taken in conjunction with the accompanying drawings. With the understanding that these drawings depict only several embodiments in accordance with the disclosure and are, therefore, not to be considered limiting of its scope, the disclosure will be described with additional specificity and detail through use of the accompanying drawings, in which:

[0007] Fig. 1 schematically shows an illustrative example of a network communications environment including a mobile operating server, an access point and an end device, arranged in accordance with at least some embodiments described herein;

[0008] Fig. 2 schematically shows an illustrative example of an authenticated access point list, arranged in accordance with at least some embodiments described herein;

[0009] Fig. 3 shows an example flow diagram of a process of an end device for connecting to a wireless local area network, arranged in accordance with at least some embodiments described herein;

[0010] Fig. 4 shows a schematic block diagram illustrating an example architecture for an end device, arranged in accordance with at least some embodiments described herein;

[0011] Fig. 5 illustrates computer program products that may be utilized to provide a scheme for connecting to a wireless local area network, arranged in accordance with at least some embodiments described herein; and

[0012] Fig. 6 is a block diagram illustrating an example computing device that may be utilized to provide a scheme for connecting to a wireless local area network, arranged in accordance with at least some embodiments described herein.

DETAILED DESCRIPTION

[0013] In the following detailed description, reference is made to the accompanying drawings, which form a part hereof. In the drawings, similar symbols typically identify similar components, unless context dictates otherwise. The illustrative embodiments described in the detailed description, drawings, and claims are not meant to be limiting. Other embodiments may be utilized, and other changes may be made, without departing from the spirit or scope of the subject matter presented herein. It will be readily understood that the aspects of the present disclosure, as generally described herein, and illustrated in the Figures, can be arranged, substituted, combined, separated, and designed in a wide variety of different configurations, all of which are explicitly contemplated herein.

[0014] This disclosure is generally drawn, *inter alia*, to methods, apparatuses, systems, devices, and computer program products related to secured wireless network

communication schemes.

[0015] Technologies are generally described for connecting to wireless networks while preventing leakage of location information of an end device.

[0016] In general, in order to connect to a wireless local area network (WLAN), an end device may search for at least one available access point around the end device. By way of example, but not limitation, the access point may be a Wi-Fi access point and the WLAN may be a Wi-Fi network. When searching, the end device may transmit a probe request frame that may include a device identifier, for the end device such as a media access control (MAC) address of the end device. In such cases, since the probe request frame that includes the device identifier is transmitted to access points around the end device, present location information of the end device may be exposed to some access points with which a user of the end device does not want to be connected and/or other devices to which the end device does not want to disclose the present location information.

[0017] In some embodiments, an end device may transmit a probe request frame that includes a fake device identifier for the end device to at least one access point around the end device. As a response to the probe request frame, the end device may receive a probe response frame from one or more access points. The probe response frame may include information regarding the access point. By way of example, but not limitation, the information regarding the access point may include a MAC address of the access point and/or a service set identifier (SSID) of the access point.

[0018] The end device may determine whether there is an authenticated access point around the end device based at least in part on the information included in the probe response frame. If there is an authenticated access point around the end device, the end device may transmit a connection request including an authentic device identifier for the end device, such as an original MAC address, to the authenticated access point. Then, the end device may connect to a wireless local area network provided by the authenticated access point without a leakage of present location information of the end device to undesirable access points.

[0019] Fig. 1 schematically shows an illustrative example of a network communications environment 100 including a mobile operating server, an access point,

and an end device, arranged in accordance with at least some embodiments described herein.

[0020] As illustrated in Fig. 1, network communications environment 100 may include a mobile operating server 110, an access point 120 and an end device 130. Mobile operating server 110 may control access point 120. In Fig 1, although only one access point (i.e., access point 120) is located around end device 130, so that end device 130 is located in a network area 140 provided by access point 120, there could be two or more access points around end device 130.

[0021] By way of example, access point 120 may include a Wi-Fi access point and provide a WLAN that includes a Wi-Fi network. Further, by way of example, end device 130 may include, but not exclusively, a personal communication terminal, such as PCS (Personal Communication System), GSM (Global System for Mobile communications), PDC (Personal Digital Cellular), PHS (Personal Handyphone System), PDA (Personal Digital Assistant), IMT (International Mobile Telecommunication)-2000, CDMA (Code Division Multiple Access)-2000, W-CDMA (W-Code Division Multiple Access) and Wibro (Wireless Broadband Internet) terminals.

[0022] End device 130 may transmit a probe request frame, which may include a fake device identifier (for example, a fake MAC address), to access point 120 for end device 130. By way of example, but not limitation, the fake device identifier may include one or both of one or more random numbers or one or more random characters. In some embodiments, end device 130 may generate the fake device identifier and transmit the generated fake device identifier to access point 120. Further, in some other embodiments, mobile operating server 110 may provide end device 130 with the fake device identifier, and end device 130 may transmit the provided fake device identifier to access point 120.

[0023] End device 130 may receive a probe response frame from access point 120 to which end device 130 transmitted the probe request frame. The probe response frame may include information regarding access point 120. By way of example, but not limitation, the information regarding access point 120 may include a MAC address of access point 120 and/or an SSID of access point 120.

[0024] End device 130 may determine whether access point 120, which

transmitted the probe response frame to end device 130, is an authenticated access point based at least in part on the information regarding access point 120. In some embodiments, end device 130 may receive an authenticated access point list including information regarding at least one authenticated access point from mobile operating server 110. End device 130 may determine whether access point 120 is an authenticated access point based at least in part on the authenticated access point list. By way of example, end device 130 may check whether the information regarding access point 120 is included in the authenticated access point list. If the information regarding access point 120 is included in the authenticated access point list, end device 130 may recognize access point 120 as an authenticated access point. By way of example, but not limitation, the authenticated access point may include an access point controlled by mobile operating server 110 and/or an access point previously connected with end device 130.

[0025] Fig. 2 schematically shows an illustrative example of an authenticated access point list 200, arranged in accordance with at least some embodiments described herein. As illustrated in Fig. 2, authenticated access point list 200 may include the information regarding at least one authenticated access point. By way of example, but not limitation, the information regarding the least one authenticated access point may include a MAC address or an SSID of each authenticated access point.

[0026] Referring back to Fig. 1, end device 130 may transmit a connection request, including an authentic device identifier, to authenticated access point 120 for end device 130. By way of example, but not limitation, the authentic device identifier may include an original MAC address of end device 130. In some embodiments, the connection request may include an authentication request for authenticated access point 120 to authenticate end device 130. Further, the authentication request may include a shared key between access point 120 and end device 130.

[0027] End device 130 may receive an approval of the connection request from access point 120. In some embodiments, the approval of the connection request may include an authentication response.

[0028] End device 130 may transmit an association request to access point 120 in response to the approval of the connection request and, in response to the association request, access point 120 may transmit an association response to end

device 130. Then, end device 130 may connect to the wireless local area network provided by access point 120.

[0029] Fig. 3 shows an example flow diagram of a process 300 of an end device 130 for connecting to a wireless local area network, arranged in accordance with at least some embodiments described herein. The method in Fig. 3 may be implemented in the network communication environment including mobile operating server 110, access point 120 and end device 130, as illustrated in Fig. 1. An example process may include one or more operations, actions, or functions as illustrated by one or more blocks 310, 320, 330, 340, 350 and/or 360. Although illustrated as discrete blocks, various blocks may be divided into additional blocks, combined into fewer blocks, or eliminated, depending on the desired implementation. Processing may begin at block 310.

[0030] At block 310 (Transmit Probe Request Frame), end device 130 may transmit a probe request frame, which may include a fake device identifier (for example, a fake MAC address), to access point 120 for end device 130. By way of example, but not limitation, the fake device identifier may include at least one of a random number or a random character. Processing may proceed from block 310 to block 320.

[0031] At block 320 (Receive Probe Response Frame), end device 130 may receive a probe response frame from access point 120 as a response to the probe request frame. The probe response frame may include information regarding access point 120. By way of example, but not limitation, the information regarding access point 120 may include a MAC address of access point 120 and/or an SSID of access point 120. Processing may proceed from block 320 to block 330.

[0032] At block 330 (Determine Whether Access Point is Authenticated Access Point), end device 130 may determine whether access point 120, which transmitted the probe response frame to end device 130, is an authenticated access point based at least in part on the information regarding access point 120 included in the probe response frame. In some embodiments, end device 130 may receive authenticated access point list 200, as illustrated in Fig. 2, from mobile operating server 110. Authenticated access point list 200 may include information regarding at least one authenticated access point.

[0033] At block 330, end device 130 may check whether the information regarding access point 120, which is included in the probe response frame, is included in authenticated access point list 200. If the information regarding access point 120 is included in authenticated access point list 200, end device 130 may recognize access point 120 as an authenticated access point. Processing may proceed from block 330 to block 340.

[0034] At block 340 (Transmit Connection Request), end device 130 may transmit a connection request including an authentic device identifier for end device 130 to access point 120 which is recognized as the authenticated access point at block 330. By way of example, but not limitation, the authentic device identifier may include an original MAC address of end device 130. Processing may proceed from block 340 to block 350.

[0035] At block 350 (Receive Approval of Connection Request), end device 130 may receive an approval of the connection request from access point 120. Processing may proceed from block 350 to block 360.

[0036] At block 360 (Connect to Wireless Local Area Network), end device 130 may connect to a wireless local area network provided by access point 120. By way of example, but not limitation, the wireless local area network provided by access point 120 may include a Wi-Fi network.

[0037] One skilled in the art will appreciate that, for this and other processes and methods disclosed herein, the functions performed in the processes and methods may be implemented in differing order. Furthermore, the outlined steps and operations are only provided as examples, and some of the steps and operations may be optional, combined into fewer steps and operations, or expanded into additional steps and operations without detracting from the essence of the disclosed embodiments.

[0038] Fig. 4 shows a schematic block diagram illustrating an example architecture for an end device 130, arranged in accordance with at least some embodiments described herein. As depicted in Fig. 4, end device 130 may include a fake device identifier generating unit 410, a transmitting unit 420, a receiving unit 430, a determination unit 440, a memory 450, and a connecting unit 460. Although illustrated as discrete components, various components may be divided into additional components,

combined into fewer components, or eliminated altogether while being contemplated within the scope of the disclosed subject matter.

[0039] Fake device identifier generating unit 410 may generate a fake device identifier (for example, a fake MAC address) for end device 130. By way of example, but not limitation, the fake device identifier may include a random number and/or a random character.

[0040] Transmitting unit 420 may transmit, to access point 120, a probe request frame which may include the fake device identifier generated by fake device identifier generating unit 410.

[0041] Receiving unit 430 may receive a probe response frame from access point 120 to which the probe request frame is transmitted. The probe response frame may include information regarding access point 120. By way of example, but not limitation, the information regarding access point 120 may include a MAC address of access point 120 and/or an SSID of access point 120.

[0042] In some embodiments, receiving unit 430 may receive a fake device identifier (for example, a fake MAC address) for end device 130 from mobile operating server 110. In such cases, transmitting unit 420 may transmit, to access point 120, a probe request frame that includes the fake device identifier received from mobile operating server 110.

[0043] Determination unit 440 may determine whether access point 120, which transmitted the probe response frame to end device 130, is an authenticated access point based at least in part on the information regarding access point 120. In some embodiments, determination unit 440 may compare the information regarding access point 120, which is included in the probe response frame, and information regarding authenticated access points, which is included in authenticated access point list 200 as illustrated in Fig. 2. The information regarding the authenticated access points may include a MAC address and/or an SSID of each of the authenticated access points.

[0044] Determination unit 440 may determine whether the information regarding access point 120, which is included in the probe response frame, is included in authenticated access point list 200. If the information regarding

access point 120 is included in authenticated access point list 200, end device 130 may recognize access point 120 as an authenticated access point.

[0045] Memory 450 may store authenticated access point list 200. In some embodiments, receiving unit 430 may receive authenticated access point list 200 from mobile operating server 110 and memory 450 may store the received authenticated access point list 200. Further, memory 450 may store the fake device identifier which is generated by fake device identifier generating unit 410 or received from mobile operating server 110.

[0046] Transmitting unit 420 may transmit a connection request, which includes an authentic device identifier, for end device 130 to access point 120 that is recognized as the authenticated access point by determination unit 440. By way of example, but not limitation, the authentic device identifier may include an original MAC address of end device 130.

[0047] Receiving unit 430 may receive an approval of the connection request from access point 120 and connecting unit 460 may connect to a wireless local area network provided by access point 120.

[0048] Fig. 5 illustrates computer program products that may be utilized to provide a scheme for connecting to a wireless local area network, arranged in accordance with at least some embodiments described herein. Program product 500 may include a signal bearing medium 502. Signal bearing medium 502 may include one or more instructions 504 that, when executed by, for example, a processor, may provide the functionality described above with respect to Figs. 1-4. By way of example, instructions 504 may include: one or more instructions for transmitting a probe request frame including a fake device identifier (for example, a fake MAC address) of the end device to an access point, one or more instructions for receiving a probe response frame including information regarding the access point from the access point, one or more instructions for determining whether the access point is an authenticated access point based at least in part regarding the information regarding the access point, and one or more instructions for transmitting a connection request including an authentic device identifier of the end device to the access point. Thus, for example, referring to Fig. 4, end device 130 may undertake one or more of the blocks shown in Fig. 3 in response to instructions 504.

[0049] In some implementations, signal bearing medium 502 may encompass a computer-readable medium 506, such as, but not limited to, a hard disk drive, a CD, a DVD, a digital tape, memory, etc. In some implementations, signal bearing medium 502 may encompass a recordable medium 508, such as, but not limited to, memory, read/write (R/W) CDs, R/W DVDs, etc. In some implementations, signal bearing medium 502 may encompass a communications medium 510, such as, but not limited to, a digital and/or an analog communication medium (e.g., a fiber optic cable, a waveguide, a wired communications link, a wireless communication link, etc.). Thus, for example, program product 500 may be conveyed to one or more modules of mobile operating server 110 by an RF signal bearing medium 502, where the signal bearing medium 502 is conveyed by a wireless communications medium 510 (e.g., a wireless communications medium conforming with the IEEE 802.11 standard).

[0050] Fig. 6 is a block diagram illustrating an example computing device that may be utilized to provide a scheme for connecting to a wireless local area network, arranged in accordance with at least some embodiments described herein. In these examples, elements of computing device 600 may be arranged or configured for a mobile operating server or an end device. In a very basic configuration 602, computing device 600 typically includes one or more processors 604 and a system memory 606. A memory bus 608 may be used for communicating between processor 604 and system memory 606.

[0051] Depending on the desired configuration, processor 604 may be of any type including but not limited to a microprocessor (μP), a microcontroller (μC), a digital signal processor (DSP), or any combination thereof. Processor 604 may include one more levels of caching, such as a level one cache 610 and a level two cache 612, a processor core 614, and registers 616. An example processor core 614 may include an arithmetic logic unit (ALU), a floating point unit (FPU), a digital signal processing core (DSP Core), or any combination thereof. An example memory controller 618 may also be used with processor 604, or in some implementations memory controller 618 may be an internal part of processor 604.

[0052] Depending on the desired configuration, system memory 606 may be of any type including but not limited to volatile memory (such as RAM), non-volatile memory (such as ROM, flash memory, etc.) or any combination thereof. System

memory 606 may include an operating system 620, one or more applications 622, and program data 624.

[0053] Computing device 600 may have additional features or functionality, and additional interfaces to facilitate communications between basic configuration 602 and any required devices and interfaces. For example, a bus/interface controller 630 may be used to facilitate communications between basic configuration 602 and one or more data storage devices 632 via a storage interface bus 634. Data storage devices 632 may be removable storage devices 636, non-removable storage devices 638, or a combination thereof. Examples of removable storage and non-removable storage devices include magnetic disk devices such as flexible disk drives and hard-disk drives (HDD), optical disk drives such as compact disk (CD) drives or digital versatile disk (DVD) drives, solid state drives (SSD), and tape drives to name a few. Example computer storage media may include volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data.

[0054] System memory 606, removable storage devices 636 and non-removable storage devices 638 are examples of computer storage media. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which may be used to store the desired information and which may be accessed by computing device 600. Any such computer storage media may be part of computing device 600.

[0055] Computing device 600 may also include an interface bus 640 for facilitating communication from various interface devices (e.g., output devices 642, peripheral interfaces 644, and communication devices 646) to basic configuration 602 via bus/interface controller 630. Example output devices 642 include a graphics processing unit 648 and an audio processing unit 650, which may be configured to communicate to various external devices such as a display or speakers via one or more A/V ports 652. Example peripheral interfaces 644 include a serial interface controller 654 or a parallel interface controller 656, which may be configured to communicate with external devices such as input devices (e.g., keyboard, mouse, pen, voice input device, touch input device, etc.) or other peripheral devices (e.g., printer, scanner, etc.) via

one or more I/O ports 658. An example communication device 646 includes a network controller 660, which may be arranged to facilitate communications with one or more other computing devices 662 over a network communication link via one or more communication ports 664.

[0056] The network communication link may be one example of a communication media. Communication media may typically be embodied by computer readable instructions, data structures, program modules, or other data in a modulated data signal, such as a carrier wave or other transport mechanism, and may include any information delivery media. A "modulated data signal" may be a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media may include wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, radio frequency (RF), microwave, infrared (IR) and other wireless media. The term computer readable media as used herein may include both storage media and communication media.

[0057] Computing device 600 may be implemented as a portion of a small-form factor portable (or mobile) electronic device such as a cell phone, a personal data assistant (PDA), a personal media player device, a wireless web-watch device, a personal headset device, an application specific device, or a hybrid device that include any of the above functions. Computing device 600 may also be implemented as a personal computer including both laptop computer and non-laptop computer configurations.

[0058] The present disclosure is not to be limited in terms of the particular embodiments described in this application, which are intended as illustrations of various aspects. Many modifications and variations can be made without departing from its spirit and scope, as will be apparent to those skilled in the art. Functionally equivalent methods and apparatuses within the scope of the disclosure, in addition to those enumerated herein, will be apparent to those skilled in the art from the foregoing descriptions. Such modifications and variations are intended to fall within the scope of the appended claims. The present disclosure is to be limited only by the terms of the appended claims, along with the full scope of equivalents to which such claims are entitled. It is to be understood that this disclosure is not limited to particular methods, reagents, compounds, compositions or biological systems, which

can, of course, vary. It is also to be understood that the terminology used herein is for the purpose of describing particular embodiments only, and is not intended to be limiting.

[0059] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

[0060] It will be understood by those within the art that, in general, terms used herein, and especially in the appended claims (e.g., bodies of the appended claims) are generally intended as "open" terms (e.g., the term "including" should be interpreted as "including but not limited to," the term "having" should be interpreted as "having at least," the term "includes" should be interpreted as "includes but is not limited to," etc.). It will be further understood by those within the art that if a specific number of an introduced claim recitation is intended, such an intent will be explicitly recited in the claim, and in the absence of such recitation no such intent is present. For example, as an aid to understanding, the following appended claims may contain usage of the introductory phrases "at least one" and "one or more" to introduce claim recitations. However, the use of such phrases should not be construed to imply that the introduction of a claim recitation by the indefinite articles "a" or "an" limits any particular claim containing such introduced claim recitation to embodiments containing only one such recitation, even when the same claim includes the introductory phrases "one or more" or "at least one" and indefinite articles such as "a" or "an" (e.g., "a" and/or "an" should be interpreted to mean "at least one" or "one or more"); the same holds true for the use of definite articles used to introduce claim recitations. In addition, even if a specific number of an introduced claim recitation is explicitly recited, those skilled in the art will recognize that such recitation should be interpreted to mean at least the recited number (e.g., the bare recitation of "two recitations," without other modifiers, means at least two recitations, or two or more recitations). Furthermore, in those instances where a convention analogous to "at least one of A, B, and C, etc." is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (e.g., "a system having at least one of A, B, and C" would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). In those instances

where a convention analogous to "at least one of A, B, or C, etc." is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (e.g., "a system having at least one of A, B, or C" would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). It will be further understood by those within the art that virtually any disjunctive word and/or phrase presenting two or more alternative terms, whether in the description, claims, or drawings, should be understood to contemplate the possibilities of including one of the terms, either of the terms, or both terms. For example, the phrase "A or B" will be understood to include the possibilities of "A" or "B" or "A and B."

[0061] In addition, where features or aspects of the disclosure are described in terms of Markush groups, those skilled in the art will recognize that the disclosure is also thereby described in terms of any individual member or subgroup of members of the Markush group.

[0062] As will be understood by one skilled in the art, for any and all purposes, such as in terms of providing a written description, all ranges disclosed herein also encompass any and all possible subranges and combinations of subranges thereof. Any listed range can be easily recognized as sufficiently describing and enabling the same range being broken down into at least equal halves, thirds, quarters, fifths, tenths, etc. As a non-limiting example, each range discussed herein can be readily broken down into a lower third, middle third and upper third, etc. As will also be understood by one skilled in the art all language such as "up to," "at least," and the like include the number recited and refer to ranges which can be subsequently broken down into subranges as discussed above. Finally, as will be understood by one skilled in the art, a range includes each individual member. Thus, for example, a group having 1-3 cells refers to groups having 1, 2, or 3 cells. Similarly, a group having 1-5 cells refers to groups having 1, 2, 3, 4, or 5 cells, and so forth.

[0063] From the foregoing, it will be appreciated that various embodiments of the present disclosure have been described herein for purposes of illustration, and that various modifications may be made without departing from the scope and spirit of the present disclosure. Accordingly, the various embodiments disclosed herein are not intended to be limiting, with the true scope and spirit being

indicated by the following claims.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No..... N/A
Filing Date.....April 22, 2015
Confirmation No. N/A
Inventorship..... Hyoung-Gon Lee
Group Art Unit N/A
Examiner N/A
Attorney Docket No. 2582-2.737BS
Title: SCHEMES FOR CONNECTING TO WIRELESS NETWORK

**INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §1.97 & 1.98**

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

Madam:

In the matter of the above-identified application, this Information Disclosure Statement is being submitted with the following citation as specified in 37 CFR §1.97(d).

"A copy of any patent, publication or other information listed in an Information Disclosure Statement is not required to be provided if it was previously cited by or submitted to the Office in a prior application, provided that the prior application is properly identified in the statement and relied upon for an earlier filing date under 35 U.S.C. §120."

Applicant(s) are submitting herewith a copy of Form PTO-1449 which list documents cited in parent application(s) Serial No. 13/885,754, filed May 16, 2013.

It is respectfully requested that this information disclosure statement be considered by the Examiner.

Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to the deposit account of BRUNDIDGE & STANGER, P.C., Deposit Account No. 50-4888 (2582-2.737BS) please credit any excess fees to such deposit account.

Respectfully submitted,

/Daniel J. Stanger/
Daniel J. Stanger
Registration No. 32,846
BRUNDIDGE & STANGER, P.C.

DJS/nac
(703) 684-1470

What is Claimed:

1. A method performed by a server, comprising:

providing, to a device, authenticated access point information regarding one or more authenticated access points controlled by the server; and

transmitting, to the device, a fake device identifier, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame in a search for at least one of the one or more authenticated access points around the device.

2. The method of Claim 1, wherein the one or more authenticated access points include a Wi-Fi access point.

3. The method of Claim 1, wherein the fake device identifier includes a fake media access control (MAC) address.

4. The method of Claim 1, wherein the authenticated access point information regarding the one or more authenticated access points includes at least one of a media access control (MAC) address or a service set identifier (SSID) of each of the one or more authenticated access points.

5. A method performed by an access point, comprising:

receiving, from a device, a probe request frame including a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

transmitting, to the device, a probe response frame including information regarding the access point;

receiving, from the device, a connection request including an authentic device identifier for the device; and

transmitting, to the device, an approval of the connection request.

6. The method of Claim 5, further comprising:

receiving, from the device, an association request;

transmitting, to the device, an association response to the association request; and

facilitating connection of the device to a communication network via the access point in accordance with the association response.

7. The method of Claim 6, wherein the access point includes a Wi-Fi access point, and the communication network includes a Wi-Fi network.

8. The method of Claim 5, wherein the access point includes at least one of an access point controlled by a mobile operating server or an access point previously connected with the end device.

9. The method of Claim 5, wherein the authentic device identifier includes a media access control (MAC) address.

10. The method of Claim 5, wherein the information regarding the access point includes at least one of a media access control (MAC) address of the access point or a service set identifier (SSID) of the access point.

11. A method performed by a device, comprising:

receiving, from a server, a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

transmitting, to at least one access point, a probe request frame including the fake device identifier;

receiving, from the at least one access point, a probe response frame including information regarding the at least one access point;

determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point; and

transmitting, to the at least one access point, a connection request including an authentic device identifier for the device.

12. The method of claim 11, wherein the fake device identifier includes a fake media access control (MAC) address.

13. The method of claim 11, wherein determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, further comprises:

determining that the at least one access point is under control of the server.

14. The method of claim 11, wherein determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, further comprises:

determining that the at least one access point is included in an authenticated access point list;

wherein the authenticated access point list is stored in a memory; and

wherein the authenticated access point list is received from the server.

15. The method of Claim 11, further comprising:

receiving, from the access point, an approval of the connection request;

transmitting, to the at least one access point, an association request;

receiving, from the at least one access point, an association response to the association request; and

connecting to a communication network via the access point in accordance with the association response.

16. A method performed by a device, comprising:

generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

transmitting, to at least one access point, a probe request frame including the fake device identifier;

receiving, from the at least one access point, a probe response frame including information regarding the at least one access point;

determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point; and

transmitting, to the at least one access point, a connection request including an authentic device identifier for the device.

17. The method of claim 16, wherein the fake device identifier includes a fake media access control (MAC) address.

18. The method of claim 16, wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point.

19. The method of claim 16, wherein determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, further comprises:

determining that the at least one access point was previously connected with the device.

20. The method of claim 16, wherein determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, further comprises:

determining that the at least one access point is included in an authenticated access point list received from a server and stored in a memory.

21. The method of claim 20, wherein determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, further comprises:

determining that the at least one access point is under control of the server.

22. The method of Claim 16, further comprising:

receiving, from the access point, an approval of the connection request;

transmitting, to the at least one access point, an association request;

receiving, from the at least one access point, an association response to the association request; and

connecting to a communication network via the access point in accordance with the association response.

23. A method performed by a device, comprising:

generating a collection including at least one of one or more random numbers or one or more random characters faking a device identifier for the device;

transmitting, in a search for at least one available access point around the device, a probe request frame including the random collection device identifier;

receiving, from at least one access point around the device, a probe response frame including information regarding the at least one access point;

determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point; and

transmitting, to the at least one access point, a connection request including an authentic device identifier for the device.

24. The method of Claim 23,

wherein generating a collection including at least one of one or more random numbers or one or more random characters faking a device identifier for the device, comprises configuring the collection as a fake media access control (MAC) address; and

wherein the random collection device identifier includes the fake media access control (MAC) address.

25. The method of claim 23, further comprising:

storing the random collection device identifier in a memory.

26. A system, comprising:

a processor;

at least one communication interface;

a transmitting unit to transmit, to at least one access point via the at least one communication interface, a probe request frame including a fake device identifier for a device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

a receiving unit to receive, from the at least one access point via the at least one communication interface, a probe response frame including information regarding the at least one access point;

memory to store the information regarding the at least one access point; and

a determination unit to determine, under control of the processor and based at least in part on the information regarding the at least one access point, whether the at least one access point is an authenticated access point;

wherein the transmitting unit is further to transmit, to the at least one access point, a connection request including an authentic device identifier for the device in response to the determination unit determining that the at least one access point is an authenticated access point.

27. The system of Claim 26, wherein the fake device identifier includes a fake media access control (MAC) address.

28. The system of Claim 26, further comprising:

a fake device identifier generating unit to generate, under control of the processor, the fake device identifier.

29. The system of Claim 26, wherein the fake device identifier is provided to the device via the receiving unit and stored in the memory.

30. The system of Claim 26, wherein the access point includes a Wi-Fi access point, and the communication interface is configured for communication with a Wi-Fi network.

31. The system of Claim 26,

wherein the determination unit is further to determine whether the at least one access point is included in an authenticated access point list stored in the memory; and

wherein the authenticated access point list is provided via the receiving unit.

ABSTRACT

Technology is disclosed for preventing classification of objects, e.g., in an augmented reality system. The technology can identify a set of objects to be classified, determine whether context information for one or more objects in the identified set of objects to be classified is identified as not to be employed during classification, and during classification of two different objects, include context information for one object but not the other.

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK			
First Named Inventor/Applicant Name:	Hyoung-Gon Lee			
Filer:	Daniel John Stanger/Nora Colston			
Attorney Docket Number:	2582-2.737BS			
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility application filing	1011	1	280	280
Utility Search Fee	1111	1	600	600
Utility Examination Fee	1311	1	720	720
Pages:				
Claims:				
Claims in Excess of 20	1202	11	80	880
Independent claims in excess of 3	1201	3	420	1260
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				3740

Electronic Acknowledgement Receipt

EFS ID:	22123989
Application Number:	14693400
International Application Number:	
Confirmation Number:	7248
Title of Invention:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK
First Named Inventor/Applicant Name:	Hyoung-Gon Lee
Customer Number:	86636
Filer:	Daniel John Stanger/Nora Colston
Filer Authorized By:	Daniel John Stanger
Attorney Docket Number:	2582-2.737BS
Receipt Date:	22-APR-2015
Filing Date:	
Time Stamp:	16:20:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$3740
RAM confirmation Number	3026
Deposit Account	504888
Authorized User	BRUNDIDGE, CARL I.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	2582-2_PoA.pdf	221707	no	2
			f304b49a92a7be1ef7890dc1289035bcd2e3c5b		
Warnings:					
Information:					
2	Drawings-only black and white line drawings	2582-2_Drawings.pdf	140630	no	6
			d2c4b795183cdc82c4728730e90b720d0f07f6e4		
Warnings:					
Information:					
3	Oath or Declaration filed	2582-2_Declaration.pdf	799666	no	1
			461067a90b9f7330788457412445af4c449e7ee8		
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	2582-2_IDS.pdf	613035	no	5
			4999365ae58dc473033d719bb80807204a32790b		
Warnings:					
Information:					
5	Application Data Sheet	2582-2_ADS.pdf	1503708	no	6
			d9a3ac510d98fddc7f2393f3069619ea8531a5ac		
Warnings:					
Information:					
6	Specification	2582-2_Specification.pdf	111723	no	16
			752d48762b11898b4b28ef005a8d47db1d0c2375		
Warnings:					
Information:					
7	Transmittal Letter	2582-2_IDSTransmittal.pdf	40130	no	2
			901fbb5cf54705addc5ea594ef23c00623cd16a		
Warnings:					
Information:					

8	Claims	2582-2_Claims.pdf	38708 03675d82ab8ec8ba5b6869817d24274aea db3f3	no	7
Warnings:					
Information:					
9	Abstract	2582-2_Abstract.pdf	14676 8fca6bbff5ddf54c7b51bbdd5848f09590ac 4733	no	1
Warnings:					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	38195 f3135d37bd8890acce465203db5d85fed9a 65bd4	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			3522178		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.					

