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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2014 (23.01.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/014880 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04W 84/12* (2009.01)

(21) International Application Number:
PCT/US2013/050635

(22) International Filing Date:
16 July 2013 (16.07.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/552,749 19 July 2012 (19.07.2012) US

(71) Applicant: **SPRINT COMMUNICATIONS COMPANY L.P.** [US/US]; 6391 Sprint Parkway, Mailstop: KSOPHT0101-Z2100, Overland Park, Kansas 66251-2100 (US).

(72) Inventors: **GATEWOOD, John M.**; 608 NE Victoria Drive, Lee's Summit, Missouri 64086 (US). **SCHNITZER, Lee Alan**; 7805 Woodstone Lane, Lenexa, Kansas 66217 (US). **WOODRUM, Sharon L.**; 32510 Metcalf Road, P.O. Box 277, Louisburg, Kansas 66053 (US). **VORUGANTI, Bhanu Prakash**; 8759 West 121 Terrace, Apt. 104, Overland Park, Kansas 66213 (US).

(74) Agents: **SETTER, Michael J.** et al.; Setter Roche LLP, P.O. Box 780, Erie, Colorado 80516 (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).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

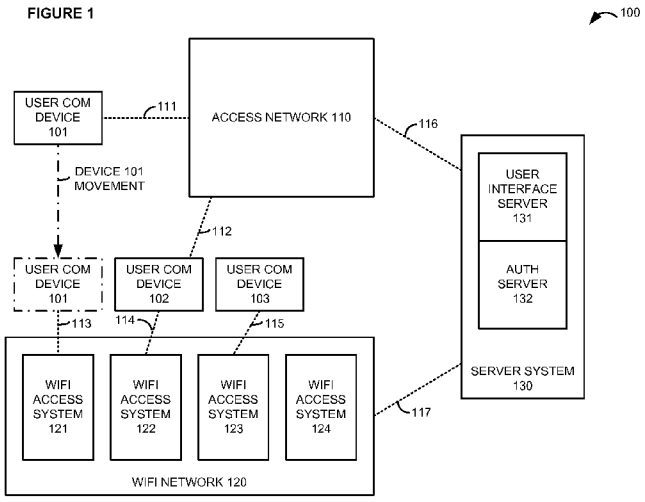
Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: USER CONTROL OVER WIFI NETWORK ACCESS

FIGURE 1



(57) Abstract: A server system (130, 730, 830, 900) transfers display data for presentation to a user who selects multiple geographically-distributed WiFi access systems (121-124, 721-724, 821-824) and a password. The server system (130, 730, 830, 900) receives user data that indicates the user-selected WiFi network access systems (121-124, 721-724, 821-824) and the user-selected password. The server system (130, 730, 830, 900) stores an association between the user-selected WiFi network access systems (121-124, 721-724, 821-824) and the user-selected password. The server system (130, 730, 830, 900) receives an access request for one of the user-selected WiFi network access systems (121-124, 721-724, 821-824) using the user-selected password. The server system (130, 730, 830, 900) transfers a positive response to the access request based on the stored association between the user-selected WiFi network access systems (121-124, 721-724, 821-824) and the user-selected password.

WO 2014/014880 A1

USER CONTROL OVER WIFI NETWORK ACCESS

TECHNICAL BACKGROUND

[1] Wireless Fidelity (WiFi) is a popular wireless protocol to obtain network access – often to the Internet. Typically, a WiFi access point broadcasts a Service Set Identification (SSID) that is detected by user devices. The user devices typically respond to the SSID with an access code that is pre-stored in the WiFi access point. The WiFi access point provides network access if the user-provided access code matches the pre-stored access code. The user typically manages multiple access codes for the various WiFi access points that they use. Unfortunately, these WiFi access points are not used to provide effective and efficient user control over WiFi network access.

[2] Other wireless networks also include user authorization systems that control network access. For example, 3G networks may have an Authentication, Authorization, and Accounting (AAA) system, and 4G networks may have a Home Subscriber Server (HSS). These other wireless networks also provide network access to user devices. Unfortunately, the other wireless networks are not used to provide effective and efficient user control over WiFi network access.

[3] In particular, WiFi access points and these other wireless networks are not effectively used in an integrated manner to provide efficient user control over WiFi network access.

TECHNICAL OVERVIEW

[4] A server system transfers display data for presentation to a user who selects multiple geographically-distributed WiFi access systems and a password. The server system receives user data that indicates the user-selected WiFi network access systems and the user-selected password. The server system stores an association between the user-selected WiFi network access systems and the user-selected password. The server system receives an access request for one of the user-selected WiFi network access systems using the user-selected password. The server system transfers a positive response to the access request based on the stored association between the user-selected WiFi network access systems and the user-selected password.

DESCRIPTION OF THE DRAWINGS

[5] Figure 1 illustrates a communication system to provide user control over access to a WiFi network having geographically-distributed WiFi access systems.

[6] Figure 2 illustrates the operation of a communication system to provide user control over access to a WiFi network having geographically-distributed WiFi access systems.

[7] Figure 3 illustrates the operation of a communication system to provide user control over access to a WiFi network having geographically-distributed WiFi access systems by allowing user-selection of communication devices.

[8] Figure 4 illustrates the operation of a communication system to provide user control over access to a WiFi network having geographically-distributed WiFi access systems by transferring configuration data to a user communication device.

[9] Figure 5 illustrates the operation of a communication system to provide user control over access to a WiFi network having geographically-distributed WiFi access systems by using dynamic access keys.

[10] Figure 6 illustrates a communication device display that renders a geographic map for a user to select WiFi network access systems and specify passwords.

[11] Figure 7 illustrates a wireless Long Term Evolution (LTE) network to provide user control over access to a WiFi network having geographically-distributed WiFi access systems.

[12] Figure 8 illustrates an WiFi system to provide user control over access to a WiFi network having geographically-distributed WiFi access systems.

[13] Figure 9 illustrates a server system to provide user control over access to WiFi networks.

[14] Figure 10 illustrates wireless communication device to provide user control over access to WiFi networks.

DETAILED DESCRIPTION

[15] Figure 1 illustrates communication system 100 to provide user control over access to WiFi network 120 having geographically-distributed WiFi access systems 121-124. Communication system 100 comprises user communication devices 101-103, access network 110, WiFi network 120, and server system 130. Server system 130 comprises user interface server 131 and authorization server 132.

[16] User communication devices 101-103 comprise phones, computers, media players, machine transceivers, or some other WiFi communication equipment. User communication devices 101-102 and access network 110 communicate over respective access links 111-112. User communication devices 101-103 and WiFi access systems 121-123 communicate over respective WiFi links 113-115. Access network 110 and WiFi network 120 communicate with server system 130 over respective network links 116-117.

[17] In operation, user interface server 131 transfers display data to user communication device 101 over access network 110 and links 111 and 116 for presentation to a user. In response to the display data, the user selects WiFi access systems 121-123 but not access system 124. The user also selects a single password for the user-selected WiFi access systems 121-123. In some examples, the display data renders geographic maps that indicate WiFi access systems 121-124 for selection. The display data may also include a data collection module to collect the password from the user.

[18] User communication device 101 transfers user data for delivery to user interface server 131. The user data indicates the user-selected WiFi network access systems 121-123, the user-selected password, and possibly other user selections and data. User interface server 131 receives and transfers the user data to user authorization server 132.

[19] Authorization server 132 stores an association between the user-selected WiFi network access systems 121-123 and the user-selected password. Subsequently, user communication device 101 moves near WiFi access system 121 and transfers an access request to WiFi access system 121 using the user-selected password. WiFi access system 121 transfers the access request for delivery to authorization server 132.

[20] Authorization server 132 receives the access request for access to user-selected WiFi network access system 121 using the user-selected password. Based on the stored

association between the user-selected WiFi network access system 121 and the user-selected password, authorization server 132 transfers a positive response for delivery to WiFi network access system 121. WiFi network access system 121 then provides WiFi access (typically to the Internet) to wireless communication device 101 over WiFi link 113.

[21] User wireless communication device 102 could select and use multiple WiFi access systems with a single password in a similar manner. In some examples, wireless communication device 101 is used to select the WiFi access systems and password, while communication device 102 and/or communication device 103 are used to access the selected WiFi access systems with the password. Also note that a user may have different passwords for different groups of access systems, devices, timeframes, and the like. If desired, the user may also use a given password for only one access system. Note that a password could be any sequence of letters, numbers, symbols, or other data.

[22] In some examples, additional items are selected by the user responsive to the display data. These additional items may be indicated in the user data, stored in the association, and used in combination to transfer the positive response to the access request. For example, the user may specify a user name to use when accessing their selected WiFi network access systems. In other examples, the user specifies a communication device to use when accessing their selected WiFi network access systems. In yet other examples, the user specifies a timeframe for access to their selected WiFi network access systems.

