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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 May 2014 (30.05.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/081427 A1

(51) International Patent Classification:
G06F 7/04 (2006.01)

(21) International Application Number:
PCT/US2012/066306

(22) International Filing Date:
21 November 2012 (21.11.2012)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **EMPIRE TECHNOLOGY DEVELOPMENT** [US/US]; 2711 Centerville Road, Suite 400, Wilmington, DE 19808 (US).

(72) Inventor: **LEE, Hyoung-Gon**; 101-705, Daechi Hyundai Apt. 974, Daechi 2-dong, Gangnam-gu, Seoul 135-850 (KR).

(74) Agent: **LEE, David, S.**; Brundidge & Stanger, P.C., 2318 Mill Road, Suite 1020, Alexandria, VA 22314 (US).

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

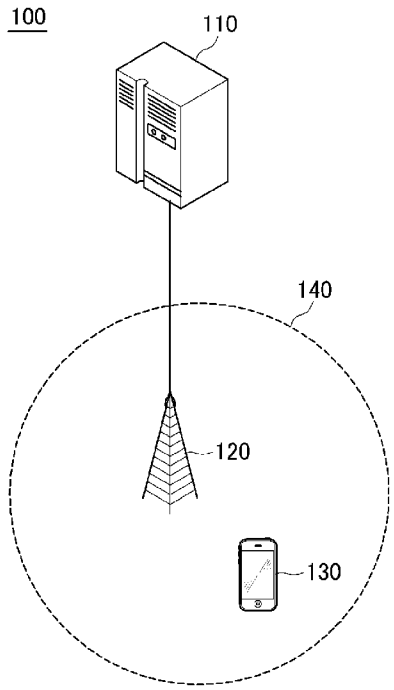
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SCHEMES FOR CONNECTING TO WIRELESS NETWORK

(57) Abstract: Technologies are generally described for connecting to a wireless local area network. In some examples, a method performed under control of an end 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.

FIG. 1



WO 2014/081427 A1

Published:

— *with international search report (Art. 21(3))*

SCHEMES FOR CONNECTING TO WIRELESS NETWORK

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), GMS (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 origianl 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 510. Signal bearing medium 510 may include one or more instructions 520 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 520 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 520.

[0049] In some implementations, signal bearing medium 510 may encompass a computer-readable medium 530, 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 510 may encompass a recordable medium 540, such as, but not limited to, memory, read/write (R/W) CDs, R/W DVDs, etc. In some implementations, signal bearing medium 510 may encompass a communications medium 550, 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 520, where the signal bearing medium 520 is conveyed by a wireless communications medium 550 (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 nonvolatile, 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.

CLAIMS

What is claimed is:

1. A method performed under control of an end device, comprising:

transmitting, to an access point, a probe request frame including a fake device identifier for the end device;

receiving, from the access point, a probe response frame including information regarding 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, to the access point, a connection request including an authentic device identifier for the end device.

2. The method of Claim 1, further comprising:

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

connecting to a wireless local area network provided by the access point.

3. The method of Claim 2, wherein the access point includes a Wi-Fi access point, and the wireless local area network provided by the access point includes a Wi-Fi network.

4. The method of Claim 2, wherein the authenticated 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.

5. The method of Claim 1, further comprising:

generating the fake device identifier before transmitting the probe request frame.

6. The method of Claim 1, further comprising:

receiving the fake device identifier from a mobile operating server before transmitting the probe request frame.

7. The method of Claim 1, wherein the fake device identifier includes at least one of a random number or a random character.

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

9. The method of Claim 1, further comprising:

receiving, from a mobile operating server, an authenticated access point list including information regarding at least one authenticated access point,

wherein the determining is further based at least in part on the authenticated access point list.

10. The method of Claim 9, wherein the information regarding the at least one authenticated access point includes at least one of a media access control (MAC) address or a service set identifier (SSID) of each of the at least one authenticated access point, and

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

11. An end device, comprising:

a transmitting unit configured to transmit, to an access point, a probe request frame including a fake device identifier;

a receiving unit configured to receive, from the access point, a probe response frame including information regarding 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,

wherein the transmitting unit is further configured to transmit, to the access point, a connection request including an authentic device identifier, and the receiving unit is further configured to receive, from the access point, an approval of the connection request.

12. The end device of Claim 11, further comprising:

a fake device identifier generating unit configured to generate the fake device identifier.

13. The end device of Claim 11, wherein the receiving unit is further configured to receive the fake device identifier from a mobile operating server.