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 14/693,400			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	600		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720		
TOTAL CLAIMS (37 CFR 1.16(j))	31	minus 20 = *	11			x 80 =	880		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	6	minus 3 = *	3			x 420 =	1260		
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 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).						0.00		
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00		
				TOTAL		TOTAL	3740		
* If the difference in column 1 is less than zero, enter "0" in column 2.									
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		x =	
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE		TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		x =	
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE		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 found in the appropriate box in column 1.									



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
14/693,400	04/22/2015	2111	3740	2582-2.737BS	31	6

CONFIRMATION NO. 7248

86636
BRUNDIDGE & STANGER, P.C.
2318 MILL ROAD, SUITE 1020
ALEXANDRIA, VA 22314

FILING RECEIPT



Date Mailed: 05/05/2015

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**

Inventor(s)

Hyoung-Gon LEE, Seoul, KOREA, REPUBLIC OF;

Applicant(s)

Empire Technology Development LLC, Wilmington, DE

Power of Attorney: The patent practitioners associated with Customer Number 86636

Domestic Priority data as claimed by applicant

This application is a CON of 13/885,754 05/16/2013
which is a 371 of PCT/US12/66306 11/21/2012

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 05/01/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/693,400**

Projected Publication Date: 08/13/2015

Non-Publication Request: No

Early Publication Request: No

Title

SCHEMES FOR CONNECTING TO WIRELESS NETWORK

Preliminary Class

710

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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 Assets Control, 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).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



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
14/693,400	04/22/2015	Hyoung-Gon LEE	2582-2.737BS

CONFIRMATION NO. 7248

86636
BRUNDIDGE & STANGER, P.C.
2318 MILL ROAD, SUITE 1020
ALEXANDRIA, VA 22314

PUBLICATION NOTICE



OC000000076852514

Title:SCHEMES FOR CONNECTING TO WIRELESS NETWORK

Publication No.US-2015-0230096-A1

Publication Date:08/13/2015

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 Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14693400
	Filing Date		2015-04-22
	First Named Inventor	Hyoung-Gon LEE	
	Art Unit	2431	
	Examiner Name	TBA	
	Attorney Docket Number	2582-2.737BS	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20120076072	A1	2012-03-29	Marc JALFON et al.	
	2	20070097904	A1	2007-05-03	Rajat MUKHERJEE et al.	
	3	20060150250	A1	2006-07-06	Sok LEE et al.	
	4	20120064912	A1	2012-03-15	Min-Taek OH	
	5	20050059416	A1	2005-03-17	Yoshihiro ONO	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14693400	
	Filing Date		2015-04-22	
	First Named Inventor	Hyoung-Gon LEE		
	Art Unit	2431		
	Examiner Name	TBA		
	Attorney Docket Number	2582-2.737BS		

6	20130301617	A1	2013-11-14	Matthias KUHN et al.	
---	-------------	----	------------	----------------------	--

If you wish to add additional U.S. Published Application citation information please click the Add button. [Add](#)

FOREIGN PATENT DOCUMENTS	Remove
---------------------------------	------------------------

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button [Add](#)

NON-PATENT LITERATURE DOCUMENTS	Remove
--	------------------------

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button [Add](#)

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	14693400
Filing Date	2015-04-22
First Named Inventor	HyounG-Gon LEE
Art Unit	2431
Examiner Name	TBA
Attorney Docket Number	2582-2.737BS

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Daniel J. Stanger/	Date (YYYY-MM-DD)	2015-10-14
Name/Print	Daniel J. Stanger	Registration Number	32846

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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.

Electronic Acknowledgement Receipt

EFS ID:	23776516
Application Number:	14693400
International Application Number:	
Confirmation Number:	7248
Title of Invention:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK
First Named Inventor/Applicant Name:	Hyoung-Gon LEE
Customer Number:	86636
Filer:	Daniel John Stanger/Beatriz Sanchez
Filer Authorized By:	Daniel John Stanger
Attorney Docket Number:	2582-2.737BS
Receipt Date:	14-OCT-2015
Filing Date:	22-APR-2015
Time Stamp:	15:01:02
Application Type:	Utility under 35 USC 111(a)

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	Information Disclosure Statement (IDS) Form (SB08)	KR-839496-03-US-CON_20151014_IDS.pdf	612492 83d3ae75b1df2cd11dc881e88edfd3b3d1a dae1e	no	4

Warnings:

Information:

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.
14/693,400	04/22/2015	Hyoung-Gon LEE	2582-2.737BS	7248

86636 7590 11/02/2016
BRUNDIDGE & STANGER, P.C.
2318 MILL ROAD, SUITE 1020
ALEXANDRIA, VA 22314

EXAMINER

GOODCHILD, WILLIAM J

ART UNIT	PAPER NUMBER
----------	--------------

2433

MAIL DATE	DELIVERY MODE
-----------	---------------

11/02/2016

PAPER

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.

Office Action Summary	Application No. 14/693,400	Applicant(s) LEE, HYOUNG-GON	
	Examiner WILLIAM GOODCHILD	Art Unit 2433	AIA (First Inventor to File) Status No

-- 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 MONTHS 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 04/22/2015.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
- 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) 1-31 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) 1-31 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 04/22/2015 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).

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)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) ☒ Notice of References Cited (PTO-892) | 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date <u>04/22/2015, 10/14/2015</u> | 4) ☐ Other: _____ |

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 04/22/2015 and 10/14/2015 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 103

3. The following is a quotation of pre-AIA 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, 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 negated by the manner in which the invention was made.

4. Claims 1-31 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Sinha et al., (US Publication No. 2008/0052779), hereinafter "Sinha", and further in view of Haverinen, (US Publication No. 2004/0078571).

Regarding claim 1, Sinha discloses

Art Unit: 2433

providing, to a device, authenticated access point information regarding one or more authenticated access points controlled by the server [Sinha, paragraphs 34 and 38]; transmitting, to the device, a fake device identifier [Sinha, paragraphs 34 and 38],

Sinha does not specifically disclose, however Haverinen teaches wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device [Haverinen, paragraph 191, random value].

It would have been obvious to one having ordinary skill in the art at the time the invention was made to include a random value in the device identifier in order to hide the real device id when accessing an access point when the user does not wish there device id to be known.

Sinha further discloses

in a probe request frame in a search for at least one of the one or more authenticated access points around the device [Sinha, paragraphs 34 and 38].

Regarding claims 2 and 12, Sinha-Haverinen further discloses

wherein the one or more authenticated access points include a Wi-Fi access point [Sinha, paragraphs 34 and 38].

Regarding claims 3, 17 and 27, Sinha-Haverinen further discloses

Art Unit: 2433

wherein the fake device identifier includes a fake media access control (MAC) address [Sinha, paragraphs 34 and 38].

Regarding claims 4 and 18, Sinha-Haverinen further discloses wherein the authenticated access point information regarding the one or more authenticated access points includes at least one of a media access control (MAC) address or a service set identifier (SSID) of each of the one or more authenticated access points [Sinha, paragraphs 34 and 38].

Regarding claim 5, Sinha-Haverinen further discloses receiving, from a device, a probe request frame including a fake device identifier for the device [Sinha, paragraphs 34 and 38], wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters [Haverinen, paragraph 191, random value]; transmitting, to the device, a probe response frame including information regarding the access point [Sinha, paragraphs 34 and 38]; receiving, from the device, a connection request including an authentic device identifier for the device [Sinha, paragraphs 34 and 38]; and transmitting, to the device, an approval of the connection request [Sinha, paragraphs 34 and 38].

Regarding claim 6, Sinha-Haverinen further discloses

Art Unit: 2433

receiving, from the device, an association request [Sinha, paragraphs 34 and 39];
transmitting, to the device, an association response to the association request [Sinha, paragraphs 34 and 38]; and
facilitating connection of the device to a communication network via the access point in accordance with the association response [Sinha, paragraphs 34 and 38].

Regarding claim 7, Sinha-Haverinen further discloses
wherein the access point includes a Wi-Fi access point, and the communication network includes a Wi-Fi network [Sinha, paragraphs 34 and 41].

Regarding claim 8, Sinha-Haverinen further discloses
wherein the access point includes at least one of an access point controlled by a mobile operating server or an access point previously connected with the end device [Sinha, paragraphs 34, 40 and 41].

Regarding claim 9, Sinha-Haverinen further discloses
wherein the authentic device identifier includes a media access control (MAC) address [Sinha, paragraphs 34 and 38].

Regarding claim 10, Sinha-Haverinen further discloses

Art Unit: 2433

wherein the information regarding the access point includes at least one of a media access control (MAC) address of the access point or a service set identifier (SSID) of the access point [Sinha, paragraphs 34, 38, 40 and 41].

Claims 11, 16, 23 and 26 are similar to and rejected for the same reasons as claims 1 and 5.

Regarding claim 13, Sinha-Haverinen further discloses determining that the at least one access point is under control of the server [Sinha, paragraph 67 and figure 6, access point connects devices to the server / network].

Regarding claim 14, Sinha-Haverinen further discloses determining that the at least one access point is included in an authenticated access point list [Sinha, paragraph 67 and figure 6]; wherein the authenticated access point list is stored in a memory [Sinha, paragraph 67 and figure 6]; and wherein the authenticated access point list is received from the server [Sinha, paragraph 67 and figure 6, obvious that the access point is under control of the server, within the network that it is connected to].

Regarding claims 15 and 22, Sinha-Haverinen further discloses

Art Unit: 2433

receiving, from the access point, an approval of the connection request [Sinha, paragraphs 34 and 38-41];

transmitting, to the at least one access point, an association request [Sinha, paragraphs 34 and 38-41];

receiving, from the at least one access point, an association response to the association request [Sinha, paragraphs 34 and 38-41]; and

connecting to a communication network via the access point in accordance with the association response [Sinha, paragraphs 34 and 38-41].

Regarding claim 19, Sinha-Haverinen further discloses determining that the at least one access point was previously connected with the device [Sinha, paragraphs 34, 38, 40 and 41].

Regarding claim 20, Sinha-Haverinen further discloses determining that the at least one access point is included in an authenticated access point list received from a server and stored in a memory [Sinha, paragraph 67].

Regarding claim 21, Sinha-Haverinen further discloses determining that the at least one access point is under control of the server [Sinha, paragraph 67].

Regarding claim 24, Sinha-Haverinen further discloses

Art Unit: 2433

wherein generating a collection including at least one of one or more random numbers or one or more random characters faking a device identifier for the device, comprises configuring the collection as a fake media access control (MAC) address [Sinha, paragraphs 34, 38-41]; and

wherein the random collection device identifier includes the fake media access control (MAC) address [Sinha, paragraphs 34, 38-41].

Regarding claim 25, Sinha-Haverinen further discloses storing the random collection device identifier in a memory [Sinha, paragraphs 34, 38-41].

Regarding claim 28, Sinha-Haverinen further discloses a fake device identifier generating unit to generate, under control of the processor, the fake device identifier [Sinha, paragraphs 34, 38-41].

Regarding claim 29, Sinha-Haverinen further discloses wherein the fake device identifier is provided to the device via the receiving unit and stored in the memory [Sinha, paragraphs 34, 38-41].

Regarding claim 30, Sinha-Haverinen further discloses

wherein the access point includes a Wi-Fi access point, and the communication interface is configured for communication with a Wi-Fi network [Sinha, paragraphs 34, 38-41].

Regarding claim 31, Sinha-Haverinen further discloses wherein the determination unit is further to determine whether the at least one access point is included in an authenticated access point list stored in the memory [S Sinha, paragraphs 34, 38-41]; and wherein the authenticated access point list is provided via the receiving unit [Sinha, paragraphs 34, 38-41].

Conclusion

Examiner's Note: Examiner has cited particular paragraphs / columns and line numbers in the reference(s) applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the cited passages as taught by the prior art or relied upon by the examiner.

Art Unit: 2433

Should applicant amend the claims of the claimed invention, it is respectfully requested that applicant clearly indicate the portion(s) of applicant's specification that support the amended claim language for ascertaining the metes and bounds of applicant's claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to WILLIAM GOODCHILD whose telephone number is (571)270-1589. The examiner can normally be reached on Monday - Friday / 8:00 AM - 4:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Pwu can be reached on (571) 272-6798. 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.

/WILLIAM GOODCHILD/

Application/Control Number: 14/693,400

Page 11

Art Unit: 2433

Primary Examiner, Art Unit 2433

Notice of References Cited	Application/Control No. 14/693,400		Applicant(s)/Patent Under Reexamination LEE, HYOUNG-GON	
	Examiner WILLIAM GOODCHILD		Art Unit 2433	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2011/0083165 A1	04-2011	Gopinath; K. N.	H04W48/04	726/4
*	B	US-2004/0078571 A1	04-2004	Haverinen, Henry	H04L9/0869	713/168
*	C	US-2008/0052779 A1	02-2008	Sinha; Amit	H04L63/1441	726/22
	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	CPC 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.

[Manage](#)
[Discover](#)
[Map](#)



[New Query](#)

Main Concept Text

false mac address random numbers character id...

[Filter](#)
[Discover](#)

[Save Query](#)

[Export Results](#)

[Quick Downloads](#)

[Views:](#)

[Sort:](#) [Relevance](#)

[Relevance Filter:](#) [None](#)

0 Selected Documents

[ACTIONS](#)

1 - 50

12,345,678 results

229,479 Results

[VIEW](#)

[COLLAPSE MENU](#)

1. Wireless LAN transmitting and receiving apparatus and key distribution method

Two stations in a wireless local area network generate a key from a shared key by generating respective proprietary random numbers, using the shared key to encrypt the communication data of the wireless LAN, making it difficult to identify the location of the information communication apparatus. By A wireless communication unit 5 for transmitting and receiving data, a MAC header generator...

CURRENT ASSIGNEES: LAPID SEMICON CO LTD
US2007018952B | US APPLICATIONS | 16-AUG-2007
2. Information communication device

The present invention also is illegally acquired MAC address included in the communication data of the wireless LAN, making it difficult to identify the location of the information communication apparatus. By A wireless communication unit 5 for transmitting and receiving data, a MAC header generator...

CURRENT ASSIGNEES: SHARP KK
JP2015002412A | JAPANESE APPLICATIONS | 05-JAN-2015
3. Schemes for connecting to wireless network

Technology is disclosed for preventing classification of objects, e.g., in an augmented reality system. The technology can identify a set of objects to be classified, determine whether context information for one or more objects in the identified set of objects to be classified is identified as not...

CURRENT ASSIGNEES: EMPIRE TECH DEV LLC
US20150230096 | US APPLICATIONS | 13-AUG-2015
4. Wireless lan encryption communications system

CURRENT ASSIGNEES: MITSUBISHI ELEC CORP
JP2007074369A | JAPANESE APPLICATIONS | 22-MAR-2007
5. Wireless lan transmission reception apparatus and key delivery method in wireless lan

PROBLEM TO BE SOLVED: To provide a technology of protecting the security by transmitting a random number configuring an encryption key in a form not easily confirmed by a third party. SOLUTION: A random number generating section 13 of a message frame generating circuit 10 generates a random number...

CURRENT ASSIGNEES: OKI ELEC IND CO LTD (- I)
JP2007221204A | JAPANESE APPLICATIONS | 30-AUG-2007
6. Wireless lan encryption communication system

CURRENT ASSIGNEES: MITSUBISHI ELEC CORP
JP2011064099A | JAPANESE APPLICATIONS | 06-JAN-2011
7. Method for verifying wireless local area network access point and station for the same

The invention claims a wireless local area network access point authentication method and site relates to communication field it is used to solve false the the ap sta user accessing illegal network to steal sta of the user information or control sta user to a method for the sta that the user suffers...

CURRENT ASSIGNEES: HUAWEI TECH CO LTD
CN103096301A | CHINESE APPLICATIONS | 08-MAY-2013
8. Wireless communication system and wireless communication method

CURRENT ASSIGNEES: 株式会社エーピー
JP5895678B2 | JAPANESE PATENTS | 30-MAR-2016
9. Wireless local area network access authentication service attack denial resisting method based on radio frequency tag

New Query Save Query Export Results Quick Downloads COLLAPSE MENU	This invention claims a based on radio frequency tag a wireless local area network access authentication method using service set identifier (SSID) attack method which mainly solves the problem that wireless local area network access authentication process in the denial of service attack it solves the problem of. The... CURRENT ASSIGNEES: KUNSHAN HUNOV INET XIDIAN UHV [+1] CN103596179A CHINESE APPLICATIONS 19-FEB-2014 16. Geographic tagging of network access points CURRENT ASSIGNEES: RICOH CO LTD EP2046084B1 EUROPEAN PATENTS 07-SEP-2016 11. Geographic tagging of network access points A system (100) for geographic tagging of network access points comprises a plurality of access points (104,106,108) that have been configured to provide location information as part of their beacon. Each access point (104,106,108) provides a service set identifier (SSID) that includes an encoded... CURRENT ASSIGNEES: RICOH CO LTD EP2046084A1 EUROPEAN APPLICATIONS 08-APR-2009 12. Communication system and communication device <P>PROBLEM TO BE SOLVED: To provide high security by preventing eavesdropping, an unauthorized use of an access point (AP), and impersonation of the AP in a wireless LAN system. <P>SOLUTION: Key information upon previous communication is recorded in an AP 101 and a terminal device (STA) 103 to be... CURRENT ASSIGNEES: 株式会社日立製作所 JP4550759B2 JAPANESE PATENTS 22-SEP-2010 13. Geographic tagging of network access points A system for geographic tagging of network access points comprises a plurality of access points that have been configured to provide location information as part of their beacon. Each access point provides a service set identifier (SSID) that includes an encoded value that represents the location of... CURRENT ASSIGNEES: RICOH CO LTD US20090088182 US APPLICATIONS 02-APR-2009 14. Geographic tagging of network access points A system for geographic tagging of network access points comprises a plurality of access points that have been configured to provide location information as part of their beacon. Each access point provides a service set identifier (SSID) that includes an encoded value that represents the location of... CURRENT ASSIGNEES: RICOH CO LTD US8265652 US PATENTS 11-SEP-2012 15. Protection for wireless devices against false access-point attacks Mechanisms and methods for providing a mobile/wireless device with protection against false access-point/base-station attacks using MAC address protection are presented. The mobile/wireless device known as mobile client (MC) gains access to wireless network by discovering and selectively associating... CURRENT ASSIGNEES: ALCATEL LUCENT SA EP1891791A1 EUROPEAN APPLICATIONS 27-FEB-2008 18. Protection for wireless devices against false access-point attacks Mechanisms and methods for providing a mobile/wireless device with protection against false access-point/base-station attacks using MAC address protection are presented. The mobile/wireless device known as mobile client (MC) gains access to wireless network by discovering and selectively associating... CURRENT ASSIGNEES: ALCATEL LUCENT SA EP1891791B1 EUROPEAN PATENTS 21-OCT-2009 17. Protection for wireless devices against false access-point attacks Mechanisms and methods for providing a mobile/wireless device with protection against false access-point/base-station attacks using MAC address protection are presented. The mobile/wireless device known as mobile client (MC) gains access to wireless network by discovering and selectively associating... CURRENT ASSIGNEES: ALCATEL SA WO200700404A1 WIPO APPLICATIONS 11-JAN-2007
--	---

STIC

New Query

Save Query

Export Results

Quick Downloads

COLLAPSE MENU

Manage
Discover
Map

18. Protection for wireless devices against false access-point attacks

Mechanisms and methods for providing a mobile/wireless device with protection against false access-point/base-station attacks using MAC address protection are presented. The mobile/wireless device known as mobile client (MC) gains access to wireless network by discovering and selectively associating...

CURRENT ASSIGNEES: ALCATEL LUCENT SA
US20060274643 | US APPLICATIONS | 07-DEC-2006

19. Geographically self-labeling access points

The present invention provides systems and methods for self-labeling access points with their geographic location from received beacon frames. In particular, the present invention transmits beacon frames including temporary location information from mobile devices. The beacon frames are received by...

CURRENT ASSIGNEES: RICOH CO LTD
US20090088183 | US APPLICATIONS | 02-APR-2009

20. Real user identity-oriented host moving method

The invention claims a surface of the real user identity of the main machine moving method the method comprises: Main machine from off-line state is connected to the first network the main machine with the first network identifier in the server carries out interaction to verify the host computer of...

CURRENT ASSIGNEES: UNIV TSINGHUA
CN102769621A | CHINESE APPLICATIONS | 07-NOV-2012

21. System and method for indicating a service set identifier

A method for securing communications between an access point and a station includes generating a first hashed service set identifier (SSID) by applying a first hash function to a first SSID known by the station (block 811), transmitting a first message to the access point, wherein the first message...

CURRENT ASSIGNEES: HUAWEI TECH CO LTD
EP2979401A1 | EUROPEAN APPLICATIONS | 03-FEB-2016

22. System and Method for Indicating a Service Set Identifier

A method for securing communications between an access point and a station includes generating a first hashed service set identifier (SSID) by applying a first hash function to a first SSID known by the station, transmitting a first message to the access point, wherein the first message includes the...

CURRENT ASSIGNEES: FUTUREWEI TECH INC
US20140337693 | US APPLICATIONS | 13-NOV-2014

23. Protection for wireless devices against false access-point attacks

Mechanisms and methods for providing a mobile/wireless device with protection against false access-point/base-station attacks using MAC address protection are presented. The mobile/wireless device known as mobile client (MC) gains access to wireless network by discovering and selectively associating...

CURRENT ASSIGNEES: ALCATEL LUCENT SA
US7782756 | US PATENTS | 24-AUG-2010

24. System and method for indicating a service set identifier

A method for securing communications between an access point and a station includes generating a first hashed service set identifier (SSID) by applying a first hash function to a first SSID known by the station (block 811), transmitting a first message to the access point, wherein the first message...

CURRENT ASSIGNEES: HUAWEI TECH CO LTD [+1]
WO2014182836A1 | WIPO APPLICATIONS | 13-NOV-2014

25. Geographically self-labeling access points

The present invention provides systems and methods for self-labeling access points with their geographic location from received beacon frames. In particular, the present invention transmits beacon frames including temporary location information from mobile devices. The beacon frames are received by...

CURRENT ASSIGNEES: RICOH CO LTD
US8711034 | US PATENTS | 29-APR-2014

26. Wireless communication apparatus, projector apparatus, wireless communication system, and wireless communication method each for use in wireless lan

Sample 26 RESULTS

Relevance View more relevance results

0 Results

18 Results

2002 Results

0 Results

0 Results

Publication Date View

Cur Assignee by Relevance View

LAPIC SEMICON CO LTD (7)

CHAPP KK (2)

EMPIRE TECH DEV LLC (2)

MITSUBISHI ELEC CORP (6)

OKE ELEC IND CO LTD (5)

HUAWEI TECH CO LTD (44)

株式会社日本... (6)

New Query	A wireless communication apparatus is for use in a wireless LAN, and performs wireless communication with an access point. The apparatuses each having a function of a wireless LAN relay. A network identification information storage unit stores predetermined network identification information indicating... CURRENT ASSIGNEES: PANASONIC IP MGMT CO LTD US20130657191 US APPLICATIONS 07-MAR-2013
Save Query	27. Real user identity-oriented host moving method The invention claims a surface of the real user identity of the main machine moving method the method comprises: Main machine from off-line state is connected to the first network the main machine with the first network identifier in the server carries out interaction to verify the host computer of... CURRENT ASSIGNEES: UNIV TSINGHUA CN102769621B CHINESE PATENTS 04-MAR-2015
Export Results	28. Applications for Geographically Coded Access Points The present invention provides systems and methods for self-labeling access points with their geographic location from received beacon frames. In particular, the present invention transmits beacon frames including temporary location information from mobile devices. The beacon frames are received by... CURRENT ASSIGNEES: RICOH CO LTD US20120162019 US APPLICATIONS 28-JUN-2012
Quick Downloads	29. False-AP detecting and blocking method, wireless device and router The invention claims a wireless network application field claims a pseudo ap detects blocking method wireless device and router through the broadcasting sending with the given to the field of beacon message receiving the periphery of the access point of broadcast beacon message judging whether the... CURRENT ASSIGNEES: ZHUHAI BETBOX INFO TECH CO LTD CN10365713A CHINESE APPLICATIONS 06-JUN-2016
COLLAPSE MENU	30. Applications for geographically coded access points The present invention provides systems and methods for self-labeling access points with their geographic location from received beacon frames. In particular, the present invention transmits beacon frames including temporary location information from mobile devices. The beacon frames are received by... CURRENT ASSIGNEES: RICOH CO LTD US9244149 US PATENTS 26-JAN-2016
	31. Using ridairekuto, the system and the method of controlling the access to network Radio local area network (WLAN) it is the mechanism which improves the access control of security and with the network the way, clear separate communication session with hot spot network and service provider network necessity do, interaction of the web browser is utilized. The method the Mobile... CURRENT ASSIGNEES: トムソン ライセンシング THOMSON LICENSING JP2007500976A JAPANESE APPLICATIONS 18-JAN-2007
	32. Protection for wireless devices against false access-point attacks The invention claims the use of the mac address to provide the protection protecting moving and wireless device from the virtual base station and access point attacking device and method for. Through the current and selectively and access point associated is called mobile client of the mobile or... CURRENT ASSIGNEES: SA ALCATEL CIT CN1874271B CHINESE PATENTS 30-MAR-2011
	33. Method of using geographic code, method of adding geographic code of network service provider, method of registering access point, and method of judging position of apparatus capable of detecting position CURRENT ASSIGNEES: RICOH CO LTD JP2009089396A JAPANESE APPLICATIONS 23-APR-2009
	34. Wireless terminal A wireless terminal stores shared information, which is shared in authentication processing executed between the wireless terminal and an authentication device when the wireless terminal logs on to a first base station. When the connection destination is to be switched from the first base station to...

STIC

New Query	CURRENT ASSIGNEES: FUJITSU LTD Management US20090264965 15-NOV-2009 STIC
Save Query	35. Protection for wireless devices against false access-point attacks The invention claims the use of the mac address to provide the protection protecting moving and wireless device from the virtual base station and access point attacking device and method for. Through the current and selectively and access point associated is called mobile client of the mobile or... CURRENT ASSIGNEES: SA ALCATEL CIT CN1874271A CHINESE APPLICATIONS 06-DEC-2006
Export Results	
Quick Downloads	
COLLAPSE MENU	36. Radio local network system with protection function and method for preventing offence A wireless local area network anti-attack method and application of it to the access point and of the mobile station in a network system said wireless local area network anti-attack method comprises: Through the access point is generated false media access control address; Through the access point... CURRENT ASSIGNEES: HONG FU HN PREC IND CO LTD CN101090331A CHINESE APPLICATIONS 19-DEC-2007 37. Wireless terminal A wireless terminal stores shared information, which is shared in authentication processing executed between the wireless terminal and an authentication device when the wireless terminal logs on to a first base station. When the connection destination is to be switched from the first base station to... CURRENT ASSIGNEES: FUJITSU LTD US20070264965 US APPLICATIONS 15-NOV-2007 38. Wireless terminal and authentication device A wireless terminal (2) stores shared information, i.e. a session key or connection key, which is shared in authentication processing executed between the wireless terminal and an authentication device (4) when the wireless terminal logs on to a first base station (3A). When the connection... CURRENT ASSIGNEES: FUJITSU LTD EP1841260A2 EUROPEAN APPLICATIONS 03-OCT-2007 39. Video game processing program, video game processing method, and video game processing device I will provide a processing program, such as a video game that realizes the character generation reliance on [issue] communication equipment is low. Video game processing program according to [SOLUTION] embodiment, by controlling the actions of the character to be displayed on the display screen of... CURRENT ASSIGNEES: GENIUS SCOPRETY KK JP2013153963A JAPANESE APPLICATIONS 15-AUG-2013 40. Applications for geographically coded access points Applications and uses for geographic coded of network access points includes a method for generating a geographic code and an associated graphical user-interface; a method for rejecting or filtering out geographic codes of inaccurately labeled access points; a method for using geographic codes as... CURRENT ASSIGNEES: RICOH CO LTD US20090085806 US APPLICATIONS 02-APR-2009 41. System and method for indicating service set identifier The invention claims a device for keeping access point and station the communication between the method of said method comprises: Through the first hash function applied to said station of the known first ssid generates the first hash service set identifier ssid block 811: Transmitting the first... CURRENT ASSIGNEES: HUAWEI TECH CO LTD CN105379190A CHINESE APPLICATIONS 02-MAR-2016 42. Method and Apparatus for Secure Communications in a Wireless Network A method and apparatus for secure communications between an access point and a station in a wireless network is provided. The station receives a first message from the access point in the wireless network, the first message includes a first hashed service set identifier (SSID) generated by the...