[23] In some examples, user interface server 131 transfers configuration data for delivery to user communication device 101 and/or user communication device 102 over access network 110. The configuration data associates broadcast identification signals for the user-selected WiFi network access systems with the user-selected password. User communication devices 101-102 use the configuration data to obtain the password from the

user and to transfer the access request when in range of one of the selected WiFi network access systems.

[24] In some examples, the configuration data includes an access key that is correlated to the broadcast identification signals for the user-selected WiFi network access systems and with the user-selected password. The access key is stored in authorization server 132 in association with the user-selected WiFi network access systems. User communication device 101 would provide the access key in their access request when in range of one of the selected WiFi network access systems and if the password is provided by the user. Authorization server 132 could then return a positive response based on its own stored access key.

[25] In some examples, the configuration data indicates a dynamically-changing network key, such as time-of-day, that is correlated to the broadcast identification signals for the user-selected WiFi network access systems and with the user-selected password. When in range of one of the selected WiFi network access systems and if the password is provided by the user, user communication device 101 uses the dynamically-changing network key to generate a hash value for their access request. In response to the access request, authorization server 132 could generate its own hash value based the dynamically-changing network key for comparison to the hash value from the access request. If the comparison indicates the relationship, then authorization server 132 returns the positive response for WiFi access. For example, if the dynamically-changing network key is time-of-day, then both hash values should correlate if calculated within the same timeframe.

[26] Access network 110 comprises computer and communications equipment that use Wireless Fidelity (WiFi), Long Term Evolution (LTE), Global System for Mobile Communications (GSM), Evolution Data Only (EVDO), Bluetooth, DOCSYS, T1, Ethernet, Internet Protocol (IP), or some other communication protocols – including combinations

thereof. Server system 130 comprises computer equipment and software that may be implemented in a single platform or may be distributed across multiple platforms. Communication links 111-112 and 116-117 might be wireless, optical, metallic, or some other communication media – including combinations thereof. Communication links 111-112 and 116-117 may individually comprise multiple parallel connections that utilize different protocols and paths. Communication links 111-112 and 116-117 may also include various intermediate networks, systems, and devices.

[27] Figure 2 illustrates the operation of communication system 100 to provide user control over access to WiFi network 120. User interface server 131 transfers display data to user communication device 101 over access network 110, and user communication device 101 graphically presents the resulting display data to the user. For example, user communication device might present the display data in the form of geographic maps that indicate WiFi access systems 121-124 for selection. In response to the display data, the user selects WiFi access systems 121-123. The user also specifies a password for user-selected WiFi access systems 121-123.

[28] User communication device 101 transfers user data over access network 110 to user interface server 131. The user data indicates user-selected WiFi network access systems 121-123, the user-selected password, and possibly other user selections and data. User interface server 131 transfers the user data to user authorization server 132. Authorization server 132 stores an association between the user-selected WiFi network access systems 121-123 and the user-selected password – and typically other pertinent data. Various techniques to store this association are described herein.

[29] WiFi access system 121 transmits a wireless identification signal for reception by in-range devices, such as an SSID signal, pilot signal, and the like. Subsequently, user

communication device 101 detects the identification signal from WiFi access system 121 and prompts the user for a password. The user provides their selected password to user communication device 101, and device 101 transfers an access request to WiFi access system 121 using the user-selected password. Various techniques to use the password are described herein. WiFi access system 121 transfers the access request to authorization server 132.

[30] Authorization server 132 processes the access request and the stored association between user-selected WiFi network access system 121 and user-selected password to determine that the request should be granted. Authorization server 132 then transfers a positive response to WiFi network access system 121. Based on the positive response, WiFi network access system 121 provides wireless communication device 101 and the user with WiFi network access to some other data system, such as the Internet (not shown).

[31] Figure 3 illustrates the operation of communication system 100 to provide user control over access to WiFi network 120 by allowing user-selection of communication devices. User interface server 131 transfers display data to user communication device 101 over access network 110, and user communication device 101 graphically presents the resulting display data to the user. In response to the display data, the user selects WiFi access systems 121-123 and a password. In this example, the user also selects communication device 103 to access user-selected WiFi access systems 121-123. The user may specify communication device 103 by name, address, number, and the like. User interface server 131 may also identify communication device 103 in the display data for selection by the user.

[32] User communication device 101 transfers user data over access network 110 to user interface server 131. The user data indicates user-selected WiFi network access systems 121-123, user-selected communication device 103, the user-selected password, and possibly other information. User interface server 131 transfers the user data to user authorization

server 132. Authorization server 132 stores an association between the user-selected WiFi network access systems 121-123, user-selected communication device 103, the user-selected password, and other data. Various techniques to store this association are described herein.

[33] WiFi access system 123 transmits its wireless identification signal. User communication device 103 detects the identification signal from WiFi access system 123 and prompts the user for a password. The user provides their selected password to user communication device 103, and device 103 transfers an access request to WiFi access system 123 using the user-selected password. Various techniques to use the password are described herein.

[34] WiFi access system 123 transfers the access request to authorization server 132. Authorization server 132 processes the access request and the stored association between user-selected WiFi network access system 123, user-selected communication device 103, and the user-selected password to determine that the request should be granted. Authorization server 132 then transfers a positive response to WiFi network access system 123. Based on the positive response, WiFi network access system 123 provides user communication device 103 with WiFi network access to another data system, such as the Internet (not shown). Note that other items could be also selected by the user and used for authorization, such as timeframes, security formats, and the like.

[35] Figure 4 illustrates the operation of communication system 100 to provide user control over access to WiFi network 120 by transferring configuration data to user communication device 101. User interface server 131 transfers display data to user communication device 101 over access network 110, and user communication device 101 graphically presents the resulting display data to the user. In response to the display data, the user selects WiFi access systems 121-123 and a password.

[36] User communication device 101 transfers user data over access network 110 to user interface server 131. The user data indicates user-selected WiFi network access systems 121-123, the user-selected password, and possibly other user selections and data. User interface server 131 transfers the user data to user authorization server 132. Authorization server 132 stores an association between the user-selected WiFi network access systems 121-123 and one or more access keys for systems 121-123. The stored association may also indicate the user-selected password and other pertinent data.

[37] Responsive to the user-selections, user interface server 131 transfers configuration data over access network 110 to user communication device 101. The configuration data indicates identification signals (SSIDs and the like) for user-selected WiFi network access systems 121-123. The configuration data also indicates the password, the access key, and perhaps other data. Note that user interface server 131 may also transfer the configuration data to other user-selected communication devices.

[38] User-selected WiFi access system 121 transmits its wireless identification signal, and eventually, user communication device 101 detects this identification signal from WiFi access system 121. Based on the configuration data and the ID signal, user communication device 101 prompts the user for a password. The user provides their selected password to user communication device 101, and device 101 transfers an access request to WiFi access system 121 using the user-selected password. In this example, user communication device 101 uses the password for verification, and if the user-supplied password matches the password from the configuration data, then device 101 transfers the access key to user-selected WiFi access system 121.

[39] WiFi access system 121 transfers the access request including the access key to authorization server 132. Authorization server 132 processes the access request and the

stored association between user-selected WiFi network access system 121 and user-supplied access key to determine that the request should be granted. Authorization server 132 then transfers a positive response to WiFi network access system 121. Based on the positive response, WiFi network access system 121 provides user communication device 101 and the user with WiFi network access to some other data system, such as the Internet (not shown).

[40] Figure 5 illustrates the operation of communication system 100 to provide user control over access to WiFi network 120 by using dynamic access keys. User interface server 131 transfers display data to user communication device 101 over access network 110, and user communication device 101 graphically presents the resulting display data to the user. In response to the display data, the user selects WiFi access systems 121-123, a password, and user communication device 102.

[41] User communication device 101 transfers user data over access network 110 to user interface server 131. The user data indicates user-selected WiFi network access systems 121-123, user communication device 102, the user-selected password, and possibly other data. User interface server 131 transfers the user data to user authorization server 132. Authorization server 132 stores an association between the user-selected WiFi network access systems 121-123 and a secret code used to generate the dynamic key. The stored association may also indicate the user-selected password and other pertinent data.

[42] Responsive to the user-selections, user interface server 131 transfers configuration data over access network 110 to user communication device 102. The configuration data indicates identification signals for user-selected WiFi network access systems 121-123. The configuration data also indicates the password, secret code, dynamic key instructions, and perhaps other data. Note that user interface server 131 may also transfer the configuration data to other user-selected communication devices.