14. The end device of Claim 11, wherein the fake device identifier includes at least one of a random number or a random character.

15. The end device of Claim 11, wherein the authentic device identifier includes a media access control (MAC) address.

16. The end device of Claim 11, wherein the determination unit further configured to determine whether the information regarding the access point is included in the authenticated access point list.

17. The end device of Claim 11, wherein the information regarding the at least one authenticated access point includes at least one of a media access control (MAC) address or a service set identifier (SSID) for each of the at least one authenticated access point, and

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

18. The end device of Claim 11, wherein the access point includes a Wi-Fi access point, and the wireless local area network provided by the access point includes a Wi-Fi network.

19. The end device of Claim 11, wherein the authenticated 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.

20. A computer-readable storage medium having stored thereon computer-executable instructions that, in response to execution, cause an end device to perform operations, comprising:

transmitting, to an access point, a probe request frame including a fake device identifier of the end device;

receiving, from the access point, a probe response frame including information regarding 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, to the access point, a connection request including an authentic device identifier of the end device.

21. The computer-readable storage medium of Claim 20, wherein the operations further comprise:

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

connecting to a wireless local area network provided by the access point.

22. The computer-readable storage medium of Claim 20, wherein the operations further comprise:

generating the fake device identifier.

23. The computer-readable storage medium of Claim 20, wherein the authentic device identifier includes a media access control (MAC) address.

24. The computer-readable storage medium of Claim 20, wherein the access point includes a Wi-Fi access point, and the wireless local area network provided by the access point includes a Wi-Fi network.