	CURRENT ASSIGNEES: SUTEL POWER TECH INC US8083793 DISCOVER INFORMATION NOV-2014
New Query	45. Applications for geographically coded access points Applications and uses for geographic coded of network access points includes a method for generating a geographic code and an associated graphical user-interface; a method for rejecting or filtering out geographic codes of inaccurately labeled access points; a method for using geographic codes as... CURRENT ASSIGNEES: RICOH CO LTD US8083405 US PATENTS 03-JAN-2012
Save Query	
Export Results	
Quick Downloads	
COLLAPSE MENU	44. Position detecting device and position detection method Applications and uses for geographic coded of network access points includes a method for generating a geographic code and an associated graphical user-interface; a method for rejecting or filtering out geographic codes of inaccurately labeled access points; a method for using geographic codes as... CURRENT ASSIGNEES: 株式会社日立... JP529874282 JAPANESE PATENTS 25-SEP-2013
	45. Method and system for preventing illegal access point in wireless local area network The invention claims a wireless local area network for preventing illegal access point method and system include: Access point controller for controlling one or more monitoring terminal to all access point sends the detecting message and the accessing point to control device in advance through the... CURRENT ASSIGNEES: ZTE CORP CN103067922A CHINESE APPLICATIONS 24-APR-2015
	46. Method and system for generating ip addresses of access terminals and transmitting messages for generation of ip addresses in an ip system The invention claims a method for sending and it is used for producing internet protocol version 6 the second ipv6 address of message system. The system comprises at least one access terminal access point and router. Access terminal sending comprises its own the mac address and fast address setting... CURRENT ASSIGNEES: SAMSUNG ELECT CO LTD CN1701584A CHINESE APPLICATIONS 23-NOV-2005
	47. Radio communication system and radio communication method I want to start the projection operation of the wireless terminal device that {problem} connection. A random number generator 15 for generating a BSSID a random number, and SSID generator 16 which generates an SSID, including unique identification information, wireless terminal device is [SOLUTION]... CURRENT ASSIGNEES: RICOH CO LTD JP2013222993A JAPANESE APPLICATIONS 28-OCT-2013
	48. Video game treatment program, video game treatment manner, and video game central processing unit < Topic >The treatment program and the like of the video game which implements the character generation whose degree of dependence to the communication equipment is low is offered. SolutionsThe video game treatment program which relates to execution configuration displays the character on the... CURRENT ASSIGNEES: ショース・ソノリテ株式会社 JP40510815681 JAPANESE PATENTS 26-DEC-2012
	49. Methods and Systems For Wired Equivalent Privacy and Wi-Fi Protected Access Protection Methods and systems for disrupting potential attacks on a wireless network through transmission of random data. CURRENT ASSIGNEES: AIRDEFENSE LLC US20080052779 US APPLICATIONS 28-FEB-2008
	50. Method and apparatus for transmitting and receiving a frame supporting a short MAC header in wireless LAN system Claims a method for the wireless lan wlan system for transmitting and receiving the short supports the mac header frame a method and device in wireless lan wlan system is used to encrypt mac protocol data unit mpdu method comprises: Through the first station sta structure comprises frame control...



	CURRENT ASSIGNEES: 15 IN NC INC
	MANAGE FORGERS DISCLOSE APPLICATIONS : 10 JUN 2015
New Query	Show next: 50 100 250 500 1000 Results
Save Query	
Export Results	
Quick Downloads	
COLLAPSE MENU	

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	243862	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:37
S2	20	("7808958", "7185204", "8005458").PN.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:53
S3	41	"20080052779" "20110083165" "20110314147" "20080043686" "20070286143" "20030221006" "20120221955" "20090235077" "20120210395" "20120311328" "20130179943" "20130281056"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:55
S4	12	"20080052779" "20110083165" "20110314147" "20080043686" "20070286143" "20030221006" "20120221955" "20090235077" "20120210395" "20120311328" "20130179943" "20130281056"	US-PGPUB	OR	ON	2016/10/27 07:58
S5	5	"20120076072" "2007007904" "20060150250" "20120064912" "20050059416" "20130301617"	US-PGPUB	OR	ON	2016/10/27 08:18
S6	6	"20120076072" "20070097904" "20060150250" "20120064912" "20050059416" "20130301617"	US-PGPUB	OR	ON	2016/10/27 08:18
S7	20015	((fake faked faking false) SAME (id MAC))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S8	243862	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S9	1627	S8 AND S7	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S10	2805	((fake faked faking false) NEAR3 (id MAC))	US-PGPUB; USPAT;	OR	ON	2016/10/27 15:58

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S11	272	S8 AND S10	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:59
S12	244067	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S13	2805	((fake faked faking false) NEAR3 (id MAC))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S14	188	S12 AND S13 AND (random rnd)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S15	74	((((fake faked faking false) NEAR3 (id MAC)) SAME (rnd random))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:42
S16	14	S12 AND S15	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:42
S17	76	("lee, hyoung-gon").IN.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 17:14

EAST Search History (Interference)

< This search history is empty >

10/ 31/ 2016 2:11:02 PM

C:\ Users\ wgoodchild\ Documents\ EAST\ Workspaces\ 14693400.wsp



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. 7248

SERIAL NUMBER 14/693,400	FILING or 371(c) DATE 04/22/2015 RULE	CLASS 726	GROUP ART UNIT 2433	ATTORNEY DOCKET NO. 2582-2.737BS		
APPLICANTS Empire Technology Development LLC, Wilmington, DE; INVENTORS Hyoung-Gon LEE, Seoul, KOREA, REPUBLIC OF; ** CONTINUING DATA ***** This application is a CON of 13/885,754 05/16/2013 which is a 371 of PCT/US12/66306 11/21/2012 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 05/01/2015						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and /WILLIAM J GOODCHILD/ Acknowledged Examiner's Signature		☐ Met after Allowance Initials	STATE OR COUNTRY KOREA, REPUBLIC OF	SHEETS DRAWINGS 6	TOTAL CLAIMS 31	INDEPENDENT CLAIMS 6
ADDRESS BRUNDIDGE & STANGER, P.C. 2318 MILL ROAD, SUITE 1020 ALEXANDRIA, VA 22314 UNITED STATES						
TITLE SCHEMES FOR CONNECTING TO WIRELESS NETWORK						
FILING FEE RECEIVED 3740	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			

Doc code: IDS

PTO/SB/08a (01-10)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2012. OMB 0651-0031

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2015-04-22
	First Named Inventor	Lee, Hyoung-Gon	
	Art Unit		
	Examiner Name	/William J. Goodchild/	
	Attorney Docket Number	2582-2.737BS	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/WJG/	1	7808958	B1	2010-10-05	Hernacki et al	
/WJG/	2	7185204	B2	2007-02-27	Narayanaswami et al	
/WJG/	3	8005458	B2	2011-08-23	Baik et al	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/WJG/	1	20080052779	A1	2008-02-28	Sinha et al	
/WJG/	2	20110083165	A1	2011-04-07	Gopinath et al	
/WJG/	3	20110314147	A1	2011-12-22	Whelan et al	

/William J. Goodchild/

10/27/2016

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number		14693400 - GAO: 243	
Filing Date		2015-04-22	
First Named Inventor	Lee, Hyoung-Gon		
Art Unit			
Examiner Name	/William J. Goodchild/		
Attorney Docket Number		2582-2.737BS	

/WJG/	4	20080043686	A1	2008-02-21	Sperti et al	
/WJG/	5	20070286143	A1	2007-12-13	Olson et al	
/WJG/	6	20030221006	A1	2003-11-27	Kuan et al	
/WJG/	7	20120221955	A1	2012-08-30	Raleigh et al	
/WJG/	8	20090235077	A1	2009-09-17	Cam Winget et al.	
/WJG/	9	20120210395	A1	2012-08-16	Cam Winget et al.	
/WJG/	10	20120311328	A1	2012-12-06	Wang et al.	
/WJG/	11	20130179943	A1	2013-07-11	Sun et al.	
/WJG/	12	20130281056	A1	2013-10-24	Abraham et al	

If you wish to add additional U.S. Published Application citation information please click the Add button. **Add**

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number			
Filing Date		2015-04-22	
First Named Inventor	Lee, Hyoung-Gon		
Art Unit			
Examiner Name	/William J. Goodchild/		
Attorney Docket Number		2582-2.737BS	

	1							☐
--	---	--	--	--	--	--	--	--------------------------

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
/WJG/	1	International Search Report from International Application No.: PCT/US12/66306 mailed Feb. 8, 2013.	☐
/WJG/	2	Singelee, et al., "Enabling Location Privacy in Wireless Personal Area Networks", 20 pages, Sept. 2006.	☐
/WJG/	3	Gruteser, et al., "Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis", Sept. 19, 2003, 10 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

Add

EXAMINER SIGNATURE

Examiner Signature	/William J. Goodchild/	Date Considered	10/27/2016
--------------------	------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

Doc code: IDS

PTO/SB/08a (01-10)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2012. OMB 0651-0031

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14693400
	Filing Date		2015-04-22
	First Named Inventor	Hyoung-Gon LEE	
	Art Unit	2431	
	Examiner Name	TBA /William J. Goodchild/	
	Attorney Docket Number	2582-2.737BS	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/WJG/	1	20120076072	A1	2012-03-29	Marc JALFON et al.	
/WJG/	2	20070097904	A1	2007-05-03	Rajat MUKHERJEE et al.	
/WJG/	3	20060150250	A1	2006-07-06	Sok LEE et al.	
/WJG/	4	20120064912	A1	2012-03-15	Min-Taek OH	
/WJG/	5	20050059416	A1	2005-03-17	Yoshihiro ONO	

/William J. Goodchild/

10/27/2016

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	14693400
Filing Date	2015-04-22
First Named Inventor	HyounG-Gon LEE
Art Unit	2431
Examiner Name	TBA /William J. Goodchild/
Attorney Docket Number	2582-2.737BS

/WJG/	6	20130301617	A1	2013-11-14	Matthias KUHN et al.	
-------	---	-------------	----	------------	----------------------	--

If you wish to add additional U.S. Published Application citation information please click the Add button. **Add**

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button. **Add**

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button. **Add**

EXAMINER SIGNATURE

Examiner Signature	/William J. Goodchild/	Date Considered	10/27/2016
--------------------	------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	14693400
Filing Date	2015-04-22
First Named Inventor	Hyoung-Gon LEE
Art Unit	2431
Examiner Name	TBA
Attorney Docket Number	2582-2.737BS

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Daniel J. Stanger/	Date (YYYY-MM-DD)	2015-10-14
Name/Print	Daniel J. Stanger	Registration Number	32846

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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.



false mac address random numbers characters id access point patent

Sign in

[All](#)
[Images](#)
[Shopping](#)
[Videos](#)
[News](#)
[More ▾](#)
[Search tools](#)

About 57,500 results (0.29 seconds)

How (and Why) to Change Your MAC Address on Windows, Linux ...
www.howtogeek.com/.../how-and-why-to-change-your-mac-address-on-windows-lin... ▾

Jun 30, 2014 - MAC stands for "media access control. ... You may need to change your router or computer's MAC address to connect. ... Apple's iOS 8 will use a random MAC address each time it scans for nearby ... Enable the Value option and enter your desired MAC address without any separating characters --- don't ...

Missing: **point patent****MAC Address in Windows: Change, Lookup, Spoofing**
www.thewindowsclub.com/change-mac-address-in-windows ▾

Apr 11, 2015 - How to change MAC Address in Windows 10 / 8.1 ... A MAC Address or Media Access Control Address is a unique identifier ... Also, unlike the four characters used in IP address per set, the MAC address ... That is the simplest method to change the MAC (Media Access Control) ID of the network adaptor.

Missing: **patent****Patent US20090088182 - Geographic tagging of network access ...**
<https://www.google.ch/patents/US20090088182> ▾ Google ▾

The use of an encoded location value in the SSID of the access point is particularly ... The method of claim 3 wherein the geographic code is 9 characters of the ... the location corresponding to the access point MAC address from the database. the locatable devices 102 by the association ID that the access point 104, 106 ...

MAC spoofing - Wikipedia
https://en.wikipedia.org/wiki/MAC_spoofing ▾ Wikipedia ▾

MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address that is hard-coded on a network interface controller (NIC) Main page · Contents · Featured content · Current events · Random article · Donate to Wikipedia ...

Missing: **character patent****Patent US8265652 - Geographic tagging of network access points ...**
<https://www.google.com/patents/US8265652> Google ▾

Sep 11, 2012 - Each access point provides a service set identifier (SSID) that includes ... wherein base 60 is a number system that uses 60 digits. ... The method of claim 2 wherein the geographic code is 9 characters of the service set identifier. location corresponding to the access point MAC address from the database.

Application # 2015/0230096. SCHEMES FOR ... - Patents.com
patents.com/us-20150230096.html

Apr 22, 2015 - Family ID: 1000001120852 ... The method of claim 1, wherein the authenticated access point information regarding ... at least one of one or more random numbers or one or more random characters; transmitting, ... as a fake media access control (MAC) address; and wherein the random collection device ...

RFC 5080 - Common Remote Authentication Dial In User Service ...
<https://tools.ietf.org/html/rfc5080> ▾ Internet Engineering Task Force ▾

by DB Nelson · 2007 · Cited by 48 · Related articles

Where an EAP-Message attribute is included in an Access-Challenge or ... solely on the end-point identifier information, such as phone number or Media Access Control ... implementing MAC address checking without using a Service-Type of Call ... characters", which is compatible with the description of Acct-Session-Id.

Patent US8046583 - Wireless terminal - Google Patents
www.google.com/gt/patents/US8046583

The method using MAC address and the method using mobile terminal ID are capable of ... of server authentication for identifying a false wireless LAN access point. ... in advance between a user and a server and dynamic random numbers. ... The access point 26 creates the encryption key (1) from the connection key (1). ...

Patent EP2912920A1 - Multiple access point name and ip service ...
<https://www.google.com.au/patents/EP2912920A1> Google ▾

A mobile device may communicate through multiple access point names ... The APN may be a character string that contains a reference to a Packet ... corresponding to the APN ID value and the 802.11 MAC address of this mobile device. ... to retrieve network information from memory (e.g., random access memory 610, etc.) ...

PDF ProCurve Wireless Access Point 530 - FTP Hp

<ftp://ftp.hp.com/pub/.../530-MgmtCig-May2006-5991-2193.pdf>  Hewlett-Packard

CLI: Configuring MAC Address Authentication - For example: ProCurve Access Point 530 (ethernet)ftp address password are used; character number 9 and above are ignored at log in. 3. VLAN ID: Sets the default VLAN ID for the SSID interface. 0 Warning conditions (e.g., return false, unexpected return).

Searches related to false mac address random numbers characters id access point patent

spoof mac address windows 8	how to change mac address in windows 10
spoof mac address windows 10	mac address changer windows 10
mac address spoofing windows 10	technitium mac address changer
spoof mac address windows 7	spoof mac address android

1 2 3 4 5 6 7 8 9 10 Next

Alexandria, VA - From your Internet address - Use precise location - Learn more

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)

Search Notes 	Application/Control No. 14693400	Applicant(s)/Patent Under Reexamination LEE, HYOUNG-GON
	Examiner WILLIAM GOODCHILD	Art Unit 2433

CPC- SEARCHED		
Symbol	Date	Examiner
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	10/31/2016	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	10/31/2016	WJG

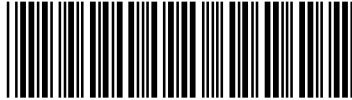
CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	004	10/31/2016	WJG

SEARCH NOTES		
Search Notes	Date	Examiner
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	10/31/2016	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	10/31/2016	WJG
Inventor search in PALM and EAST	10/31/2016	WJG
see IP.com search	10/31/2016	WJG
see Google search	10/31/2016	WJG
see EAST search	10/31/2016	WJG

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/WILLIAM GOODCHILD/ Primary Examiner.Art Unit 2433
--	---

<i>Index of Claims</i> 	Application/Control No. 14693400	Applicant(s)/Patent Under Reexamination LEE, HYOUNG-GON
	Examiner WILLIAM GOODCHILD	Art Unit 2433

✓	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	10/31/2016									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	✓									
	7	✓									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	✓									
	14	✓									
	15	✓									
	16	✓									
	17	✓									
	18	✓									
	19	✓									
	20	✓									
	21	✓									
	22	✓									
	23	✓									
	24	✓									
	25	✓									
	26	✓									
	27	✓									
	28	✓									
	29	✓									
	30	✓									
	31	✓									

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Hyoung-Gon Lee	Examiner:	Goodchild, William J
Appl. No.:	14/693,400	Art Unit:	2433
Filed:	April 22, 2015	Confirmation No.:	7248
		Docket No.:	2582-2.737BS

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

RESPONSE TO NON-FINAL OFFICE ACTION

Sir:

In response to the non-Final Office Action dated November 2, 2016, the following amendments and the accompanying remarks are submitted. Favorable consideration is respectfully requested. An Information Disclosure Statement is also submitted herewith. Consideration and acknowledgement of the documents associated with this Information Disclosure Statement is respectfully requested. This paper is submitted along with a Petition for one-month extension of time and the associated fee.

Amendments to the Specification begin on page 2.

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

Remarks begin on page 12.

Amendments to the Specification

The amendments to the specification are herein submitted. No new subject matter has been added.

Please amend the cross reference section on page 1 of the specification as follows:

CROSS-REFERENCE TO RELATED APPLICATIONS

This Application is a Continuation-~~Application~~ under 35 U.S.C. § 120 of U.S. ~~Application~~ Ser. No. 13/885,754, filed on May 16, 2013, which is a U.S. National Stage filing under 35 U.S.C. § 371 of ~~PCT-International Application~~ Ser. No. PCT/US12/66306, filed on November 21, 2012. The disclosures of both ~~applications~~-U.S. Application Ser. No. 13/885,754 and International Application Ser. No. PCT/US12/66306 are hereby incorporated herein by reference in their entireties.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

1. **(Currently Amended)** A method performed by a server, the method comprising:
providing, to a device, authenticated access point information regarding one or more authenticated access points controlled by the server; and
transmitting, to the device, a fake device identifier, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame in a search for at least one of the one or more authenticated access points around the device.

2. **(Original)** The method of Claim 1, wherein the one or more authenticated access points include a Wi-Fi access point.

3. **(Currently Amended)** The method of Claim 1, wherein the transmitting the fake device identifier includes transmitting a fake media access control (MAC) address.

4. **(Currently Amended)** The method of Claim 1, wherein the providing the authenticated access point information regarding the one or more authenticated access points includes providing at least one of a media access control (MAC) address or a service set identifier (SSID) of each of the one or more authenticated access points.

5. **(Currently Amended)** A method performed by an access point, the method comprising:

receiving, from a device, a probe request frame ~~including~~that includes a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

transmitting, to the device, a probe response frame ~~including~~that includes information regarding the access point;

receiving, from the device, a connection request ~~including~~that includes an authentic device identifier for the device; and

transmitting, to the device by the access point, an approval of the connection request, wherein the access point is controlled by a server.

6. **(Original)** The method of Claim 5, further comprising:

receiving, from the device, an association request;

transmitting, to the device, an association response to the association request; and

facilitating connection of the device to a communication network via the access point in accordance with the association response.

7. **(Currently Amended)** The method of Claim 6, wherein the access point includes a Wi-Fi access point, and wherein the communication network includes a Wi-Fi network.

8. **(Currently Amended)** The method of Claim 5, wherein the access point ~~includes at least one of an access point controlled by a mobile operating server or an access point was previously connected~~communicatively coupled with the ~~end~~ device.

9. **(Original)** The method of Claim 5, wherein the authentic device identifier includes a media access control (MAC) address.

10. **(Original)** The method of Claim 5, wherein the information regarding the access point includes at least one of a media access control (MAC) address of the access point or a service set identifier (SSID) of the access point.

11. **(Currently Amended)** A method performed by a device, the method comprising:
receiving, from a server, a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame;

transmitting, to at least one access point, ~~a~~ the probe request frame including that includes the fake device identifier;

receiving, from the at least one access point, a probe response frame ~~including that~~ includes information regarding the at least one access point;

determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point; and

transmitting, to the at least one access point, a connection request ~~including that includes~~ an authentic device identifier for the device.

12. **(Currently Amended)** The method of Claim 11, wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address.

13. **(Currently Amended)** The method of Claim 11, wherein the determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, ~~further~~ comprises:

determining that the at least one access point is under control of the server.

14. **(Currently Amended)** The method of Claim 11, wherein the determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, ~~further~~ comprises:

determining that the at least one access point is included in an authenticated access point list[[;]],

wherein the authenticated access point list is stored in a memory[[;]], and

wherein the authenticated access point list is received from the server.

15. **(Currently Amended)** The method of Claim 11, further comprising:
receiving, from the at least one access point, an approval of the connection request;
transmitting, to the at least one access point, an association request;
receiving, from the at least one access point, an association response to the association request; and

connecting to a communication network via the at least one access point in accordance with the association response.

16. **(Currently Amended)** A method performed by a device, the method comprising:

generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

transmitting, to at least one access point, a probe request frame ~~including that~~ includes the fake device identifier;

receiving, from the at least one access point, a probe response frame ~~including that~~ includes information regarding the at least one access point;

determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, wherein the determining includes determining that the at least one access point is under control of a server; and

transmitting, to the at least one access point, a connection request ~~including that~~ includes an authentic device identifier for the device.

17. **(Original)** The method of Claim 16, wherein the fake device identifier includes a fake media access control (MAC) address.

18. **(Original)** The method of Claim 16, wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point.

19. **(Currently Amended)** The method of Claim 16, wherein the determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, ~~further comprises~~ includes:

determining that the at least one access point was previously connected with the device.

20. **(Currently Amended)** The method of Claim 16, wherein the determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, ~~further comprises~~ includes:

determining that the at least one access point is included in an authenticated access point list received from ~~a~~ the server and stored in a memory.

21. **(Canceled)**

22. **(Currently Amended)** The method of Claim 16, further comprising:

receiving, from the at least one access point, an approval of the connection request;

transmitting, to the at least one access point, an association request;

receiving, from the at least one access point, an association response to the association request; and

connecting to a communication network via the at least one access point in accordance with the association response.

23. **(Currently Amended)** A method performed by a device, the method comprising:

generating a collection including at least one of one or more random numbers or one or more random characters ~~faking a~~ to provide a fake device identifier for the device so to falsely identify the device in a probe request frame;

transmitting, in a search for at least one available access point around the device, ~~a~~ the probe request frame ~~including that includes the random collection fake device identifier~~;

receiving, from at least one access point around the device, a probe response frame ~~including~~that includes information regarding the at least one access point;

determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point; and

transmitting, to the at least one access point, a connection request ~~including~~that includes an authentic device identifier for the device.

24. **(Currently Amended)** The method of Claim 23, wherein:

~~wherein the generating a~~ the collection including that includes at least one of one or more random numbers or one or more random characters ~~faking a device identifier for the device,~~ comprises configuring the collection as a fake media access control (MAC) address[[]], and

~~wherein the random collection fake~~ device identifier includes the fake media access control (MAC) address.

25. **(Currently Amended)** The method of Claim 23, further comprising:

storing the ~~random collection fake~~ device identifier in a memory.

26. **(Currently Amended)** A system, comprising:

a processor;

at least one communication interface;

a ~~transmitting unit~~transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame including a fake device identifier for a device,

wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

a ~~receiving unit~~ receiver to receive, from the at least one access point via the at least one communication interface, a probe response frame including information regarding the at least one access point;

a memory to store the information regarding the at least one access point; and

a determination unit to determine, under control of the processor and based at least in part on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of a server[[;]],

wherein the ~~transmitting unit is~~ transmitter further ~~to transmit,~~ transmits to the at least one access point, a connection request including an authentic device identifier for the device in response to a determination by the determination unit ~~determining~~ that the at least one access point is ~~an~~ the authenticated access point and is under control of the server.

27. **(Original)** The system of Claim 26, wherein the fake device identifier includes a fake media access control (MAC) address.

28. **(Currently Amended)** The system of Claim 26, further comprising:

a fake device identifier ~~generating~~ generation unit to generate, under control of the processor, the fake device identifier.

29. **(Currently Amended)** The system of Claim 26, wherein memory stores the fake device identifier ~~is provided to the device via the receiving unit and stored in the memory~~.

30. **(Currently Amended)** The system of Claim 26, wherein the at least one access point includes a Wi-Fi access point, and the at least one communication interface is configured for communication with a Wi-Fi network.

31. **(Currently Amended)** The system of Claim 26, wherein:
~~wherein~~ the determination unit ~~is further to determine~~ determines whether the at least one access point is included in an authenticated access point list stored in the memory[[;]], and
~~wherein~~ the authenticated access point list is provided via the ~~receiving unit~~ receiver.

REMARKS

Reconsideration and allowance of the above-identified application are respectfully requested. **Claims 1-20 and 22-31** are currently pending. **Claims 1, 3-5, 7, 8, 11-16, 19, 20, 22-26 and 28-31** are currently amended. **Claim 21** is canceled without prejudice. No new matter is added.

Claims 1-31 were rejected under pre-AIA 35 U.S.C. § 103(a) as allegedly being unpatentable over US Publication No. 2008/0052779 (hereafter “Sinha”) in view of US Publication No. 2004/0078571 (hereafter “Haverinen”)

The rejection of **Claims 1-20 and 22-31** is respectfully traversed for at least the reasons that follow.

A. Independent Claim 1

It is respectfully submitted that the combination of Sinha and Haverinen fails to teach or suggest all the claimed features as set forth in independent **Claim 1**.

For example, independent **Claim 1** recites (with emphasis added):

A method performed by a server, the method comprising:
providing, to a device, authenticated access point information regarding one or more authenticated access points controlled by the server; and
transmitting, to the device, a fake device identifier, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame in a search for at least one of the one or more authenticated access points around the device.

The Office Action, on pages 2 and 3, states:

Sinha discloses providing, to a device, authenticated access point information regarding one or more authenticated access points controlled by the server [Sinha, paragraphs 34 and 38];

transmitting, to the device, a fake device identifier [Sinha, paragraphs 34 and 38], Sinha does not specifically disclose, however Haverinen teaches wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device [Haverinen, paragraph 191, random value]. It would have been obvious to one having ordinary skill in the art at the time the invention was made to include a random value in the device identifier in order to hide the real device id when accessing an access point when the user does not wish there device id to be known.

In particular, the Office Action cites paragraphs [0034] and [0038] of Sinha for rejecting the above referenced recitation of independent **Claim 1**. It is respectfully submitted that the alleged points of rejection are incorrect.

Further, it is respectfully submitted that the paragraphs [0082] and [0083] of Sinha describe:

FIG. 9 illustrates an example embodiment of the present disclosure **to transmit random, fake frames along with valid frames to prevent decryption of the WEP key or WPA passphrase** on a wireless network. Client 425-3 transmits frames 1 through 7 to an AP 405, but a sensor 601 transmits random frames A, B among the transmission of frames 1 through 7. Additionally, Client 425-4 transmits frame 8 through 14 and the AP also transmits random frames C, D among the transmission of frames 8 through 14. The client's 425-3, 425-4 can filter out and ignore the random, fake frames. However, a rogue device 430 cannot differentiate between valid and random fake frames.

The rogue device 430 sniffs the transmitted frames including the valid frames 1-14 and the random, fake frames A, B, C, D. The rogue device 430 uses all sniffed frames for decrypting the WEP key or WPA passphrase. Here, **the random, fake frames A, B, C, D can throw off the decryption** such that the rogue device cannot break the WEP key or WPA passphrase. On WEP protected networks, the random, fake frames are specially crafted to look like valid data with a different encryption key. For WPA protected networks, the handshakes (i.e. EAPOL management frames) are forged instead of the data frames. (Emphasis added in original).

Sinha, in the above paragraphs, describes a method for protecting the existing WEP and WPA encryption by simulating random traffic. Further, Sinha describes transmitting fake frames crafted to look like valid data with a different encryption key along with the valid frame to prevent decryption of WEP key and WPA key.

Accordingly, Sinha, at best, describes transmitting random fake frames (presumably equated to the claimed “fake device identifier”) from a WLAN. Further, the transmission of fake frames in Sinha is intended towards protecting the existing WEP and WPA encryption by preventing decryption of WEP key or WPA passphrase by the rogue devices. However, Sinha fails to teach or suggest that the fake frames **falsely identify a device**. Accordingly, Sinha does not teach or suggest “*transmitting, to the device, a fake device identifier... to falsely identify the device in a probe request frame,*” as recited in independent **Claim 1**.

Further, the fake device identifier, as recited in independent **Claim 1**, is utilized by the device to falsely identify the device in a probe request frame in a search for at least one of the one or more authenticated APs. In comparison, Sinha does not teach or suggest such utilization of the fake frames. In particular, Sinha does not teach that either a rogue device or a client device, which receive the fake frames, uses the fake frames while connecting with an access point, for hiding its own identity. Therefore, Sinha completely fails to teach or suggest the above referenced recitation of independent **Claim 1**.

Additionally, the independent **Claim 1** recites “providing, to a device, authenticated access point information regarding one or more authenticated access points controlled by the server.”

In this regard, Sinha describes that access points (APs) and stations broadcast their presence by default and the APs send out beacon frames and relay information such as

timestamp, service set identifier (SSID), supported rates, power save information, among others. Client stations actively send out probe request frames to seek out other IEEE 802.11 devices available for association.

At best, Sinha describes that APs broadcast their information by sending out beacon frames.

Haverinen does not teach or suggest the above mentioned feature, thus failing to compensate for the deficiencies of Sinha, nor was Haverinen cited for that purpose.

Thus, the combination of Sinha and Haverinen fails to teach or suggest “...*providing, to a device, authenticated access point information regarding one or more authenticated access points controlled by the server, and transmitting, to the device, a fake device identifier*, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters *to falsely identify the device in a probe request frame* in a search for at least one of the one or more authenticated access points around the device.”

Therefore, it is respectfully requested that the rejection of **Claim 1** under 35 U.S.C. § 103(a) be withdrawn.

B. Independent Claim 5

It is respectfully submitted that the combination of Sinha and Haverinen fails to teach or suggest all the claimed features as set forth in amended independent **Claim 5**.

For example, independent **Claim 5** recites, in part (with emphasis added):

A method performed by an access point, the method comprising: ...
transmitting, by the access point, to the device, an approval of the connection request, wherein the access point is controlled by a server.

Independent **Claim 5** has been amended to incorporate features from dependent **Claim 8**.

