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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 December 2014 (31.12.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/209380 Al

(51) International Patent Classification:
H04W 12/08 (2009.01)

(21) International Application Number:
PCT/US20 13/048683

(22) International Filing Date:
28 June 2013 (28.06.2013)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95052 (US).

(72) Inventor; and
(71) Applicant : **ELLIOTT, Brent** [US/US]; 2111 NE 25th Ave, Hillsboro, Oregon 97124 (US).

(74) Agents: **MADDEN, Robert B.** et al; Schwegman, Lundberg, & Woessner, P.A., P.O. Box 2938, Minneapolis, Minnesota 55402-0938 (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, 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, KM, ML, MR, NE, SN, TD, TG).

Published:

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

WO 2014/209380 A1

(54) Title: OPEN AND ENCRYPTED WIRELESS NETWORK ACCESS

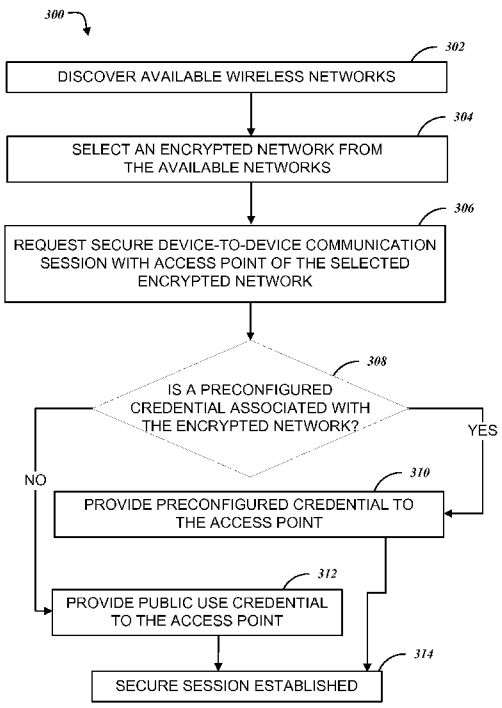

FIG. 3

(57) Abstract: Embodiments of a system and method for establishing secure communications between devices via a wireless network are generally described herein. In some embodiments a device may transmit a public use credential to a second device to establish a secure device-to-device communication session. In some embodiments a device may prompt a user to provide a network-specific credential or utilize a public use credential to establish a communication session with an access point. In some embodiments a communication module in a device may automatically establish a connection with an access point utilizing a public use credential in response to a previously established relationship with the access point. In some embodiments a plurality of devices may establish unique encrypted communication connections with an access point utilizing an identical public use credential. In some embodiments an access point may provide a certificate identifying the access point to a device utilizing a public use credential.

OPEN AND ENCRYPTED WIRELESS NETWORK ACCESS

TECHNICAL FIELD

[0001] Embodiments pertain to wireless communications. Some embodiments relate to the use of encrypted wireless communication. Some embodiments relate to secure discovery and communication between devices in a wireless network.

BACKGROUND

[0002] An issue with providing wireless network access is the choice between network availability to the public and encrypted wireless transmission. In an open network anyone can connect to the network, but information can easily be extracted from user traffic communicating over the network by third parties. In an encrypted network that prevents third-party interception, the complexity of creating user profiles and the lack of widespread provisioning mechanisms may prevent or discourage users from easily connecting to the more secure encrypted network.

[0003] Thus there are general needs for systems and methods that reduce complexity of connecting to encrypted networks, while allowing users or devices to securely discover and communicate with each other in a secure manner.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Some embodiments are illustrated by way of example and not limitation in the figures of the accompanying drawings in which:

[0005] FIG. 1 is a block diagram of an example communication system in accordance with some embodiments;

[0006] FIG. 2 is a block diagram of an example wireless communication system in accordance with some embodiments;

[0007] FIG. 3 is a flow diagram illustrating an example method for establishing communication between devices in accordance with some embodiments;

[0008] FIG. 4 is a swim-lane chart illustrating the operation of a method for discovery and authentication of a device with a network in accordance with some embodiments;

[0009] FIG. 5 is flow diagram a illustrating the operation of an example method for connecting to a network in accordance with some embodiments;

[0010] FIG. 6 is a block diagram illustrating a mobile device in accordance with some embodiments;

[0011] FIG. 7 is a diagrammatic representation of a machine in the example form of a computer system within which a set of instructions for causing the machine to perform any one or more of the methodologies discussed herein may be executed; and

[0012] FIG. 8 illustrates a functional block diagram of user equipment (UE) in accordance with some embodiments.

DETAILED DESCRIPTION

[0013] The following description and the drawings sufficiently illustrate specific embodiments to enable those skilled in the art to practice them. Other embodiments may incorporate structural, logical, electrical, process, and other changes. Portions and features of some embodiments may be included in, or substituted for, those of other embodiments. Embodiments set forth in the claims encompass all available equivalents of those claims.

[0014] Various techniques and configurations described herein provide for a network awareness and discovery technique used in conjunction with wireless communications and network communications. The presently described network discovery and connection techniques may be used in conjunction with an authentication technique establishing an authenticated or secure

communication channel between devices. For example, a wireless local area network (e.g., Wi-Fi) may be based on or compatible with one of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards.

[0015] With some network technologies, discovery and authentication uses an exchange of authentication keys, verification of identifiers via a server, or other broadcasts, exchanges, and provisions of previously established credentials. For example, wireless techniques employing Wi-Fi Protected Access with Pre-shared Keys (WPA-PSK) or WPA2-PSK (a.k.a., WPA-Personal or WPA2-Personal) have been introduced but offer virtually no security in an open access point (e.g., Hotspot) setting. In this public setting such as a coffee shop, a pre-shared key must be made available to the broad public (e.g., posted publicly on a chalkboard in a coffee shop) in order to enable the general public access. However, the implementations of WPA-PSK and WPA2-PSK are such that any user with access to the broadly available pre-shared key may decode the communications of any other user on the network. As a result, pubic wireless network access providers have typically provided unencrypted and open network access in spite of the risks associated with the security and privacy of the customers, partners, employees, or other users of these open networks.

[0016] In connection with the presently described techniques, a wireless communications device is enabled to discover and establish a connection with a wireless communications access point without the use of a previously established credential that is unique to the device or a user of the device. In an example embodiment, one or more predefined de facto or standardized public use credentials (PUC) may be utilized during authentication by a wireless device when associating with a WPA-ENTERPRISE or WPA2-ENTERPRISE configured network without the need for existing provisioned or configured credentials specific to the wireless device or user.

[0017] The discovery and authentication techniques may facilitate connections established using any of a variety of network protocols and standards in licensed or unlicensed spectrum bands, including Wi-Fi communications performed in connection with an IEEE 802.1 1 standard (for example, Wi-Fi communications facilitated by fixed access points), 3GPP

LTE/LTE-A communications (for example, LTE Direct (LTE-D) communications established in a portion of an uplink segment or other designated resources), machine-to-machine (M2M) communications performed in connection with an IEEE 802.16 standard, and the like.

[0018] FIG. 1 provides an illustration of an example configuration of a communication network architecture 100. Within the communication network architecture 100, a carrier-based network such as an IEEE 802.11 compatible wireless access point or a LTE/LTE-A cell network operating according to a standard from a 3GPP standards family is established by network equipment 102. The network equipment 102 may include a wireless access point, a Wi-Fi hotspot, or an enhanced or evolved node B (eNodeB) communicating with communication devices 104A, 104B, 104C (e.g., a user equipment (UE) or communication station (STA)). The carrier-based network includes wireless network connections 106A, 106B, and 106C with the communication devices 104A, 104B, and 104C, respectively. The communication devices 104A, 104B, 104C are illustrated as conforming to a variety of form factors, including a smartphone, a mobile phone handset, and a personal computer having an integrated or external wireless network communication device.

[0019] The network equipment 102 is illustrated in FIG. 1 as being connected via a network connection 114 to network servers 118 in a cloud network 116. The servers 118 may operate to provide various types of information to, or receive information from, communication devices 104A, 104B, 104C, including device location, user profiles, user information, web sites, e-mail, and the like. The techniques described herein enable the establishment of communications between the various communication devices 104A, 104B, 104C, and the network equipment 102 without requiring authentication techniques to the cloud network 116 and the network servers 118.

[0020] Communication devices 104A, 104B, 104C can communicate with the network equipment 102 when in range or otherwise in proximity for wireless communications. As illustrated, the connection 106A may be established between the mobile device 104A (e.g., a smartphone) and the network equipment 102; the connection 106B may be established between the mobile

device 104B (e.g., a mobile phone) and the network equipment 102; and the connection 106C may be established between the mobile device 104C (e.g., a personal computer) and the network equipment 102.

[0021] The wireless communications 106A, 106B, 106C between devices 104A, 104B, 104C may utilize a Wi-Fi or IEEE 802.11 standard protocol, or a protocol such as the current 3rd Generation Partnership Project (3GPP) long term evolution (LTE) time division duplex (TDD)-Advanced systems. In one embodiment, the communications network 116 and network equipment 102 comprises an evolved universal terrestrial radio access network (EUTRAN) using the 3rd Generation Partnership Project (3GPP) long term evolution (LTE) standard and operating in time division duplexing (TDD) mode. The devices 104A, 104B, 104C may include one or more antennas, receivers, transmitters, or transceivers that are configured to utilize a Wi-Fi or IEEE 802.11 standard protocol, or a protocol such as 3GPP, LTE, or TDD-Advanced or any combination of these or other communications standards.

[0022] In establishing a connection between a wireless communication device and an access point, public use credential authentication techniques may provide for an exchange of authentication information and discovery information to establish a unique and secure communication session. For example, when a user or automated process triggers an attempt by a device to connect to a securely configured network (e.g., an encrypted network), the device will first attempt to associate with credentials that are provisioned or otherwise configured on the device. If these are not available, connection management or connection enhancement software running on the device may automatically attempt to authenticate with one or more public use credentials or may prompt the user with the option to attempt authentication with the public use credentials or to offer their own credentials e.g., a username and password. In the event that a first public use credential fails authentication, the device may attempt to use a secondary public use credential, may prompt the user to provide their personal credentials, or may simply fail the association with the currently selected network.