[43] User-selected WiFi access system 122 transmits its wireless identification signal, and eventually, user communication device 102 detects this identification signal from WiFi access system 122. Based on the configuration data and the ID signal, user communication device 102 prompts the user for a password. The user provides their selected password to user communication device 102, and device 102 transfers an access request to WiFi access system 122 using the user-selected password.

[44] In this example, user communication device 102 uses the password for verification, and if the user-supplied password matches the password from the configuration data, then device 102 generates and transfers a dynamic access key to user-selected WiFi access system 122. In this example, the dynamic key is a mathematical hash between the secret code from the configuration data and dynamically changing network data. For example, the secret code could be mathematically combined with the current time-of-day to generate the dynamic access key.

[45] WiFi access system 122 transfers the access request including the dynamic access key to authorization server 132. Authorization server 132 processes the access request and the stored association (the secret code) to generate the dynamic access key in a similar manner to device 102. If the two dynamic access keys correlate, then the access request should be granted. Note that the correlation may not require a strict match. For example, if time of day is used for the dynamic key, then two keys generated around the same time would have a detectable mathematical relationship and would correlate. Various other dynamic key techniques could be used in a similar manner.

[46] Authorization server 132 then transfers a positive response to WiFi network access system 122. Based on the positive response, WiFi network access system 122

provides user communication device 102 and the user with WiFi network access to some other data system, such as the Internet (not shown).

[47] Figure 6 illustrates communication device display 600 that renders a geographic map for a user to select WiFi network access systems 601-604 and specify passwords. For clarity, the geographic map is depicted by a simple grid on Figure 6. Note that navigation controls would be provided on the map, but they are not depicted for clarity. In this example, the user has selected WiFi access systems 602-603 as indicated by the frame around systems 602-603. Text boxes are associated with the selected WiFi access systems 602-603 and provide a mechanism for the user to specify passwords, user names, user devices, security settings, and the like. The text boxes also provide access system information, such as SSIDs, location, and possibly other data.

[48] Figure 7 illustrates LTE/WiFi communication system 700 to provide user control over access to WiFi network 720 having geographically-distributed WiFi access systems 721-724. LTE/WiFi communication system 700 comprises user communication devices 701-703, wireless LTE network 710, WiFi network 720, IP Multimedia Subsystem (IMS) 717, and IP networks 718. Wireless LTE network 710 includes eNodeB 711, serving gateway 712, Packet Data Network (PDN) gateway 713, Mobility Management Entity (MME) 714, Home Subscriber Server (HSS) 715, and Policy Charging and Rules Function (PCRF) 716.

[49] Wireless LTE network 710 also includes server system 730 that comprises user interface server 731 and authorization server 732. User interface server 731 and authorization server 732 operate like servers 131-132 described above. Note that the authorization server 732 is hosted by or integrated within HSS 715. In a like manner, wireless LTE network 710 operates like access network 110 described above. Thus, wireless

LTE network 710 transfers the display data, receives user-selections, transfers configuration data, and provides WiFi authorization as described above.

[50] For example, the user may operate one of communication devices 701-703 to access user interface server 731 and select WiFi access systems 721-722 and 724, a user name, a password, user devices 701-703, timeframes, and the like. When one of the selected user communication devices 701-703 is proximate to one of the selected WiFi access systems 721-722 and 724, then the user device will interact with the proximate WiFi access system as described above. The proximate WiFi access system will transfer access requests to authorization server 732 in HSS 715 – typically through various proxies and interfaces. Authorization server 732 in HSS 715 transfers positive responses as described above.

[51] Figure 8 illustrates WiFi communication system 800 to provide user control over access to WiFi network 820 having geographically-distributed WiFi access systems 821-824. WiFi communication system 800 comprises user communication devices 801-803, IP access network 810, IP networks 818, and server system 830. Server system 830 resides in the core of a nationwide wireless communication network.

[52] Server system 830 comprises user interface server 831 and authorization server 832. User interface server 831 and authorization server 832 and operate like servers 131-132 described above. Thus, server system 830 transfers the display data, receives user-selections, transfers configuration data, and provides WiFi authorization as described above.

[53] For example, the user may operate one of communication devices 801-803 to access user interface server 831 and select WiFi access systems 821-822 and 824, a user name, a password, user devices 801-803, timeframes, and the like. When one of the selected user communication devices 801-803 is proximate to one of the selected WiFi access systems 821-822 and 824, then the user device will interact with the proximate WiFi access system as

described above. The proximate WiFi access system will transfer access requests to authorization server 832. Authorization server 832 transfers positive responses as described above.

[54] In other examples, portions of the server systems described herein could be integrated into the authorization systems of other networks. For example, the AAA system in a 2G or 3G network could host the user interface server and/or the authorization servers described herein.

[55] Figure 9 illustrates server system 900 to provide user control over access to WiFi networks. Server system 900 is an example of the server system 130, although system 130 may use alternative configurations and operations. Server system 900 comprises communication transceivers 901 and processing system 903. Processing system 903 comprises micro-processing circuitry 911 and memory 912. Memory 912 stores software 913. Server system 900 may be integrated into a single platform or may be distributed across multiple diverse computer and communication systems. Some conventional aspects of server system 900 are omitted for clarity, such as power supplies, enclosures, and the like.

[56] Communication transceivers 901 comprise communication components, such as ports, circuitry, memory, software, and the like. Communication transceivers 901 typically utilize Ethernet, Internet, or some other networking protocol – including combinations thereof.

[57] Micro-processor circuitry 911 comprises circuit boards that hold integrated circuitry and associated electronics. Memory 912 comprises non-transitory, computer-readable, data storage media, such as flash drives, disc drives, and the like. Software 913 comprises computer-readable instructions that control the operation of micro-processor circuitry 911 when executed. Software 913 includes modules 921-923 and may also include

operating systems, applications, utilities, databases, and the like. Micro-processor circuitry 911 and memory 912 may be integrated into a single computer system or may be distributed across multiple computer systems.

[58] When executed by circuitry 911, user module 921 directs circuitry 911 to interact with user devices to enable the user to select access systems, passwords, and the like. User module 921 also directs circuitry 911 to transfer configuration data in some examples. When executed by circuitry 911, database module 922 directs circuitry 911 to stores the associations as described above. When executed by circuitry 911, authorization module 923 directs circuitry 911 to provide positive or negative responses to WiFi access requests based on the stored associations.

[59] Figure 10 illustrates wireless communication device 1000 to provide user control over access to WiFi networks. Wireless communication device 1000 is an example of user communication devices 101-103, although devices 101-103 may use alternative configurations and operations. Wireless communication device 1000 comprises access network transceiver 1001, network transceiver 1002, processing system 1003, and user interface 1004. Processing system 1003 comprises micro-processing circuitry 1011 and memory 1012. Memory 1012 stores software 1013. Some conventional aspects of wireless communication device 1000 are omitted for clarity, such as power supplies, enclosures, and the like. Wireless communication device 1000 may be integrated into other systems or devices.

[60] Access network transceiver 1001 and WiFi transceiver 1002 each comprise communication components, such as circuitry, memory, software, antennas, amplifiers, filters, modulators, signal processors, and the like. In some examples, the radio communications include multiple transceiver sub-systems for near-field, local network, and

wide-area network data communications. Access network transceiver 1001 exchanges user data and configuration data as described above. WiFi network transceiver 1002 detects WiFi identification signals, transfers WiFi access requests, and provides WiFi network access.

[61] User interface 1004 includes components to interact with a human operator, such as a touch display, speaker, microphone, camera, buttons, and switches. User interface 1004 displays maps, text boxes, user prompts and the like. Typically a touch display in user interface 1004 receives the user instructions that trigger the actions described herein.

[62] Micro-processor circuitry 1011 comprises one or more circuit boards that hold integrated circuit chips and associated electronics. Memory 1012 comprises non-transitory data storage media, such as flash drives, disc drives, and the like. Software 1013 comprises computer-readable instructions that control the operation of micro-processor circuitry 1011 when executed. Software 1013 includes modules 1021-1023 and may also include additional operating systems, applications, utilities, databases, and the like.

[63] When executed by circuitry 1011, display module 1021 directs circuitry 1011 to display maps, text boxes, and the like to receive user selections. When executed by circuitry 1011, configuration module 1022 direct circuitry 1011 to receive and store configuration data as described herein. When executed by circuitry 1011, WiFi module 1023 directs circuitry 1011 to prompt for passwords and transfer access requests as described herein.

[64] The above description and associated figures teach the best mode of the invention. The following claims specify the scope of the invention. Note that some aspects of the best mode may not fall within the scope of the invention as specified by the claims. Those skilled in the art will appreciate that the features described above can be combined in various ways to form multiple variations of the invention. As a result, the invention is not limited to the

specific embodiments described above, but only by the following claims and their equivalents.