FIG. 1

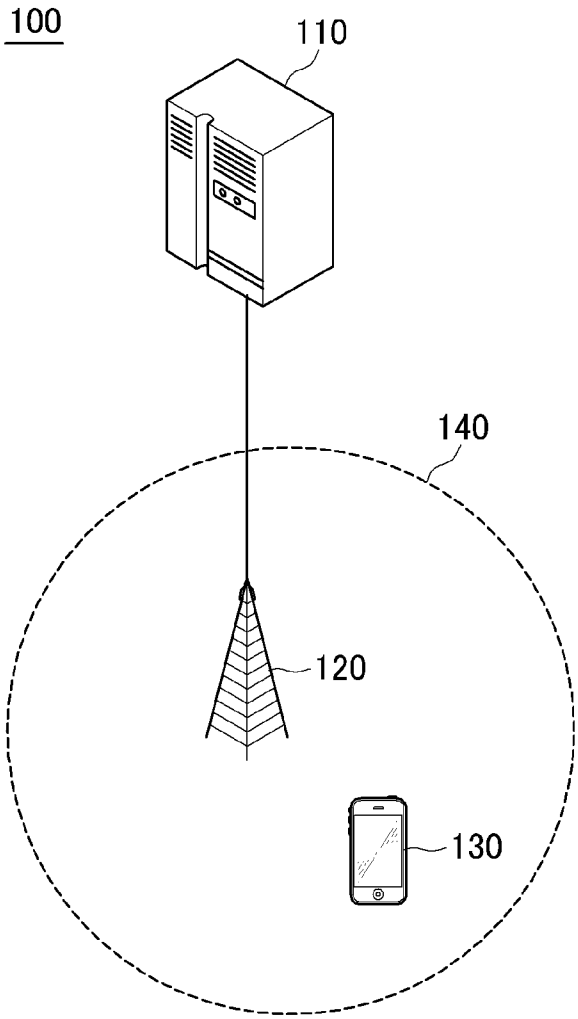


FIG. 2

200

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

FIG. 3

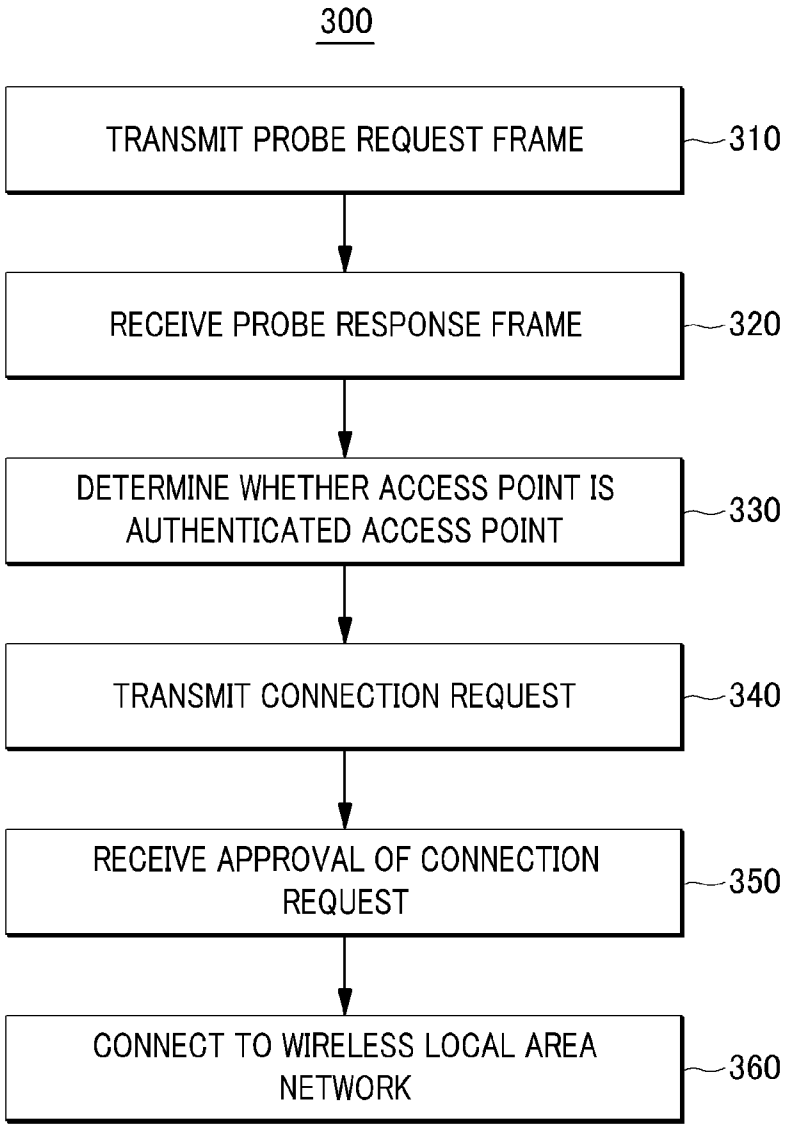

300
TRANSMIT PROBE REQUEST FRAME
310
RECEIVE PROBE RESPONSE FRAME
320
DETERMINE WHETHER ACCESS POINT IS AUTHENTICATED ACCESS POINT
330
TRANSMIT CONNECTION REQUEST
340
RECEIVE APPROVAL OF CONNECTION REQUEST
350
CONNECT TO WIRELESS LOCAL AREA NETWORK
360