[0023] The secure network may include a network configured to conform to a WPA-ENTERPRISE or WPA2-ENTERPRISE security protocol. In comparison with the WPA-PSK and WPA2-PSK network example, the existing implementation and standards defining the WPA-ENTERPRISE and WPA2-ENTERPRISE protocols ensures full encryption of the communications between devices, even those devices using identical public use credentials. For example, the IEEE 802.11i security standard (e.g., IEEE 802.11i-2004) with CCMP/AES encryption provides specifies security mechanisms for wireless networks that may prevent the interception of wireless communication between devices such as network equipment 102 and communication devices 104A, 104B, 104C.

[0024] The discovery and authentication techniques may also facilitate connections established using any of a variety of network protocols and standards in licensed or unlicensed spectrum bands, including Wi-Fi P2P communications performed in connection with an IEEE 802.1 1 standard (for example, Wi-Fi Direct communications facilitated by software access points (Soft APs)), 3GPP LTE/LTE-A communications (for example, LTE Direct (LTE-D) communications established in a portion of an uplink segment or other designated resources), machine-to-machine (M2M) communications performed in connection with an IEEE 802.16 standard, and the like.

[0025] Antennas in or on devices 104A, 104B, 104C may comprise one or more directional or omnidirectional antennas, including, for example, dipole antennas, monopole antennas, patch antennas, loop antennas, microstrip antennas or other types of antennas suitable for transmission of RF signals. In some embodiments, instead of two or more antennas, a single antenna with multiple apertures may be used. In these embodiments, each aperture may be considered a separate antenna. In some multiple-input multiple-output (MIMO) embodiments, antennas may be effectively separated to utilize spatial diversity and the different channel characteristics that may result between each of the antennas and the antennas of a transmitting station. In some MIMO embodiments, antennas may be separated by up to 1/10 of a wavelength or more.

[0026] In some embodiments, the mobile device 104A may include one or more of a keyboard, a display, a non-volatile memory port, multiple antennas, a graphics processor, an application processor, speakers, and other mobile device elements. The display may be an LCD screen including a touch screen. The mobile device 104B may be similar to mobile device 104A, but does not need to be identical. The mobile device 104C may include some or all of the features, components, or functionality described with respect to mobile device 104A.

[0027] A base station, such as an enhanced or evolved node B (eNodeB), may provide wireless communication services to communication devices, such as device 102. While the exemplary communication system 100 of FIG. 1 depicts only three devices users 104A, 104B, 104C any combination of multiple users, devices, servers and the like may be coupled to network device 102 in various embodiments. For example, three or more users located in a venue, such as a building, campus, mall area, or other area, and may utilize any number of mobile wireless-enabled computing devices to independently communicate with network equipment 102.

[0028] Although communication system 100 is illustrated as having several separate functional elements, one or more of the functional elements may be combined and may be implemented by combinations of software-configured elements, such as processing elements including digital signal processors (DSPs), and/or other hardware elements. For example, some elements may comprise one or more microprocessors, DSPs, application specific integrated circuits (ASICs), radio-frequency integrated circuits (RFICs) and combinations of various hardware and logic circuitry for performing at least the functions described herein. In some embodiments, the functional elements of system 100 may refer to one or more processes operating on one or more processing elements.

[0029] Embodiments may be implemented in one or a combination of hardware, firmware and software. Embodiments may also be implemented as instructions stored on a computer-readable storage device, which may be read and executed by at least one processor to perform the operations described herein. A computer-readable storage device may include any non-transitory

mechanism for storing information in a form readable by a machine (e.g., a computer). For example, a computer-readable storage device may include read-only memory (ROM), random-access memory (RAM), magnetic disk storage media, optical storage media, flash-memory devices, and other storage devices and media. In some embodiments, system 100 may include one or more processors and may be configured with instructions stored on a computer-readable storage device.

[0030] FIG. 2 is a block diagram of an example wireless communication system 200 that may utilize the communication network architecture 100 of FIG. 1. The exemplary communication system 200 may include a first device 202 and a second device 204 that are both capable of wireless communication. In an example, the first device 202 and the second device 204 may be a mobile computing device such as a cellular phone, a smartphone, a laptop, a tablet computer, a personal digital assistant or other electronic device. An access point 206 may, for example, be a base station or a fixed wireless router. The devices 202, 204 may establish a communication session with the access point 206 in order to reach a network 208 such as the Internet. In an example, the devices 202, 204 may communicate with a service provider 210 through the network 208.

[0031] In an example, the access point 206 may support both an open and unencrypted networks to support legacy devices. An access point operator may advertise these networks as having an alternative secure option, or encourage users to transition to the more secure network. For example, a grocery store may offer an open extended service set identification (ESSID) or service set identification (SSID) such as, "Grocery-Open", and also offer an encrypted network ESSID or SSID such as, "Grocery-Secure". The grocery store in this example may add a PUC to the authentication database for an existing "Grocery-Secure" network, or create the Grocery-Secure ESSID at access point 206 and configure it to use WPA-ENTERPRISE or WPA2-Enterprise with the PUC to the referenced new or existing authentication database with a valid authentication certificate.

[0032] The PUC may be used by any wireless authentication mechanism. These include, but are not limited to, Protected Extensible Authentication Protocol (PEAP) or Microsoft Challenge Handshake Protocol, version 2 (MSCHAPv2), Extensible Authentication Protocol with Tunneled Transport Layer Security (EAP-TTLS), Extensible Authentication Protocol with Transport Layer Security (EAP-TLS), etc. The PUC does not need to be visible to an end-user of a PUC-enabled device, the language and contents of the credentials need not be recognizable or remembered by users. For example, an embodiment may define the credential type, username and password either as a de-facto or standardized to be PEAP/MSCHAPv2 with a username of "public-use" and a password of "RESERVED-public-password-00".

[0033] In an example, a device may attempt to establish a secure device-to-device communication session with an access point of an encrypted wireless network with a first class of credential, the first class of credential may be specific to an individual user. In response to a failure to connect with the first class of credential, the device may attempt to connect to the access point with a second class of credential where the second class of credential may be specific to an organization. In response to a failure to establish the secure device-to-device communication session with the access point with the second class of credential, the device may attempt to connect to the access point with the pre-configured public-use credential.

[0034] Different credential types or classes such as organization specific, *defacto* or industry standards may provide wireless access point 206 a measure of flexibility in the type of credential that may be implemented in a network. In the case of a failure to determine the preferred or supported credential type for a public use credential, a default credential type and corresponding credentials may be defined. As in the above example, this may for example be PEAP/MSCHAPv2 with username "public-use" and password "RESERVED-public-password-00".

[0035] The device 202 may establish an encrypted communication session with the access point 206 by providing a public use credential to the access point 206 as part of initiating a secure device-to-device communication

session. The device 204 may use a public use credential to connect with the access point 206 that is identical to the public use credential provided to the access point 206. The access point 206 may support encrypted device-to-device communication sessions with both device 202 and the device 204 such that neither device 202 nor device 204 is able to inject or intercept data (e.g., data packets) associated with the other device.

[0036] The device-to-device communication session initiated with the use of the public use credential may be established for wireless communication at a data link or network layer that provides an interface between a device and an access point, or two devices, and is separate from higher layer (e.g., application layer) data communication. For example, data communication between device 202 and service provider 210 may utilize a separate encryption mechanism or protocol (e.g., TLS/SSL SSH, etc.) that encrypts or authenticates communications that span multiple devices, network equipment, or networks.

[0037] Generally, WPA-ENTERPRISE and WPA2-ENTERPRISE compliant networks may include, for various credential types, network infrastructure equipment that offers a public certificate signed by an authority that is known and trusted by the client devices. For example, the access point 206 may include a public certificate 216 that has been signed by an authority that is known and trusted by the client devices such as the first device 202 or the second device 204. Devices 202, 204 may optionally have credential data or may be configured to obtain information to ensure that the access point 206 with which it is authenticating contains the legitimate private key (e.g., public certificate 216) corresponding to the credentials expected for the access point 206.

[0038] Upon successful association between a device and an access point using a public use credential, a connection manager module 212 or connection enhancement module 214 on the device 202 or device 204 may create a profile to enable accelerated or prioritized selection and connection to the access point in the futures using the public use credential. For appropriate credential types, a fingerprint or other identifying information regarding the public certificate provided by the access point 206 with a specific ESSID may be stored by the

device 202, 204 to ensure that subsequent associations are not fraudulent. This fraud protection may include determining whether the public certificate provided by the access point comes from the same trust authority and contain the same encrypted information associated with the original connection with the access point. A determination that the public certificate is invalid or has changed may result in a request to verify the legitimacy of the newly provided public certificate, or a failure of the device 202, 204 to connect with the access point 206.

[0039] FIG. 3 is a flowchart illustrating an example method 300 for establishing communication between devices. In an example, the method 300 may be performed by device 202 of FIG. 2 in an attempt to establish a communication session with access point 206 of FIG. 2.

[0040] At 302, a device may attempt to discover available wireless networks. The wireless networks may utilize a Wi-Fi or IEEE 802.1 1 standard protocol, or a protocol such as the current 3GPP, LTE, or TDD-Advanced. The device may attempt to discover one or more ESSID being broadcast by an access point or other network equipment. The wireless networks may be open (e.g., unencrypted) or encrypted.

[0041] At 304, the device may select an encrypted network from the available networks. The selection may be based upon a list of networks the device has previously connected to, a list of networks provided by a user or otherwise indicated as being desirable, or the properties (e.g., protocol compatibility) of the encrypted network.

[0042] At 306, the device may request a secure device-to-device communication session with an access point of the selected encrypted network. The request may conform to a wireless protocol (e.g., WPA-ENTERPRISE or WPA2-ENTERPRISE) that defines a handshake procedure for establishing a secure communication session.

[0043] At 308, the device may check to determine if it has a preconfigured credential is associated with the encrypted network. The preconfigured credential may include a username and password combination provided by an end-user to the device, or a public key configured to allow the

device to access the network coupled to the access point. If the device determines that it has a preconfigured credential then, at 310, the preconfigured credential is provided to the access point. If the device determines that it does not have a preconfigured credential associated with the encrypted network then, at 312, the device may provide a public use credential to the access point. At 314, a secure session is established between the device and the access point based on either the preconfigured credential or the public use credential.

[0044] The device may optionally create a record of the secure session established with the access point in order to verify the integrity of future sessions where the public use credential is utilized to connect to the access point. These operations may also be performed by the device 104A, or a combination of devices 104B, 104C or processors in communication with network equipment 102 of FIG. 1.