With regards to **Claim 8**, the Office Action, at page 5, alleges that “Sinha-Haverinen further discloses wherein the access point includes at least one of an access point controlled by a mobile operating server or an access point previously connected with the end device [Sinha, paragraphs 34, 40 and 41].”

Reference Citations

Sinha, in paragraph [0041] recites:

In addition to tricking an unsuspecting user into connecting to their laptop, hackers have the benefit of taking advantage of the increasingly wireless-friendly nature of the Windows XP operating system. Due to the self-deploying nature of wireless, **a wireless laptop that is Wi-Fi enabled with continue to probe for APs it has been connected to in the past**. These probes can be picked up in the air by freely available wireless monitoring tools. If the Wireless Connection Manager in Windows XP (available from Microsoft Corp. of Redmond, Wash.) sees a legitimate SSID it will automatically re-connect to that AP. All the hacker has to do is give his soft AP a detected SSID.

Sinha merely describes that a wireless laptop will continue to probe for APs that it has been connected to in the past (presumably equated to “access point previously connected with the end device” by the Office Action). However, Sinha fails to teach or suggest “*wherein the access point is controlled by a server,*” as recited in amended independent **Claim 5**.

Further, it is respectfully submitted that Sinha’s description is directed towards disrupting potential attacks on a wireless network. Sinha describes that a masquerade attack steals an authorized user’s identity (MAC address) on the wireless network and a hacker can change his MAC address to a victim’s MAC address using a spoofing utility such as SMAC (Spoof MAC). Hence, the hacker bypasses any MAC address filtering, and can connect to the WLAN. Thus, in Sinha, disrupting the masquerade attack on the wireless network serves the intended purpose.

The Office Action, on page 3, alleges that “[i]t would have been obvious to one having ordinary skill in the art at the time the invention was made to include a random value in the device identifier in order to hide the real device id when accessing an access point when the user does not wish [their] device id to be known.”

In this regard, it is respectfully submitted that independent **Claim 5** teaches that the access point receives, from a device, a probe request frame including a fake device identifier for the device. Thus, modification of Sinha to include a fake identifier (ID_c) of Haverinen in the client’s “probe request frame” of Sinha will result in faking MAC ID of the client device and connecting to the WLAN, thereby resulting in a masquerade attack or spoofing. Since, Sinha’s intended purpose is to prevent masquerade attack or spoofing, the combination of Sinha with the cited teachings of Haverinen will render the invention of Sinha “unsatisfactory for its intended purpose.”

MPEP § 2143.01(V) states that “[i]f proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.”

Thus, it is respectfully submitted that there is no suggestion or motivation to a person of ordinary skill in the art to modify Sinha with Haverinen, as alleged by the Office Action. Thus, a prima facie case of obviousness has not been established in the rejection of independent **Claim 5**.

Therefore, it is respectfully requested that the rejection of **Claim 5** under 35 U.S.C. § 103(a) be withdrawn.

C. Independent Claims 16 and 26

It is respectfully submitted that Sinha and Haverinen fails to teach or suggest all the claimed features as set forth in amended independent **Claims 16 and 26**.

For example, independent **Claim 16** recites, in part (with emphasis added):

A method performed by a device, the method comprising:
...
determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, wherein the determining includes determining that the at least one access point is under control of the server.

This feature of amended independent **Claim 16** is in general analogous to above discussed feature of amended independent **Claim 5**. Hence, the remarks presented above for amended independent **Claim 5** apply analogously to amended independent **Claim 16**.

Amended independent **Claim 26** recites at least some of the features that are generally analogous to above discussed features of amended independent **Claim 16**, and the analysis discussed above with respect to amended independent **Claim 16** applies analogously to independent **Claim 26**.

Therefore, it is respectfully requested that the rejection of **Claims 16 and 26** under 35 U.S.C. § 103(a) be withdrawn.

D. Independent Claims 11 and 23

It is respectfully submitted that Sinha and Haverinen fails to teach or suggest all the claimed features as set forth in amended independent **Claims 11 and 23**.

For example, independent **Claim 11** recites, in part (with emphasis added):

A method performed by a device, the method comprising:
receiving, from a server, a fake device identifier for the device, wherein the fake device identifier includes at least one of

one or more random numbers or one or more random characters to falsely identify the device in a probe request frame

This feature of amended independent **Claim 11** is in general analogous to the above discussed feature of independent **Claim 1**. Hence, the remarks presented above for independent **Claim 1** apply analogously to amended independent **Claim 11**.

Amended independent **Claim 23** recites at least some of the features that are generally analogous to above discussed features of independent **Claim 11**, and the analysis discussed above with respect to independent **Claim 11** applies analogously to amended independent **Claim 23**.

Therefore, it is respectfully requested that the rejection of **Claims 11 and 23** under 35 U.S.C. § 103(a) be withdrawn.

E. Dependent Claims 2-4, 6-10, 12-15, 17-20, 22, 24, 25, and 27-31

Dependent **Claims 2-4, 6-10, 12-15, 17-20, 22, 24, 25, and 27-31** are also allowable at least by virtue of their dependency on respective independent **Claims 1, 5, 11, 16, 23 and 26**, which have been shown to be allowable above, and as well as for their additional claimed features. Therefore, it is respectfully requested that the rejection of **Claims 2-4, 6-10, 12-15, 17-20, 22, 24, 25, and 27-31** under pre-AIA 35 U.S.C. § 103(a) be withdrawn as well.

The rejection of **Claim 21** is rendered moot in view of the cancellation thereof.

Conclusion

Therefore, in light of at least the foregoing, it is respectfully believed that the present application is in condition for allowance. As a result, issuance of a Notice of Allowance for the pending claims is respectfully requested.

The Examiner's consideration of these Amendments and Remarks is appreciated and the Examiner is cordially invited to call the undersigned, should the Examiner have any questions, comments, or suggestions.

Please charge any fees that may be due to Deposit Account, 50-4888.

Respectfully submitted,

Brundidge & Stanger, P.C.

Date: March 02, 2017

By: /David S. Lee/
David S. Lee
Registration No. 38,222
Attorney of Record

Electronic Patent Application Fee Transmittal

Application Number:	14693400			
Filing Date:	22-Apr-2015			
Title of Invention:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK			
First Named Inventor/Applicant Name:	Hyoung-Gon LEE			
Filer:	David S. Lee/Mariah Duell			
Attorney Docket Number:	2582-2.737BS			
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
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:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension - 1 month with \$0 paid	1251	1	200	200
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				380

Electronic Acknowledgement Receipt

EFS ID:	28517232
Application Number:	14693400
International Application Number:	
Confirmation Number:	7248
Title of Invention:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK
First Named Inventor/Applicant Name:	Hyoung-Gon LEE
Customer Number:	86636
Filer:	David S. Lee/Mariah Duell
Filer Authorized By:	David S. Lee
Attorney Docket Number:	2582-2.737BS
Receipt Date:	02-MAR-2017
Filing Date:	22-APR-2015
Time Stamp:	15:39:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$380
RAM confirmation Number	030317INTEFSW15422700
Deposit Account	504888
Authorized User	Mariah Duell

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

Petitioner's Exhibit 1003 Page 119 of 285

37 CFR 1.19 (Document supply fees)
37 CFR 1.20 (Post Issuance fees)
37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	KR-839496-03-US-CON_20170302_IDS.pdf	1035332	no	4
			1448c795c9a2237dfeee808e82b9621f801477b4		
Warnings:					
Information:					
2	Extension of Time	KR-839496-03-US-CON_20170302_Petition_for_Extension.pdf	163422	no	2
			acf9514258cf0da9291e0a08554e9f7755728ccf		
Warnings:					
Information:					
3	Amendment/Req. Reconsideration-After Non-Final Reject	KR-839496-03-US-CON_20170302_FirstOA_Response.pdf	97230	no	20
			f1c805b4c020c0a475c3a15dd4e88cde1420b0d4		
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	32741	no	2
			38d4ea9797029920aa6a6f2f0b40799cc6898266		
Warnings:					
Information:					
Total Files Size (in bytes):			1328725		

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14693400
	Filing Date	2015-04-22
	First Named Inventor	HyounG-Gon Lee
	Art Unit	2433
	Examiner Name	William J Goodchild
	Attorney Docket Number	2582-2.737BS

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040264427	A1	2004-12-30	Jaakkola et al.	
	2	20070060128	A1	2007-03-15	Kil	
	3	20120201201	A1	2012-08-09	Liu et al.	
	4	20120230304	A1	2012-09-13	Barbu et al.	
	5	20130150012	A1	2013-06-13	Chhabra et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	14693400
Filing Date	2015-04-22
First Named Inventor	HyounG-Gon Lee
Art Unit	2433
Examiner Name	William J Goodchild
Attorney Docket Number	2582-2.737BS

6	20130176897	A1	2013-07-11	Wang et al.
---	-------------	----	------------	-------------

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	14693400
Filing Date	2015-04-22
First Named Inventor	Hyoung-Gon Lee
Art Unit	2433
Examiner Name	William J Goodchild
Attorney Docket Number	2582-2.737BS

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David S. Lee/	Date (YYYY-MM-DD)	2017-03-02
Name/Print	David S. Lee	Registration Number	38,222

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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.

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.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)		Docket Number (Optional) 2582-2.737BS
Application Number 14/693,400	Filed April 22, 2015	
For Hyoung-Gon Lee		
Art Unit 2433	Examiner GOODCHILD, WILLIAM J	

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	<u>Fee</u>	<u>Small Entity Fee</u>	<u>Micro Entity Fee</u>	
☒ One month (37 CFR 1.17(a)(1))	\$200	\$100	\$50	\$ <u>200.00</u>
☐ Two months (37 CFR 1.17(a)(2))	\$600	\$300	\$150	\$ _____
☐ Three months (37 CFR 1.17(a)(3))	\$1,400	\$700	\$350	\$ _____
☐ Four months (37 CFR 1.17(a)(4))	\$2,200	\$1,100	\$550	\$ _____
☐ Five months (37 CFR 1.17(a)(5))	\$3,000	\$1,500	\$750	\$ _____

☐ Applicant asserts small entity status. See 37 CFR 1.27.
☐ Applicant certifies micro entity status. See 37 CFR 1.29.
 Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.
☐ A check in the amount of the fee is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director has already been authorized to charge fees in this application to a Deposit Account.
☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to
 Deposit Account Number 50-4888.
☒ Payment made via EFS-Web.

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.

I am the

☐ applicant.
☒ attorney or agent of record. Registration number 38,222.
☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/David S. Lee/

Signature

March 02, 2017

Date

David S. Lee

Typed or printed name

(703) 684-1470

Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. 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 1.136(a). 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 6 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: Mail Stop PCT, 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 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.

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 14/693,400	Filing Date 04/22/2015	☒ To be Mailed
---	---	----------------------------------	--

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO**APPLICATION AS FILED – PART I**

(Column 1)

(Column 2)

FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	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 \$310 (\$155 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))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

(Column 1)

(Column 2)

(Column 3)

AMENDMENT	03/02/2017	CLAIMS REMAINING AFTER AMENDMENT	Minus	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 30	Minus	** 31	= 0	X \$80 =	0
	Independent (37 CFR 1.16(h))	* 6	Minus	***6	= 0	X \$420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
TOTAL ADD'L FEE						0	

(Column 1)

(Column 2)

(Column 3)

AMENDMENT	CLAIMS REMAINING AFTER AMENDMENT	Minus	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$ =
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =
	☐ Application Size Fee (37 CFR 1.16(s))					
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					
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.

LIE
ANGELA JOHNSON

This collection of information is required by 37 CFR 1.16. 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, 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.



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.
14/693,400	04/22/2015	Hyoung-Gon LEE	2582-2.737BS	7248

86636 7590 05/24/2017
BRUNDIDGE & STANGER, P.C.
2318 MILL ROAD, SUITE 1020
ALEXANDRIA, VA 22314

EXAMINER

GOODCHILD, WILLIAM J

ART UNIT	PAPER NUMBER
----------	--------------

2433

MAIL DATE	DELIVERY MODE
-----------	---------------

05/24/2017

PAPER

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.

Office Action Summary	Application No. 14/693,400	Applicant(s) LEE, HYOUNG-GON	
	Examiner WILLIAM GOODCHILD	Art Unit 2433	AIA (First Inventor to File) Status No

-- 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 MONTHS 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 03/02/2017.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
- 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) 1-20 and 22-31 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) 1-20 and 22-31 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).

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)).

** 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/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date 03/02/2017
- 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 4) ☐ Other: _____

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

Response to Arguments

2. Applicant's arguments with respect to claims 1-20 and 22-31 have been considered but are moot because the arguments do not apply to any of the references being used in the current rejection.
3. Applicant's arguments, filed 03/02/2017, with respect to claims 1-20 and 22-31 have been fully considered and are persuasive.

Claim Rejections - 35 USC § 103

4. The following is a quotation of pre-AIA 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, 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 negated by the manner in which the invention was made.

5. Claims 1-20 and 22-31 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Jalfon et al., (US Publication No. 2012/0076072), hereinafter "Jalfon",

Art Unit: 2433

and further in view of Mukherjee et al., (US Publication No. 2007/007904), hereinafter “Mukherjee”.

Regarding claim 1, Jalfon discloses

transmitting, to the device, a fake device identifier [Jalfon, paragraph 35, a response], wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame in a search for at least one or the one or more access points around the device [Jalfon, paragraphs 31 and 35].

Jalfon does not specifically disclose

providing, to a device, authenticated access point information regarding one or more authenticated access points controlled by the server.

However, Mukherjee teaches a list of allowed access points (authenticated by the server) that are stored on the wireless nodes [Mukherjee, paragraph 34].

It would have been obvious to one having ordinary skill in the art at the time the invention was made to include authenticated access points for the mobile devices use to ensure that access points are not hijacked or impersonated [Mukherjee, paragraph 33].

Regarding claim 2, Jalfon-Mukherjee further discloses

Art Unit: 2433

wherein the one or more authenticated access points include a Wi-Fi access point [Jalfon, paragraph 34].

Regarding claim 3, Jalfon-Mukherjee further discloses

wherein the transmitting the fake device identifier includes transmitting a fake media access control (MAC) address [Jalfon, paragraphs 31 and 35].

Regarding claim 4, Jalfon-Mukherjee further discloses

wherein the providing the authenticated access point information regarding the one or more authenticated access points includes providing at least one of a media access control (MAC) address or a service set identifier (SSID) of each of the one or more authenticated access points [Mukherjee, paragraph 34].

Regarding claim 5, Jalfon-Mukherjee further discloses

receiving, from a device, a probe request frame that includes a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters [Jalfon, paragraphs 31 and 35]; transmitting, to the device, a probe response frame that includes information regarding the access point [Jalfon, paragraph 35]; receiving, from the device, a connection request that includes an authentic device identifier for the device [Jalfon, paragraph 33]; and

Art Unit: 2433

transmitting, to the device by the access point, an approval of the connection request [Jalfon, paragraphs 31 and 33], wherein the access point is controlled by a server [Mukherjee, paragraph 34].

Regarding claim 6, Jalfon-Mukherjee further discloses receiving, from the device, an association request [Jalfon, paragraph 33]; transmitting to the device, an association response to the association request [Jalfon, paragraphs 33 and 35]; and facilitating connection of the device to a communication network via the access point in accordance with the association response [Jalfon, paragraphs 33 and 35].

Regarding claim 7, Jalfon-Mukherjee further discloses wherein the access point includes a Wi-Fi access point, and wherein the communication network includes a Wi-Fi network [Jalfon, paragraphs 34].

Regarding claim 8, Jalfon-Mukherjee further discloses wherein the access point was previously communicatively coupled with the end device [Mukherjee, paragraph 34].

Regarding claim 9, Jalfon-Mukherjee further discloses wherein the authentic device identifier includes a media access control (MAC) address [Jalfon, paragraphs 33-35].

Regarding claim 10, Jalfon-Mukherjee further discloses wherein the information regarding the access point includes at least one of a media access control (MAC) address of the access point or a service set identifier (SSID) of the access point [Mukherjee, paragraph 34].

Regarding claim 11, Jalfon-Mukherjee further discloses receiving, from a server [Mukherjee, paragraph 34], a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame [Jalfon, paragraphs 33 and 35]; transmitting, to at least one access point, the probe request frame that includes the fake device identifier [Jalfon, paragraphs 31 and 35]; receiving, from the at least one access point, a probe response frame that includes information regarding the at least one access point [Jalfon, paragraphs 31 and 35]; determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point [Mukherjee, paragraph 34]; and transmitting, to the at least one access point, a connection request that includes an authentic device identifier for the device [Jalfon, paragraphs 33-35].

Regarding claim 12, Jalfon-Mukherjee further discloses

Art Unit: 2433

wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address [Jalfon, paragraphs 33-35].

Regarding claim 13, Jalfon-Mukherjee further discloses determining that the at least one access point is under control of the server [Mukherjee, paragraph 34].

Regarding claim 14, Jalfon-Mukherjee further discloses determining that the at least one access point is included in an authenticated access point list [Mukherjee, paragraph 34], wherein the authenticated access point list is stored in a memory [Mukherjee, paragraph 34], and wherein the authenticated access point list is received from the server [Mukherjee, paragraph 34, the list is approved by the server].

Regarding claim 15, Jalfon-Mukherjee further discloses receiving, from the at least one access point, an approval of the connection request [Jalfon, paragraphs 33-35]; transmitting, to the at least one access point, an association request [Jalfon, paragraphs 33-35]; receiving, from the at least one access point, an association response to the association request [Jalfon, paragraphs 33-35]; and

Art Unit: 2433

connecting to a communication network via the at least one access point in accordance with the association response [Jalfon, paragraphs 33-35].

Regarding claim 16, Jalfon-Mukherjee further discloses
generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters [Jalfon, paragraphs 33-35];
transmitting, to at least one access point, a probe request frame that includes the fake device identifier [Jalfon, paragraphs 33-35];
receiving, from the at least one access point, a probe response frame that includes information regarding the at least one access point [Jalfon, paragraphs 33-35];
determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point, wherein the determining includes determining that the at least one access point is under control of a server [Mukherjee, paragraph 34]; and
transmitting, to the at least one access point, a connection request that includes an authentic device identifier for the device [Jalfon, paragraphs 33-35].

Regarding claim 17, Jalfon-Mukherjee further discloses
wherein the fake device identifier includes a fake media access control (MAC) address [Jalfon, paragraphs 33-35].

Regarding claim 18, Jalfon-Mukherjee further discloses wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point [Mukherjee, paragraph 34].

Regarding claim 19, Jalfon-Mukherjee further discloses determining that the at least one access point was previously connected with the device [Mukherjee, paragraph 34].

Regarding claim 20, Jalfon-Mukherjee further discloses determining that the at least one access point is included in an authenticated access point list received from the server and stored in a memory [Mukherjee, paragraph 34].

Regarding claim 22, Jalfon-Mukherjee further discloses receiving, from the at least one access point, an approval of the connection request [Jalfon, paragraphs 33-35]; transmitting, to the at least one access point, an association request [Jalfon, paragraphs 33-35]; receiving, from the at least one access point, an association response to the association request [Jalfon, paragraphs 33-35]; and connecting to a communication network via the at least one access point in accordance with the association response [Jalfon, paragraphs 33-35].

Regarding claim 23, Jalfon-Mukherjee further discloses generating a collection including at least one of one or more random numbers or one or more random characters to provide a fake device identifier for the device so to falsely identify the device in a probe request frame [Jalfon, paragraphs 33-35]; transmitting, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier [Jalfon, paragraphs 33-35]; receiving, from tat least one access point around the device, a probe response frame that includes information regarding the at least one access point [Jalfon, paragraphs 33-35]; determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point [Mukherjee, paragraph 34]; and transmitting, to the at least one access point, a connection request that includes an authentic device identifier for the device [Jalfon, paragraphs 33-35].

Regarding claim 24, Jalfon-Mukherjee further discloses wherein the generating the collection that includes at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address [Jalfon, paragraphs 33-35], and the fake device identifier includes the fake media access control (MAC) address [Jalfon, paragraphs 33-35].

Regarding claim 25, Jalfon-Mukherjee further discloses
storing the fake device identifier in a memory [Jalfon, paragraph 33-35].

Regarding claim 26, Jalfon-Mukherjee further discloses
a processor [Jalfon, paragraph 38];
at least one communication interface [Jalfon, paragraph 38];
a transmitter to transmit, to at least one access point via the at least one communication
interface, a probe request frame including a fake device identifier for a device, wherein
the fake device identifier includes at least one of the one or more random numbers or
one or more random characters [Jalfon, paragraphs 33-35];
a receiver to receive, from the at least one access point via the at least one
communication interface, a probe response frame including information regarding the at
least one access point [Jalfon, paragraphs 33-35];
a memory to store the information regarding the at least one access point [Mukherjee,
paragraph 34]; and
a determination unit to determine, under control of the processor and based at least in
part on the information regarding the at least one access point, whether the at least one
access point is an authenticated access point and under control of a server [Mukherjee,
paragraph 34];
wherein the transmitter further transmits to the at least one access point, a connection
request including an authentic device identifier of the device [Jalfon, paragraphs 33-35]

Art Unit: 2433

in response to a determination by the determination unit that the at least one access point is the authenticated access point and under control of the server [Mukherjee, paragraph 34].

Regarding claim 27, Jalfon-Mukherjee further discloses wherein the fake device identifier includes a fake media access control (MAC) address [Jalfon, paragraphs 33-35].

Regarding claim 28, Jalfon-Mukherjee further discloses a fake device identifier generation unit to generate, under control of the processor, the fake device identifier [Jalfon, paragraphs 33-35].

Regarding claim 29, Jalfon-Mukherjee further discloses wherein memory stores the fake device identifier [Jalfon, paragraphs 33-35].

Regarding claim 30, Jalfon-Mukherjee further discloses wherein the at least one access point includes a Wi-Fi access point, and the at least one communication interface is configured for communication with a Wi-Fi network [Jalfon, paragraphs 33-35].

Regarding claim 31, Jalfon-Mukherjee further discloses

Art Unit: 2433

wherein the determination unit further determines whether the at least one access point is included in an authenticated access point list stored in the memory [Mukherjee, paragraph 34], and the authenticated access point list is provided via the receiver [Mukherjee, paragraph 34].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to WILLIAM GOODCHILD whose telephone number is (571)270-1589. The examiner can normally be reached on Monday - Friday / 8:00 AM - 4:00 PM EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Pwu can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2433

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.

/WILLIAM GOODCHILD/
Primary Examiner, Art Unit 2433

Notice of References Cited	Application/Control No. 14/693,400		Applicant(s)/Patent Under Reexamination LEE, HYOUNG-GON	
	Examiner WILLIAM GOODCHILD		Art Unit 2433	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2008/0052779 A1	02-2008	Sinha; Amit	H04L63/1441	726/22
*	B	US-2007/0097904 A1	05-2007	Mukherjee; Rajat Pritam	H04W12/06	370/328
*	C	US-2011/0083165 A1	04-2011	Gopinath; K. N.	H04W48/04	726/4
*	D	US-2004/0078571 A1	04-2004	Haverinen, Henry	H04L9/0869	713/168
*	E	US-2012/0076072 A1	03-2012	JALFON; Marc	H04W12/02	370/328
	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	CPC 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.

Doc code: IDS

PTO/SB/08a (03-15)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2016. OMB 0651-0031

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14693400
	Filing Date	2015-04-22
	First Named Inventor	HyounG-Gon Lee
	Art Unit	2433
	Examiner Name	William J Goodchild
	Attorney Docket Number	2582-2.737BS

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/WJG/	1	20040264427	A1	2004-12-30	Jaakkola et al.	
/WJG/	2	20070060128	A1	2007-03-15	Kil	
/WJG/	3	20120201201	A1	2012-08-09	Liu et al.	
/WJG/	4	20120230304	A1	2012-09-13	Barbu et al.	
/WJG/	5	20130150012	A1	2013-06-13	Chhabra et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	14693400
Filing Date	2015-04-22
First Named Inventor	Hyoung-Gon Lee
Art Unit	2433
Examiner Name	William J Goodchild
Attorney Docket Number	2582-2.737BS

/WJG/	6	20130176897	A1	2013-07-11	Wang et al.
-------	---	-------------	----	------------	-------------

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/William J. Goodchild/	Date Considered	05/19/2017
--------------------	------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	14693400
Filing Date	2015-04-22
First Named Inventor	Hyoung-Gon Lee
Art Unit	2433
Examiner Name	William J Goodchild
Attorney Docket Number	2582-2.737BS

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David S. Lee/	Date (YYYY-MM-DD)	2017-03-02
Name/Print	David S. Lee	Registration Number	38,222

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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.

Search Notes 	Application/Control No. 14693400	Applicant(s)/Patent Under Reexamination LEE, HYOUNG-GON
	Examiner WILLIAM GOODCHILD	Art Unit 2433

CPC- SEARCHED		
Symbol	Date	Examiner
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	10/31/2016	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	10/31/2016	WJG

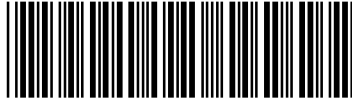
CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	004	10/31/2016	WJG

SEARCH NOTES		
Search Notes	Date	Examiner
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	10/31/2016	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	10/31/2016	WJG
Inventor search in PALM and EAST	10/31/2016	WJG
see IP.com search	10/31/2016	WJG
see Google search	10/31/2016	WJG
see EAST search	10/31/2016	WJG
updated EAST search	5/22/2017	WJG
see updated IP.com search	5/22/2017	WJG

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/WILLIAM GOODCHILD/ Primary Examiner.Art Unit 2433
--	---

<i>Index of Claims</i> 	Application/Control No. 14693400	Applicant(s)/Patent Under Reexamination LEE, HYOUNG-GON
	Examiner WILLIAM GOODCHILD	Art Unit 2433

✓	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	10/31/2016	05/22/2017						
	1	✓	✓						
	2	✓	✓						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	✓	✓						
	7	✓	✓						
	8	✓	✓						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	✓	✓						
	14	✓	✓						
	15	✓	✓						
	16	✓	✓						
	17	✓	✓						
	18	✓	✓						
	19	✓	✓						
	20	✓	✓						
	21	✓	-						
	22	✓	✓						
	23	✓	✓						
	24	✓	✓						
	25	✓	✓						
	26	✓	✓						
	27	✓	✓						
	28	✓	✓						
	29	✓	✓						
	30	✓	✓						
	31	✓	✓						

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	243862	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:37
S2	20	("7808958", "7185204", "8005458").PN.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:53
S3	41	"20080052779" "20110083165" "20110314147" "20080043686" "20070286143" "20030221006" "20120221955" "20090235077" "20120210395" "20120311328" "20130179943" "20130281056"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:55
S4	12	"20080052779" "20110083165" "20110314147" "20080043686" "20070286143" "20030221006" "20120221955" "20090235077" "20120210395" "20120311328" "20130179943" "20130281056"	US-PGPUB	OR	ON	2016/10/27 07:58
S5	5	"20120076072" "2007007904" "20060150250" "20120064912" "20050059416" "20130301617"	US-PGPUB	OR	ON	2016/10/27 08:18
S6	6	"20120076072" "20070097904" "20060150250" "20120064912" "20050059416" "20130301617"	US-PGPUB	OR	ON	2016/10/27 08:18
S7	20015	((fake faked faking false) SAME (id MAC))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S8	243862	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S9	1627	S8 AND S7	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S10	2805	((fake faked faking false) NEAR3 (id MAC))	US-PGPUB; USPAT;	OR	ON	2016/10/27 15:58

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S11	272	S8 AND S10	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:59
S12	244067	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S13	2805	((fake faked faking false) NEAR3 (id MAC))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S14	188	S12 AND S13 AND (random rnd)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S15	74	((((fake faked faking false) NEAR3 (id MAC)) SAME (rnd random))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:42
S16	14	S12 AND S15	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:42
S17	76	("lee, hyoung-gon").IN.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 17:14
S18	5	"20040264427" "20070060128" "20120201201" "20120230304" "20130150012"	US-PGPUB	OR	ON	2017/05/19 15:56
S19	6	"20040264427" "20070060128" "20120201201" "20120230304" "20130150012" "20130176897"	US-PGPUB	OR	ON	2017/05/19 15:56
S20	12	"2014081427"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/20 13:20
S21	280129	(726/004 H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20	US-PGPUB; USPAT;	OR	ON	2017/05/22 08:36

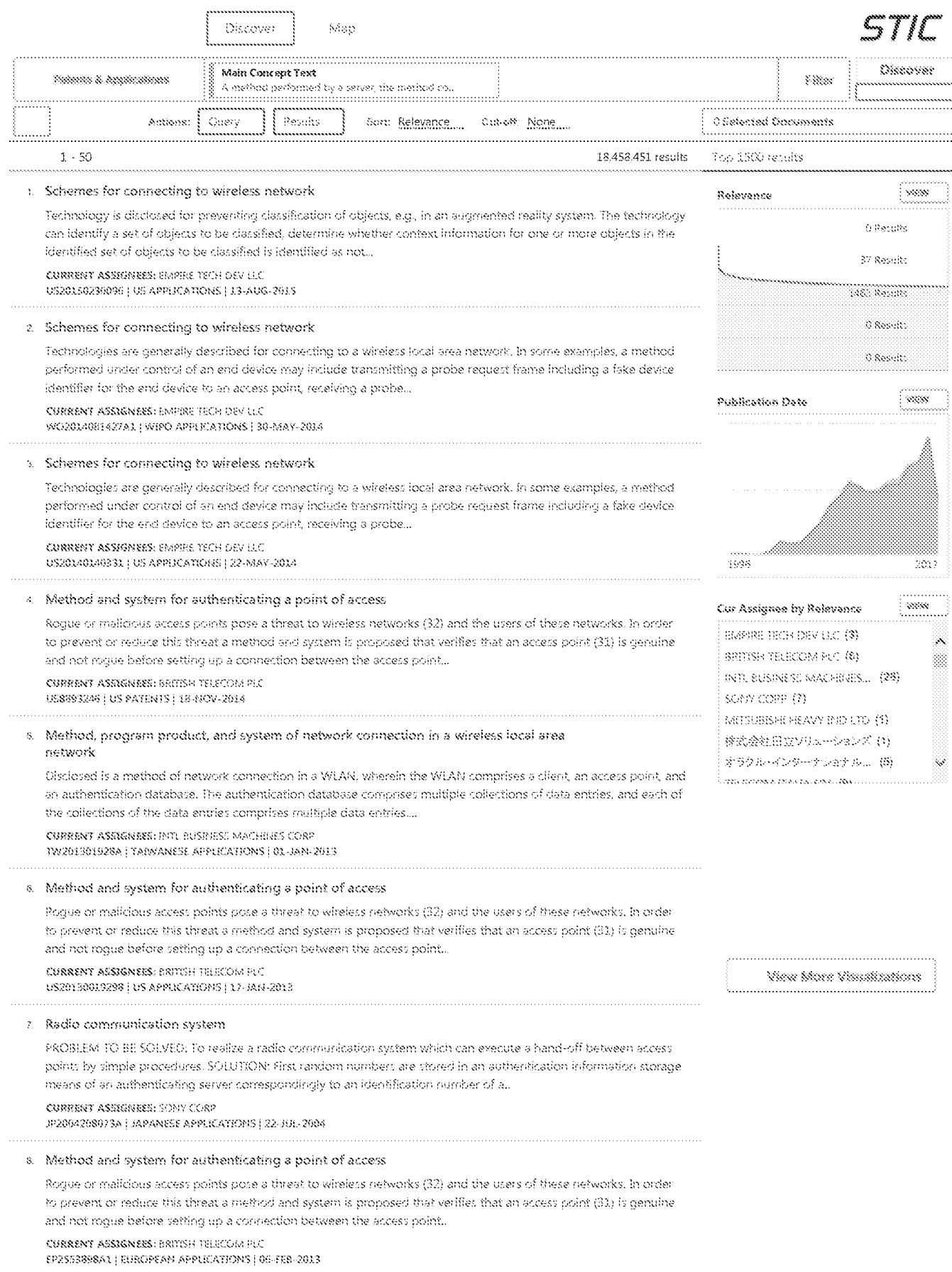
		H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00 H04L4/00).CLAS,OCLS,CPC,CPCL.	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S22	3346	((fake faked faking false dummy) SAME MAC)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 08:37
S23	852	((fake faked faking false dummy) NEAR5 MAC)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 08:38
S24	187	S21 AND S23	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 08:38
S25	42	((fake faked faking false dummy) NEAR5 MAC) AND (probe NEAR2 request)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 09:01
S26	31	S21 AND S25	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 09:01
S27	4002	(authenticated SAME access SAME point SAME information)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 12:59
S28	49	(authenticated NEAR5 ((access ADJ point) NEAR2 information))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 13:00
S29	646	(authentica\$6 NEAR5 ((access ADJ point) NEAR2 information))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:06
S30	6403	(authentica\$6 NEAR3 ((access ADJ point)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:07
S31	4520	(authentica\$6 NEAR2 ((access ADJ point)))	US-PGPUB; USPAT;	OR	ON	2017/05/22 14:07

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S32	1771	(authenticat\$6 NEAR2 ((access ADJ point))) SAME (information list)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:07
S33	700	(authenticat\$6 NEAR2 ((access ADJ point))) SAME server SAME (information list)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:13
S34	131	((authenticat\$6 NEAR2 (access ADJ point)) SAME server SAME (MAC NEAR2 address))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:24
S35	82	((authenticat\$6 NEAR2 (access ADJ point)) SAME server SAME (MAC NEAR2 address) SAME (information list))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:57
S36	3360	((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) SAME (send\$5 transmit\$5 request\$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 15:17
S37	1327	((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) NEAR4 (send\$5 transmit\$5 request\$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 15:18
S38	1013	((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) NEAR2 (send\$5 transmit\$5 request\$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 15:18
S39	117	((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) NEAR2 (send\$5 transmit\$5 request\$5) NEAR2 server)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 15:37

EAST Search History (Interference)

< This search history is empty >

5/ 22/ 2017 7:44:44 PM
C:\ Users\ wgoodchild\ Documents\ EAST\ Workspaces\ 14693400.wsp



STIC

9. Method and system for authenticating a point of access

Discover Map
Rogue or malicious access points pose a threat to wireless networks (32) and the users of these networks. In order to prevent or reduce this threat a method and system is proposed that verifies that an access point (31) is genuine and not rogue before setting up a connection between the access point..