FIG. 4

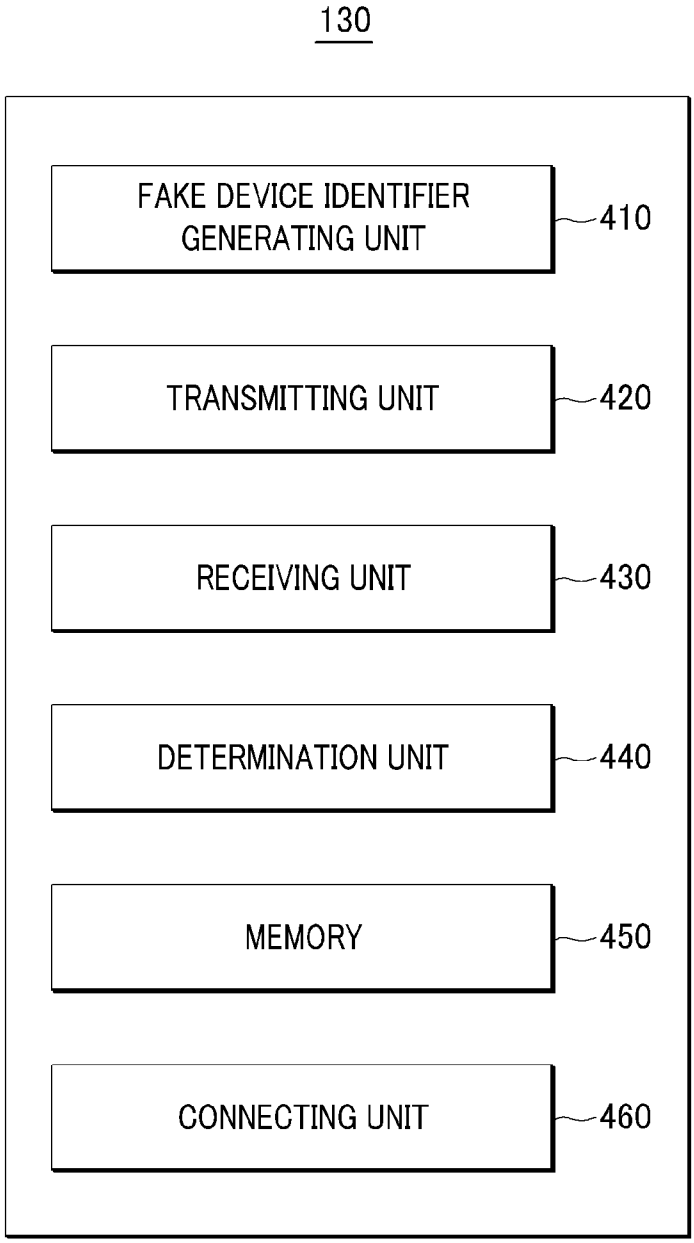

130
FAKE DEVICE IDENTIFIER GENERATING UNIT
410
TRANSMITTING UNIT
420
RECEIVING UNIT
430
DETERMINATION UNIT
440
MEMORY
450
CONNECTING UNIT
460