[0045] Though arranged serially in the example of FIG. 3, other examples may reorder the operations, omit one or more operations, and/or execute two or more operations in parallel using multiple processors or a single processor organized as two or more virtual machines or sub-processors. Moreover, still other examples may implement the operations as one or more specific interconnected hardware or integrated circuit modules with related control and data signals communicated between and through the modules. Thus, any process flow is applicable to software, firmware, hardware, and hybrid implementations.

[0046] FIG. 4 is a swim-lane chart illustrating the operation of a method 400 for discovery and authentication of a device with a network in accordance with some embodiments, such as the device 202 and the access point 206 of FIG. 2.

[0047] At 402, the method 400 may begin with the device 202 attempting to initiate network discovery. Network discovery may include receiving one or more network identifiers, e.g., ESSID, that are broadcast by one or more network equipment within range of the device 202. Upon receipt of a network identifier that is known to the device 202 or compatible with a wireless protocol supported by device 202, at 404, the device 202 may send a network

access request 404 to the access point 206 that is broadcasting the selected network identifier.

[0048] At 408, the method 400 may continue with the access point 206 processing the network access request from the device 202. In response to the request, at 410, the access point 206 may generate or retrieve authentication data to establish a secure session between the device 202 and the access point 206.

[0049] At 412, the access point 206 may transmit an access response to the device 202. The access response may include the authentication data. The authentication data may include an encrypted public certificate provided to the access point 206 by a trusted authority verifying the identity of a service provider that operates the access point 206 or a network coupled to the access point.

[0050] Upon receipt of the access response, at 414, the device 202 may verify the authentication data. The verification may include attempting to confirm the validity of the encrypted public certificate, or performing a check to determine if the encrypted public certificate originated from a trusted authority. At 416, the device, upon verifying the authentication data, may acknowledge that a secure device-to-device connection is established between the device 202 and the access point 206. The method 400 is complete at 418, when the device 202 and the access point 206 exchange data securely via the device-to-device connection.

[0051] Optionally, method 400 may include one or more operations defined by any of a variety of network protocols and standards in licensed or unlicensed spectrum bands, including Wi-Fi P2P communications performed in connection with an IEEE 802.1 1 standard (for example, Wi-Fi Direct communications facilitated by software access points (Soft APs)), 3GPP LTE/LTE-A communications (for example, LTE Direct (LTE-D) communications established in a portion of an uplink segment or other designated resources), machine-to-machine (M2M) communications performed in connection with an IEEE 802.16 standard, and the like.

[0052] FIG. 5 illustrates the operation of a method 500 illustrating the operation of an example method for connecting to a network. At 502, a

communication station (STA) or user equipment (UE) device may discover any available wireless networks and prioritize the available networks upon discovery. The device may periodically perform a check, at 504, to query whether any wireless networks are available. If no wireless networks are available the device, at 506, may abort its attempt to connect to a network. If one or more wireless networks are available, at 508, the device may attempt to connect with any previously provisioned or configured networks. In this manner priority is given to networks that the devices has previously connected with, or has been explicitly configured to favor.

[0053] At 510, the device may check to determine if a connection has been established with one of the provisioned or configured networks. If a secure connection is established, at 512, the method 500 may terminate. If the device determines that a connection cannot be established with a preconfigured or previously known network, at 514, the device may prompt a user to enter credentials specific to one or more of the available networks (e.g., a user name and password combination) or choose to connect to a network utilizing a public use credential. The use may also choose to abort the connection attempt and, at 506, the attempt to connect will terminate.

[0054] At 518, upon selection of the public use credential option by the user, or an indication that the user does not possess a network specific credential, the device may attempt to connect to the access point with a public use credential. The public use credential may be a predefined de facto identity, or a standardized character string or sequence that is not unique to the device or to an access point that the device is attempting to establish a connection with. If the user chooses to provide a specific credential, at 520, the device may attempt to connect to the access point with the user provided credential. The method 500 is complete at 512, when a secure communication session is established between the device and the access point (e.g., the device and the access point are connected by a device-to-device connection).

[0055] Though arranged serially in the example of FIG. 5, other examples may reorder the operations, omit one or more operations, and/or execute two or more operations in parallel using multiple processors or a single

processor organized as two or more virtual machines or sub-processors. Moreover, still other examples may implement the operations as one or more specific interconnected hardware or integrated circuit modules with related control and data signals communicated between and through the modules. Thus, any process flow is applicable to software, firmware, hardware, and hybrid implementations.

[0056] Although the preceding examples indicated the use of device-to-device communications in connection with 3GPP and 802.11 standard communications, it will be understood that a variety of other communication standards capable of facilitating device-to-device, machine-to-machine, and P2P communications may be used in connection with the presently described techniques. These standards include, but are not limited to, standards from 3GPP (e.g., LTE, LTE-A, HSPA+, UMTS), IEEE 802.11 (e.g., 802.11a, 802.11b, 802.llg, 802.11η, 802.11ac), 802.16 (e.g., 802.16p), or Bluetooth (e.g., Bluetooth 4.0, or other standard defined by the Bluetooth Special Interest Group) standards families. Bluetooth, as used herein, may refer to a short-range digital communication protocol defined by the Bluetooth Special Interest Group, the protocol including a short-haul wireless protocol frequency-hopping spread-spectrum (FHSS) communication technique operating in the 2.4 GHz spectrum.

[0057] FIG. 6 is a block diagram illustrating a mobile device 600, upon which any one or more of the techniques (e.g., methodologies) discussed herein may be performed. The mobile device 600 may include a processor 610. The processor 610 may be any of a variety of different types of commercially available processors suitable for mobile devices, for example, an XScale architecture microprocessor, a Microprocessor without Interlocked Pipeline Stages (MIPS) architecture processor, or another type of processor. A memory 620, such as a Random Access Memory (RAM), a Flash memory, or other type of memory, is typically accessible to the processor 610. The memory 620 may be adapted to store an operating system (OS) 630, as well as application programs 640. The OS 630 or application programs 640 may include instructions stored on a computer readable medium (e.g., memory 620) that may cause the processor 610 of the mobile device 600 to perform any one or more of the

techniques discussed herein. The processor 610 may be coupled, either directly or via appropriate intermediary hardware, to a display 650 and to one or more input/output (I/O) devices 660, such as a keypad, a touch panel sensor, a microphone, etc. Similarly, in an example embodiment, the processor 610 may be coupled to a transceiver 670 that interfaces with an antenna 690. The transceiver 670 may be configured to both transmit and receive cellular network signals, wireless data signals, or other types of signals via the antenna 690, depending on the nature of the mobile device 600. Further, in some configurations, a GPS receiver 680 may also make use of the antenna 690 to receive GPS signals.

[0058] FIG. 7 illustrates a block diagram of an example machine 700 upon which any one or more of the techniques (e.g., methodologies) discussed herein may be performed. In alternative embodiments, the machine 700 may operate as a standalone device or may be connected (e.g., networked) to other machines. In a networked deployment, the machine 700 may operate in the capacity of a server machine, a client machine, or both in server-client network environments. In an example, the machine 700 may act as a peer machine in peer-to-peer (P2P) (or other distributed) network environment. The machine 700 may be a personal computer (PC), a tablet PC, a Personal Digital Assistant (PDA), a mobile telephone, a web appliance, or any machine capable of executing instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein, such as cloud computing, software as a service (SaaS), other computer cluster configurations.

[0059] Examples, as described herein, may include, or may operate on, logic or a number of components, modules, or mechanisms. Modules are tangible entities capable of performing specified operations and may be configured or arranged in a certain manner. In an example, circuits may be arranged (e.g., internally or with respect to external entities such as other circuits) in a specified manner as a module. In an example, the whole or part of

one or more computer systems (e.g., a standalone, client or server computer system) or one or more hardware processors may be configured by firmware or software (e.g., instructions, an application portion, or an application) as a module that operates to perform specified operations. In an example, the software may reside (1) on a non-transitory machine-readable medium or (2) in a transmission signal. In an example, the software, when executed by the underlying hardware of the module, causes the hardware to perform the specified operations.

[0060] Accordingly, the term "module" is understood to encompass a tangible entity, be that an entity that is physically constructed, specifically configured (e.g., hardwired), or temporarily (e.g., transitorily) configured (e.g., programmed) to operate in a specified manner or to perform part or all of any operation described herein. Considering examples in which modules are temporarily configured, each of the modules need not be instantiated at any one moment in time. For example, where the modules comprise a general-purpose hardware processor configured using software, the general-purpose hardware processor may be configured as respective different modules at different times. Software may accordingly configure a hardware processor, for example, to constitute a particular module at one instance of time and to constitute a different module at a different instance of time.

[0061] Machine (e.g., computer system) 700 may include a hardware processor 702 (e.g., a processing unit, a graphics processing unit (GPU), a hardware processor core, or any combination thereof), a main memory 704, and a static memory 706, some or all of which may communicate with each other via a link 708 (e.g., a bus, link, interconnect, or the like). The machine 700 may further include a display device 710, an input device 712 (e.g., a keyboard), and a user interface (UI) navigation device 714 (e.g., a mouse). In an example, the display device 710, input device 712, and UI navigation device 714 may be a touch screen display. The machine 700 may additionally include a mass storage (e.g., drive unit) 716, a signal generation device 718 (e.g., a speaker), a network interface device 720, and one or more sensors 721, such as a global positioning system (GPS) sensor, camera, video recorder, compass, accelerometer, or other sensor. The machine 700 may include an output controller 728, such as a serial

(e.g., universal serial bus (USB), parallel, or other wired or wireless (e.g., infrared (IR)) connection to communicate or control one or more peripheral devices (e.g., a printer, card reader, etc.).

[0062] The mass storage 716 may include a machine-readable medium 722 on which is stored one or more sets of data structures or instructions 724 (e.g., software) embodying or utilized by any one or more of the techniques or functions described herein. The instructions 724 may also reside, completely or at least partially, within the main memory 704, within static memory 706, or within the hardware processor 702 during execution thereof by the machine 700. In an example, one or any combination of the hardware processor 702, the main memory 704, the static memory 706, or the mass storage 716 may constitute machine-readable media.

[0063] While the machine-readable medium 722 is illustrated as a single medium, the term "machine readable medium" may include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that configured to store the one or more instructions 724.