CURRENT ASSIGNEES: BRITISH TELECOM PLC
WO2011121294A1 | WIFG APPLICATIONS | 06-OCT-2011

10. User authentication system, authentication server and network user authentication method

CURRENT ASSIGNEES: MITSUBISHI HEAVY IND LTD
JP2008287321A | JAPANESE APPLICATIONS | 27-NOV-2008

11. Being keyboard entry supervisory module and

CURRENT ASSIGNEES: 株式会社日立ソリューションズ
JP4979127B2 | JAPANESE PATENTS | 18-JUL-2012

12. Decryption and online data encryption

Data transmitted in a computer network implementation, system and method for performing at the time of input into the computer of a user, the encryption and decryption of user authentication identifier data such as a password, preferably. The system and method, from one of the elements that are...

CURRENT ASSIGNEES: オラクル・インターナショナル・コーポレーション
JP200924881A | JAPANESE APPLICATIONS | 02-JUL-2009

13. Method and system for authenticating a point of access

Rogue or malicious access points pose a threat to wireless networks (32) and the users of these networks. In order to prevent or reduce this threat a method and system is proposed that verifies that an access point (31) is genuine and not rogue before setting up a connection between the access point..

CURRENT ASSIGNEES: BRITISH TELECOM PLC
EP2372971A1 | EUROPEAN APPLICATIONS | 05-OCT-2011

14. Methods and software program product for mutual authentication in a communications network

A method for mutual authentication between a subscriber and a communications network, in which a random number is generated at the subscriber's terminal (1, 1'). The random number is sent to the authentication sub-system (6, 6') managing the authentication of the subscriber for the access to the...

CURRENT ASSIGNEES: TELECOM ITALIA SPA
EP1602194B1 | EUROPEAN PATENTS | 23-JUL-2008

15. Computer-implemented authentication method

Data sent SOLVED] computer implemented network, preferably to provide a system and method for performing at the time of input to the computer of the user, the encryption and decryption of user authentication identifier data such as a password. From one of the elements that are randomly placed on a...

CURRENT ASSIGNEES: ORACLE INTERNATL CORP
JP2012185845A | JAPANESE APPLICATIONS | 27-SEP-2012

16. Method, Program Product, and System of Network Connection in a Wireless Local Area Network

Disclosed is a method of network connection in a wireless local area network. The wireless local area network comprises a client, an access point, and an authentication database coupled to the access point. The authentication database comprises a plurality of collections of data entries, wherein...

CURRENT ASSIGNEES: INTL BUSINESS MACHINES CORP
US20130007843 | US APPLICATIONS | 03-JAN-2013

17. Online data encryption and decryption

The invention claims a method for the input to the user computer in time in the computer realizes the network the transmission of data is preferably a user authentication identifier data such as password the invention claims the encryption and decryption system and method for. The system and method..

CURRENT ASSIGNEES: BHAROSA INC
CN191601222A | CHINESE APPLICATIONS | 09-DEC-2009

18. Computer-implemented authentication interface system

CURRENT ASSIGNEES: ORACLE INTERNATL CORP
JP2012185844A | JAPANESE APPLICATIONS | 27-SEP-2012

19. Mutual authentication methods and software programs in a communication network

CURRENT ASSIGNEES: テレコム・イタリア・エッセ・ゼー・アール
JP4898427B2 | JAPANESE PATENTS | 14-MAR-2012

STIC

20. Software program product and method for mutual authentication in a communication network

Discover Map

Method for mutual authentication of the communication network with the subscriber to generate a random number and a subscriber terminal at (1, 1'). For example, together with the identifier of the subscriber, this random number is sent to the (6, 6') authentication subsystem that manages the...

CURRENT ASSIGNEES: タイム・イタリア・エッセ・ビー・アー
JP2006022514A | JAPANESE APPLICATIONS | 28-SEP-2006

21. Online data encryption and decryption

The invention claims a method for the input to the user computer in time in the computer realizes the network the transmission of data is preferably a user authentication identifier data such as password the invention claims the encryption and decryption system and method for. The system and method...

CURRENT ASSIGNEES: BHAROSA INC US
CN101501222B | CHINESE PATENTS | 03-APR-2013

22. For identifying fake of the base station method and device for

The embodiment of this invention claims a method for identifying false of the base station method and device used for effectively identifying false base station the method comprises: The terminal in gsm network base station time to the base station corresponding to the network side equipment...

CURRENT ASSIGNEES: HUAWEI TECH CO LTD
CN106028331A | CHINESE APPLICATIONS | 12-OCT-2016

23. Online data encryption and decryption

Is realized by computer network is transmitted by the data providing encryption and decryption system and method for better method is input to the user computer is such as password a user authentication identifier the invention claims a data encryption and decryption. Said system and method for...

CURRENT ASSIGNEES: BHAROSA INC
CN101627630A | CHINESE APPLICATIONS | 29-AUG-2007

24. Method for verifying wireless local area network access point and station for the same

The invention claims a wireless local area network access point authentication method and site relates to communication field it is used to solve false the the ap sta user accessing illegal network to steal sta of the user information or control sta user to a method for the sta that the user suffers...

CURRENT ASSIGNEES: HUAWEI TECH CO LTD
CN103096301A | CHINESE APPLICATIONS | 08-MAY-2013

25. Wireless local area network access point authentication method and site

The invention claims a wireless local area network access point authentication method and site relates to communication field it is used to solve false the the ap sta user accessing illegal network to steal sta of the user information or control sta user to a method for the sta that the user suffers...

CURRENT ASSIGNEES: HUAWEI TECH CO LTD
CN103096301B | CHINESE PATENTS | 12-APR-2017

26. Computer-implemented authentication method

CURRENT ASSIGNEES: オラクル・インターナショナル・コーポレーション
JP5297483B2 | JAPANESE PATENTS | 17-JUL-2013

27. Method and software program product for mutual authentication in a communications network

A method for mutual authentication between a subscriber and a communications network, in which a random number is generated at the subscriber's terminal. The random number is sent to the authentication sub-system managing the authentication of the subscriber for the access to the network, e.g....

CURRENT ASSIGNEES: TIM ITALIA SPA
US20060189298 | US APPLICATIONS | 24-AUG-2006

28. Method and software program product for mutual authentication in a communications network

A method for mutual authentication between a subscriber and a communications network, in which a random number is generated at the subscriber's terminal (1, 1'). The random number is sent to the authentication sub-system (5, 6') managing the authentication of the subscriber for the access to the...

CURRENT ASSIGNEES: TELECOM ITALIA MOBILE SPA
WO200407995A1 | WFO APPLICATIONS | 16-SEP-2004

29. Method and software program product for mutual authentication in a communications network

STIC

A method for mutual authentication between a subscriber and a communications network, in which a random number is generated at the subscriber's terminal. The random number is sent to the authentication sub-system managing the authentication of the subscriber for the access to the network, e.g.,...

CURRENT ASSIGNEES: TIM ITALIA SPA
US7251293 | US PATENTS | 12-JUN-2007

30. Method for increasing network plaintext authentication security

The invention claims a method for increasing network ming-wen authentication security method for. Firstly the method in wireless local area network built in the basic service set which comprises user terminal wireless access point and authenticating server. The learning table establishing. And then...

CURRENT ASSIGNEES: HONG FU JIN PREC IND CO LTD (+1)
CN1885858 | CHINESE PATENTS | 04-MAY-2011

31. Methods and software program product for mutual authentication in a communications network

A method for mutual authentication between a subscriber and a communications network, in which a random number is generated at the subscriber's terminal (1, 1'). The random number is sent to the authentication sub-system (5, 6') managing the authentication of the subscriber for the access to the...

CURRENT ASSIGNEES: TELECOM ITALIA SPA
EP1602194A1 | EUROPEAN APPLICATIONS | 07-DEC-2005

32. Device and process for wireless local area network association

The present invention concerns WLAN association device and process for associating a new station to a WLAN, via a central apparatus. The association device comprises receiving and sending means for exchanging signals between the station and central apparatus, recording means for recording the...

CURRENT ASSIGNEES: THOMSON LICENSING
US7941122 | US PATENTS | 10-MAY-2011

33. For preventing false device of wifi system and its safety verification method

The invention claims a special network system the invention claims a it can prevent the anti-counterfeiting device of wifi system comprises router authentication server and is matched with the user terminal authentication each route of the writing and its basid related to the authenticating...

CURRENT ASSIGNEES: XIAN HAN JU NETWORK SCIENCE & TECH CO LTD
CN106162644A | CHINESE APPLICATIONS | 23-NOV-2016

34. Wireless security based client automatic connection protecting method and system

The invention claims a based on wireless safe to the client computer is connected with the automatic protection method comprises: Step 1: Obtaining to be identified is connected to the object information wherein said to be identified is connected to the object information comprises a base station...

CURRENT ASSIGNEES: DUNYU SHANGHAI INFO TECH CO LTD
CN105101210A | CHINESE APPLICATIONS | 25-NOV-2015

35. The server device, through authentication manner

CURRENT ASSIGNEES: 沖電気工業株式会社
JP5176629B2 | JAPANESE PATENTS | 03-APR-2013

36. Methods and Systems For Wired Equivalent Privacy and Wi-Fi Protected Access Protection

Methods and systems for disrupting potential attacks on a wireless network through transmission of random data.

CURRENT ASSIGNEES: EXTREME NETWORKS INC
US20080052779 | US APPLICATIONS | 26-FEB-2008

37. Method and system of providing access point data associated with a network access point

A method includes sending a faked authentication request from a client device wherein the faked authentication request includes identification credentials. A faked authentication request indicates that a reply message in response to the faked authentication request is to include data for updating a...

CURRENT ASSIGNEES: IPACS INC
US20140082714 | US APPLICATIONS | 20-MAR-2014

38. Method and device for secure wireless transmission of information

Method and device for secure wireless transmission of information from a sender to a receiver. A sending device is arranged for obtaining a message, a sender identity and a receiver identity and includes encryption means for encrypting the message to be transmitted. A transmission channel is...

CURRENT ASSIGNEES: ANOTO AB
WO2001095599A1 | WIFO APPLICATIONS | 13-DEC-2001

39. Methods and software program product for mutual authentication in a communications network

STIC

A method for mutual authentication between a subscriber and a communications network, in which a random number is generated at the subscriber's terminal (1, 104). The random number is sent to the authentication sub-system (5, 6-) managing the authentication of the subscriber for the access to the...

CURRENT ASSIGNEES: TIM ITALIA SPA
CA2518032C | CANADIAN PATENTS | 17-JUL-2012

40. Computer-implemented authentication interface system

CURRENT ASSIGNEES: オラクル・インターナショナル・コーポレーション
JP5023075B2 | JAPANESE PATENTS | 12-SEP-2012

41. Device and process for wireless local area network association and corresponding products

The present invention concerns WLAN association device and process for associating a new station to a WLAN, via a central apparatus. The association device comprises receiving and sending means for exchanging signals between the station and central apparatus, securing means for automatically...

CURRENT ASSIGNEES: THOMSON LICENSING
US7866485 | US PATENTS | 28-DEC-2010

42. Method and device for secure wireless transmission of information

Method and device for secure wireless transmission of information from a sender to a receiver. A sending device is arranged for obtaining a message, a sender identity and a receiver identity and includes encryption means for encrypting the message to be transmitted. A transmission channel is...

CURRENT ASSIGNEES: ANOTO AB
EP1293061A1 | EUROPEAN APPLICATIONS | 19-MAR-2003

43. Method and device for secure wireless transmission of information

Method and device for secure wireless transmission of information from a sender to a receiver. A sending device is arranged for obtaining a message, a sender identity and a receiver identity and includes encryption means for encrypting the message to be transmitted. A transmission channel is...

CURRENT ASSIGNEES: ANOTO IP LIC HB [+1]
US26020035687 | US APPLICATIONS | 21-MAR-2002

44. Method and device for secure wireless transmission of information

A method for secure transmission of information from a digital pen to a receiving device is provided. The method includes obtaining, in the digital pen, a message in the form of a plurality of position indications recorded from a position code on a substrate; sending at least one of the position...

CURRENT ASSIGNEES: ANOTO ANOTO AB
US7278017 | US PATENTS | 02-OCT-2007

45. Wireless communication device and wireless communication method

CURRENT ASSIGNEES: 富士通セミコンダクター株式会社
JP5708183B2 | JAPANESE PATENTS | 30-APR-2015

46. Web authentication using client platform root of trust

Systems and methods for performing web authentication using a client platform root of trust are disclosed herein. Website and user validity and integrity may be authenticated based on the user device's attempt to access the website. A user device may securely access the website once the user device is...

CURRENT ASSIGNEES: INTEL CORP
TW201347499A | TAIWANESE APPLICATIONS | 16-NOV-2013

47. Method for increasing security of plaintext authentication in wireless local area network

A method for increasing security of plaintext authentication in a wireless local area network (WLAN) is provided. The method includes steps of: establishing a basic service set in the WLAN; establishing a blank learning table for saving identities of faked users; generating the identities of the...

CURRENT ASSIGNEES: HON HAI PREC IND CO LTD
US7441698 | US PATENTS | 28-OCT-2008

48. Online data encryption and decryption

Is realized by computer network is transmitted by the data providing encryption and decryption system and method for better method is input to the user computer is such as password a user authentication identifier the invention claims a data encryption and decryption. Said system and method for...

CURRENT ASSIGNEES: BHAROSA INC
CN190567356C | CHINESE PATENTS | 04-NOV-2009

49. Computer-implemented authentication interface system

Systems and methods for providing encryption and decryption of data transmitted on a computer implemented network, preferably user authentication identifier data, such as a password, at the point of entry into the user's computer. The systems and methods enable an end user to mentally select a...

CURRENT ASSIGNEES: オフィス・システム・ソリューションズ
JP533056782 | JAPANESE PATENT | 2013-08-20
Map

STIC

50. Active base station fraud prevention method based on client computer and system thereof

The invention claims a based on client the active base station and the special method comprises following steps
probe: Client of the target base station sends a group or a plurality of groups of authentication information at least
one group of authentication information device information false;...

CURRENT ASSIGNEES: DUNYU SHANGHAI INFO TECH CO LTD
CN105209562A | CHINESE APPLICATIONS | 20-DEC-2015

Show next: 50 | 100 | 250 | 500 | 1000 Results

Application Serial No. 14/693,400
Response to Non-Final Office Action mailed on May 24, 2017
Docket No.: 2582-2.737BS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Hyoung-Gon LEE	Examiner:	GOODCHILD, WILLIAM J.
Appl. No.:	14/693,400	Art Unit:	2433
Filed:	April 22, 2015	Confirmation No.:	7248
		Docket No.:	2582-2.737BS

To: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

From: Daniel J. Stanger
Customer No. 86636
Brundidge & Stanger, PC
1925 Ballenger Ave., Suite 560
Alexandria, VA 22314

RESPONSE TO NON-FINAL OFFICE ACTION

Dear Commissioner:

In response to the Non-Final Office Action dated May 24, 2017, entry of the following amendments and consideration of the accompanying remarks is respectfully requested.

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks begin on page 9 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

1. (Currently Amended) A method performed by a server, the method comprising:
~~providing, transmitting, by the server~~ to a device, authenticated access point information regarding one or more authenticated access points, wherein the one or more authenticated access points are controlled by the server; and
transmitting, by the server to the device, a fake device identifier, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame in a search for at least one of the one or more authenticated access points around the device.
2. (Original) The method of Claim 1, wherein the one or more authenticated access points include a Wi-Fi access point.
3. (Previously Presented) The method of Claim 1, wherein the transmitting the fake device identifier includes transmitting a fake media access control (MAC) address.
4. (Currently Amended) The method of Claim 1, wherein the ~~providing, transmitting~~ the authenticated access point information regarding the one or more authenticated access points includes ~~providing, transmitting~~ at least one of a media access control (MAC) address or a service set identifier (SSID) of each of the one or more authenticated access points.
5. (Currently Amended) A method performed by an access point, the method comprising:
receiving, by the access point from a device, a probe request frame that includes a fake device identifier for the device, wherein the fake device identifier is received at the device from a server, and wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

transmitting, by the access point to the device, a probe response frame that includes information regarding the access point;

receiving, by the access point from the device, a connection request that includes an authentic device identifier for the device; and

transmitting, by the access point to the device ~~by the access point~~, an approval of the connection request, wherein the access point is controlled by [[a]] the server.

6. (Original) The method of Claim 5, further comprising:

receiving, from the device, an association request;

transmitting, to the device, an association response to the association request; and

facilitating connection of the device to a communication network via the access point in accordance with the association response.

7. (Previously Presented) The method of Claim 6, wherein the access point includes a Wi-Fi access point, and wherein the communication network includes a Wi-Fi network.

8. (Previously Presented) The method of Claim 5, wherein the access point was previously communicatively coupled with the device.

9. (Original) The method of Claim 5, wherein the authentic device identifier includes a media access control (MAC) address.

10. (Original) The method of Claim 5, wherein the information regarding the access point includes at least one of a media access control (MAC) address of the access point or a service set identifier (SSID) of the access point.

11. (Currently Amended) A method performed by a device, the method comprising:

receiving, from a server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters, to falsely identify the device in a probe request frame;

transmitting, to at least one access point, the probe request frame that includes the received fake device identifier;

receiving, from the at least one access point, a probe response frame that includes information regarding the at least one access point;

determining, based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point; and

transmitting, to the at least one access point, a connection request that includes an authentic device identifier for the device.

12. (Previously Presented) The method of Claim 11, wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address.

13. (Currently Amended) The method of Claim 11, wherein the determining, based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point, comprises:

determining that the at least one access point is under control of the server.

14. (Currently Amended) The method of Claim 11, wherein the determining, based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point, comprises:

determining that the at least one access point is included in an authenticated access point list,

wherein the authenticated access point list is stored in a memory, and

wherein the authenticated access point list is received from the server.

15. (Previously Presented) The method of Claim 11, further comprising:
receiving, from the at least one access point, an approval of the connection request;
transmitting, to the at least one access point, an association request;
receiving, from the at least one access point, an association response to the association request; and

connecting to a communication network via the at least one access point in accordance with the association response.

16. (Currently Amended) A method performed by a device, the method comprising:
generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
transmitting, to at least one access point, a probe request frame that includes the fake device identifier;
receiving, from the at least one access point, a probe response frame that includes information regarding the at least one access point;
determining, based at least₂ in part₂ on the information regarding the at least one access point, that the at least one access point is an authenticated access point, wherein the determining includes determining that the at least one access point is under control of a server; and
transmitting, to the at least one access point, a connection request that includes an authentic device identifier for the device.

17. (Original) The method of Claim 16, wherein the fake device identifier includes a fake media access control (MAC) address.

18. (Original) The method of Claim 16, wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point.

19. (Currently Amended) The method of Claim 16, wherein the determining, based at least₂ in part₂ on the information regarding the at least one access point, that the at least one access point is an authenticated access point, includes:
determining that the at least one access point was previously connected with the device.

20. (Currently Amended) The method of Claim 16, wherein the determining, based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point, includes:

determining that the at least one access point is included in an authenticated access point list received from the server and stored in a memory.

21. (Canceled)

22. (Previously Presented) The method of Claim 16, further comprising:

receiving, from the at least one access point, an approval of the connection request;

transmitting, to the at least one access point, an association request;

receiving, from the at least one access point, an association response to the association request; and

connecting to a communication network via the at least one access point in accordance with the association response.

23. (Currently Amended) A method performed by a device, the method comprising:

generating a collection ~~including~~ that includes at least one of one or more random numbers or one or more random characters to provide a fake device identifier for the device so to falsely identify the device in a probe request frame;

transmitting, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier;

receiving, from at least one access point around the device, a probe response frame that includes information regarding the at least one access point;

determining, based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point, wherein the determining includes determining that the at least one access point is under control of a server; and

transmitting, to the at least one access point, a connection request that includes an authentic device identifier for the device.

24. (Previously Presented) The method of Claim 23, wherein:
the generating the collection that includes at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address, and
the fake device identifier includes the fake media access control (MAC) address.

25. (Previously Presented) The method of Claim 23, further comprising:
storing the fake device identifier in a memory.

26. (Currently Amended) A system, comprising:
a processor;
at least one communication interface;
a transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame ~~including that includes~~ a fake device identifier for a device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
a receiver to receive, from the at least one access point via the at least one communication interface, a probe response frame ~~including that includes~~ information regarding the at least one access point;
a memory to store the information regarding the at least one access point; and
a determination unit to determine, under control of the processor and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of a server,
wherein the transmitter further transmits to the at least one access point, a connection request ~~including that includes~~ an authentic device identifier for the device, in response to a determination by the determination unit that the at least one access point is the authenticated access point and is under control of the server.

27. (Original) The system of Claim 26, wherein the fake device identifier includes a fake media access control (MAC) address.

28. (Previously Presented) The system of Claim 26, further comprising:
a fake device identifier generation unit to generate, under control of the processor, the fake device identifier.

29. (Currently Amended) The system of Claim 26, wherein the memory stores the fake device identifier.

30. (Previously Presented) The system of Claim 26, wherein the at least one access point includes a Wi-Fi access point, and the at least one communication interface is configured for communication with a Wi-Fi network.

31. (Previously Presented) The system of Claim 26, wherein:
the determination unit further determines whether the at least one access point is included in an authenticated access point list stored in the memory, and
the authenticated access point list is provided via the receiver.

REMARKS

Reconsideration and allowance of the above-identified application are respectfully requested. Claims 1-20 and 22-31 are currently pending. Claims 1, 4, 5, 11, 13, 14, 16, 19, 20, 23, 26, and 29 are currently amended. Support for the amendments can be found at least in paragraph [0023] of the specification as filed. Claim 21 was previously canceled without prejudice. No new matter is added.

Claim Rejections – 35 U.S.C. § 103

Claims 1-20 and 22-31 were rejected under pre-AIA 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent Application Publication No. 2012/0076072 (Jalfon) in view of U.S. Patent Application Publication No. 2007/007904 (Mukherjee).

Note: In the list of references cited (form PTO-892), the Mukherjee reference corresponds to U.S. Application Publication No. 2007/0097904. However, at pages 2 and 3, in the rejection heading of claims 1-20 and 22-31, it appears that the Office Action has inadvertently cited “U.S. Application Publication No. 2007/007904” as being the Mukherjee reference.

The rejection of claims 1-20 and 22-31 is respectfully traversed as detailed below:

Independent claims 1, 16, 23, and 26

It is respectfully submitted that Jalfon and Mukherjee, either alone or in combination, fail to teach or suggest all the features as set forth in amended independent claim 1.

For example, amended independent claim 1 recites “transmitting, by the server to a device, authenticated access point information regarding one or more authenticated access points, wherein the one or more authenticated access points are controlled by the server” (emphasis added), which is not taught or suggested by the combination of Jalfon and Mukherjee.

The Office Action on page 3, states that “Jalfon does not specifically disclose providing, to a device, authenticated access point information regarding one or more authenticated access points controlled by the server,” as previously recited in independent claim 1. Further, the Office Action, on page 3, alleges that “Mukherjee teaches a list of allowed access points (authenticated by the server) that are stored on the wireless nodes [Mukherjee, paragraph 34].”

Mukherjee, in paragraphs [0027], [0028], and [0034] respectively recites:

“The access point 70 and wireless nodes 60 communicate using packets. Each packet comprises an authentication token, an origination address and a destination address. The addresses may be MAC addresses, for example.”

“During the communicating, the access point 70 reads and stores the respective authentication tokens and origination addresses wirelessly transmitted from the wireless nodes 60 for defining an allowed wireless node list 72. Each wireless node 60 reads and stores the authentication token and origination address wirelessly transmitted from the access point 70 for defining an allowed access point list 62.”

“In office networks where there may be several access points with different MAC addresses using the same AAA authentication token, the MAC addresses of all allowed access points along with the authenticating token of the AAA server (in most cases the public key) be stored on all wireless nodes. The authentication tokens and MAC addresses of all clients are also stored on all access points.” (Emphasis Added)

Mukherjee, in the cited portions or elsewhere, describes a method to detect and prevent attack on wireless nodes and access points in a wireless network. During communication, the wireless nodes read and store respective authentication tokens and origination addresses from the access points to define an allowed access point list. Further, an authentication server is connected to a distribution system, to authenticate a wireless node that connects to the distribution system.

The Office Action appears to equate Mukherjee’s “allowed access point list” with the recited “authenticated access points” of amended independent claim 1.

Mukherjee, at best, describes that the wireless nodes are configured to read and store respective authentication tokens and origination addresses of the access points that communicate with the wireless nodes, to define the allowed access point list. *However, Mukherjee, does not disclose that the authentication server transmits authenticated access point information to the wireless nodes, regarding one or more authenticated access points that are controlled by the authentication server.*

Assuming, *arguendo*, Mukherjee’s authentication server (presumably equated to the recited “server” of amended independent claim 1) is connected to the distribution system and authenticates the wireless node that connects to the distribution server, it is submitted that the

allowed access point list of Mukherjee shall still be generated by a wireless node and not by the authentication server.

Furthermore, Mukherjee fails to disclose that the allowed access point list is received at the authentication server from the wireless node to facilitate further transmission by the authentication server.

In view thereof, it is respectfully submitted that the authentication server of Mukherjee **cannot** transmit authenticated access point information regarding one or more authenticated access points to a wireless node, wherein the one or more authenticated access points are controlled by the authentication server.

Therefore, Mukherjee fails to contemplate “transmitting, by the authentication server to a wireless node, authenticated access point information regarding one or more authenticated access points, wherein the one or more authenticated access points are controlled by the authentication server” as recited in amended independent claim 1

Jalfon, in the cited portions or elsewhere, describes system and method to maintain privacy in a wireless network. The wireless network includes one or more access points and a device to be communicatively coupled with respective one or more access points. The device transmits a probe request frame using different fake MAC addresses, in search of the respective one or more access points.