5 CLAIMS

What is claimed is:

1. A method of operating a server system to control access to a Wireless Fidelity (WiFi) network that comprises a plurality of geographically-distributed WiFi access systems, the method characterized by:

10 transferring display data from the server system for presentation to a user who selects more than one of the geographically-distributed WiFi access systems and a single password for the multiple user-selected WiFi access systems;

receiving user data into the server system that indicates the user-selected WiFi network access systems and the user-selected password and storing an association between 15 the user-selected WiFi network access systems and the user-selected password;

receiving an access request into the server system for access to one of the user-selected WiFi network access systems using the user-selected password; and

transferring a positive response to the access request from the server system based on the stored association between the user-selected WiFi network access systems and the user-20 selected password.

2. The method of claim 1 wherein the display data renders geographic map displays that indicate the WiFi network access systems.

25 3. The method of claim 1 wherein:

the user selects a user name for the user-selected WiFi access systems responsive to the display data;

receiving the user data comprises receiving the user-selected user name;

storing the association comprises storing the association between the user-selected WiFi network access systems and the user-selected password and the user-selected user name;

receiving the access request comprises receiving the access request that indicates the user-selected user name; and

transferring the positive response based on the stored association comprises transferring the positive response based on the stored association between the user-selected WiFi network access systems and the user-selected password and the user-selected user name.

4. The method of claim 1 wherein:

the user selects a communication device for the user-selected WiFi access systems responsive to the display data;

receiving the user data comprises receiving the user data indicating the user-selected communication device;

storing the association comprises storing the association between the user-selected WiFi network access systems and the user-selected password and the user-selected communication device;

receiving the access request comprises receiving the access request indicating the user-selected communication device; and

transferring the positive response based on the stored association comprises transferring the positive response based on the stored association between the user-selected

WiFi network access systems and the user-selected password and the user-selected communication device.

5. The method of claim 4 further comprising processing the user data to transfer configuration data for delivery to the user-selected communication device, wherein the configuration data associates broadcast identification signals for the user-selected WiFi network access systems with the user-selected password.

6. The method of claim 1 further comprising:

processing the user data to transfer configuration data for delivery to a user communication device, wherein the configuration data associates broadcast identification signals for the user-selected WiFi network access systems with the user-selected password and an access key, wherein the user communication device detects one of the broadcast identification signals, receives the user-selected password from the user, and processes the user-selected password to transfer the access key; and

wherein receiving the access request using the user-selected password comprises receiving the access request indicating the access key.

7. The method of claim 6 wherein:

storing the association between the user-selected WiFi network access systems and the user-selected password comprises storing the access key in association with the user-selected WiFi network access systems;

transferring the positive response based on the stored association comprises transferring the positive response by comparing the access key from the access request and the stored access key.

8. The method of claim 1 further comprising:

processing the user data to transfer configuration data for delivery to a user communication device, wherein the configuration data associates broadcast identification signals for the user-selected WiFi network access systems with the user-selected password and a dynamically-changing network key, wherein the user communication device detects one of the broadcast identification signals, receives the user-selected password from the user, and processes the user-selected password and the dynamically-changing network key to transfer a hash value; and

wherein receiving the access request using the user-selected password comprises receiving the access request indicating the hash value; and

wherein transferring the positive response to the access request comprises processing the hash value with the dynamically-changing network key.

9. The method of claim 8 wherein the dynamically-changing network key comprises time of day.

10. The method of claim 1 wherein the server system comprises a portion of an authorization system for a wireless Long Term Evolution (LTE) network and wherein transferring the

display data and receiving the user data comprises communicating over the wireless LTE network.

11. A server system to control access to a Wireless Fidelity (WiFi) network that comprises a plurality of geographically-distributed WiFi access systems, the server system characterized by:

a user interface server configured to transfer display data from the server system for presentation to a user who selects more than one of the geographically-distributed WiFi access systems and a single password for the user-selected WiFi access systems responsive to the display data, the user interface server further configured to receive user data into the server system that indicates the user-selected WiFi network access systems and the user-selected password; and

an authorization server operationally coupled to the user interface server and configured to store an association between the user-selected WiFi network access systems and the user-selected password, to receive an access request into the server system for access to one of the user-selected WiFi network access systems using the user-selected password, and to transfer a positive response to the access request from the server system based on the stored association between the user-selected WiFi network access systems and the user-selected password.

12. The server system of claim 11 wherein the user interface server is configured to transfer the display data to render geographic map displays that indicate the WiFi network access systems.

13. The server system of claim 11 wherein:

the user interface server is configured to receive the user data indicating a user name selected by the user for the user-selected WiFi access systems responsive to the display data; and

the authorization server is configured to store the association between the user-selected WiFi network access systems and the user-selected password and the user-selected user name, receive the access request that indicates the user-selected user name, and transfer the positive response based on the stored association between the user-selected WiFi network access systems and the user-selected password and the user-selected user name.

14. The server system of claim 11 wherein:

the user interface server is configured to receive the user data indicating a user-selected communication device selected by the user for the user-selected WiFi access systems responsive to the display data; and

the authorization server is configured to store the association between the user-selected WiFi network access systems and the user-selected password and the user-selected communication device, receive the access request that indicates the user-selected communication device, and transfer the positive response based on the stored association between the user-selected WiFi network access systems and the user-selected password and the user-selected communication device.

15. The server system of claim 14 wherein the user interface server is configured to transfer configuration data for delivery to the user-selected communication device, wherein the configuration data associates broadcast identification signals for the user-selected WiFi network access systems with the user-selected password.

16. The server system of claim 11 wherein:

the user interface server is configured to transfer configuration data for delivery to a user communication device, wherein the configuration data associates broadcast identification signals for the user-selected WiFi network access systems with the user-selected password and an access key, wherein the user communication device detects one of the broadcast identification signals, receives the user-selected password from the user, and processes the user-selected password to transfer the access key; and

the authorization server is configured to receive the access request using the user-selected password by receiving the access request indicating the access key.

17. The server system of claim 16 wherein the authorization server is configured to store the association between the user-selected WiFi network access systems and the user-selected password by storing the access key in association with the user-selected WiFi network access systems and to transfer the positive response by comparing the access key from the access request and the stored access key.

18. The server system of claim 11 wherein:

the user interface server is configured to transfer configuration data for delivery to a user communication device, wherein the configuration data associates broadcast identification signals for the user-selected WiFi network access systems with the user-selected password and a dynamically-changing network key, wherein the user communication device detects one of the broadcast identification signals, receives the user-selected password from the user, and processes the user-selected password and the dynamically-changing network key to transfer a hash value; and

the authorization server is configured to receive the access request using the user-selected password by receiving the access request indicating the hash value and to transfer the positive response by processing the hash value from the access request and the dynamically-changing network key.

19. The server system of claim 18 wherein the dynamically-changing network key comprises time of day.

20. The server system of claim 11 wherein:

the authorization server comprises a portion of an authorization system for a wireless Long Term Evolution (LTE) network; and

the user interface server is configured to transfer the display data and receive the user data over the wireless LTE network.