[0064] The term "machine-readable medium" may include any tangible medium that is capable of storing, encoding, or carrying instructions for execution by the machine 700 and that cause the machine 700 to perform any one or more of the techniques of the present disclosure, or that is capable of storing, encoding or carrying data structures used by or associated with such instructions. Non-limiting machine-readable medium examples may include solid-state memories, and optical and magnetic media. Specific examples of machine-readable media may include: non-volatile memory, such as semiconductor memory devices (e.g., Electrically Programmable Read-Only Memory (EPROM), Electrically Erasable Programmable Read-Only Memory (EEPROM)) and flash memory devices; magnetic disks, such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks.

[0065] The instructions 724 may further be transmitted or received over a communications network 726 using a transmission medium via the network interface device 720 utilizing any one of a number of transfer protocols (e.g.,

frame relay, internet protocol (IP), transmission control protocol (TCP), user datagram protocol (UDP), hypertext transfer protocol (HTTP), etc.). The term "transmission medium" shall be taken to include any intangible medium that is capable of storing, encoding or carrying instructions for execution by the machine 700, and includes digital or analog communications signals or other intangible medium to facilitate communication of such software.

[0066] Embodiments may be implemented in one or a combination of hardware, firmware and software. Embodiments may also be implemented as instructions stored on a computer-readable storage device, which may be read and executed by at least one processor to perform the operations described herein. A computer-readable storage device may include any non-transitory mechanism for storing information in a form readable by a machine (e.g., a computer). For example, a computer-readable storage device may include read-only memory (ROM), random-access memory (RAM), magnetic disk storage media, optical storage media, flash-memory devices, and other storage devices and media.

[0067] FIG. 8 illustrates a functional block diagram of a UE 800 in accordance with some embodiments. The UE 800 may be suitable for use as device 112 (FIG. 1) or device 202 (FIG. 2). The UE 800 may include physical layer circuitry 802 for transmitting and receiving signals to and from eNBs using one or more antennas 801. UE 800 may also include processing circuitry 806 that may include, among other things a channel estimator. UE 800 may also include a memory 808. The processing circuitry may be configured to determine several different feedback values discussed below for transmission to the eNB. The processing circuitry may also include a media access control (MAC) layer 804.

[0068] In some embodiments, the UE 800 may include one or more of a keyboard, a display, a non-volatile memory port, multiple antennas, a graphics processor, an application processor, speakers, and other mobile device elements. The display may be an LCD screen including a touch screen.

[0069] The one or more antennas 801 utilized by the UE 800 may comprise one or more directional or omnidirectional antennas, including, for

example, dipole antennas, monopole antennas, patch antennas, loop antennas, microstrip antennas or other types of antennas suitable for transmission of RF signals. In some embodiments, instead of two or more antennas, a single antenna with multiple apertures may be used. In these embodiments, each aperture may be considered a separate antenna. In some multiple-input multiple-output (MIMO) embodiments, the antennas may be effectively separated to take advantage of spatial diversity and the different channel characteristics that may result between each of antennas and the antennas of a transmitting station. In some MIMO embodiments, the antennas may be separated by up to 1/10 of a wavelength or more.

[0070] Although the UE 800 is illustrated as having several separate functional elements, one or more of the functional elements may be combined and may be implemented by combinations of software-configured elements, such as processing elements including digital signal processors (DSPs), and/or other hardware elements. For example, some elements may comprise one or more microprocessors, DSPs, application specific integrated circuits (ASICs), radio-frequency integrated circuits (RFICs) and combinations of various hardware and logic circuitry for performing at least the functions described herein. In some embodiments, the functional elements may refer to one or more processes operating on one or more processing elements.

[0071] Embodiments may be implemented in one or a combination of hardware, firmware and software. Embodiments may also be implemented as instructions stored on a computer-readable storage medium, which may be read and executed by at least one processor to perform the operations described herein. A computer-readable storage medium may include any non-transitory mechanism for storing information in a form readable by a machine (e.g., a computer). For example, a computer-readable storage medium may include read-only memory (ROM), random-access memory (RAM), magnetic disk storage media, optical storage media, flash-memory devices, and other storage devices and media. In these embodiments, one or more processors of the UE 800 may be configured with the instructions to perform the operations described herein.

[0072] In some embodiments, the UE 800 may be configured to receive OFDM communication signals over a multicarrier communication channel in accordance with an OFDMA communication technique. The OFDM signals may comprise a plurality of orthogonal subcarriers. In some broadband multicarrier embodiments, eNBs (including macro eNB and pico eNBs) may be part of a broadband wireless access (BWA) network communication network, such as a Worldwide Interoperability for Microwave Access (WiMAX) communication network or a 3rd Generation Partnership Project (3GPP) Universal Terrestrial Radio Access Network (UTRAN) Long-Term-Evolution (LTE) or a Long-Term-Evolution (LTE) communication network, although the scope of the inventive subject matter described herein is not limited in this respect. In these broadband multicarrier embodiments, the UE 800 and the eNBs may be configured to communicate in accordance with an orthogonal frequency division multiple access (OFDMA) technique. The UTRAN LTE standards include the 3rd Generation Partnership Project (3GPP) standards for UTRAN-LTE, release 8, March 2008, and release 10, December 2010, including variations and evolutions thereof.

[0073] In some LTE embodiments, the basic unit of the wireless resource is the Physical Resource Block (PRB). The PRB may comprise 12 sub-carriers in the frequency domain x 0.5 ms in the time domain. The PRBs may be allocated in pairs (in the time domain). In these embodiments, the PRB may comprise a plurality of resource elements (REs). A RE may comprise one sub-carrier x one symbol.

[0074] Two types of reference signals may be transmitted by an eNB including demodulation reference signals (DM-RS), channel state information reference signals (CIS-RS) and/or a common reference signal (CRS). The DM-RS may be used by the UE for data demodulation. The reference signals may be transmitted in predetermined PRBs.

[0075] In some embodiments, the OFDMA technique may be either a frequency domain duplexing (FDD) technique that uses different uplink and downlink spectrum or a time-domain duplexing (TDD) technique that uses the same spectrum for uplink and downlink.

[0076] In some other embodiments, the UE 800 and the eNBs may be configured to communicate signals that were transmitted using one or more other modulation techniques such as spread spectrum modulation (e.g., direct sequence code division multiple access (DS-CDMA) and/or frequency hopping code division multiple access (FH-CDMA)), time-division multiplexing (TDM) modulation, and/or frequency-division multiplexing (FDM) modulation, although the scope of the embodiments is not limited in this respect.

[0077] In some embodiments, the UE 800 may be part of a portable wireless communication device, such as a PDA, a laptop or portable computer with wireless communication capability, a web tablet, a wireless telephone, a wireless headset, a pager, an instant messaging device, a digital camera, an access point, a television, a medical device (e.g., a heart rate monitor, a blood pressure monitor, etc.), or other device that may receive and/or transmit information wirelessly.

[0078] In some LTE embodiments, the UE 800 may calculate several different feedback values which may be used to perform channel adaption for closed-loop spatial multiplexing transmission mode. These feedback values may include a channel-quality indicator (CQI), a rank indicator (RI) and aprecoding matrix indicator (PMI). By the CQI, the transmitter selects one of several modulation alphabets and code rate combinations. The RI informs the transmitter about the number of useful transmission layers for the current MIMO channel, and the PMI indicates the codebook index of the precoding matrix (depending on the number of transmit antennas) that is applied at the transmitter. The code rate used by the eNB may be based on the CQI. The PMI may be a vector that is calculated by the UE and reported to the eNB. In some embodiments, the UE may transmit a physical uplink control channel (PUCCH) of format 2, 2a or 2b containing the CQI/PMI or RI.

[0079] In these embodiments, the CQI may be an indication of the downlink mobile radio channel quality as experienced by the UE 800. The CQI allows the UE 800 to propose to an eNB an optimum modulation scheme and coding rate to use for a given radio link quality so that the resulting transport block error rate would not exceed a certain value, such as 10%. In some

embodiments, the UE may report a wideband CQI value which refers to the channel quality of the system bandwidth. The UE may also report a sub-band CQI value per sub-band of a certain number of resource blocks which may be configured by higher layers. The full set of sub-bands may cover the system bandwidth. In case of spatial multiplexing, a CQI per code word may be reported.

[0080] In some embodiments, the PMI may indicate an optimum precoding matrix to be used by the eNB for a given radio condition. The PMI value refers to the codebook table. The network configures the number of resource blocks that are represented by a PMI report. In some embodiments, to cover the system bandwidth, multiple PMI reports may be provided. PMI reports may also be provided for closed loop spatial multiplexing, multi-user MIMO and closed-loop rank 1 precoding MIMO modes.

[0081] In some cooperating multipoint (CoMP) embodiments, the network may be configured for joint transmissions to a UE in which two or more cooperating/coordinating points, such as remote-radio heads (RRHs) transmit jointly. In these embodiments, the joint transmissions may be MIMO transmissions and the cooperating points are configured to perform joint beamforming.

[0082] The example embodiments discussed herein may be utilized by wireless network access providers of all types including, but not limited to, mobile broadband providers looking to increase cellular offload ratios for cost-avoidance and performance gains, fixed broadband providers looking to extend their coverage footprint outside of customers' homes or businesses, wireless network access providers looking to monetize access networks via access consumers or venue owners, public venues looking to provide wireless network (e.g., Internet) access, or digital services (e.g. location services, advertisements, entertainment, etc.) over a wireless network, and business, educational or non-profit enterprises that desire to simplify guest Internet access or Bring-Your-Own-Device (BYOD) access.

[0083] The Abstract is provided to comply with 37 C.F.R. Section 1.72(b) requiring an abstract that will allow the reader to ascertain the nature and

gist of the technical disclosure. It is submitted with the understanding that it will not be used to limit or interpret the scope or meaning of the claims. The following claims are hereby incorporated into the detailed description, with each claim standing on its own as a separate embodiment.

CLAIMS

What is claimed is:

1. A network equipment comprising:

processing circuitry;

an antenna; and

a transceiver coupled to the processing circuitry and the antenna;

wherein the processing circuitry is configured to:

provide a beacon indicating support for a public-use credential to the transceiver, the transceiver being configured to transmit the beacon;

receive a request from a first device to establish a first encrypted network connection between the network equipment and the first device, the request including the pre-configured public-use credential and the beacon;

provide, in response to the request, an authenticity certificate previously signed by a certificate authority;

establish a first encrypted network connection with the first device based at least in part on the pre-configured public-use credential and the authenticity certificate;

wherein the secure device-to-device communication session is unique to the first device and the network equipment.