However, Jalfon fails to cure the deficiencies of Mukherjee.

Further, the Office Action on page 3, alleges that “[i]t would have been obvious to one having ordinary skill in the art at the time the invention was made to include authenticated access points for the mobile devices use to ensure that access points are not hijacked or impersonated.”

In this regard, it is respectfully submitted that Jalfon’s device is configured to not reveal and share information, data or parameters with other devices of the wireless network, unless authenticated. In fact, an allocated unique MAC address associated with the Jalfon’s device is not meant to be revealed and shared while searching for the respective access point. Thus, Jalfon’s principle of operation implies transmitting a probe request frame by use of the different fake MAC addresses in search of the respective access point, without revealing the allocated unique MAC address associated with the device.

In view thereof, it is further submitted that the modification in Jalfon to include “authenticated access points” of Mukherjee to define an authenticated access point list for Jalfon’s device, *will require an initial revelation of the allocated unique MAC address associated with the wireless devices to the other wireless devices (alleged “access points”), thereby changing the basic principle under which Jalfon’s device is meant to be operated.* Hence, the proposed modification would change the basic principle under which Jalfon’s teaching was meant to be implemented.

However, MPEP § 2143.01(VI) states that “[i]f the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious.”

Therefore, it is respectfully submitted that there is no suggestion or motivation to a person of ordinary skill in the art to modify Jalfon with Mukherjee, as alleged by the Office Action. Hence, a prima facie case of obviousness has not been established.

Hence, Jalfon and Mukherjee, either alone or in combination, fails to teach or suggest “*transmitting, by the server to a device, authenticated access point information regarding one or more authenticated access points, wherein the one or more authenticated access points are controlled by the server*” as recited by amended independent claim 1.

Independent claim 16 and 23

Independent claims 16 and 23 recite “*wherein the determining includes determining that the at least one access point is under control of a server*” analogous to independent claim 1. Hence, with reference to the reasons submitted above for independent claim 1, the combination of Jalfon and Mukherjee fails to teach or suggest all the recitations as set forth in independent claims 16 and 23.

Independent claim 26

Independent claim 26 recites “*a determination unit to determine, under control of the processor and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of a*

server” analogous to independent claim 1. Hence, with reference to the reasons submitted above for independent claim 1, the combination of Jafon and Mukherjee fails to teach or suggest all the recitations as set forth in independent claim 26.

Accordingly, it is respectfully requested that the rejection of independent claims 1, 16, 23, and 26 under pre-AIA 35 U.S.C. § 103(a) be withdrawn.

Independent claims 5 and 11

It is respectfully submitted that Jafon and Mukherjee fail to teach or suggest all the claimed features as set forth in amended independent claim 11.

For example, amended independent claim 11 recites “*receiving, from a server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters, to falsely identify the device in a probe request frame*” (emphasis added), which is not taught or suggested by the combination of Jafon and Mukherjee.

With regard to claim 11, the Office Action, on page 6, alleges, “Jafon-Mukherjee further discloses receiving, from a server [Mukherjee, paragraph 34], a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame [Jafon, paragraphs 33 and 35].”

Mukherjee, at best, describes a storage of an authenticating token on the wireless nodes which is in contrast with the aspect of amended independent claim 11 that recites “*receiving, from a server, a fake device identifier for the device.*” As such, Mukherjee’s authenticating token comprises MAC address of allowed devices and thus, cannot include the fake device identifier for the device.

Further, Jafon, in paragraphs [0029], [0031], and [0035] respectively recites:

“As shown, **wireless communication device 110 may include a memory 122 to store MAC address sets 123 and 124.**”

“As shown by blocks 260, 261 and 262, in a method or flow according to embodiments of the invention, wireless **communication device A may transmit probe request frames to a broadcast address** in search of an access point. **To send such probe request frames, wireless communication device A**

may use MAC addresses other than its allocated MAC address. As further shown by blocks 260, 261 and 262, wireless communication device A may use a number of different fake or ‘dummy’ MAC addresses until a connection is made with the AP. As shown by block 260, in the first probe request frame (transmitted to a broadcast address), wireless communication device A may use MAC addresses ‘A1’.”

“For example, a MAC address may be selected (according to any algorithm or method) from a set of MAC addresses, e.g., MAC address set 124 shown in FIG. 1...As shown by block 415, a flow may include determining a probe response frame was received. For example, following transmission of one or more probe request frames (that may include respective one or more MAC addresses) as shown by block 410 a probe response may be received, e.g., from an access point. As shown, if a probe response frame is not received (e.g., within a predefined period after a probe request frame was transmitted) then sending a probe request frame as shown by block 410 may be repeated. (Emphasis Added)”

Jalfon, in the cited portions or elsewhere, describes a system and method to maintain privacy in a wireless network that includes one or more access points and a device to be communicatively coupled with respective one or more access points. The device transmits a probe request frame using different fake MAC addresses selected from a MAC address set stored in a memory of the device, in search of the respective one or more access points. In response, the device receives a probe response frame from the respective one or more access points.

Jalfon, at best, describes that the device receives a probe response frame from the respective one or more access points, in response to the device’s probe request frame that includes a fake or dummy MAC address associated with the device. *However, Jalfon, nowhere teaches or suggests, receiving, from a server, the fake MAC addresses that are to be associated with the device.*

Further, it is respectfully submitted that the dummy or fake MAC addresses associated with the device, are generated from the MAC address sets, stored in the memory of the device such is in contrast with *receiving, from a server, a fake device identifier for the device.*

In fact, Jalfon is silent on the server configured to transmit the fake device identifier to the device.

Hence, Jalfon and Mukherjee, either alone or in combination, fails to teach or suggest “receiving, from a server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame” as recited by amended independent claim 11.

Independent claim 5 recites features analogous to amended independent claim 11. Hence, with reference to the reasons submitted above for amended independent claim 11, the combination of Jalfon and Mukherjee fails to teach or suggest all the recitations as set forth in independent claim 5.

Accordingly, it is respectfully requested that the rejection of independent claim 5 and 11 under pre-AIA 35 U.S.C. § 103(a) be withdrawn.

Dependent claims 2-4, 6-10, 12-15, 17-20, 22, 24-25, and 27-31

Claims 2-4, 6-10, 12-15, 17-20, 22, 24-25, and 27-31 are also allowable at least by virtue of their dependencies on claims 1, 5, 11, 16, 23, and 26 respectively, which have been shown to be allowable above, and as well as for their additional recited features.

Accordingly, it is respectfully requested that the rejection of claims 2-4, 6-10, 12-15, 17-20, 22, 24-25, and 27-31 under pre-AIA 35 U.S.C. § 103(a) be withdrawn as well.

Various other amendments are made to the claims as shown, so as to provide more appropriate antecedent basis, to make the recitations within and between related claims more consistent, to more precisely recite the subject matter contained therein, to make typographical/grammatical edits, and/or to otherwise place such claims in better form.

Conclusion

Therefore, in light of at least the foregoing, it is respectfully believed that the present application is in condition for allowance. As a result, issuance of a Notice of Allowance for the pending claims is respectfully requested.

The Examiner's consideration of these Amendments and Remarks is appreciated and the Examiner is cordially invited to contact the undersigned, should the Examiner have any questions, comments, or suggestions.

Please charge any fees that may be due to Deposit Account No. 50-4888.

Respectfully submitted,

Brundidge & Stanger, P.C.

Date August 24, 2017

By: /Daniel J. Stanger/
Daniel J. Stanger
Reg. No. 32,846

Electronic Acknowledgement Receipt

EFS ID:	30175377
Application Number:	14693400
International Application Number:	
Confirmation Number:	7248
Title of Invention:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK
First Named Inventor/Applicant Name:	Hyoung-Gon LEE
Customer Number:	86636
Filer:	Daniel John Stanger/Mariah Duell
Filer Authorized By:	Daniel John Stanger
Attorney Docket Number:	2582-2.737BS
Receipt Date:	24-AUG-2017
Filing Date:	22-APR-2015
Time Stamp:	15:32:08
Application Type:	Utility under 35 USC 111(a)

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	Amendment/Req. Reconsideration-After Non-Final Reject	KR-839496-03-US-CON_20170824_SecondOA_Response.pdf	82192 ebf50483426353ae7b844ed611bb935bbd bd2260	no	16

Warnings:

Information:	
Total Files Size (in bytes):	82192
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.	

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 14/693,400	Filing Date 04/22/2015	☐ To be Mailed
---	---	----------------------------------	---------------------------------------

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO**APPLICATION AS FILED – PART I**

(Column 1)

(Column 2)

FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	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 \$310 (\$155 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))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

(Column 1)

(Column 2)

(Column 3)

	08/24/2017	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT	Total (37 CFR 1.16(i))	* 30	Minus	** 31	= 0	X \$80 =	0
	Independent (37 CFR 1.16(h))	* 6	Minus	***6	= 0	X \$420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
TOTAL ADD'L FEE							0

(Column 1)

(Column 2)

(Column 3)

	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$ =
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =
	☐ Application Size Fee (37 CFR 1.16(s))					
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					
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.

LIE
DANTE SMITH

This collection of information is required by 37 CFR 1.16. 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, 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.



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.
14/693,400	04/22/2015	Hyoung-Gon LEE	2582-2.737BS	7248

86636 7590 09/11/2017
BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

EXAMINER

GOODCHILD, WILLIAM J

ART UNIT	PAPER NUMBER
----------	--------------

2433

MAIL DATE	DELIVERY MODE
-----------	---------------

09/11/2017

PAPER

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.

Office Action Summary	Application No. 14/693,400	Applicant(s) LEE, HYOUNG-GON	
	Examiner WILLIAM GOODCHILD	Art Unit 2433	AIA (First Inventor to File) Status No

-- 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 MONTHS 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 08/24/2017.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.
- 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) 1-20 and 22-31 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) 1-20 and 22-31 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).

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)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) ☒ Notice of References Cited (PTO-892) | 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date ____. | 4) ☐ Other: ____. |

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

Response to Arguments

2. Applicant's arguments filed 08/24/2017 have been fully considered but they are not persuasive.

A – Applicant argues: “It is respectfully submitted that Jalfon and Mukherjee, either alone or in combination, fail to teach or suggest all the features as set forth in amended independent claim 1.

For example, amended independent claim 1 recites “transmitting, by the server to a device, authenticated access point information regarding one or more authenticated access points, wherein the one or more authenticated access points are controlled by the server” (emphasis added), which is not taught or suggested by the combination of Jalfon and Mukherjee.

The Office Action on page 3, states that “Jalfon does not specifically disclose providing, to a device, authenticated access point information regarding one or more authenticated access points controlled by the server,” as previously recited in independent claim 1.

Further, the Office Action, on page 3, alleges that “Mukherjee teaches a list of allowed

Art Unit: 2433

access points (authenticated by the server) that are stored on the wireless nodes [Mukherjee, paragraph 34]."

Mukherjee, in paragraphs [0027], [0028], and [0034] respectively recites:

"The access point 70 and wireless nodes 60 communicate using packets. Each packet comprises an authentication token, an origination address and a destination address.

The addresses may be MAC addresses, for example." "During the communicating, the access point 70 reads and stores the respective authentication tokens and origination addresses wirelessly transmitted from the wireless nodes 60 for defining an allowed wireless node list 72. Each wireless node 60 reads and stores the authentication token and origination address wirelessly transmitted from the access point 70 for defining an allowed access point list 62."

"In office networks where there may be several access points with different MAC addresses using the same AAA authentication token, the MAC addresses of all allowed access points along with the authenticating token of the AAA server (in most cases the public key) be stored on all wireless nodes.

The authentication tokens and MAC addresses of all clients are also stored on all access points." (Emphasis Added)

Mukherjee, in the cited portions or elsewhere, describes a method to detect and prevent attack on wireless nodes and access points in a wireless network. During communication, the wireless nodes read and store respective authentication tokens and origination addresses from the access points to define an allowed access point list.

Art Unit: 2433

Further, an authentication server is connected to a distribution system, to authenticate a wireless node that connects to the distribution system.

The Office Action appears to equate Mukherjee's "allowed access point list" with the recited "authenticated access points" of amended independent claim 1.

Mukherjee, at best, describes that the wireless nodes are configured to read and store respective authentication tokens and origination addresses of the access points that communicate with the wireless nodes, to define the allowed access point list. However, Mukherjee, does not disclose that the authentication server transmits authenticated access point information to the wireless nodes, regarding one or more authenticated access points that are controlled by the authentication server.

Assuming, arguendo, Mukherjee's authentication server (presumably equated to the recited "server" of amended independent claim 1) is connected to the distribution system and authenticates the wireless node that connects to the distribution server, it is submitted that the allowed access point list of Mukherjee shall still be generated by a wireless node and not by the authentication server.

Furthermore, Mukherjee fails to disclose that the allowed access point list is received at the authentication server from the wireless node to facilitate further transmission by the authentication server.

In view thereof, it is respectfully submitted that the authentication server of Mukherjee cannot transmit authenticated access point information regarding one or more authenticated access points to a wireless node, wherein the one or more authenticated access points are controlled by the authentication server.

Art Unit: 2433

Therefore, Mukherjee fails to contemplate "transmitting, by the authentication server to a wireless node, authenticated access point information regarding one or more authenticated access points, wherein the one or more authenticated access points are controlled by the authentication server" as recited in amended independent claim 1. Jalfon, in the cited portions or elsewhere, describes system and method to maintain privacy in a wireless network. The wireless network includes one or more access points and a device to be communicatively coupled with respective one or more access points. The device transmits a probe request frame using different fake MAC addresses, in search of the respective one or more access points. However, Jalfon fails to cure the deficiencies of Mukherjee."

A – The Examiner respectfully disagrees:

Mukherjee teaches several access points using the same AAA authentication token from the AAA server [Mukherjee, paragraph 34] and wireless nodes connected to the network require an authentication token from the authentication server [Mukherjee, paragraph 26]. Further, it is the combination of Jalfon and Mukherjee used in the rejection, and Jalfon teaches sending the fake MAC address, Mukherjee teaches that the server (authentication) control the access points and it is obvious from the combination that the MAC address source can be by design.

B – Applicant argues: "Further, the Office Action on page 3, alleges that "[i]t would have been obvious to one having ordinary skill in the art at the time the invention was

Art Unit: 2433

made to include authenticated access points for the mobile devices use to ensure that access points are not hijacked or impersonated." In this regard, it is respectfully submitted that Jalfon's device is configured to not reveal and share information, data or parameters with other devices of the wireless network, unless authenticated. In fact, an allocated unique MAC address associated with the Jalfon's device is not meant to be revealed and shared while searching for the respective access point. Thus, Jalfon's principle of operation implies transmitting a probe request frame by use of the different fake MAC addresses in search of the respective access point, without revealing the allocated unique MAC address associated with the device.

In view thereof, it is further submitted that the modification in Jalfon to include "authenticated access points" of Mukherjee to define an authenticated access point list for Jalfon's device, will require an initial revelation of the allocated unique MAC address associated with the wireless devices to the other wireless devices (alleged "access points"), thereby changing the basic principle under which Jalfon's device is meant to be operated. Hence, the proposed modification would change the basic principle under which Jalfon's teaching was meant to be implemented.

However, MPEP § 2143.01(VI) states that "[i]f the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious."

Art Unit: 2433

Therefore, it is respectfully submitted that there is no suggestion or motivation to a person of ordinary skill in the art to modify Jalfon with Mukherjee, as alleged by the Office Action. Hence, a prima facie case of obviousness has not been established. Hence, Jalfon and Mukherjee, either alone or in combination, fails to teach or suggest "transmitting, by the server to a device, authenticated access point information regarding one or more authenticated access points, wherein the one or more authenticated access points are controlled by the server" as recited by amended independent claim 1."

B – The Examiner respectfully disagrees:

The combination of Jalfon with Mukherjee could be accomplished by using the concepts identified, not by changing the intended invention, but adding concepts.

C – Applicant argues: "

Independent claim 16 and 23

Independent claims 16 and 23 recite "wherein the determining includes determining that the at least one access point is under control of a server" analogous to independent claim 1. Hence, with reference to the reasons submitted above for independent claim 1, the combination of Jalfon and Mukherjee fails to teach or suggest all the recitations as set forth in independent claims 16 and 23.

Independent claim 26 Independent claim 26 recites "a determination unit to determine, under control of the processor and based at least, in part, on the information regarding

Art Unit: 2433

the at least one access point, whether the at least one access point is an authenticated access point and is under control of a server" analogous to independent claim 1. Hence, with reference to the reasons submitted above for independent claim 1, the combination of Jalfon and Mukherjee fails to teach or suggest all the recitations as set forth in independent claim 26.

Accordingly, it is respectfully requested that the rejection of independent claims 1, 16, 23, and 26 under pre-AIA 35 U.S.C. § 103(a) be withdrawn.

Independent claims 5 and 11

It is respectfully submitted that Jalfon and Mukherjee fail to teach or suggest all the claimed features as set forth in amended independent claim 11.

For example, amended independent claim 11 recites "receiving, from a server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters, to falsely identify the device in a probe request frame" (emphasis added), which is not taught or suggested by the combination of Jalfon and Mukherjee.

With regard to claim 11, the Office Action, on page 6, alleges, "Jalfon-Mukherjee further discloses receiving, from a server [Mukherjee, paragraph 34], a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame [Jalfon, paragraphs 33 and 35]."

Mukherjee, at best, describes a storage of an authenticating token on the wireless nodes which is in contrast with the aspect of amended independent claim 11 that recites

Art Unit: 2433

"receiving, from a server, a fake device identifier for the device." As such, Mukherjee's authenticating token comprises MAC address of allowed devices and thus, cannot include the fake device identifier for the device.

Further, Jalfon, in paragraphs [0029], [0031], and [0035] respectively recites:

"As shown, wireless communication device 110 may include a memory 122 to store MAC address sets 123 and 124."

"As shown by blocks 260, 261 and 262, in a method or flow according to embodiments of the invention, wireless communication device A may transmit probe request frames to a broadcast address in search of an access point. To send such probe request frames, wireless communication device A may use MAC addresses other than its allocated MAC address. As further shown by blocks 260, 261 and 262, wireless communication device A may use a number of different fake or 'dummy' MAC addresses until a connection is made with the AP. As shown by block 260, in the first probe request frame (transmitted to a broadcast address), wireless communication device A may use MAC addresses 'A1'."

"For example, a MAC address may be selected (according to any algorithm or method) from a set of MAC addresses, e.g., MAC address set 124 shown in FIG. 1... As shown by block 415, a flow may include determining a probe response frame was received. For example, following transmission of one or more probe request frames (that may include respective one or more MAC addresses) as shown by block 410 a probe response may be received, e.g., from an access point. As shown, if a probe response frame is not received (e.g., within a predefined period after a probe request frame was transmitted)

Art Unit: 2433

then sending a probe request frame as shown by block 410 may be repeated.

(Emphasis Added)"

Jalfon, in the cited portions or elsewhere, describes a system and method to maintain privacy in a wireless network that includes one or more access points and a device to be communicatively coupled with respective one or more access points. The device transmits a probe request frame using different fake MAC addresses selected from a MAC address set stored in a memory of the device, in search of the respective one or more access points. In response, the device receives a probe response frame from the respective one or more access points.

Jalfon, at best, describes that the device receives a probe response frame from the respective one or more access points, in response to the device's probe request frame that includes a fake or dummy MAC address associated with the device. However, Jalfon, nowhere teaches or suggests, receiving, from a server, the fake MAC addresses that are to be associated with the device.

Further, it is respectfully submitted that the dummy or fake MAC addresses associated with the device, are generated from the MAC address sets, stored in the memory of the device such is in contrast with receiving, from a server, a fake device identifier for the device.

In fact, Jalfon is silent on the server configured to transmit the fake device identifier to the device.

Hence, Jalfon and Mukherjee, either alone or in combination, fails to teach or suggest "receiving, from a server, a fake device identifier for the device, wherein the received

Art Unit: 2433

fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame" as recited by amended independent claim 11.

Independent claim 5 recites features analogous to amended independent claim 11.

Hence, with reference to the reasons submitted above for amended independent claim 11, the combination of Jafon and Mukherjee fails to teach or suggest all the recitations as set forth in independent claim 5.

Accordingly, it is respectfully requested that the rejection of independent claim 5 and 11 under pre-AIA 35 U.S.C. § 103(a) be withdrawn.

Dependent claims 2-4, 6-10, 12-15, 17-20, 22, 24-25, and 27-31

Claims 2-4, 6-10, 12-15, 17-20, 22, 24-25, and 27-31 are also allowable at least by virtue of their dependencies on claims 1, 5, 11, 16, 23, and 26 respectively, which have been shown to be allowable above, and as well as for their additional recited features.

Accordingly, it is respectfully requested that the rejection of claims 2-4, 6-10, 12-15, 17-20, 22, 24-25, and 27-31 under pre-AIA 35 U.S.C. § 103(a) be withdrawn as well.

Various other amendments are made to the claims as shown, so as to provide more appropriate antecedent basis, to make the recitations within and between related claims more consistent, to more precisely recite the subject matter contained therein, to make typographical/grammatical edits, and/or to otherwise place such claims in better form.”.

C – The Examiner respectfully disagrees:

See arguments related to **A and B** above.

Claim Rejections - 35 USC § 103

3. The following is a quotation of pre-AIA 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, 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 negated by the manner in which the invention was made.

4. Claims 1-20 and 22-31 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Jalfon et al., (US Publication No. 2012/0076072), hereinafter “Jalfon”, and further in view of Mukherjee et al., (US Publication No. 2007/007904), hereinafter “Mukherjee”.

Regarding claim 1, Jalfon discloses transmitting, to the device, a fake device identifier [Jalfon, paragraph 35, a response], wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame in a search for at least one or the one or more access points around the device [Jalfon, paragraphs 31 and 35].

Jalfon does not specifically disclose transmitting, by the server to a device, authenticated access point information regarding one or more authenticated access points, wherein the one or more authenticated access points are controlled by the server.

Art Unit: 2433

However, Mukherjee teaches access points authenticated by the server that are stored on the wireless nodes [Mukherjee, paragraphs 26 and 34].

It would have been obvious to one having ordinary skill in the art at the time the invention was made to include authenticated access points for the mobile devices use to ensure that access points are not hijacked or impersonated [Mukherjee, paragraph 33].

Regarding claim 2, Jalfon-Mukherjee further discloses wherein the one or more authenticated access points include a Wi-Fi access point [Jalfon, paragraph 34].

Regarding claim 3, Jalfon-Mukherjee further discloses wherein the transmitting the fake device identifier includes transmitting a fake media access control (MAC) address [Jalfon, paragraphs 31 and 35].

Regarding claim 4, Jalfon-Mukherjee further discloses wherein the transmitting the authenticated access point information regarding the one or more authenticated access points includes transmitting at least one of a media access control (MAC) address or a service set identifier (SSID) of each of the one or more authenticated access points [Mukherjee, paragraph 34].

Regarding claim 5, Jalfon-Mukherjee further discloses

Art Unit: 2433

receiving, by the access point from a device, a probe request frame that includes a fake device identifier for the device, wherein the fake device identifier is received at the device from a server [Mukherjee, paragraphs 26 and 34], and wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters [Jalfon, paragraphs 31 and 35];

transmitting, by the access point to the device, a probe response frame that includes information regarding the access point [Jalfon, paragraph 35];

receiving, by the access point from the device, a connection request that includes an authentic device identifier for the device [Jalfon, paragraph 33]; and

transmitting, by the access point to the device, an approval of the connection request [Jalfon, paragraphs 31 and 33], wherein the access point is controlled by the server [Mukherjee, paragraph 34].

Regarding claim 6, Jalfon-Mukherjee further discloses

receiving, from the device, an association request [Jalfon, paragraph 33];

transmitting to the device, an association response to the association request [Jalfon, paragraphs 33 and 35]; and

facilitating connection of the device to a communication network via the access point in accordance with the association response [Jalfon, paragraphs 33 and 35].

Regarding claim 7, Jalfon-Mukherjee further discloses

Art Unit: 2433

wherein the access point includes a Wi-Fi access point, and wherein the communication network includes a Wi-Fi network [Jalfon, paragraphs 34].

Regarding claim 8, Jalfon-Mukherjee further discloses

wherein the access point was previously communicatively coupled with the end device [Mukherjee, paragraph 34].

Regarding claim 9, Jalfon-Mukherjee further discloses

wherein the authentic device identifier includes a media access control (MAC) address [Jalfon, paragraphs 33-35].

Regarding claim 10, Jalfon-Mukherjee further discloses

wherein the information regarding the access point includes at least one of a media access control (MAC) address of the access point or a service set identifier (SSID) of the access point [Mukherjee, paragraph 34].

Regarding claim 11, Jalfon-Mukherjee further discloses

receiving, from a server [Mukherjee, paragraphs 26 and 34], a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame [Jalfon, paragraphs 33 and 35];

Art Unit: 2433

transmitting, to at least one access point, the probe request frame that includes the received fake device identifier [Jalfon, paragraphs 31 and 35];
receiving, from the at least one access point, a probe response frame that includes information regarding the at least one access point [Jalfon, paragraphs 31 and 35];
determining, based at least in part on the information regarding the at least one access point, that the at least one access point is an authenticated access point [Mukherjee, paragraph 34]; and
transmitting, to the at least one access point, a connection request that includes an authentic device identifier for the device [Jalfon, paragraphs 33-35].

Regarding claim 12, Jalfon-Mukherjee further discloses
wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address [Jalfon, paragraphs 33-35].

Regarding claim 13, Jalfon-Mukherjee further discloses
determining that the at least one access point is under control of the server [Mukherjee, paragraphs 26 and 34].

Regarding claim 14, Jalfon-Mukherjee further discloses
determining that the at least one access point is included in an authenticated access point list [Mukherjee, paragraphs 26 and 34],

Art Unit: 2433

wherein the authenticated access point list is stored in a memory [Mukherjee, paragraphs 26 and 34], and

wherein the authenticated access point list is received from the server [Mukherjee, paragraphs 26 and 34, the list is approved by the server].

Regarding claim 15, Jalfon-Mukherjee further discloses

receiving, from the at least one access point, an approval of the connection request [Jalfon, paragraphs 33-35];

transmitting, to the at least one access point, an association request [Jalfon, paragraphs 33-35];

receiving, from the at least one access point, an association response to the association request [Jalfon, paragraphs 33-35]; and

connecting to a communication network via the at least one access point in accordance with the association response [Jalfon, paragraphs 33-35].

Regarding claim 16, Jalfon-Mukherjee further discloses

generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters [Jalfon, paragraphs 33-35];

transmitting, to at least one access point, a probe request frame that includes the fake device identifier [Jalfon, paragraphs 33-35];

Art Unit: 2433

receiving, from the at least one access point, a probe response frame that includes information regarding the at least one access point [Jalfon, paragraphs 33-35];
determining, based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point, wherein the determining includes determining that the at least one access point is under control of a server [Mukherjee, paragraph 34]; and
transmitting, to the at least one access point, a connection request that includes an authentic device identifier for the device [Jalfon, paragraphs 33-35].

Regarding claim 17, Jalfon-Mukherjee further discloses
wherein the fake device identifier includes a fake media access control (MAC) address [Jalfon, paragraphs 33-35].

Regarding claim 18, Jalfon-Mukherjee further discloses
wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point [Mukherjee, paragraph 34].

Regarding claim 19, Jalfon-Mukherjee further discloses
determining that the at least one access point was previously connected with the device [Mukherjee, paragraph 34].

Regarding claim 20, Jalfon-Mukherjee further discloses determining that the at least one access point is included in an authenticated access point list received from the server and stored in a memory [Mukherjee, paragraph 34].

Regarding claim 22, Jalfon-Mukherjee further discloses receiving, from the at least one access point, an approval of the connection request [Jalfon, paragraphs 33-35]; transmitting, to the at least one access point, an association request [Jalfon, paragraphs 33-35]; receiving, from the at least one access point, an association response to the association request [Jalfon, paragraphs 33-35]; and connecting to a communication network via the at least one access point in accordance with the association response [Jalfon, paragraphs 33-35].

Regarding claim 23, Jalfon-Mukherjee further discloses generating a collection that includes at least one of one or more random numbers or one or more random characters to provide a fake device identifier for the device so to falsely identify the device in a probe request frame [Jalfon, paragraphs 33-35]; transmitting, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier [Jalfon, paragraphs 33-35];

receiving, from at least one access point around the device, a probe response frame that includes information regarding the at least one access point [Jalfon, paragraphs 33-35];

determining, based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point, wherein the determining includes determining that the at least one access point is under control of a server [Mukherjee, paragraphs 26 and 34]; and

transmitting, to the at least one access point, a connection request that includes an authentic device identifier for the device [Jalfon, paragraphs 33-35].

Regarding claim 24, Jalfon-Mukherjee further discloses

wherein the generating the collection that includes at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address [Jalfon, paragraphs 33-35], and

the fake device identifier includes the fake media access control (MAC) address [Jalfon, paragraphs 33-35].

Regarding claim 25, Jalfon-Mukherjee further discloses

storing the fake device identifier in a memory [Jalfon, paragraph 33-35].

Regarding claim 26, Jalfon-Mukherjee further discloses

a processor [Jalfon, paragraph 38];

Art Unit: 2433

at least one communication interface [Jalfon, paragraph 38];

a transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame that includes a fake device identifier for a device, wherein the fake device identifier includes at least one of the one or more random numbers or one or more random characters [Jalfon, paragraphs 33-35];

a receiver to receive, from the at least one access point via the at least one communication interface, a probe response frame that includes information regarding the at least one access point [Jalfon, paragraphs 33-35];

a memory to store the information regarding the at least one access point [Mukherjee, paragraph 34]; and

a determination unit to determine, under control of the processor and based at least in part on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and under control of a server [Mukherjee, paragraph 34];

wherein the transmitter further transmits to the at least one access point, a connection request that includes an authentic device identifier of the device [Jalfon, paragraphs 33-35] in response to a determination by the determination unit that the at least one access point is the authenticated access point and under control of the server [Mukherjee, paragraph 34].