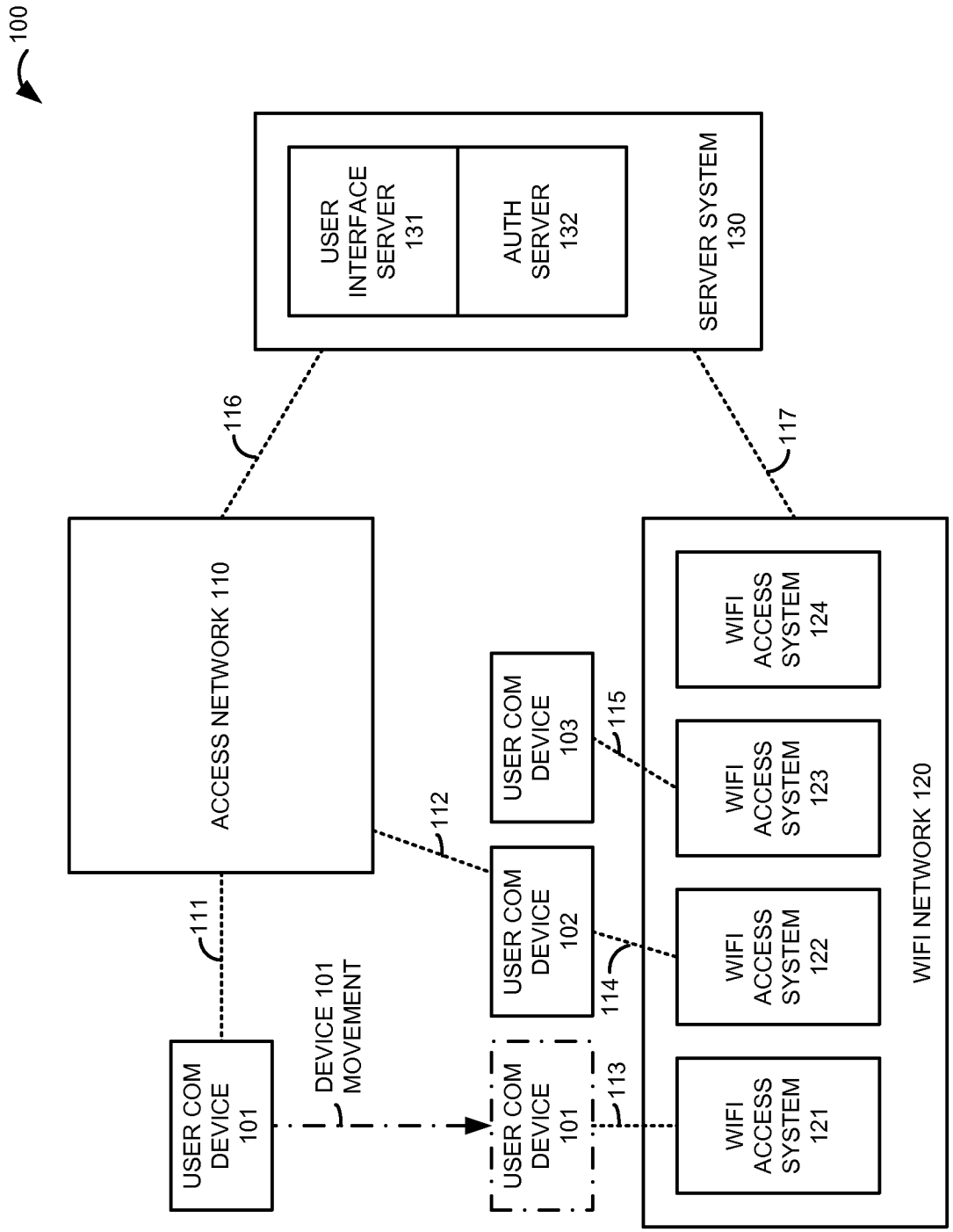

100
SERVER SYSTEM 130
USER INTERFACE SERVER 131
AUTH SERVER 132
116
117
ACCESS NETWORK 110
WIFI NETWORK 120
WIFI ACCESS SYSTEM 124
WIFI ACCESS SYSTEM 123
WIFI ACCESS SYSTEM 122
WIFI ACCESS SYSTEM 121
USER COM DEVICE 103
USER COM DEVICE 102
USER COM DEVICE 101
USER COM DEVICE 101
111
112
113
114
115
DEVICE 101 MOVEMENT

FIGURE 1

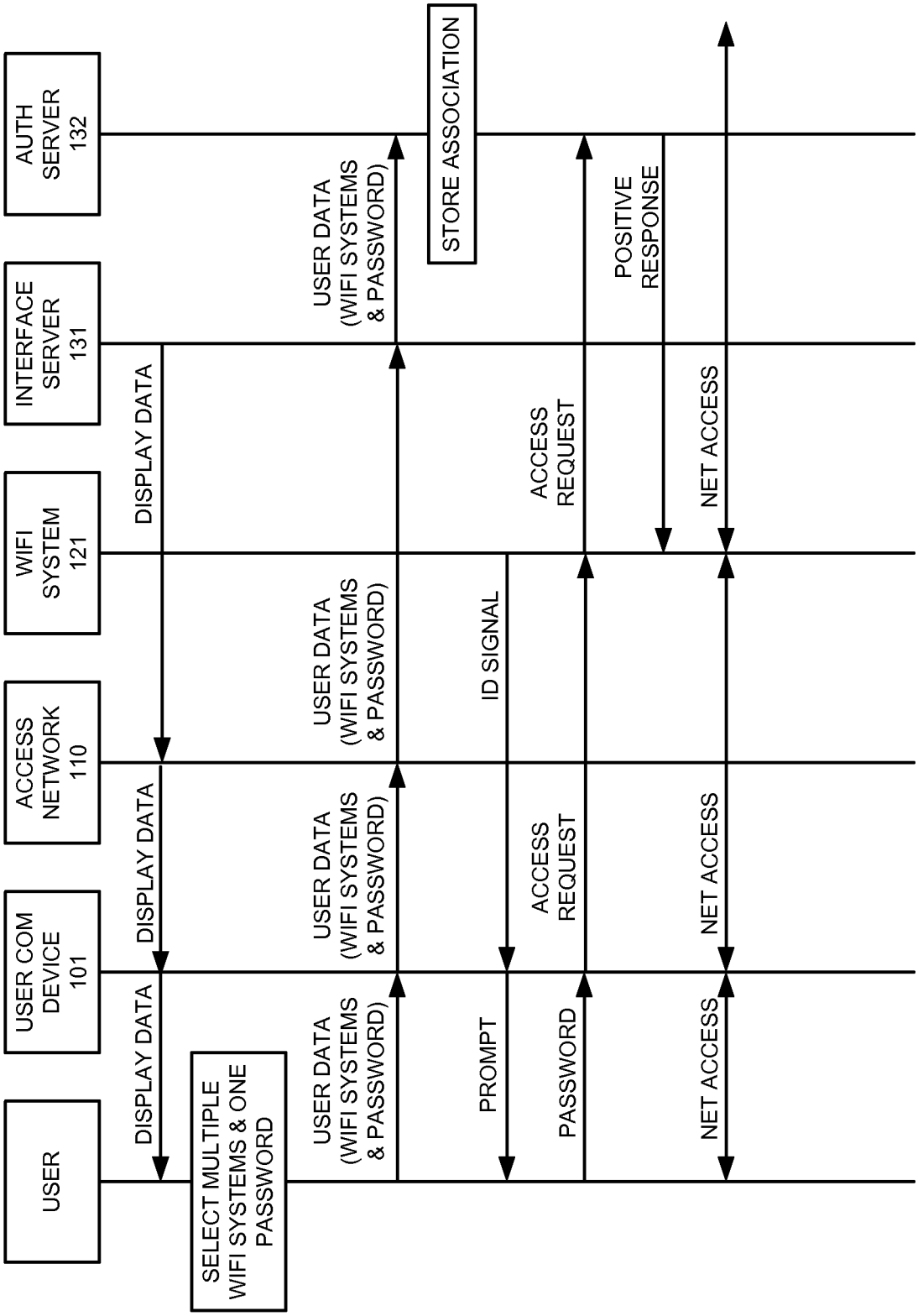

USER
USER COM DEVICE 101
ACCESS NETWORK 110
WIFI SYSTEM 121
INTERFACE SERVER 131
AUTH SERVER 132
DISPLAY DATA
DISPLAY DATA
DISPLAY DATA
SELECT MULTIPLE WIFI SYSTEMS & ONE PASSWORD
USER DATA (WIFI SYSTEMS & PASSWORD)
USER DATA (WIFI SYSTEMS & PASSWORD)
USER DATA (WIFI SYSTEMS & PASSWORD)
USER DATA (WIFI SYSTEMS & PASSWORD)
STORE ASSOCIATION
PROMPT
ID SIGNAL
PASSWORD
ACCESS REQUEST
ACCESS REQUEST
POSITIVE RESPONSE
NET ACCESS
NET ACCESS
NET ACCESS