2. The network equipment of claim 1, wherein the processing circuitry is further configured to:

receive the pre-configured public-use credential from a second device, and

in response to receiving the pre-configured public-use credential establish a second encrypted network connection with the second device that is distinct from the first encrypted network connection.

3. The network equipment of any of claims 1 or 2, wherein the processing circuitry is further configured to:

receive, via the secure device-to-device communication session, a user-specific credential from the first device;

authenticate the user-specific credential; and

provide, in response to the authentication of the user specific credential, access by the first device to a resource on a network coupled to the network equipment.

4. The network equipment of any of claims 1 or 2, wherein the first encrypted network connection is established between the first device and the network equipment to create a direct wireless network connection, the first encrypted network connection performing wireless communications in accordance with a standard from: a standard from an IEEE 802.11 standards family, a standard from an IEEE 802.16 standards family, or a standard from a Bluetooth Special Interest Group standards family.

5. A method performed by a communication station (STA) for establishing an encrypted wireless connection comprising:

discovering one or more wireless networks with a wireless receiver of the STA;

attempting, by the STA, to establish an encrypted device-to-device communication session with an access point of an wireless network of the one or more available wireless networks, in response to discovering the wireless network, by providing a pre-configured public-use credential to the access point of the encrypted network; and

establishing the secure device-to-device communication session based at least in part on the pre-configured public-use credential;

wherein the secure device-to-device communication session is unique to the STA and the access point and the public-use credential is not unique to the STA.

6. The method of claim 5, further comprising:

providing a prompt to a user, the prompt requesting the user provide a user specific credential to the STA or an instruction to provide the pre-configured public-use credential to the access point;

receiving a response to the prompt, the response including the user specific credential or the instruction to use the pre-configured public-use credential; and

transmitting the user specific credential or the pre-configured public-use credential to the access point based on the response.

7. The method of any of claims 5 or 6, wherein establishing the secure device-to-device communication session further comprises:

attempting to establish the secure device-to-device communication session with the access point of the encrypted wireless network with a first class of credential, the first class of credential being specific to a user;

in response to failing to connect with the first class of credential, attempting to connect to the access point with a second class of credential, the second class of credential being specific to an organization;

in response to failing to establish the secure device-to-device communication session with the access point with the second class of credential, attempting to connect to the access point network the pre-configured public-use credential.

8. The method of any of claims 5 or 6, further comprising:

receiving, at the STA in response to providing the pre-configured public-use credential to the access point, an electronically signed authenticity certificate from the access point of the encrypted wireless network;

wherein establishing the secure device-to-device communication session is based at least in part on the pre-configured public-use credential and the electronically signed authenticity certificate.

9. The method of claim 5, wherein the STA is included in a user equipment (UE), and the secure device-to-device communication session includes a direct wireless network connection performing wireless communications in accordance with a standard from: a 3GPP Long Term Evolution or Long Term Evolution-Advanced standards family, a standard from an IEEE 802.11 standards family, a standard from an IEEE 802.16 standards family, or a standard from a Bluetooth Special Interest Group standards family.

10. The method of claim 9, wherein the UE and the access point include an encryption mechanism in accordance with a standard from an Advanced Encryption Standard (AES) family.

11. The method of any of claims 9 or 10, wherein the UE includes a first device comprising processing circuitry arranged to communicate with an evolved NodeB (eNB);

wherein the network includes a Long Term Evolution/Long Term Evolution-Advanced (LTE/LTE-A) network; and

where in the UE is configured to establish an encrypted wireless connection for direct device-to-device communications network with the access point, by performing operations to communicate with a certificate authority over the LTE/LTE-A network to verify the validity of the electronically signed authenticity certificate.

12. A wireless communication method comprising:

transmitting, from an access point, a network identifier;

receiving, at the access point, a request from a communication station (STA) to establish a secure device-to-device communication session between the access point and the STA, the request including a pre-configured public-use credential and the network identifier;

providing, in response to the request, an authenticity certificate previously signed by a certificate authority; and

establishing the secure device-to-device communication session between the access point and the STA based at least in part on the pre-configured public-use credential and the authenticity certificate;

wherein the secure device-to-device communication session is unique to the UE and the access point.

13. The method of claim 12, further comprising:

receiving, at the access point via the secure device-to-device communication session, a user-specific credential from the STA;

authenticating the user-specific credential; and

providing, in response to the authentication of the user specific credential, access to a resource on a network coupled to the access point.

14. The method of any of claims 12 or 13, further comprising:

providing, via the secure device-to-device communication session, a request for user specific information;

establishing, in response to receiving the user specific information, a user specific credential at the access point; and

providing, in response to establishing the user specific credential, access to a resource on a network coupled to the access point.

15. The method of any of claims 12 or 13, further comprising:

receiving, at the access point via the secure device-to-device communication session, a group credential from the STA;

authenticating the group credential; and

providing, in response to the authentication of the user specific credential, access to a group resource on a network coupled to the access point.

16. The method of any of claims 12 or 13, wherein the STA is included in a user equipment (UE), and the secure device-to-device communication session includes a direct wireless network connection performing wireless communications in accordance with a standard from: a 3GPP Long Term Evolution or Long Term Evolution-Advanced standards family, a standard from an IEEE 802.11 standards family, a standard from an IEEE 802.16 standards family, or a standard from a Bluetooth Special Interest Group standards family.

17. A communication station (STA), comprising a memory coupled to processing circuitry, the processing circuitry arranged to communicate with a network and to establish an encrypted wireless connection with an access point coupled to the network, by performing operations to:

discover the wireless network;

providing a pre-configured public-use credential to the access point, in response to discovering the network; and

establish the secure device-to-device communication session based at least in part on the pre-configured public-use credential;

wherein the secure device-to-device communication session is unique to the STA and the access point.

18. The STA of claim 17, further comprising:

a user interface coupled to the processing circuitry;

wherein the processing circuitry is further arranged to perform operations to:

provide, via the user interface, a prompt to either provide a user specific credential to the STA or an instruction to provide the pre-configured public-use credential;

receive, via the user interface, a response to the prompt, the response including the user specific credential or the instruction to connect with the pre-configured public-use credential; and

transmit the response to the access point.

19. The STA of claim 17, comprising circuitry arranged to:

attempt to establish the secure device-to-device communication session with the access point of the encrypted wireless network with a first class of credential, the first class of credential being specific to a user;

in response to failing to connect with the first class of credential, attempt to connect to the access point of the encrypted wireless network with a second class of credential, the second class of credential being specific to an organization;

in response to failing to establish the secure device-to-device communication session with the access point of the encrypted wireless network with the second class of credential, attempt to connect to the access point of the encrypted wireless network with the pre-configured public-use credential.

20. The STA of any of claims 17, 18 or 19, comprising circuitry arranged to:

receive, at the STA in response to providing the pre-configured public-use credential to the access point, an electronically signed authenticity certificate from the access point of the encrypted wireless network;

wherein establishing the secure device-to-device communication session is based at least in part on the pre-configured public-use credential and the electronically signed authenticity certificate.

21. The STA of any of claims 17, 18 or 19, further comprising user equipment (UE);

wherein the encrypted wireless connection is established between a first device and the access point to create a secure wireless network connection, the secure wireless network connection performing wireless communications in accordance with a standard from: a 3GPP Long Term Evolution or Long Term Evolution-Advanced standards family, a standard from an IEEE 802.1 1

standards family, a standard from an IEEE 802.16 standards family, or a standard from a Bluetooth Special Interest Group standards family.

22. The STA of claim 21, wherein the UE and the access point include an encryption mechanism in accordance with a standard from an Advanced Encryption Standard (AES) family.