Regarding claim 27, Jalfon-Mukherjee further discloses

Art Unit: 2433

wherein the fake device identifier includes a fake media access control (MAC) address [Jalfon, paragraphs 33-35].

Regarding claim 28, Jalfon-Mukherjee further discloses a fake device identifier generation unit to generate, under control of the processor, the fake device identifier [Jalfon, paragraphs 33-35].

Regarding claim 29, Jalfon-Mukherjee further discloses wherein the memory stores the fake device identifier [Jalfon, paragraphs 33-35].

Regarding claim 30, Jalfon-Mukherjee further discloses wherein the at least one access point includes a Wi-Fi access point, and the at least one communication interface is configured for communication with a Wi-Fi network [Jalfon, paragraphs 33-35].

Regarding claim 31, Jalfon-Mukherjee further discloses wherein the determination unit further determines whether the at least one access point is included in an authenticated access point list stored in the memory [Mukherjee, paragraph 34], and the authenticated access point list is provided via the receiver [Mukherjee, paragraph 34].

Conclusion

1. **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 WILLIAM GOODCHILD whose telephone number is (571)270-1589. The examiner can normally be reached on Monday - Friday / 8:00 AM - 4:00 PM EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Pwu can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2433

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.

/WILLIAM GOODCHILD/
Primary Examiner, Art Unit 2433

Notice of References Cited	Application/Control No. 14/693,400		Applicant(s)/Patent Under Reexamination LEE, HYOUNG-GON	
	Examiner WILLIAM GOODCHILD		Art Unit 2433	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2008/0052779 A1	02-2008	Sinha; Amit	H04L63/1441	726/22
*	B	US-2007/0097904 A1	05-2007	Mukherjee; Rajat Pritam	H04W12/06	370/328
*	C	US-2011/0083165 A1	04-2011	Gopinath; K. N.	H04W48/04	726/4
*	D	US-2004/0078571 A1	04-2004	Haverinen, Henry	H04L9/0869	713/168
*	E	US-2012/0076072 A1	03-2012	JALFON; Marc	H04W12/02	370/328
	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	CPC 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. 14693400	Applicant(s)/Patent Under Reexamination LEE, HYOUNG-GON
	Examiner WILLIAM GOODCHILD	Art Unit 2433

CPC- SEARCHED		
Symbol	Date	Examiner
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	10/31/2016	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	10/31/2016	WJG
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	9/7/2017	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	9/7/2017	WJG

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	004 text searched	10/31/2016	WJG

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

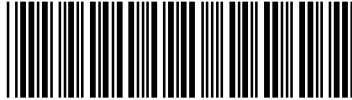
SEARCH NOTES		
Search Notes	Date	Examiner
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	10/31/2016	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	10/31/2016	WJG
Inventor search in PALM and EAST	10/31/2016	WJG
see IP.com search	10/31/2016	WJG
see Google search	10/31/2016	WJG
see EAST search	10/31/2016	WJG
updated EAST search	5/22/2017	WJG
see updated IP.com search	5/22/2017	WJG
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	9/7/2017	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	9/7/2017	WJG
see updated EAST search history	9/7/2017	WJG

	/WILLIAM GOODCHILD/ Primary Examiner.Art Unit 2433
--	---

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/WILLIAM GOODCHILD/
Primary Examiner.Art Unit 2433

<i>Index of Claims</i> 	Application/Control No. 14693400	Applicant(s)/Patent Under Reexamination LEE, HYOUNG-GON
	Examiner WILLIAM GOODCHILD	Art Unit 2433

✓	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	10/31/2016	05/22/2017												
	1	✓	✓												
	2	✓	✓												
	3	✓	✓												
	4	✓	✓												
	5	✓	✓												
	6	✓	✓												
	7	✓	✓												
	8	✓	✓												
	9	✓	✓												
	10	✓	✓												
	11	✓	✓												
	12	✓	✓												
	13	✓	✓												
	14	✓	✓												
	15	✓	✓												
	16	✓	✓												
	17	✓	✓												
	18	✓	✓												
	19	✓	✓												
	20	✓	✓												
	21	✓	-												
	22	✓	✓												
	23	✓	✓												
	24	✓	✓												
	25	✓	✓												
	26	✓	✓												
	27	✓	✓												
	28	✓	✓												
	29	✓	✓												
	30	✓	✓												
	31	✓	✓												

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	292536	(726/004 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/10 H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/09/07 13:11
L2	3049	((fake faked faking false) NEAR3 (id MAC))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/09/07 13:11
L3	311	L1 AND L2	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/09/07 13:11
S1	243862	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:37
S2	20	("7808958", "7185204", "8005458").PN.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:53
S3	41	"20080052779" "20110083165" "20110314147" "20080043686" "20070286143" "20030221006" "20120221955" "20090235077" "20120210395" "20120311328" "20130179943" "20130281056"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:55
S4	12	"20080052779" "20110083165" "20110314147" "20080043686" "20070286143" "20030221006" "20120221955" "20090235077" "20120210395" "20120311328" "20130179943" "20130281056"	US-PGPUB	OR	ON	2016/10/27 07:58
S5	5	"20120076072" "2007007904" "20060150250" "20120064912" "20050059416" "20130301617"	US-PGPUB	OR	ON	2016/10/27 08:18
S6	6	"20120076072" "20070097904" "20060150250" "20120064912" "20050059416" "20130301617"	US-PGPUB	OR	ON	2016/10/27 08:18
S7	20015	((fake faked faking false) SAME (id MAC))	US-PGPUB; USPAT;	OR	ON	2016/10/27 15:58

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S8	243862	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S9	1627	S8 AND S7	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S10	2805	((fake faked faking false) NEAR3 (id MAC))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S11	272	S8 AND S10	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:59
S12	244067	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S13	2805	((fake faked faking false) NEAR3 (id MAC))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S14	188	S12 AND S13 AND (random rnd)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S15	74	((((fake faked faking false) NEAR3 (id MAC)) SAME (rnd random))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:42
S16	14	S12 AND S15	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:42
S17	76	("lee, hyoung-gon").IN.	US-PGPUB; USPAT;	OR	ON	2016/10/29 17:14

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S18	5	"20040264427" "20070060128" "20120201201" "20120230304" "20130150012"	US-PGPUB	OR	ON	2017/05/19 15:56
S19	6	"20040264427" "20070060128" "20120201201" "20120230304" "20130150012" "20130176897"	US-PGPUB	OR	ON	2017/05/19 15:56
S20	12	"2014081427"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/20 13:20
S21	280129	(726/004 H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00 H04L4/00).CLAS,OCLS,CPC,CPCL.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 08:36
S22	3346	((fake faked faking false dummy) SAME MAC)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 08:37
S23	852	((fake faked faking false dummy) NEAR5 MAC)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 08:38
S24	187	S21 AND S23	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 08:38
S25	42	((fake faked faking false dummy) NEAR5 MAC) AND (probe NEAR2 request)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 09:01
S26	31	S21 AND S25	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 09:01
S27	4002	(authenticated SAME access SAME point SAME information)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 12:59
S28	49	(authenticated NEAR5 ((access ADJ point) NEAR2 information))	US-PGPUB; USPAT;	OR	ON	2017/05/22 13:00

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S29	646	(authenticat\$6 NEAR5 ((access ADJ point) NEAR2 information))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:06
S30	6403	(authenticat\$6 NEAR3 ((access ADJ point)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:07
S31	4520	(authenticat\$6 NEAR2 ((access ADJ point)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:07
S32	1771	(authenticat\$6 NEAR2 ((access ADJ point))) SAME (information list)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:07
S33	700	(authenticat\$6 NEAR2 ((access ADJ point))) SAME server SAME (information list)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:13
S34	131	((authenticat\$6 NEAR2 (access ADJ point)) SAME server SAME (MAC NEAR2 address))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:24
S35	82	((authenticat\$6 NEAR2 (access ADJ point)) SAME server SAME (MAC NEAR2 address) SAME (information list))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:57
S36	3360	((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) SAME (send\$5 transmit\$5 request\$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 15:17
S37	1327	((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) NEAR4 (send\$5 transmit\$5 request\$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 15:18
S38	1013	((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) NEAR2 (send\$5	US-PGPUB; USPAT;	OR	ON	2017/05/22 15:18

		transmit\$5 request\$5))	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S39	117	((((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) NEAR2 (send\$5 transmit\$5 request\$5) NEAR2 server)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 15:37

EAST Search History (Interference)

< This search history is empty>

9/ 7/ 2017 1:17:23 PM
C:\ Users\ wgoodchild\ Documents\ EAST\ Workspaces\ 14693400.wsp

Application Serial No. 14/693,400
Response to Final Office Action dated September 11, 2017
Docket No.: 2582-2.737BS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Hyoung-Gon LEE	Examiner:	GOODCHILD, WILLIAM J
Appl. No.:	14/693,400	Art Unit:	2433
Filed:	April 22, 2015	Confirmation No.:	7248
		Docket No.:	2582-2.737BS

To: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

From: Daniel J. Stanger
Customer No. 86636
Brundidge & Stanger, PC
1925 Ballenger Ave., Suite 560
Alexandria, VA 22314

RESPONSE TO FINAL OFFICE ACTION UNDER 37 C.F.R. § 1.116

Sir:

In response to the Final Office Action dated September 11, 2017, entry of the following amendments and consideration of the accompanying remarks is respectfully requested. This paper is being submitted concurrently with a Certification and Request for Consideration under the After Final Consideration Pilot Program 2.0.

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

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

Remarks begin on page 11 of this paper.

AMENDMENTS TO THE SPECIFICATION

Please amend the cross-reference paragraph (as previously submitted on March 2, 2017), on page 1 of specification, as follows:

CROSS-REFERENCE TO RELATED APPLICATIONS

This Application is a Continuation Application under 35 U.S.C. § 120 of U.S. Patent Application [[Ser.]]No. 13/885,754, filed on May 16, 2013, which is a U.S. National Stage filing under 35 U.S.C. § 371 of International Application [[Ser.]]No. PCT/US12/66306, filed on November 21, 2012. The disclosures of both U.S. Patent Application [[Ser.]]No. 13/885,754 and International Application [[Ser.]]No. PCT/US12/66306 are hereby incorporated herein by reference in their entireties.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

1. (Currently Amended) A method performed by a server, the method comprising:
transmitting, by the server to a device, ~~authenticated access point information regarding~~
an authenticated access point list that includes at least one of a media access control (MAC)
address or a service set identifier (SSID) of each of one or more authenticated access points,
wherein the one or more authenticated access points are controlled by the server; and
transmitting, by the server to the device, a fake device identifier, wherein the fake device
identifier includes at least one of one or more random numbers or one or more random characters
to falsely identify the device in a probe request frame in a search for at least one of the one or
more authenticated access points around the device.

2. (Original) The method of Claim 1, wherein the one or more authenticated access points
include a Wi-Fi access point.

3. (Previously Presented) The method of Claim 1, wherein the transmitting the fake
device identifier includes transmitting a fake media access control (MAC) address.

4. (Canceled)

5. (Currently Amended) A method performed by an access point, the method comprising:
receiving, by the access point from a device, a probe request frame that includes a fake
device identifier for the device, wherein the fake device identifier is received at the device from a
server, and wherein the fake device identifier includes at least one of one or more random
numbers or one or more random characters;

transmitting, by the access point to the device, a probe response frame that includes
information regarding the access point;

receiving, by the access point from the device in response to the transmitting the probe
response frame, a connection request that includes an authentic device identifier for the device,

wherein the receiving the connection request includes receiving the connection request in response to an authentication of the access point based on an authenticated point list received at the device from the server, and wherein the authenticated point list includes information that indicates that the access point is an authenticated access point; and

transmitting, by the access point to the device in response to the receiving the connection request, an approval of the connection request, wherein the access point is controlled by the server.

6. (Original) The method of Claim 5, further comprising:
receiving, from the device, an association request;
transmitting, to the device, an association response to the association request; and
facilitating connection of the device to a communication network via the access point in accordance with the association response.

7. (Previously Presented) The method of Claim 6, wherein the access point includes a Wi-Fi access point, and wherein the communication network includes a Wi-Fi network.

8. (Previously Presented) The method of Claim 5, wherein the access point was previously communicatively coupled with the device.

9. (Currently Amended) The method of Claim 5, wherein the authentic device identifier includes a media access control (MAC) address of the device.

10. (Original) The method of Claim 5, wherein the information regarding the access point includes at least one of a media access control (MAC) address of the access point or a service set identifier (SSID) of the access point.

11. (Currently Amended) A method performed by a device, the method comprising:
receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;

receiving, from ~~[[a]]the~~ server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters, to falsely identify the device in a probe request frame;

transmitting, to at least one access point, the probe request frame that includes the received fake device identifier;

receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;

determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, ~~[[that]]whether~~ the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server; and

transmitting, to the at least one access point in response to a determination that at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.

12. (Previously Presented) The method of Claim 11, wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address.

13. (Currently Amended) The method of Claim 11, wherein the determining, ~~based at least, in part, on the information regarding the at least one access point, that~~ whether the information regarding the at least one access point is ~~[[an]]included in the~~ authenticated access point list~~[[,]]~~ comprises~~[[:]]~~ determining ~~[[that]]whether~~ the at least one access point is under control of the server.

14. (Currently Amended) The method of Claim 11, further comprising: ~~wherein the determining, based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point, comprises:~~

~~determining that the at least one access point is included in an authenticated access point list,~~

~~wherein storing the authenticated access point list is stored in a memory; and~~

~~wherein the authenticated access point list is received from the server.~~

15. (Currently Amended) The method of Claim 11, further comprising:
receiving, from the at least one access point, an approval of the connection request;
transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;

receiving, from the at least one access point, an association response to the association request; and

connecting to a communication network via the at least one access point in accordance with the association response.

16. (Currently Amended) A method performed by a device, the method comprising:
receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;

generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

transmitting, to at least one access point, a probe request frame that includes the fake device identifier;

receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;

determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, [[that]]whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining [[that]]whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server, and wherein the determining whether the information

regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of [[a]]the server; and

transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.

17. (Currently Amended) The method of Claim 16, wherein the generating the fake device identifier includes generating a fake media access control (MAC) address.

18. (Original) The method of Claim 16, wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point.

19. (Currently Amended) The method of Claim 16, wherein the determining, ~~based at least, in part, on the information regarding the at least one access point, that~~ whether the at least one access point is [[an]]the authenticated access point[[,]] further includes[[:]] determining [[that]]whether the at least one access point was previously connected with the device.

20. (Currently Amended) The method of Claim 16, further comprising: wherein the determining, based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point, includes:

determining that the at least one access point is included in an storing the authenticated access point list, received from the server, ~~and stored~~ in a memory.

21. (Canceled)

22. (Currently Amended) The method of Claim 16, further comprising:
receiving, from the at least one access point, an approval of the connection request;
transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;

receiving, from the at least one access point, an association response to the association request; and

connecting to a communication network via the at least one access point in accordance with the association response.

23. (Currently Amended) A method performed by a device, the method comprising:
receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;

generating a collection that includes at least one of one or more random numbers or one or more random characters to provide a fake device identifier for the device ~~[[so]]~~to falsely identify the device in a probe request frame;

transmitting, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier;

receiving, from at least one access point around the device in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;

determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, ~~[[that]]whether~~ the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining ~~[[that]]whether the~~ information regarding the at least one access point is included in the authenticated access point list, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of ~~[[a]]the~~ server; and

transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.

24. (Currently Amended) The method of Claim 23, wherein:

the generating the collection that includes the at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address, and

the fake device identifier includes the fake media access control (MAC) address.

25. (Previously Presented) The method of Claim 23, further comprising:
storing the fake device identifier in a memory.

26. (Currently Amended) A system, comprising:
a processor;
at least one communication interface;
a transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame that includes a fake device identifier for a device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

a receiver to;

receive, from the at least one access point via the at least one communication interface, a probe response frame that includes information regarding the at least one access point; and

receive, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;

a memory to store the information regarding the at least one access point, and the authenticated access point list; and

a determination unit to determine, under control of the processor and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of a server,

wherein to determine whether the at least one access point is the authenticated access point and is under control of the server, the determination unit determines whether the information regarding the at least one access point is included in the authenticated access point list, and

wherein the transmitter further transmits to the at least one access point, a connection request that includes an authentic device identifier for the device, in response to a determination by the determination unit that the at least one access point is the authenticated access point and is under control of the server.

27. (Original) The system of Claim 26, wherein the fake device identifier includes a fake media access control (MAC) address.

28. (Previously Presented) The system of Claim 26, further comprising:
a fake device identifier generation unit to generate, under control of the processor, the fake device identifier.

29. (Currently Amended) The system of Claim 26, wherein the memory further stores the fake device identifier.

30. (Currently Amended) The system of Claim 26, wherein the at least one access point includes a Wi-Fi access point, and wherein the at least one communication interface is configured for communication with a Wi-Fi network.

31. (Canceled)

REMARKS

Reconsideration and allowance of the above-identified application are respectfully requested. Claims 1-3, 5-20, and 22-30 are currently pending. Claims 1, 5, 9, 11, 13-17, 19, 20, 22-24, 26, 29, and 30 are currently amended. Support for the amendments can be found at least in paragraphs [0024], [0043], and [0045] of the specification as filed. Claims 4 and 31 are canceled herein without prejudice, while claim 21 was previously canceled without prejudice. No new matter is added.

Claim Rejections – 35 U.S.C. § 103

Claims 1-20 and 22-31 were rejected under pre-AIA 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent Application Publication No. 2012/0076072 (Jalfon) in view of U.S. Patent Application Publication No. 2007/0097904 (Mukherjee).

Note: In the list of references cited (form PTO-892), the Mukherjee reference corresponds to U.S. Application Publication No. 2007/0097904. However, at page 12, in the rejection heading of claims 1-20 and 22-31, it appears that the Office Action has inadvertently cited “U.S. Application Publication No. 2007/007904” as being the Mukherjee reference.

The rejection of claims 1-20 and 22-31 is respectfully addressed as detailed below:

Independent claim 1

It is respectfully submitted that Jalfon and Mukherjee, either alone or in combination, fail to teach or suggest one or more features as set forth in amended independent claim 1.

For example, amended independent claim 1 recites “*transmitting, by the server to a device, an authenticated access point list that includes at least one of a media access control (MAC) address or a service set identifier (SSID) of each of one or more authenticated access points,*” which is not taught or suggested by the combination of Jalfon and Mukherjee.

The Office Action, on page 12, states that “Jalfon does not specifically disclose transmitting, by the server to a device, authenticated access point information regarding one or more authenticated access points, wherein the one or more authenticated access points are controlled by the server.”

However, the Office Action, on page 13, alleges that “Mukherjee teaches access points authenticated by the server that are stored on the wireless nodes [Mukherjee, paragraphs 26 and 34].”

Further, regarding, previously presented claim 4, the Office Action, on page 13, alleges that Mukherjee in paragraph [0034] discloses “transmitting the authenticated access point information regarding the one or more authenticated access points includes transmitting at least one of a media access control (MAC) address or a service set identifier (SSID) of each of the one or more authenticated access points.”

Mukherjee, in paragraphs [0026] and [0034], recites:

“When a wireless node **60** connects to the distribution system, a user name and authentication token (e.g., a password) is entered. This information is passed to the authentication server **90**. The authentication server **90** checks that the information is correct. Also connected to the distribution system is the Internet or other LAN resources **100**. The access point **70** and the wireless nodes **60** operate based upon a PSK or 802.1x protocol, for example ...A first requirement is that all nodes **60**, **70** cache the MAC address of its communicating partner along with the authenticating credential used by it. In office networks where there may be several access points with different MAC addresses using the same AAA authentication token, the MAC addresses of all allowed access points along with the authenticating token of the AAA server (in most cases the public key) be stored on all wireless nodes. The authentication tokens and MAC addresses of all clients are also stored on all access points. In other words, if node B (having, for example, a MAC address of 00-06-5B-15-04-B4 and an authenticating token joe harry56) communicates with node A at some point in the past, node A will cache the MAC address 00-06-5B-15-04-B4 with joe harry56” (emphasis added).

Mukherjee, in the cited portions or elsewhere, describes a plurality of wireless nodes and a plurality of access points, where the plurality of wireless nodes and the plurality of access points are associated with different media access control (MAC) addresses, respectively. When a wireless node from the plurality of wireless nodes connects to a distribution system, a user name and an authentication token is passed to an authentication/AAA server. The authentication/AAA server checks whether the user name and the authentication token is correct or not.

Further, Mukherjee describes that a wireless node does not associate with an access point if both an authentication token and an address for that access point are not on an allowed access point list. Similarly, an access point does not associate with a wireless node if both an authentication token and address for that wireless node are not on an allowed wireless node list. Furthermore, Mukherjee describes that the MAC addresses of all allowed access points along with the authentication token of the authentication/AAA server is stored on all wireless nodes.

Hence, Mukherjee, at best, describes that the wireless nodes store the MAC addresses of the allowed access points to determine if a particular access point is in the allowed access point list.

However, Mukherjee does not teach or suggest that the authentication/AAA server (the alleged “server”) transmits the MAC addresses of the allowed access points to the wireless nodes (the alleged “device”).

In fact, as emphasized above, Mukherjee describes that the wireless node caches MAC addresses of access points with which the wireless node has previously communicated, to generate the allowed access point list. *See*, emphasized recitations of Mukherjee reproduced above.

Since, the wireless node in Mukherjee caches the MAC addresses of the access points, based on its previous communication, to generate the allowed access point list, Mukherjee cannot teach or suggest that the authentication/AAA server (the alleged “server”) transmits the MAC addresses of the allowed access points to the wireless nodes.

In view of the foregoing, Mukherjee fails to teach or suggest “*transmitting, by the server to a device, an authenticated access point list that includes at least one of a media access control (MAC) address or a service set identifier (SSID) of each of one or more authenticated access points,*” as recited by amended independent claim 1.

Further, Jalfon fails to cure the deficiencies of Mukherjee.

Hence, the combination of Jalfon and Mukherjee, fails to teach or suggest one or more features as set forth above in amended independent claim 1.

Accordingly, it is respectfully requested that the rejection of independent claim 1 under pre-AIA 35 U.S.C. § 103(a) be withdrawn.

Independent claims 5, 11, 16, 23, and 26

It is respectfully submitted that Jalfon and Mukherjee, either alone or in combination, fail to teach or suggest one or more features as set forth in amended independent claim 11.

For example, amended independent claim 11 recites “*receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server ... wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server*” (emphasis added), which is not taught or suggested by the combination of Jalfon and Mukherjee.

As discussed above for independent claim 1, Mukherjee fails to teach or suggest transmitting, by the authentication/AAA server, the allowed access point list (*the alleged “authenticated access point list”*) to the wireless nodes. Consequently, Mukherjee cannot teach or suggest “*receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server.*”

Further, as discussed above for independent claim 1, Mukherjee describes that the wireless node does not associate with an access point if the access point is not on the allowed access point list (*the alleged “authenticated access point list”*). However, the allowed access point list of Mukherjee is generated by the wireless node themselves by caching the MAC addresses of the access points with which the wireless node has previously communicated.

Hence, Mukherjee, at best, describes determining whether the MAC address of the access point is in the allowed access point **that is generated** by the wireless node in order to determine whether to associate with the access point or not.

However, Mukherjee nowhere teaches or suggests determining whether the MAC address of the access point is in a list **that is transmitted by the authentication/AAA server**.

In fact, as discussed above, there is no disclosure, in Mukherjee, of any list that includes information regarding allowed access points, being transmitted by the authentication/AAA server to the wireless node. Consequently, Mukherjee cannot teach or suggest “*determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point*

list *that is received from the server*” (emphasis added), as recited by amended independent claim 11.

Further, Jalfon fails to cure the deficiencies of Mukherjee.

Hence, the combination of Jalfon and Mukherjee, fails to teach or suggest one or more features as set forth above in amended independent claim 11.

Amended independent claims 5, 16, 23, and 26 recite analogous features as amended independent claim 11. Hence, the remarks presented above for amended independent claim 11 apply analogously to amended independent claims 5, 16, 23, and 26 as well.

Accordingly, it is respectfully requested that the rejection of independent claims 5, 11, 16, 23, and 26 under pre-AIA 35 U.S.C. § 103(a) be withdrawn.

Dependent claims 2-4, 6-10, 12-15, 17-20, 22, 24-25, and 27-31

Claims 2, 3, 6-10, 12-15, 17-20, 22, 24-25, and 27-30 are also allowable at least by virtue of their dependencies on respective independent claims 1, 5, 11, 16, 23, and 26, which have been shown to be allowable above, and as well as for their additional recited features.

Accordingly, it is respectfully requested that the rejection of claims 2, 3, 6-10, 12-15, 17-20, 22, 24-25, and 27-30 under pre-AIA 35 U.S.C. § 103(a) be withdrawn as well.

The rejection of claims 4 and 31 is rendered moot in view of their cancelation.

Various other amendments are made to the claims as shown, so as to provide more appropriate antecedent basis, to make the recitations within and between related claims more consistent, to more precisely recite the subject matter contained therein, to make typographical/grammatical edits, and/or to otherwise place such claims in better form.

CONCLUSION

Therefore, in light of at least the foregoing, it is respectfully believed that the present application is in condition for allowance. As a result, issuance of a Notice of Allowance for the pending claims is respectfully requested.

The Examiner's consideration of these Amendments and Remarks is appreciated and the Examiner is cordially invited to contact the undersigned, should the Examiner have any questions, comments, or suggestions.

Please charge any fees that may be due to Deposit Account No. 50-4888.

Respectfully submitted,

Brundidge & Stanger, P.C.

Date: November 13, 2017

By: /Daniel J. Stanger/
Daniel J. Stanger
Reg. No.: 32,846

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0		
Practitioner Docket No.: 2582-2.737BS	Application No.: 14/693,400	Filing Date: April 22, 2015
First Named Inventor: Hyoung-Gon LEE	Title: SCHEMES FOR CONNECTING TO WIRELESS NETWORK	
APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116. 1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (<i>e.g.</i>, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c). 2. The above-identified application contains an outstanding final rejection. 3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect. 4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection. 5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response. 6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web). 7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, <i>e.g.</i>, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.] 8. By filing this certification and request, applicant acknowledges the following: • Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0. • The examiner will verify that the AFCP 2.0 submission is compliant, <i>i.e.</i>, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions: ○ The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, <i>e.g.</i>, by mailing an advisory action. ○ If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview. ▪ The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate. ▪ If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116.		
Signature /Daniel J. Stanger/	Date November 13, 2017	
Name (Print/Typed) Daniel J. Stanger	Practitioner Registration No. 32,846	
Note: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.		
☐ * Total of _____ forms are submitted.		

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:	30929374
Application Number:	14693400
International Application Number:	
Confirmation Number:	7248
Title of Invention:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK
First Named Inventor/Applicant Name:	Hyoung-Gon LEE
Customer Number:	86636
Filer:	Daniel John Stanger/Mariah Duell
Filer Authorized By:	Daniel John Stanger
Attorney Docket Number:	2582-2.737BS
Receipt Date:	13-NOV-2017
Filing Date:	22-APR-2015
Time Stamp:	14:21:35
Application Type:	Utility under 35 USC 111(a)

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	Response After Final Action	KR-839496-03-US- CON_20171113_FinalOA_Resp onse.pdf	92064 b0cb4a4131ec0a5688e8285128b172cf4da 546fa	no	16

Warnings:

Information:					
2	After Final Consideration Program Request	KR-839496-03-US-CON_20171113_AFCP.PDF	226647	no	2
			f1f221eb7fd1c948ac689ad685fb295709d4a359		
Warnings:					
Information:					
Total Files Size (in bytes):				318711	
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.					

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 14/693,400	Filing Date 04/22/2015	☐ To be Mailed
---	---	----------------------------------	---------------------------------------

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO**APPLICATION AS FILED – PART I**

(Column 1)

(Column 2)

FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	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 \$310 (\$155 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))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

(Column 1)

(Column 2)

(Column 3)

AMENDMENT	11/13/2017	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 28	Minus	** 31	= 0	X \$80 =	0
	Independent (37 CFR 1.16(h))	* 6	Minus	***6	= 0	X \$420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
TOTAL ADD'L FEE						0	

(Column 1)

(Column 2)

(Column 3)

AMENDMENT	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$ =
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =
	☐ Application Size Fee (37 CFR 1.16(s))					
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					
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.

LIE
JAMES MASON

This collection of information is required by 37 CFR 1.16. 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, 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.

AFCP 2.0 Decision

Application No.

14/693,400

Applicant(s)

LEE, Hyoung-Gon

Examiner

WILLIAM J GOODCHILD

Art Unit

2433

AIA Status

No

This is in response to the After Final Consideration Pilot request filed 13 November 2017.

1. Improper Request – The AFCP 2.0 request is improper for the following reason(s) and the after final amendment submitted with the request will be treated under pre-pilot procedure.

- ☐ An AFCP 2.0 request form PTO/SB/434 (or equivalent document) was not submitted.
- ☐ A non-broadening amendment to at least one independent claim was not submitted.
- ☐ A proper AFCP 2.0 request was submitted in response to the most recent final rejection.
- ☐ Other: _____

2. Proper Request

A. After final amendment submitted with the request will not be treated under AFCP 2.0.

The after final amendment cannot be reviewed and a search conducted within the guidelines of the pilot program.

- ☐ The after final amendment will be treated under pre-pilot procedure.

B. Updated search and/or completed additional consideration.

The examiner performed an updated search and/or completed additional consideration of the after final amendment within the time authorized for the pilot program. The result(s) of the updated search and/or completed additional consideration are:

- ☒ 1. All of the rejections in the most recent final Office action are overcome and a Notice of Allowance is issued herewith.
- ☐ 2. The after final amendment would not overcome all of the rejections in the most recent final Office action.
See attached interview summary for further details.
- ☐ 3. The after final amendment was reviewed, and it raises a new issue(s). See attached interview summary for further details.
- ☐ 4. The after final amendment raises new issues, but would overcome all of the rejections in the most recent final Office action. A decision on determining allowability could not be made within the guidelines of the pilot. See attached interview summary for further details, including any newly discovered prior art.
- ☐ 5. Other: _____

Examiner Note: Please attach an interview summary when necessary as described above.