FIG. 5

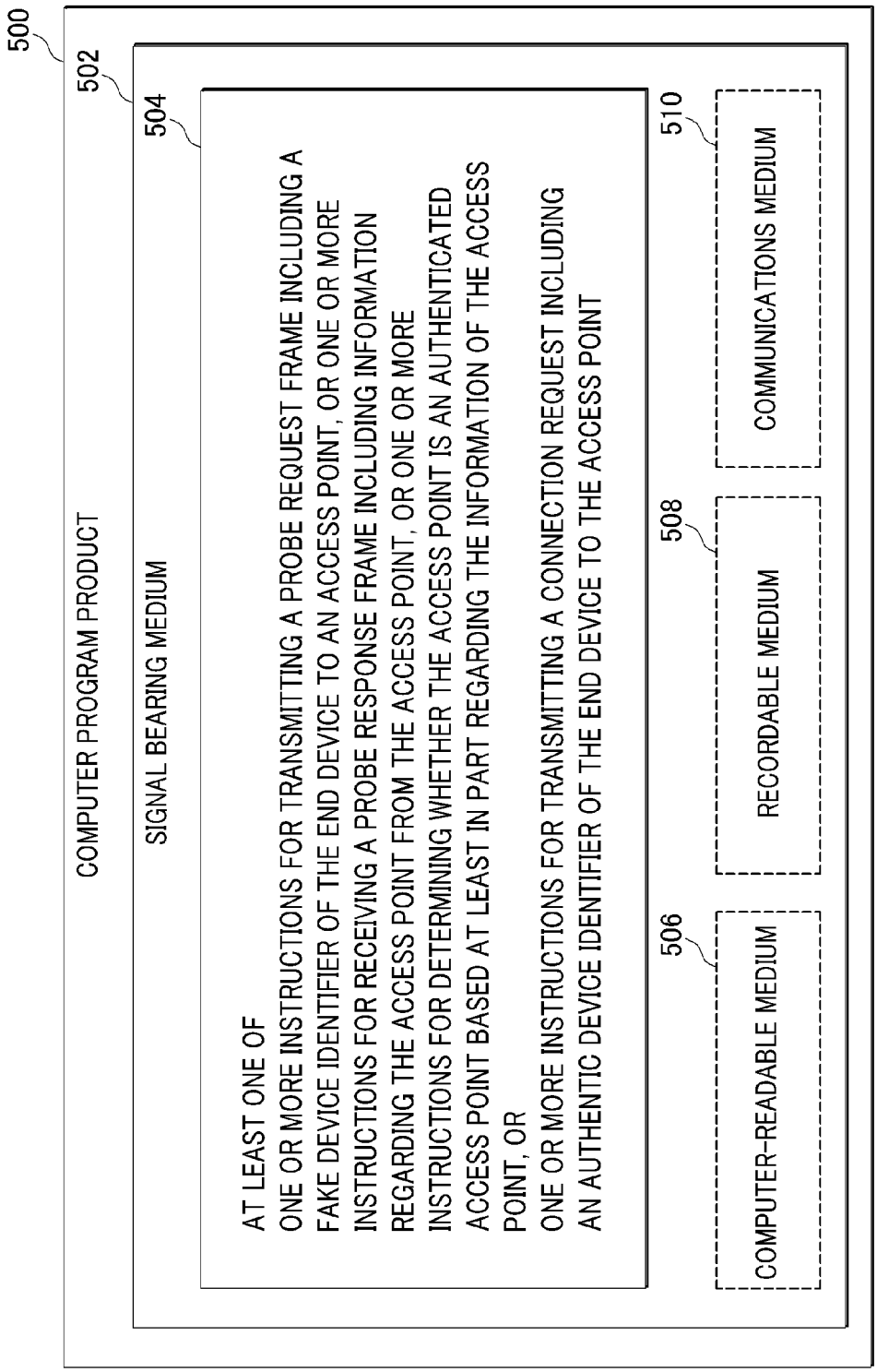
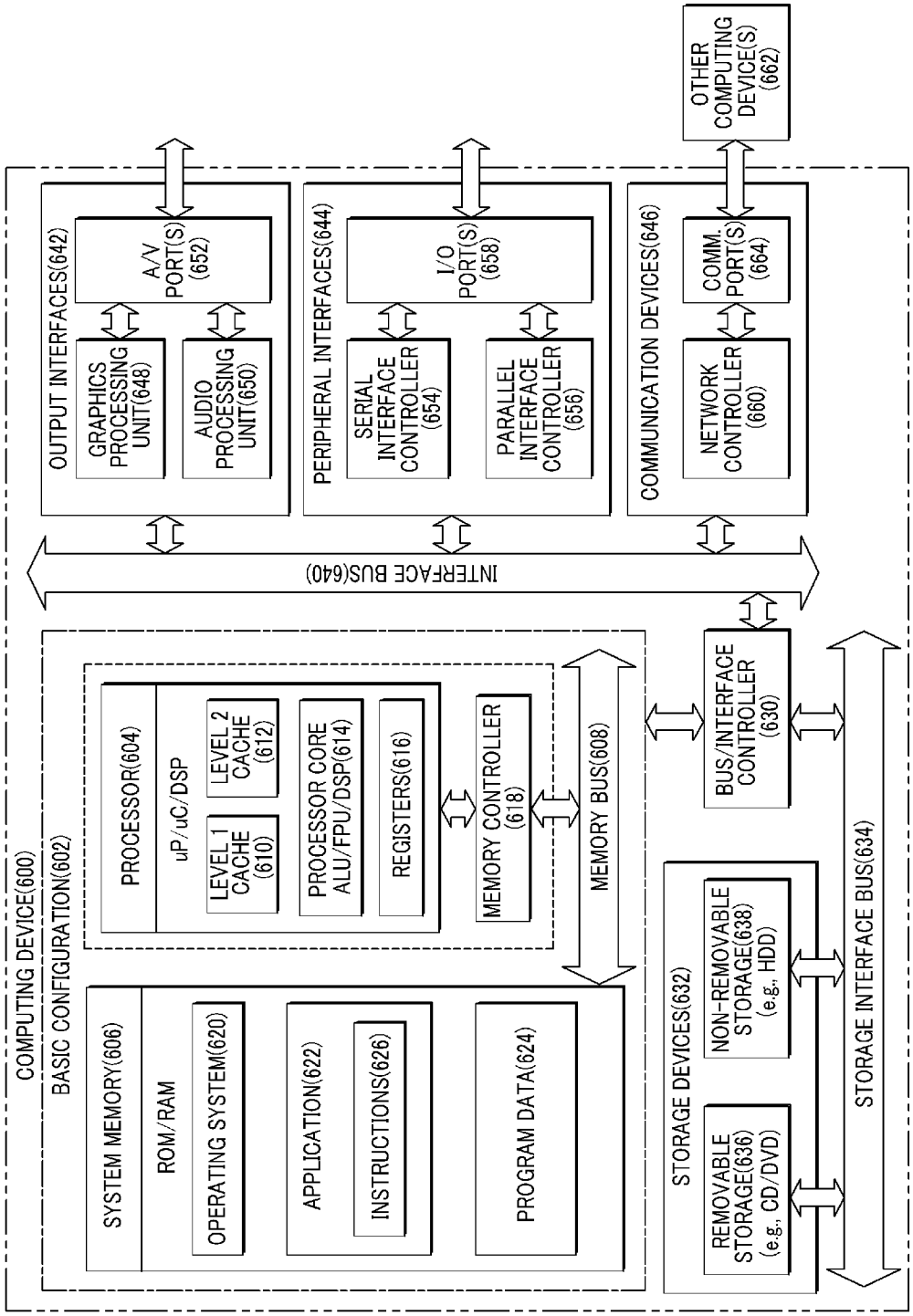