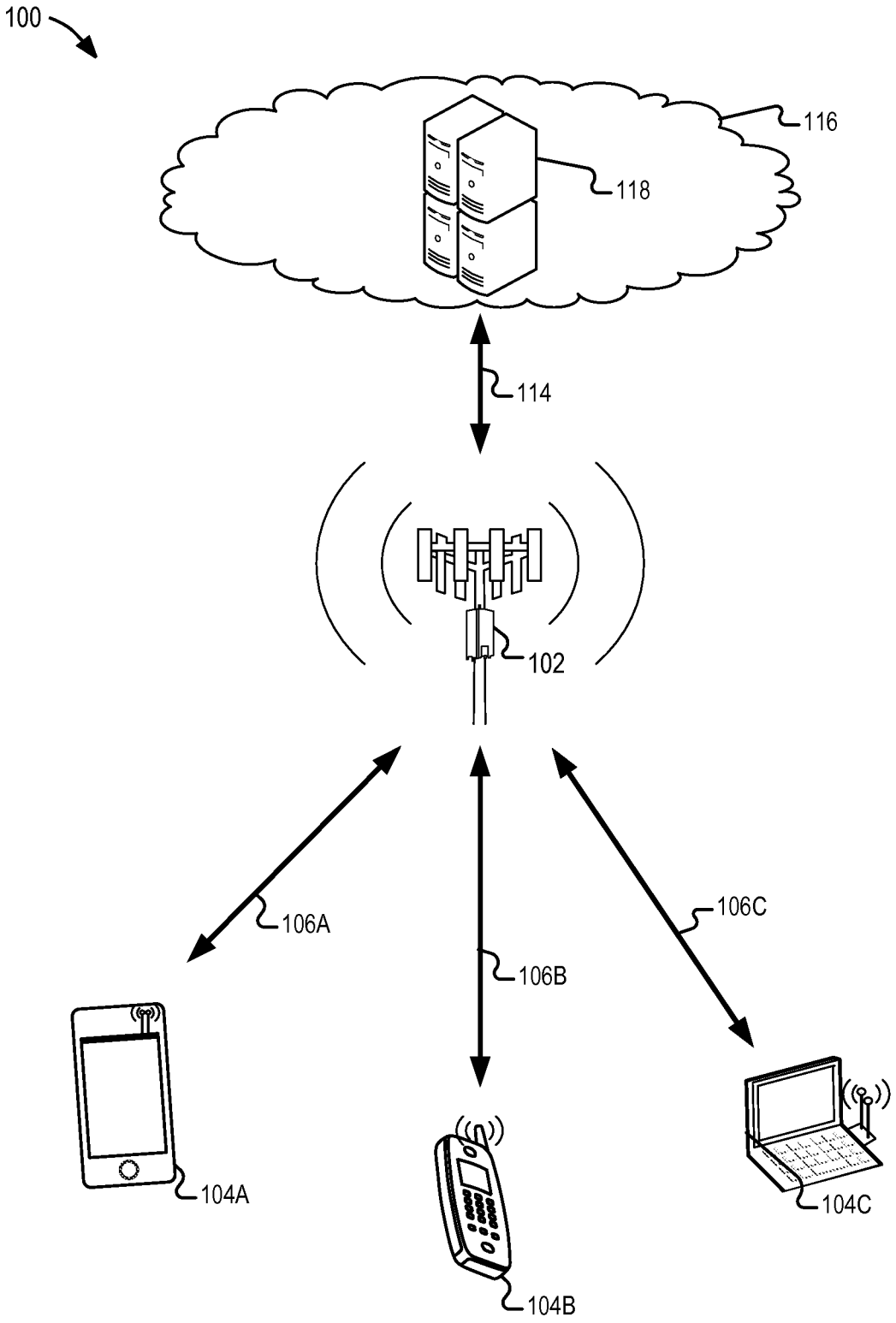

FIG. 1

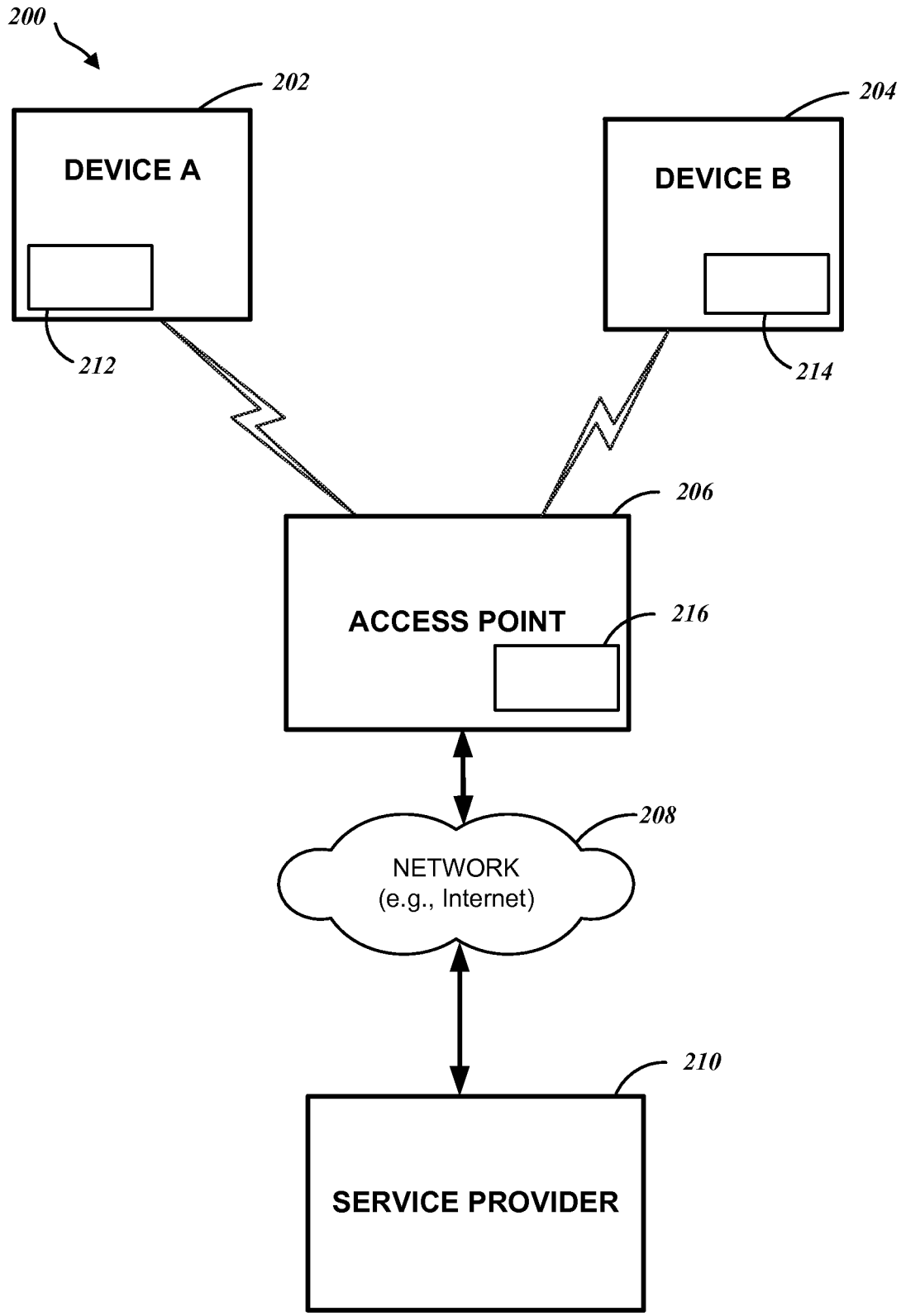
200
202
DEVICE A
204
DEVICE B
212
214
206
ACCESS POINT
216
208
NETWORK
(e.g., Internet)
210
SERVICE PROVIDER

FIG. 2

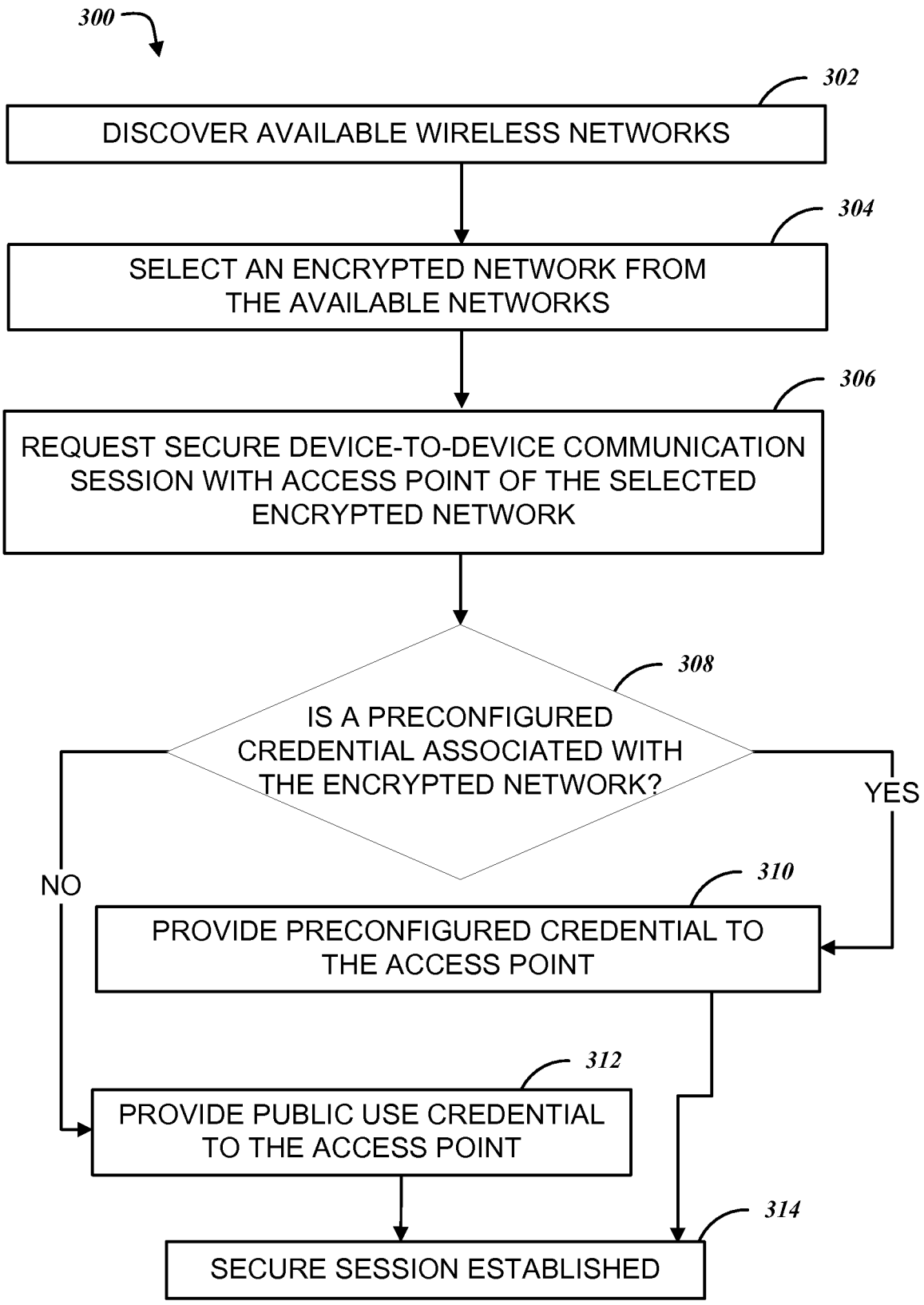
300
302
DISCOVER AVAILABLE WIRELESS NETWORKS
304
SELECT AN ENCRYPTED NETWORK FROM THE AVAILABLE NETWORKS
306
REQUEST SECURE DEVICE-TO-DEVICE COMMUNICATION SESSION WITH ACCESS POINT OF THE SELECTED ENCRYPTED NETWORK
308
IS A PRECONFIGURED CREDENTIAL ASSOCIATED WITH THE ENCRYPTED NETWORK?
YES
NO
310
PROVIDE PRECONFIGURED CREDENTIAL TO THE ACCESS POINT
312
PROVIDE PUBLIC USE CREDENTIAL TO THE ACCESS POINT
314
SECURE SESSION ESTABLISHED