Application Serial No. 14/693,400
Response to Final Office Action dated September 11, 2017
Docket No.: 2582-2.737BS OK TO ENTER: /WJG/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Hyoung-Gon LEE	Examiner:	GOODCHILD, WILLIAM J
Appl. No.:	14/693,400	Art Unit:	2433
Filed:	April 22, 2015	Confirmation No.:	7248
		Docket No.:	2582-2.737BS

To: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, VA 22313-1450

From: Daniel J. Stanger
 Customer No. 86636
 Brundidge & Stanger, PC
 1925 Ballenger Ave., Suite 560
 Alexandria, VA 22314

RESPONSE TO FINAL OFFICE ACTION UNDER 37 C.F.R. § 1.116

Sir:

In response to the Final Office Action dated September 11, 2017, entry of the following amendments and consideration of the accompanying remarks is respectfully requested. This paper is being submitted concurrently with a Certification and Request for Consideration under the After Final Consideration Pilot Program 2.0.

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

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

Remarks begin on page 11 of this paper.



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. 7248

SERIAL NUMBER 14/693,400	FILING or 371(c) DATE 04/22/2015 RULE	CLASS 726	GROUP ART UNIT 2433	ATTORNEY DOCKET NO. 2582-2.737BS		
APPLICANTS Empire Technology Development LLC, Wilmington, DE; INVENTORS Hyoung-Gon LEE, Seoul, KOREA, REPUBLIC OF; ** CONTINUING DATA ***** This application is a CON of 13/885,754 05/16/2013 PAT 9717005 which is a 371 of PCT/US12/66306 11/21/2012 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 05/01/2015						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and <u>/WILLIAM J GOODCHILD/</u> Acknowledged <u>Examiner's Signature</u>		☐ Met after Allowance <u>Initials</u>	STATE OR COUNTRY KOREA, REPUBLIC OF	SHEETS DRAWINGS 6	TOTAL CLAIMS 31	INDEPENDENT CLAIMS 6
ADDRESS BRUNDIDGE & STANGER, P.C. 1925 BALLENGER AVENUE, STE. 560 ALEXANDRIA, VA 22314 UNITED STATES						
TITLE SCHEMES FOR CONNECTING TO WIRELESS NETWORK						
FILING FEE RECEIVED 3740	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			



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

86636 7590 12/14/2017
BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

EXAMINER

GOODCHILD, WILLIAM J

ART UNIT

PAPER NUMBER

2433

DATE MAILED: 12/14/2017

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/693,400	04/22/2015	Hyoung-Gon LEE	2582-2.737BS	7248
TITLE OF INVENTION: SCHEMES FOR CONNECTING TO WIRELESS NETWORK				

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	03/14/2018

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: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

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)

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.

86636 7590 12/14/2017
BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

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.
14/693,400	04/22/2015	Hyoung-Gon LEE	2582-2.737BS	7248

TITLE OF INVENTION: SCHEMES FOR CONNECTING TO WIRELESS NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	03/14/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
GOODCHILD, WILLIAM J	2433	726-004000

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 credits 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
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

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.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



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.
14/693,400	04/22/2015	Hyoung-Gon LEE	2582-2.737BS	7248

86636	7590	12/14/2017
BRUNDIDGE & STANGER, P.C.		
1925 BALLENGER AVENUE, STE. 560		
ALEXANDRIA, VA 22314		

EXAMINER	
GOODCHILD, WILLIAM J	

ART UNIT	PAPER NUMBER
2433	

DATE MAILED: 12/14/2017

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

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.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B 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.

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. 14/693,400	Applicant(s) LEE, Hyoung-Gon	
	Examiner WILLIAM J GOODCHILD	Art Unit 2433	AIA 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 11/13/2017 .
☐ 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 1-3,5-20 and 22-30 . 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: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file areply 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 _____ .

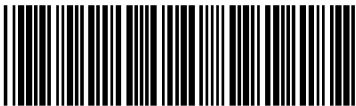
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

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 <u>PTO-2323</u> .
---	---

/William J. Goodchild/
Primary Examiner, Art Unit 2433

<i>Search Notes</i> 	Application/Control No. 14/693,400	Applicant(s)/Patent Under Reexamination LEE, Hyoung-Gon
	Examiner WILLIAM J GOODCHILD	Art Unit 2433

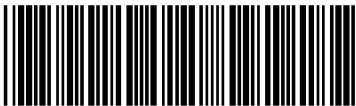
CPC - Searched*		
Symbol	Date	Examiner
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	10/31/2016	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	10/31/2016	WJG
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	9/7/2017	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	9/7/2017	WJG

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
726	004 text searched	10/31/2016	WJG

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/WILLIAM GOODCHILD/ Primary Examiner.Art Unit 2433	
--	--

<i>Search Notes</i> 	Application/Control No. 14/693,400	Applicant(s)/Patent Under Reexamination LEE, Hyoung-Gon
	Examiner WILLIAM J GOODCHILD	Art Unit 2433

Search Notes		
Search Notes	Date	Examiner
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	10/31/2016	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	10/31/2016	WJG
Inventor search in PALM and EAST	10/31/2016	WJG
see IP.com search	10/31/2016	WJG
see Google search	10/31/2016	WJG
see EAST search	10/31/2016	WJG
updated EAST search	5/22/2017	WJG
see updated IP.com search	5/22/2017	WJG
H04W 12/08 8/26 12/06 48/20 84/12 88/08 12/08 8/26 12/06 text searched	9/7/2017	WJG
H04L 63/10 63/08 63/0815 63/00 text searched	9/7/2017	WJG
see updated EAST search history	9/7/2017	WJG
see updated EAST search history	11/16/2017	WJG

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
	Claims text searched	11/16/2017	WJG

/WILLIAM GOODCHILD/ Primary Examiner.Art Unit 2433	
--	--

<i>Index of Claims</i> 	Application/Control No. 14/693,400	Applicant(s)/Patent Under Reexamination LEE, Hyoung-Gon
	Examiner WILLIAM J GOODCHILD	Art Unit 2433

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS										
☐ Claims renumbered in the same order as presented by applicant					☐ CPA		☐ T.D.		☐ R.1.47	
CLAIM		DATE								
Final	Original	10/31/2016	05/22/2017	11/16/2017						
	1	✓	✓	=						
	2	✓	✓	=						
	3	✓	✓	=						
	4	✓	✓	-						
	5	✓	✓	=						
	6	✓	✓	=						
	7	✓	✓	=						
	8	✓	✓	=						
	9	✓	✓	=						
	10	✓	✓	=						
	11	✓	✓	=						
	12	✓	✓	=						
	13	✓	✓	=						
	14	✓	✓	=						
	15	✓	✓	=						
	16	✓	✓	=						
	17	✓	✓	=						
	18	✓	✓	=						
	19	✓	✓	=						
	20	✓	✓	=						
	21	✓	-							
	22	✓	✓	=						
	23	✓	✓	=						
	24	✓	✓	=						
	25	✓	✓	=						
	26	✓	✓	=						
	27	✓	✓	=						
	28	✓	✓	=						
	29	✓	✓	=						
	30	✓	✓	=						
	31	✓	✓	-						

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	243862	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:37
S2	20	("7808958", "7185204", "8005458").PN.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:53
S3	41	"20080052779" "20110083165" "20110314147" "20080043686" "20070286143" "20030221006" "20120221955" "20090235077" "20120210395" "20120311328" "20130179943" "20130281056"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 07:55
S4	12	"20080052779" "20110083165" "20110314147" "20080043686" "20070286143" "20030221006" "20120221955" "20090235077" "20120210395" "20120311328" "20130179943" "20130281056"	US-PGPUB	OR	ON	2016/10/27 07:58
S5	5	"20120076072" "2007007904" "20060150250" "20120064912" "20050059416" "20130301617"	US-PGPUB	OR	ON	2016/10/27 08:18
S6	6	"20120076072" "20070097904" "20060150250" "20120064912" "20050059416" "20130301617"	US-PGPUB	OR	ON	2016/10/27 08:18
S7	20015	((fake faked faking false) SAME (id MAC))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S8	243862	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S9	1627	S8 AND S7	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:58
S10	2805	((fake faked faking false) NEAR3 (id MAC))	US-PGPUB; USPAT;	OR	ON	2016/10/27 15:58

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S11	272	S8 AND S10	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/27 15:59
S12	244067	(H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S13	2805	((fake faked faking false) NEAR3 (id MAC))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S14	188	S12 AND S13 AND (random rnd)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:41
S15	74	((((fake faked faking false) NEAR3 (id MAC)) SAME (rnd random))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:42
S16	14	S12 AND S15	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 16:42
S17	76	("lee, hyoung-gon").IN.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 17:14
S18	5	"20040264427" "20070060128" "20120201201" "20120230304" "20130150012"	US-PGPUB	OR	ON	2017/05/19 15:56
S19	6	"20040264427" "20070060128" "20120201201" "20120230304" "20130150012" "20130176897"	US-PGPUB	OR	ON	2017/05/19 15:56
S20	12	"2014081427"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/20 13:20
S21	280129	(726/004 H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04W48/20	US-PGPUB; USPAT;	OR	ON	2017/05/22 08:36

		H04W84/12 H04W88/08 H04L63/0815 H04L63/10 H04L63/00 H04L4/00).CLAS,CCLS,CPC,CPCL.	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S22	3346	((fake faked faking false dummy) SAME MAC)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 08:37
S23	852	((fake faked faking false dummy) NEAR5 MAC)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 08:38
S24	187	S21 AND S23	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 08:38
S25	42	((fake faked faking false dummy) NEAR5 MAC) AND (probe NEAR2 request)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 09:01
S26	31	S21 AND S25	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 09:01
S27	4002	(authenticated SAME access SAME point SAME information)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 12:59
S28	49	(authenticated NEAR5 ((access ADJ point) NEAR2 information))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 13:00
S29	646	(authenticated\$6 NEAR5 ((access ADJ point) NEAR2 information))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:06
S30	6403	(authenticated\$6 NEAR3 ((access ADJ point)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:07
S31	4520	(authenticated\$6 NEAR2 ((access ADJ point)))	US-PGPUB; USPAT;	OR	ON	2017/05/22 14:07

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S32	1771	((authenticat\$6 NEAR2 ((access ADJ point))) SAME (information list))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:07
S33	700	((authenticat\$6 NEAR2 ((access ADJ point))) SAME server SAME (information list))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:13
S34	131	((authenticat\$6 NEAR2 (access ADJ point)) SAME server SAME (MAC NEAR2 address))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:24
S35	82	((authenticat\$6 NEAR2 (access ADJ point)) SAME server SAME (MAC NEAR2 address) SAME (information list))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 14:57
S36	3360	((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) SAME (send\$5 transmit\$5 request\$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 15:17
S37	1327	((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) NEAR4 (send\$5 transmit\$5 request\$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 15:18
S38	1013	((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) NEAR2 (send\$5 transmit\$5 request\$5))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 15:18
S39	117	((authoriz\$7 authenticat\$6) NEAR2 (access ADJ point)) NEAR2 (send\$5 transmit\$5 request\$5) NEAR2 server)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/05/22 15:37
S40	292536	(726/004 H04W12/08 H04W8/26 H04W12/06 H04W48/20 H04W84/12 H04W88/08 H04L63/10 H04L63/08 H04W12/08 H04W8/26 H04W12/06 H04L63/0815 H04L63/10 H04L63/00).CLAS,CCLS,CPC,CPCL.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/09/07 13:11
S41	3049	((fake faked faking false) NEAR3 (id MAC))	US-PGPUB; USPAT;	OR	ON	2017/09/07 13:11

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S42	311	S40 AND S41	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/09/07 13:11
S43	83	((fake faked faking false) SAME (probe ADJ request))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/11/16 13:33
S44	7	((((fake faked faking false) NEAR3 (id! identif\$5)) SAME (probe ADJ request))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/11/16 13:40

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S45	7	((((fake faked faking false) AND (id! identif\$5)) AND (probe ADJ request)).CLM.	US-PGPUB; USPAT	OR	ON	2017/11/16 14:11

11/16/2017 3:04:48 PM
C:\Users\wgoodchild\Documents\EAST\Workspaces\14693400.wsp

Issue Classification 	Application/Control No. 14/693,400	Applicant(s)/Patent Under Reexamination LEE, Hyoung-Gon
	Examiner WILLIAM J GOODCHILD	Art Unit 2433

CPC						
Symbol					Type	Version
H04W	/	12	/	08	F	2013-01-01
H04W	/	8	/	26	I	2013-01-01
H04W	/	48	/	20	I	2013-01-01
H04W	/	12	/	06	I	2013-01-01
H04L	/	63	/	10	I	2013-01-01
H04W	/	84	/	12	A	2013-01-01
H04W	/	88	/	08	A	2013-01-01

CPC Combination Sets							
Symbol					Type	Set	Ranking
	/		/				

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	28	
/William J. Goodchild/ Primary Examiner, Art Unit 2433	16 November 2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5

Issue Classification 	Application/Control No. 14/693,400	Applicant(s)/Patent Under Reexamination LEE, Hyoung-Gon
	Examiner WILLIAM J GOODCHILD	Art Unit 2433

INTERNATIONAL CLASSIFICATION			
CLAIMED			
H04W	/	12	/ 08
NON-CLAIMED			
	/		/

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE		Total Claims Allowed:	
(Assistant Examiner)		28	
(Date)			
/William J. Goodchild/ Primary Examiner, Art Unit 2433		16 November 2017	
(Primary Examiner)		(Date)	
		O.G. Print Claim(s)	O.G. Print Figure
		1	5

Issue Classification 	Application/Control No. 14/693,400	Applicant(s)/Patent Under Reexamination LEE, Hyoung-Gon
	Examiner WILLIAM J GOODCHILD	Art Unit 2433

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47															
CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	9	10	18	19	26	28								
2	2	10	11	19	20	27	29								
3	3	11	12		21	28	30								
	4	12	13	20	22		31								
4	5	13	14	21	23										
5	6	14	15	22	24										
6	7	15	16	23	25										
7	8	16	17	24	26										
8	9	17	18	25	27										

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 28	
/William J. Goodchild/ Primary Examiner, Art Unit 2433 (Primary Examiner) _____ (Date) _____		16 November 2017	O.G. Print Claim(s) 1 O.G. Print Figure 5



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	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
14/693,400		2433	



Correspondence Address/Fee Address Change

The following fields have been set to Customer Number 151685 on 01/31/2018

- Correspondence Address
- Maintenance Fee Address

The address of record for Customer Number 151685 is:

151685
Clairvoilex Inc.
Allied Inventors
111 E. Broadway
Suite 725
Salt Lake City, UT 84111

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Hyoung-Gon LEE	Examiner:	GOODCHILD, WILLIAM J.
Application No.:	14/693,400	Confirmation No:	7248
Filed:	April 22, 2015	Docket No.:	2582-2.737BS
Title:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK		

TRANSMITTAL AND AMENDMENT UNDER 37 CFR § 1.312

Sir:

This paper is responsive to the Notice of Allowance mailed on December 14, 2017.

Please enter the following amendments:

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

Amendments to the Claims begin on page 3 of this paper.

Remarks begin on page 11 of this paper.

AMENDMENTS TO THE SPECIFICATION

Please amend the cross-reference paragraph (as previously amended on November 13, 2017), on page 1 of the specification, as follows:

CROSS-REFERENCE TO RELATED APPLICATIONS

This Application is a Continuation Application under 35 U.S.C. § 120 of U.S. Patent Application No. 13/885,754, filed on May 16, 2013, now U.S. Patent No. 9,717,005, which is a U.S. National Stage filing under 35 U.S.C. § 371 of International Application No. PCT/US12/66306, filed on November 21, 2012. The disclosures of both U.S. Patent Application No. 13/885,754 and International Application No. PCT/US12/66306 are hereby incorporated herein by reference in their entireties.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

1. (Previously Presented) A method performed by a server, the method comprising:
transmitting, by the server to a device, an authenticated access point list that includes at least one of a media access control (MAC) address or a service set identifier (SSID) of each of one or more authenticated access points, wherein the one or more authenticated access points are controlled by the server; and

transmitting, by the server to the device, a fake device identifier, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame in a search for at least one of the one or more authenticated access points around the device.

2. (Original) The method of Claim 1, wherein the one or more authenticated access points include a Wi-Fi access point.

3. (Previously Presented) The method of Claim 1, wherein the transmitting the fake device identifier includes transmitting a fake media access control (MAC) address.

4. (Canceled)

5. (Previously Presented) A method performed by an access point, the method comprising:

receiving, by the access point from a device, a probe request frame that includes a fake device identifier for the device, wherein the fake device identifier is received at the device from a server, and wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

transmitting, by the access point to the device, a probe response frame that includes information regarding the access point;

receiving, by the access point from the device in response to the transmitting the probe response frame, a connection request that includes an authentic device identifier for the device,

wherein the receiving the connection request includes receiving the connection request in response to an authentication of the access point based on an authenticated point list received at the device from the server, and wherein the authenticated point list includes information that indicates that the access point is an authenticated access point; and

transmitting, by the access point to the device in response to the receiving the connection request, an approval of the connection request, wherein the access point is controlled by the server.

6. (Original) The method of Claim 5, further comprising:
receiving, from the device, an association request;
transmitting, to the device, an association response to the association request; and
facilitating connection of the device to a communication network via the access point in accordance with the association response.

7. (Previously Presented) The method of Claim 6, wherein the access point includes a Wi-Fi access point, and wherein the communication network includes a Wi-Fi network.

8. (Previously Presented) The method of Claim 5, wherein the access point was previously communicatively coupled with the device.

9. (Previously Presented) The method of Claim 5, wherein the authentic device identifier includes a media access control (MAC) address of the device.

10. (Original) The method of Claim 5, wherein the information regarding the access point includes at least one of a media access control (MAC) address of the access point or a service set identifier (SSID) of the access point.

11. (Currently Amended) A method performed by a device, the method comprising:
receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;

receiving, from the server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters[[,]] to falsely identify the device in a probe request frame;

transmitting, to at least one access point, the probe request frame that includes the received fake device identifier;

receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;

determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server; and

transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.

12. (Previously Presented) The method of Claim 11, wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address.

13. (Previously Presented) The method of Claim 11, wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list comprises determining whether the at least one access point is under control of the server.

14. (Previously Presented) The method of Claim 11, further comprising:
storing the authenticated access point list in a memory.

15. (Previously Presented) The method of Claim 11, further comprising:
receiving, from the at least one access point, an approval of the connection request;

transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;

receiving, from the at least one access point, an association response to the association request; and

connecting to a communication network via the at least one access point in accordance with the association response.

16. (Previously Presented) A method performed by a device, the method comprising: receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;

generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

transmitting, to at least one access point, a probe request frame that includes the fake device identifier;

receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;

determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server; and

transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.

17. (Previously Presented) The method of Claim 16, wherein the generating the fake device identifier includes generating a fake media access control (MAC) address.

18. (Original) The method of Claim 16, wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point.

19. (Previously Presented) The method of Claim 16, wherein the determining whether the at least one access point is the authenticated access point further includes determining whether the at least one access point was previously connected with the device.

20. (Previously Presented) The method of Claim 16, further comprising:
storing the authenticated access point list, received from the server, in a memory.

21. (Canceled)

22. (Previously Presented) The method of Claim 16, further comprising:
receiving, from the at least one access point, an approval of the connection request;
transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;
receiving, from the at least one access point, an association response to the association request; and
connecting to a communication network via the at least one access point in accordance with the association response.

23. (Previously Presented) A method performed by a device, the method comprising:
receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
generating a collection that includes at least one of one or more random numbers or one or more random characters to provide a fake device identifier for the device to falsely identify the device in a probe request frame;
transmitting, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier;

receiving, from at least one access point around the device in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;

determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server; and

transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.

24. (Previously Presented) The method of Claim 23, wherein:

the generating the collection that includes the at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address, and

the fake device identifier includes the fake media access control (MAC) address.

25. (Previously Presented) The method of Claim 23, further comprising:

storing the fake device identifier in a memory.

26. (Currently Amended) A system, comprising:

a processor;

at least one communication interface;

a transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame that includes a fake device identifier for a device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;

a receiver to:

receive, from the at least one access point via the at least one communication interface, a probe response frame that includes information regarding the at least one access point; and

receive, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;

a memory to store the information regarding the at least one access point, and the authenticated access point list; and

a determination unit to determine, under control of the processor and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of ~~[[a]]~~the server,

wherein to determine whether the at least one access point is the authenticated access point and is under control of the server, the determination unit determines whether the information regarding the at least one access point is included in the authenticated access point list, and

wherein the transmitter further transmits to the at least one access point, a connection request that includes an authentic device identifier for the device, in response to a determination by the determination unit that the at least one access point is the authenticated access point and is under control of the server.

27. (Original) The system of Claim 26, wherein the fake device identifier includes a fake media access control (MAC) address.

28. (Previously Presented) The system of Claim 26, further comprising:

a fake device identifier generation unit to generate, under control of the processor, the fake device identifier.

29. (Previously Presented) The system of Claim 26, wherein the memory further stores the fake device identifier.

30. (Previously Presented) The system of Claim 26, wherein the at least one access point includes a Wi-Fi access point, and wherein the at least one communication interface is configured for communication with a Wi-Fi network.

31. (Canceled)

REMARKS

The present amendments are submitted after the Notice of Allowance in accordance with 37 CFR § 1.312.

Amendments to the Specification

The specification is amended to correct minor informalities in the Cross-Reference to Related Applications section. By entry of this amendment, the specification is made consistent with the other papers that are of record in the file wrapper of the present application. Entry of the amendments to the specification is respectfully requested.

Amendments to the Claims

Claims 11 and 26 have been amended to provide clarity, consistent use of terminology, and to correct minor informalities identified during review of the application. Entry of the amendments to claim 11 and 26 is respectfully requested.

CONCLUSION

In view of the foregoing amendments, it is respectfully requested that the amendments made to the present application be entered prior to patent issue, as allowed by 37 CFR § 1.312. If the Examiner has any questions or comments concerning this matter, the Examiner is invited to contact the undersigned attorney at the number below.

Sincerely,

/Stephen B. Schott /
Stephen B. Schott
Registration No. 51294
Spruce Law Group, LLC
1622 Spruce St
Philadelphia PA 19103
267.546.0624

Electronic Acknowledgement Receipt

EFS ID:	32015790
Application Number:	14693400
International Application Number:	
Confirmation Number:	7248
Title of Invention:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK
First Named Inventor/Applicant Name:	Hyoung-Gon LEE
Customer Number:	151685
Filer:	Stephen Burke Schott
Filer Authorized By:	
Attorney Docket Number:	2582-2.737BS
Receipt Date:	10-MAR-2018
Filing Date:	22-APR-2015
Time Stamp:	14:58:32
Application Type:	Utility under 35 USC 111(a)

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		KR-839496-03-US- CON_1312_Amendment_DMD 2.pdf	146959 585548c2558d346b6440cd9efc85ff23d311 27cf	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Amendment after Notice of Allowance (Rule 312)	1	1
	Specification	2	2
	Claims	3	10
	Applicant Arguments/Remarks Made in an Amendment	11	12

Warnings:

Information:

Total Files Size (in bytes):	146959
-------------------------------------	--------

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.

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)

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.

151685 7590 12/14/2017
BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

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.
14/693,400	04/22/2015	Hyoung-Gon LEE	2582-2.737BS	7248

TITLE OF INVENTION: SCHEMES FOR CONNECTING TO WIRELESS NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	03/14/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
GOODCHILD, WILLIAM J	2433	726-004000

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 Brundidge & Stanger, P.C.

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)

EMPIRE TECHNOLOGY DEVELOPMENT LLC

WILMINGTON, DE (US)

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 credits any overpayment, to Deposit Account Number 50-4888 (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
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

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.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Daniel J. Stanger/

Date March 14, 2018

Typed or printed name Daniel J. Stanger

Registration No. 32,846

Electronic Patent Application Fee Transmittal

Application Number:	14693400			
Filing Date:	22-Apr-2015			
Title of Invention:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK			
First Named Inventor/Applicant Name:	Hyoung-Gon LEE			
Filer:	Daniel John Stanger			
Attorney Docket Number:	2582-2.737BS			
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
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:				
UTILITY APPL ISSUE FEE	1501	1	960	960

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				960

Electronic Acknowledgement Receipt

EFS ID:	32045545
Application Number:	14693400
International Application Number:	
Confirmation Number:	7248
Title of Invention:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK
First Named Inventor/Applicant Name:	Hyoung-Gon LEE
Customer Number:	151685
Filer:	Daniel John Stanger/Mariah Duell
Filer Authorized By:	Daniel John Stanger
Attorney Docket Number:	2582-2.737BS
Receipt Date:	14-MAR-2018
Filing Date:	22-APR-2015
Time Stamp:	11:34:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$960
RAM confirmation Number	031418INTEFSW00011984504888
Deposit Account	504888
Authorized User	Mariah Duell

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

Petitioner's Exhibit 1003 Page 273 of 285

37 CFR 1.19 (Document supply fees)
37 CFR 1.20 (Post Issuance fees)
37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	KR-839496-03-US-CON_20180314_IssueFee_payment.pdf	1110729	no	1
			b650b22af924b7b7fd6b82adec57b34f82a1da52		

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30720	no	2
			c9dae66455967a64eb4b1605c7641661c5be1c1e		

Warnings:

Information:

Total Files Size (in bytes):	1141449
-------------------------------------	---------

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.

OK TO ENTER: /WJG/ 03/14/2018

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	HyounG-Gon LEE	Examiner:	GOODCHILD, WILLIAM J.
Application No.:	14/693,400	Confirmation No:	7248
Filed:	April 22, 2015	Docket No.:	2582-2.737BS
Title:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK		

TRANSMITTAL AND AMENDMENT UNDER 37 CFR § 1.312

Sir:

This paper is responsive to the Notice of Allowance mailed on December 14, 2017.

Please enter the following amendments:

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

Amendments to the Claims begin on page 3 of this paper.

Remarks begin on page 11 of this paper.



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.
14/693,400	04/22/2015	Hyoung-Gon LEE	2582-2.737BS	7248
151685	7590	03/16/2018	EXAMINER	
Clairvortex Inc.			GOODCHILD, WILLIAM J	
Allied Inventors			ART UNIT	PAPER NUMBER
111 E. Broadway			2433	
Suite 725			MAIL DATE	DELIVERY MODE
Salt Lake City, UTAH 84111			03/16/2018	PAPER
UNITED STATES OF AMERICA				

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.

Response to Rule 312 Communication	Application No.	Applicant(s)	
	14/693,400	LEE, Hyoung-Gon	
	Examiner	Art Unit	AIA Status
	WILLIAM J GOODCHILD	2433	No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

1. ☒ The amendment filed on 10 March 2018 under 37 CFR 1.312 has been considered, and has been:

a) ☒ entered.

b) ☒ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

/William J. Goodchild/ Primary Examiner, Art Unit 2433	
---	--

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	14/693,400
Filing Date	04/22/2015
First Named Inventor	LEE, Hyoung-Gon
Title	SCHEMES FOR CONNECTING TO WIRELESS NETWORK
Art Unit	2433
Examiner Name	GOODCHILD, WILLIAM J
Attorney Docket Number	2582-2.737BS

SIGNATURE of Applicant or Patent Practitioner

Signature	/Ajay K. Gambhir/	Date (Optional)	March 28, 2018
Name	Ajay K. Gambhir	Registration Number	44,115
Title (if Applicant is a juristic entity)	Attorney for Applicant		
Applicant Name (if Applicant is a juristic entity)	EMPIRE TECHNOLOGY DEVELOPMENT, LLC		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐

*Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 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.**

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☒ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above:

154241

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above 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 (if the Applicant is a juristic entity, list the Applicant name in the box):

Empire Technology Development LLC

- ☐ Inventor or Joint Inventor (title not required below)
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)
- ☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature

Date (Optional)

March 13, 2018

Name

Dong-Gun Kim

Title

CFO

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 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.

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.

Electronic Acknowledgement Receipt

EFS ID:	32189687
Application Number:	14693400
International Application Number:	
Confirmation Number:	7248
Title of Invention:	SCHEMES FOR CONNECTING TO WIRELESS NETWORK
First Named Inventor/Applicant Name:	Hyoung-Gon LEE
Customer Number:	151685
Filer:	Ajay K. Gambhir/Dawn Minter
Filer Authorized By:	Ajay K. Gambhir
Attorney Docket Number:	2582-2.737BS
Receipt Date:	28-MAR-2018
Filing Date:	22-APR-2015
Time Stamp:	22:07:06
Application Type:	Utility under 35 USC 111(a)

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	Power of Attorney	2582-2737BS_aia0082.pdf	354001	no	3
			08b79079541d69e4a3be5a1bf67d5794f48329b2		

Warnings:

Information:	
Total Files Size (in bytes):	354001
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/693,400	04/22/2015	Hyoung-Gon LEE	2582-2.737BS

CONFIRMATION NO. 7248

POA ACCEPTANCE LETTER



154241
IP Spring - AI
180 N. LaSalle St.
Suite 3700
Chicago, IL 60601

Date Mailed: 04/04/2018

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 03/28/2018.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/afesschaye/



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
14/693,400	04/22/2015	Hyoung-Gon LEE	2582-2.737BS

CONFIRMATION NO. 7248

POWER OF ATTORNEY NOTICE



151685
Clairvoilex Inc.
Allied Inventors
111 E. Broadway
Suite 725
Salt Lake City, UT 84111

Date Mailed: 04/04/2018

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 03/28/2018.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/afesschaye/



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.
14/693,400	05/01/2018	9961552	2582-2.737BS	7248

154241 7590 04/11/2018
IP Spring - AI
180 N. LaSalle St.
Suite 3700
Chicago, IL 60601

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 107 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):

HyounG-Gon LEE, Seoul, KOREA, REPUBLIC OF;
Empire Technology Development LLC, Wilmington, DE;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.