FIGURE 2

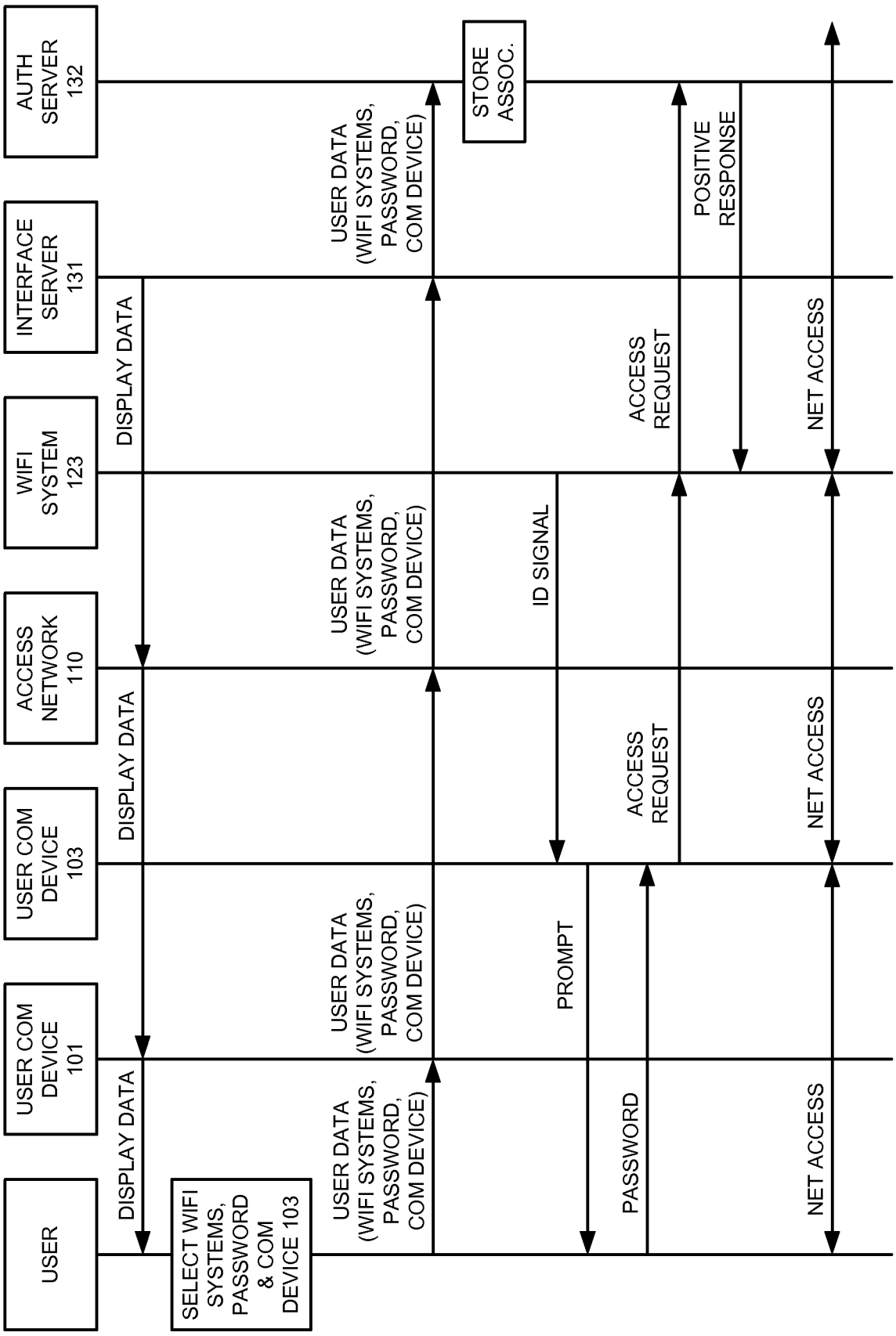

USER
USER COM DEVICE 101
USER COM DEVICE 103
ACCESS NETWORK 110
WIFI SYSTEM 123
INTERFACE SERVER 131
AUTH SERVER 132
DISPLAY DATA
SELECT WIFI SYSTEMS, PASSWORD & COM DEVICE 103
DISPLAY DATA
DISPLAY DATA
USER DATA (WIFI SYSTEMS, PASSWORD, COM DEVICE)
USER DATA (WIFI SYSTEMS, PASSWORD, COM DEVICE)
USER DATA (WIFI SYSTEMS, PASSWORD, COM DEVICE)
USER DATA (WIFI SYSTEMS, PASSWORD, COM DEVICE)
STORE ASSOC.
ID SIGNAL
PROMPT
PASSWORD
ACCESS REQUEST
ACCESS REQUEST
POSITIVE RESPONSE
NET ACCESS
NET ACCESS
NET ACCESS

FIGURE 3

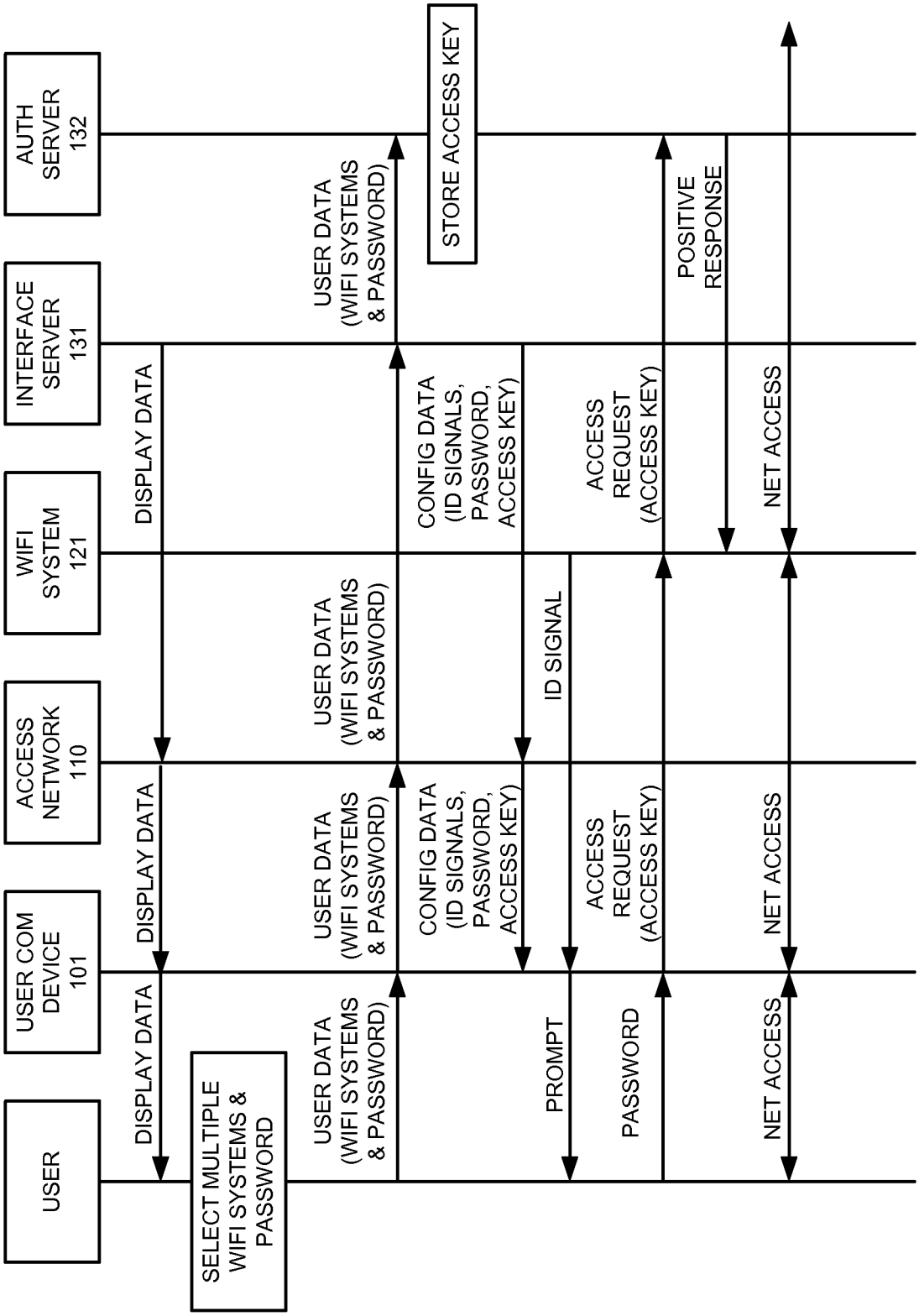

USER
USER COM DEVICE 101
ACCESS NETWORK 110
WIFI SYSTEM 121
INTERFACE SERVER 131
AUTH SERVER 132
DISPLAY DATA
SELECT MULTIPLE WIFI SYSTEMS & PASSWORD
DISPLAY DATA
DISPLAY DATA
USER DATA (WIFI SYSTEMS & PASSWORD)
USER DATA (WIFI SYSTEMS & PASSWORD)
USER DATA (WIFI SYSTEMS & PASSWORD)
USER DATA (WIFI SYSTEMS & PASSWORD)
CONFIG DATA (ID SIGNALS, PASSWORD, ACCESS KEY)
CONFIG DATA (ID SIGNALS, PASSWORD, ACCESS KEY)
STORE ACCESS KEY
ID SIGNAL
PROMPT
ACCESS REQUEST (ACCESS KEY)
ACCESS REQUEST (ACCESS KEY)
PASSWORD
POSITIVE RESPONSE
NET ACCESS
NET ACCESS
NET ACCESS