FIG. 3

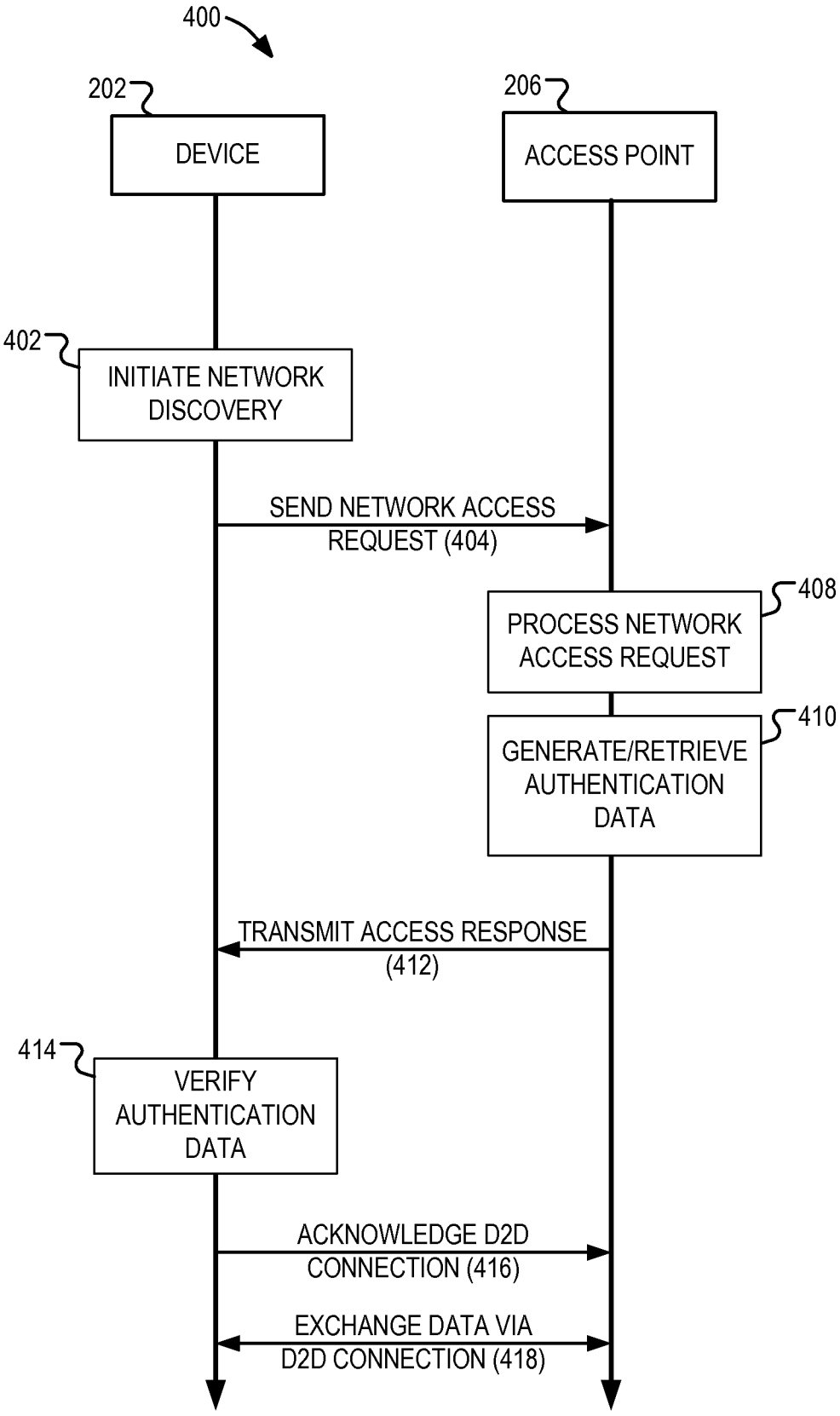
400
202
DEVICE
206
ACCESS POINT
402
INITIATE NETWORK DISCOVERY
SEND NETWORK ACCESS REQUEST (404)
408
PROCESS NETWORK ACCESS REQUEST
410
GENERATE/RETRIEVE AUTHENTICATION DATA
TRANSMIT ACCESS RESPONSE (412)
414
VERIFY AUTHENTICATION DATA
ACKNOWLEDGE D2D CONNECTION (416)
EXCHANGE DATA VIA D2D CONNECTION (418)

FIG. 4

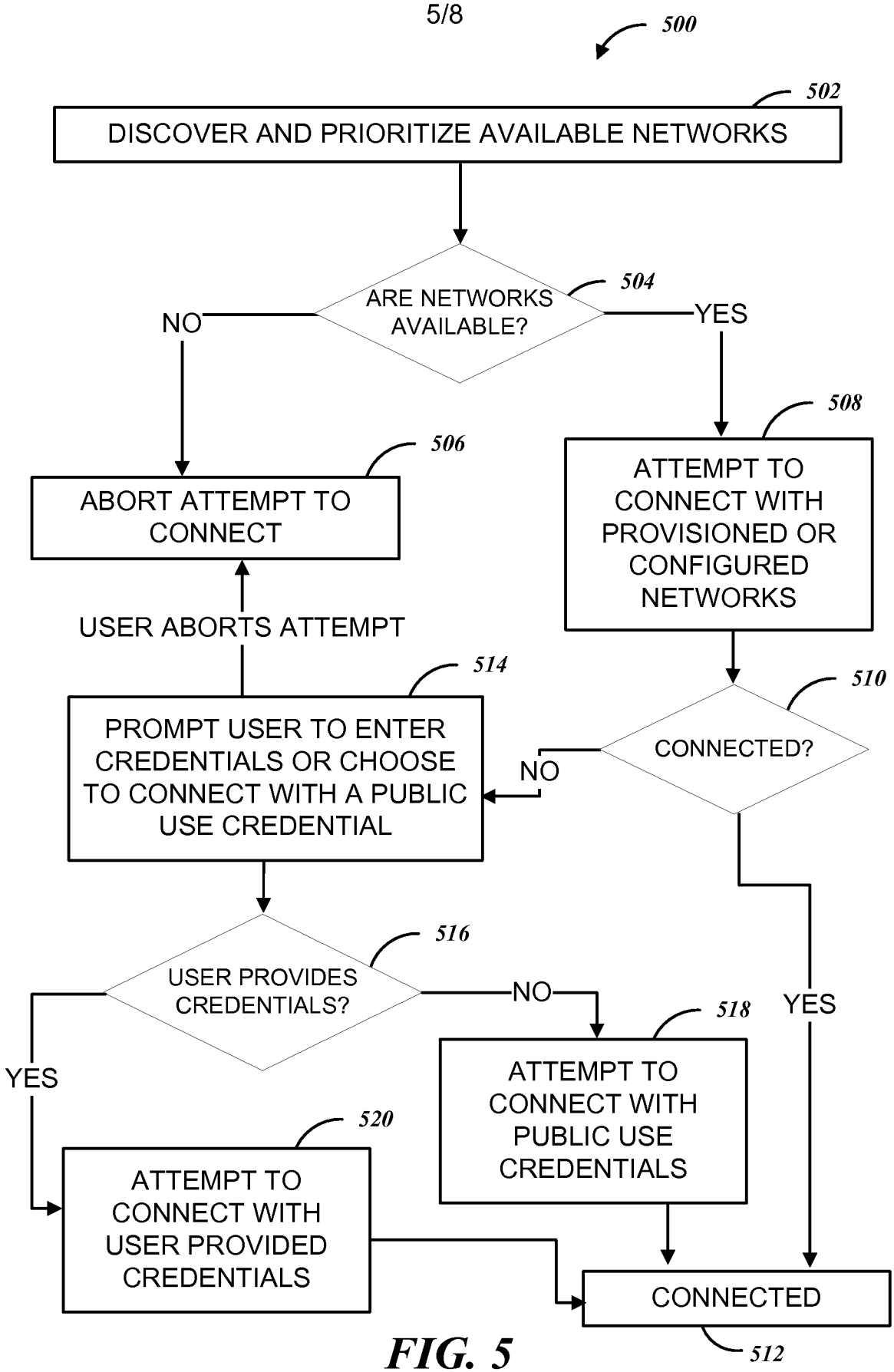
500
502
DISCOVER AND PRIORITIZE AVAILABLE NETWORKS
504
ARE NETWORKS AVAILABLE?
NO
YES
506
ABORT ATTEMPT TO CONNECT
508
ATTEMPT TO CONNECT WITH PROVISIONED OR CONFIGURED NETWORKS
USER ABORTS ATTEMPT
514
PROMPT USER TO ENTER CREDENTIALS OR CHOOSE TO CONNECT WITH A PUBLIC USE CREDENTIAL
510
CONNECTED?
NO
516
USER PROVIDES CREDENTIALS?
NO
YES
YES
518
ATTEMPT TO CONNECT WITH PUBLIC USE CREDENTIALS
520
ATTEMPT TO CONNECT WITH USER PROVIDED CREDENTIALS
CONNECTED
512

FIG. 5

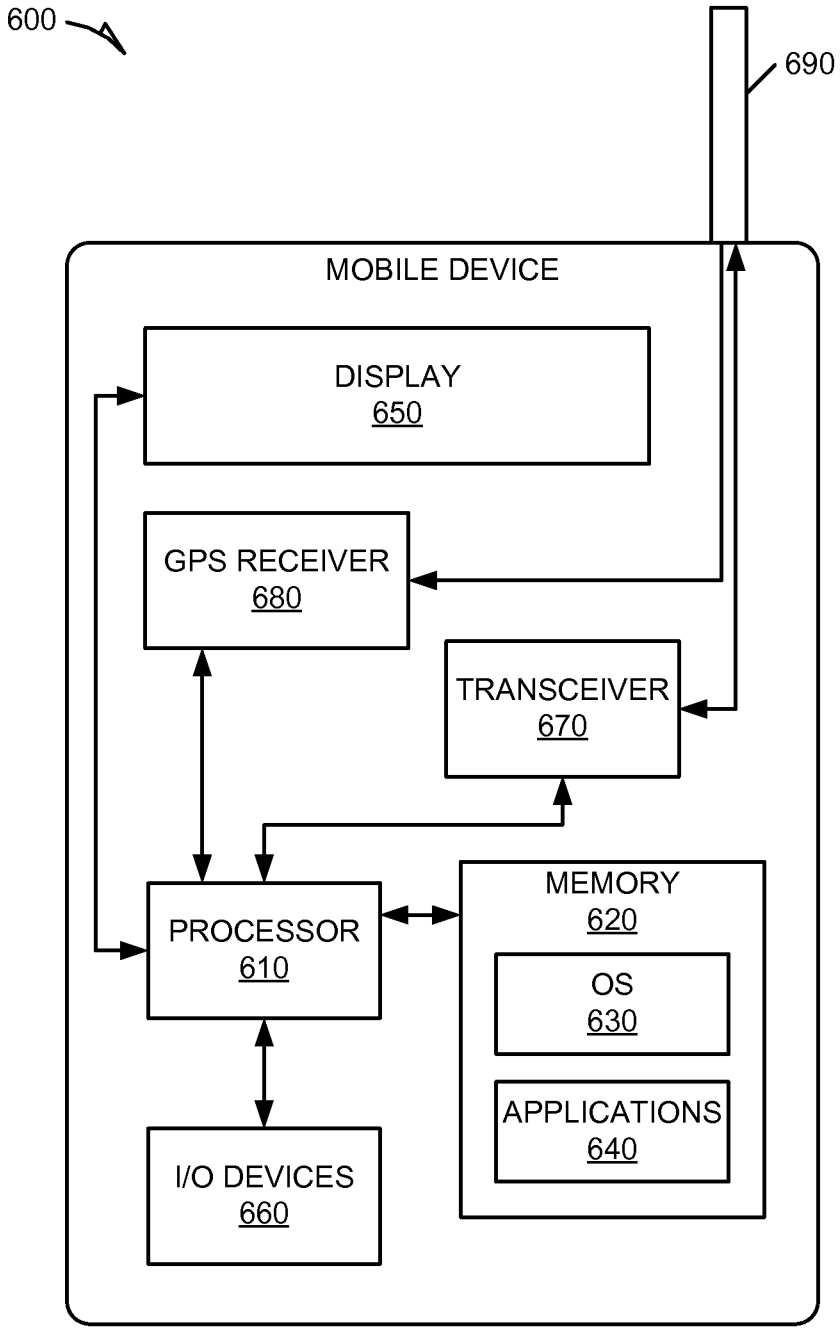
600
690
MOBILE DEVICE
DISPLAY
650
GPS RECEIVER
680
TRANSCEIVER
670
PROCESSOR
610
MEMORY
620
OS
630
APPLICATIONS
640
I/O DEVICES
660