500
COMPUTER PROGRAM PRODUCT
502
SIGNAL BEARING MEDIUM
504
AT LEAST ONE OF
ONE OR MORE INSTRUCTIONS FOR TRANSMITTING A PROBE REQUEST FRAME INCLUDING A FAKE DEVICE IDENTIFIER OF THE END DEVICE TO AN ACCESS POINT, OR ONE OR MORE INSTRUCTIONS FOR RECEIVING A PROBE RESPONSE FRAME INCLUDING INFORMATION REGARDING THE ACCESS POINT FROM THE ACCESS POINT, OR ONE OR MORE INSTRUCTIONS FOR DETERMINING WHETHER THE ACCESS POINT IS AN AUTHENTICATED ACCESS POINT BASED AT LEAST IN PART REGARDING THE INFORMATION OF THE ACCESS POINT, OR
ONE OR MORE INSTRUCTIONS FOR TRANSMITTING A CONNECTION REQUEST INCLUDING AN AUTHENTIC DEVICE IDENTIFIER OF THE END DEVICE TO THE ACCESS POINT
506
COMPUTER-READABLE MEDIUM
508
RECORDABLE MEDIUM
510
COMMUNICATIONS MEDIUM

FIG. 6


COMPUTING DEVICE(600)
BASIC CONFIGURATION(602)
PROCESSOR(604)
uP/uC/DSP
LEVEL 1 CACHE (610)
LEVEL 2 CACHE (612)
PROCESSOR CORE ALU/FPU/DSP(614)
REGISTERS(616)
MEMORY CONTROLLER (618)
SYSTEM MEMORY(606)
ROM/RAM
OPERATING SYSTEM(620)
APPLICATION(622)
INSTRUCTIONS(626)
PROGRAM DATA(624)
MEMORY BUS(608)
INTERFACE BUS(640)
OUTPUT INTERFACES(642)
GRAPHICS PROCESSING UNIT(648)
AUDIO PROCESSING UNIT(650)
A/V PORT(S) (652)
PERIPHERAL INTERFACES(644)
SERIAL INTERFACE CONTROLLER (654)
PARALLEL INTERFACE CONTROLLER (656)
I/O PORT(S) (658)
COMMUNICATION DEVICES(646)
NETWORK CONTROLLER (660)
COMM. PORT(S) (664)
OTHER COMPUTING DEVICE(S) (662)
BUS/INTERFACE CONTROLLER (630)
STORAGE DEVICES(632)
REMOVABLE STORAGE(636) (e.g., CD/DVD)
NON-REMOVABLE STORAGE(638) (e.g., HDD)
STORAGE INTERFACE BUS(634)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 12/66306

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 7/04 (2013.01)
USPC - 340/5.6
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC: 340/5.6

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
IPC: G06F 7/04; G06Q 10/10, 30/02; H04M 11/04 (2013.01); USPC: 340/5.6; 455/404.2, 456.1, 414.2; 370/338 (keyword limited - see search terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase; Google; Google Scholar
Terms: wifi, wireless, 802.11, access point, node, security, authenticate, authorize, probe, scan, beacon, request, fake, spoof, unauthorized, frame, packet, address, ssid, service, set, mac, media, access, identifier, identity, random.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2008/0052779 A1 (Sinha et al.) 28 February 2008 (28.02.2008) entire document, especially abstract, Figs. 1, 6, 9, para. [0011], [0016], [0019], [0032]-[0083]	1-6, 8-13, 15-24 --- 7, 14
Y	US 2011/0083165 A1 (Gopinath et al.) 07 April 2011 (07.04.2011) para. [0008], [0011], [0037], [0038], [0092], [0104], [0112], [0120]	7, 14
A	US 7,808,958 B1 (Hernacki et al.) 05 October 2010 (05.10.2010) entire document.	1-24
A	US 2011/0314147 A1 (Whelan et al.) 22 December 2011 (22.12.2011) ntire document.	1-24
A	US 2008/0043686 A1 (Sperti et al.) 21 February 2008 (21.02.2008) entire document.	1-24
A	US 2007/0286143 A1 (Olson et al.) 13 December 2007 (13.12.2007) entire document.	1-24
A	US 2003/0221006 A1 (Kuan et al.) 27 November 2003 (27.11.2003) entire document.	1-24
A	US 2012/0221955 A1 (Raleigh et al.) 30 August 2012 (30.08.2012) entire document.	1-24

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2013 (18.01.2013)	08 FEB 2013
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)