FIGURE 4

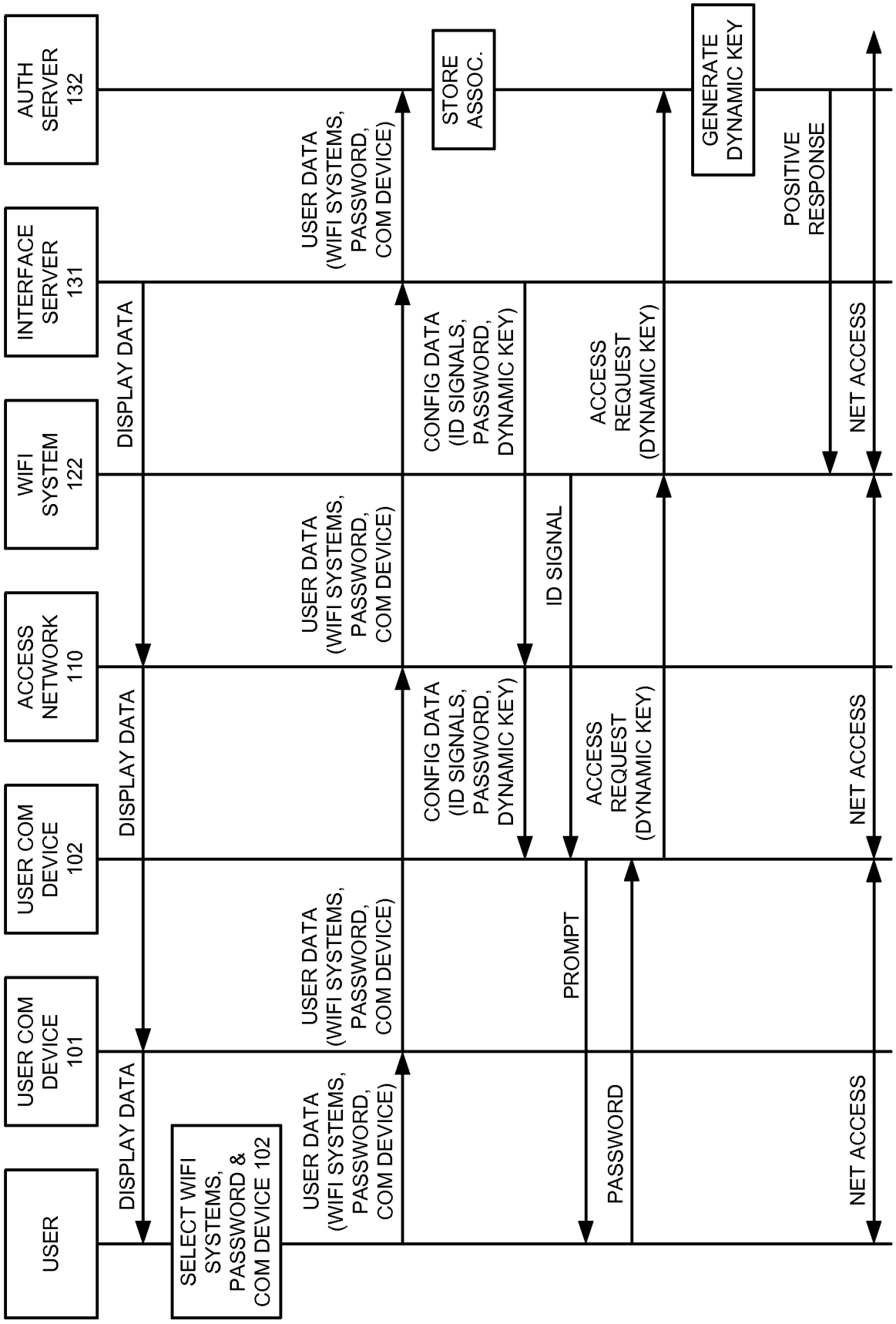

USER
USER COM DEVICE 101
USER COM DEVICE 102
ACCESS NETWORK 110
WIFI SYSTEM 122
INTERFACE SERVER 131
AUTH SERVER 132
DISPLAY DATA
SELECT WIFI SYSTEMS, PASSWORD & COM DEVICE 102
USER DATA (WIFI SYSTEMS, PASSWORD, COM DEVICE)
PROMPT
PASSWORD
CONFIG DATA (ID SIGNALS, PASSWORD, DYNAMIC KEY)
ID SIGNAL
ACCESS REQUEST (DYNAMIC KEY)
STORE ASSOC.
GENERATE DYNAMIC KEY
POSITIVE RESPONSE
NET ACCESS

FIGURE 5

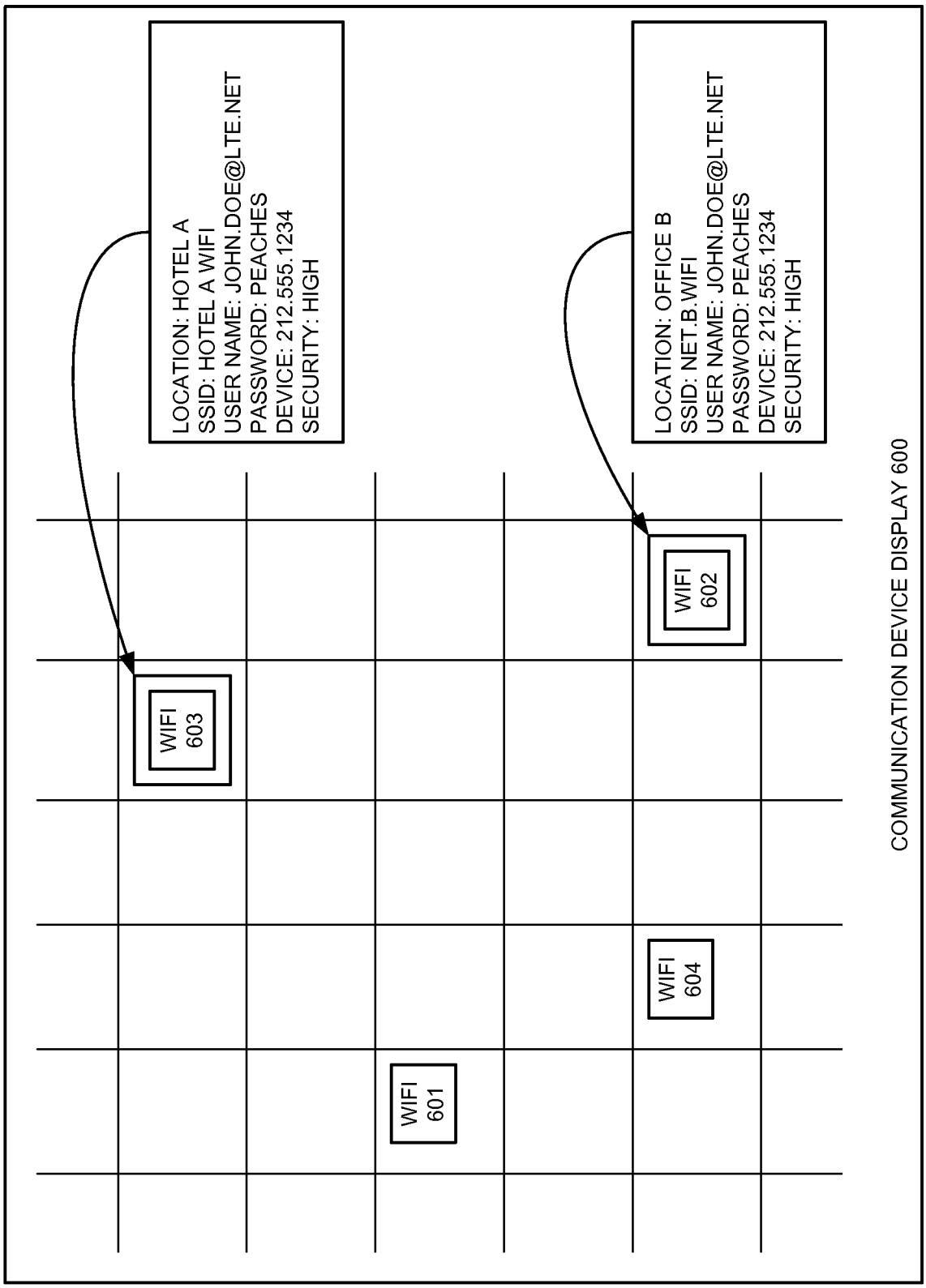

LOCATION: HOTEL A
SSID: HOTEL A WIFI
USER NAME: JOHN.DOE@LTE.NET
PASSWORD: PEACHES
DEVICE: 212.555.1234
SECURITY: HIGH
LOCATION: OFFICE B
SSID: NET.B.WIFI
USER NAME: JOHN.DOE@LTE.NET
PASSWORD: PEACHES
DEVICE: 212.555.1234
SECURITY: HIGH
WIFI 603
WIFI 602
WIFI 604
WIFI 601
COMMUNICATION DEVICE DISPLAY 600