FIG. 6

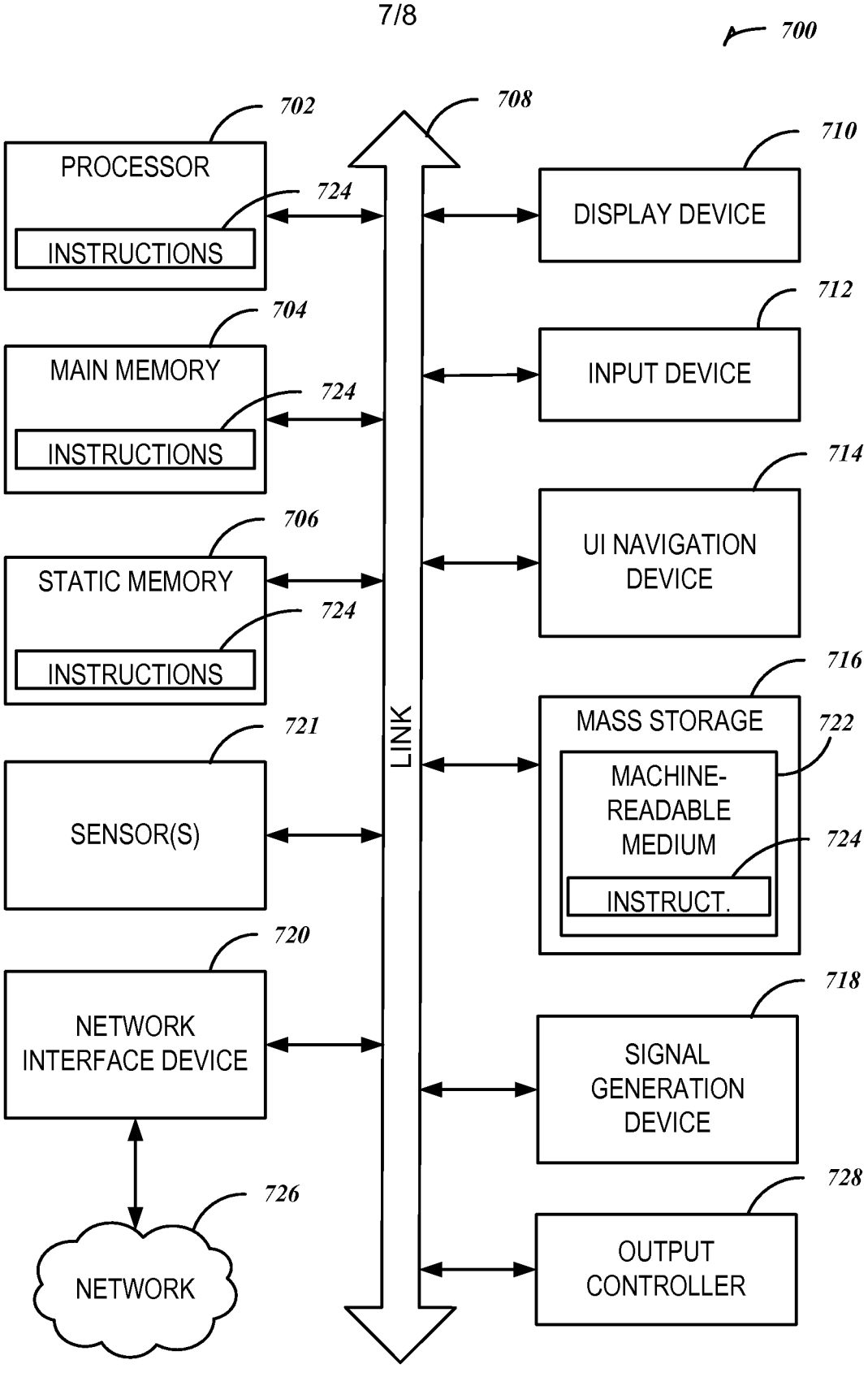
700
PROCESSOR
INSTRUCTIONS
MAIN MEMORY
INSTRUCTIONS
STATIC MEMORY
INSTRUCTIONS
SENSOR(S)
NETWORK INTERFACE DEVICE
NETWORK
LINK
DISPLAY DEVICE
INPUT DEVICE
UI NAVIGATION DEVICE
MASS STORAGE
MACHINE-READABLE MEDIUM
INSTRUCT.
SIGNAL GENERATION DEVICE
OUTPUT CONTROLLER
702
704
706
708
710
712
714
716
718
720
721
722
724
726
728

FIG. 7

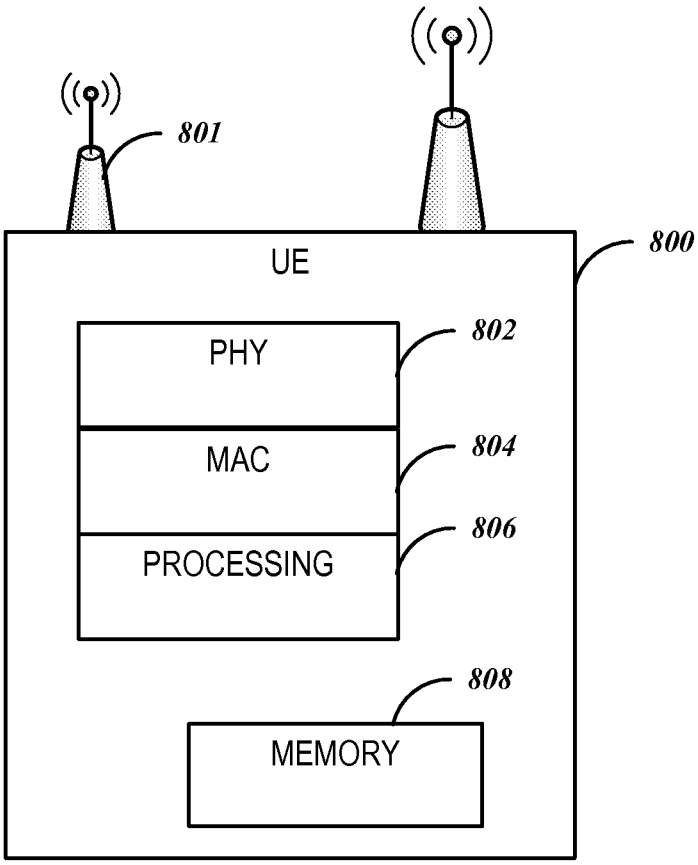

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/048683

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/08(2009.01)i

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)
H04W 12/08; H04W 48/16; H04L 9/32; H04L 29/06; H04W 88/06; H04W 12/06; H04W 48/20; G06F 21/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: encrypt* , network, credential, authenti*

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011-0119492 Al (ANAND PALANIGOUNDER et al.) 19 May 2011 See abstract, figures 2-5 and claims 1-54.	1-22
A	KR 10-2013-0055501 A (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) 28 May 2013 See abstract, figure 4 and claims 1-11 .	1-22
A	US 2011-0269423 Al (STEPHAN V. SCHELL et al.) 03 November 2011 See abstract, figures 6-8 and claims 1-20.	1-22
A	US 2011-0314522 Al (ANAND PALANIGOUNDER et al.) 22 December 2011 See abstract, figures 2-5, 11 and claims 1-43 .	1-22

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent 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
26 March 2014 (26.03.2014)	**27 March 2014 (27.03.2014)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea
Facsimile No. +82-42-472-7140

Authorized officer
YOO, Sun Jung
Telephone No. +82-42-481-5775

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/048683

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0119492 Al	19/05/2011	CN 102440016 A	02/05/2012
		EP 2430847 A2	21/03/2012
		JP 2012-527184A	01/11/2012
		KR 10-2012-0024757 A	14/03/2012
		TW 201127099 A	01/08/2011
		US 8589689 B2	19/11/2013
		WO 2010-132499 A2	18/11/2010
		WO 2010-132499 A3	03/03/2011
		WO 2010-132499 A8	24/11/2011
		WO 2010-132499 A8	18/11/2010
KR 10-2013-0055501 A	28/05/2013	None	
US 2011-0269423 Al	03/11/2011	AU 2011-248610 Al	04/10/2012
		CA 2793028 Al	10/11/2011
		CN 102859966 A	02/01/2013
		EP 2567527 Al	13/03/2013
		JP 2013-529019A	11/07/2013
		KR 10-2013-0032873 A	02/04/2013
		MX 2012012750 A	21/11/2012
		SG 184790A1	29/11/2012
		TW 201208405 A	16/02/2012
		US 8666368 B2	04/03/2014
		WO 2011-139795 Al	10/11/2011
US 2011-0314522 Al	22/12/2011	AR 082019A1	07/11/2012
		CN 102893646 A	23/01/2013
		EP 2583481 Al	24/04/2013
		JP 2013-534755A	05/09/2013
		KR 10-2013-0023350 A	07/03/2013
		TW 201218790 A	01/05/2012
		WO 2011-160070 Al	22/12/2011