FIGURE 6

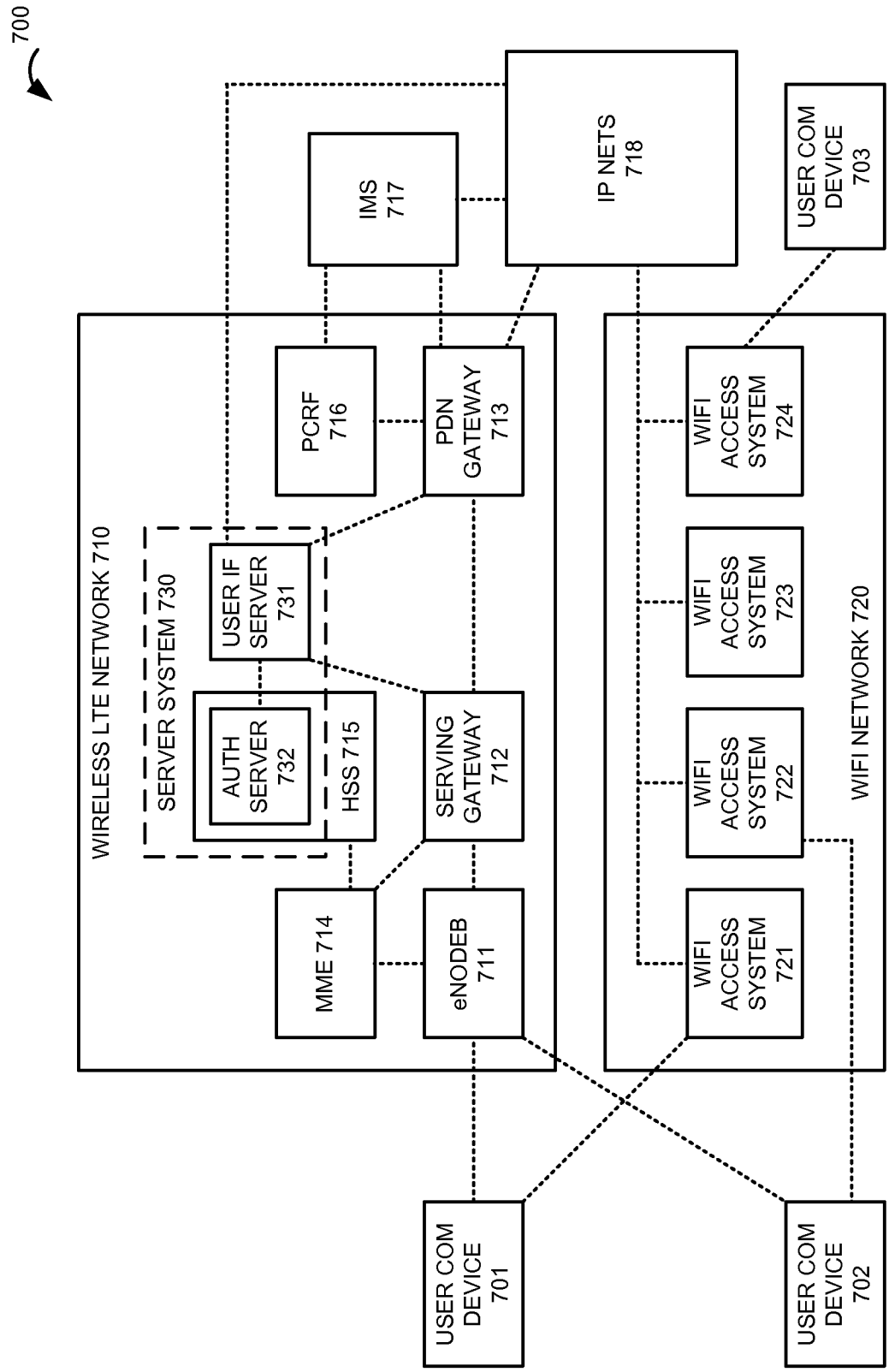

700
IMS 717
IP NETS 718
USER COM DEVICE 703
PCRF 716
PDN GATEWAY 713
WIFI ACCESS SYSTEM 724
WIRELESS LTE NETWORK 710
SERVER SYSTEM 730
USER IF SERVER 731
WIFI ACCESS SYSTEM 723
AUTH SERVER 732
HSS 715
SERVING GATEWAY 712
WIFI ACCESS SYSTEM 722
WIFI NETWORK 720
MME 714
eNODEB 711
WIFI ACCESS SYSTEM 721
USER COM DEVICE 701
USER COM DEVICE 702

FIGURE 7

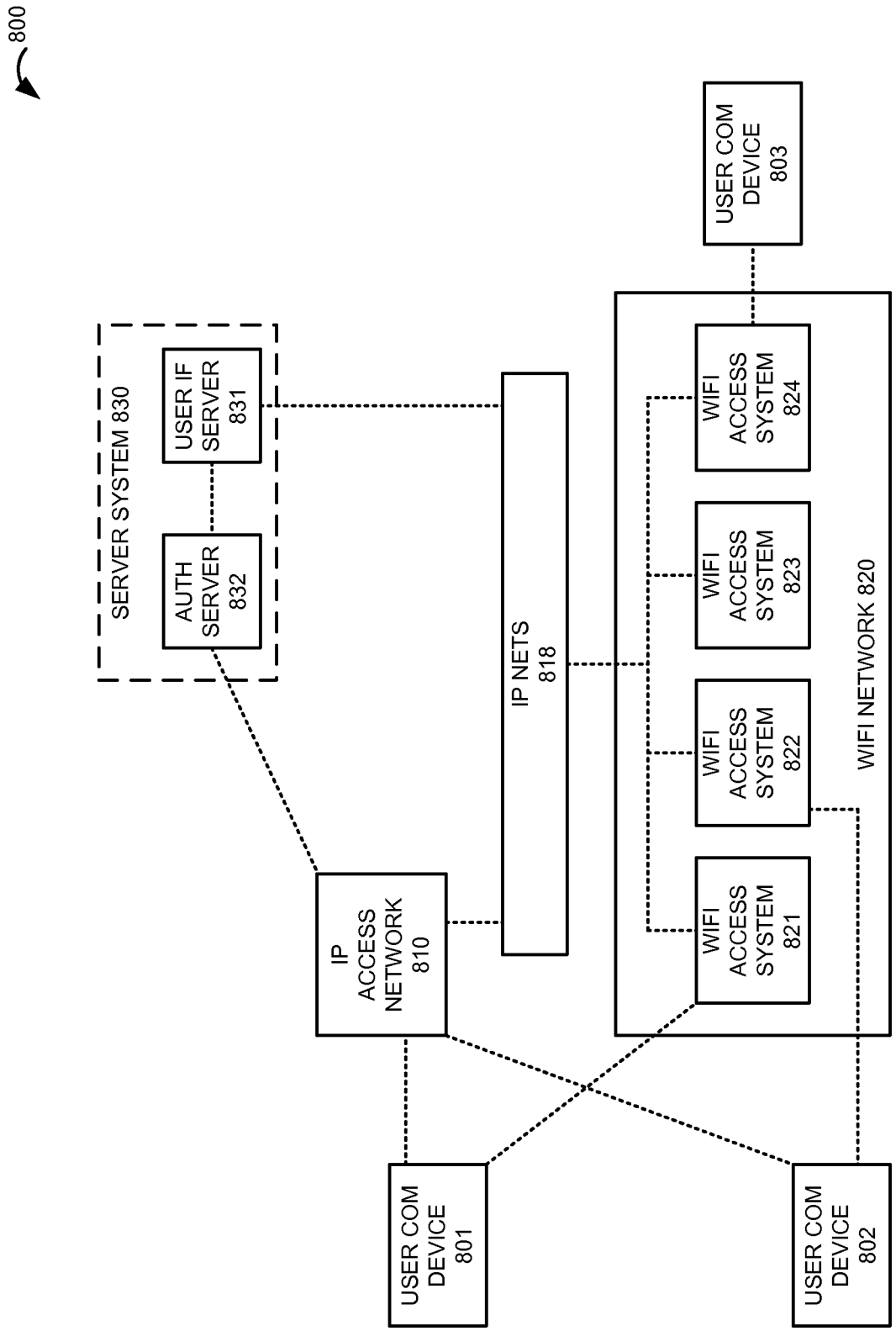

800
SERVER SYSTEM 830
USER IF SERVER 831
AUTH SERVER 832
IP NETS 818
IP ACCESS NETWORK 810
USER COM DEVICE 803
WIFI ACCESS SYSTEM 824
WIFI ACCESS SYSTEM 823
WIFI ACCESS SYSTEM 822
WIFI ACCESS SYSTEM 821
WIFI NETWORK 820
USER COM DEVICE 801
USER COM DEVICE 802

FIGURE 8

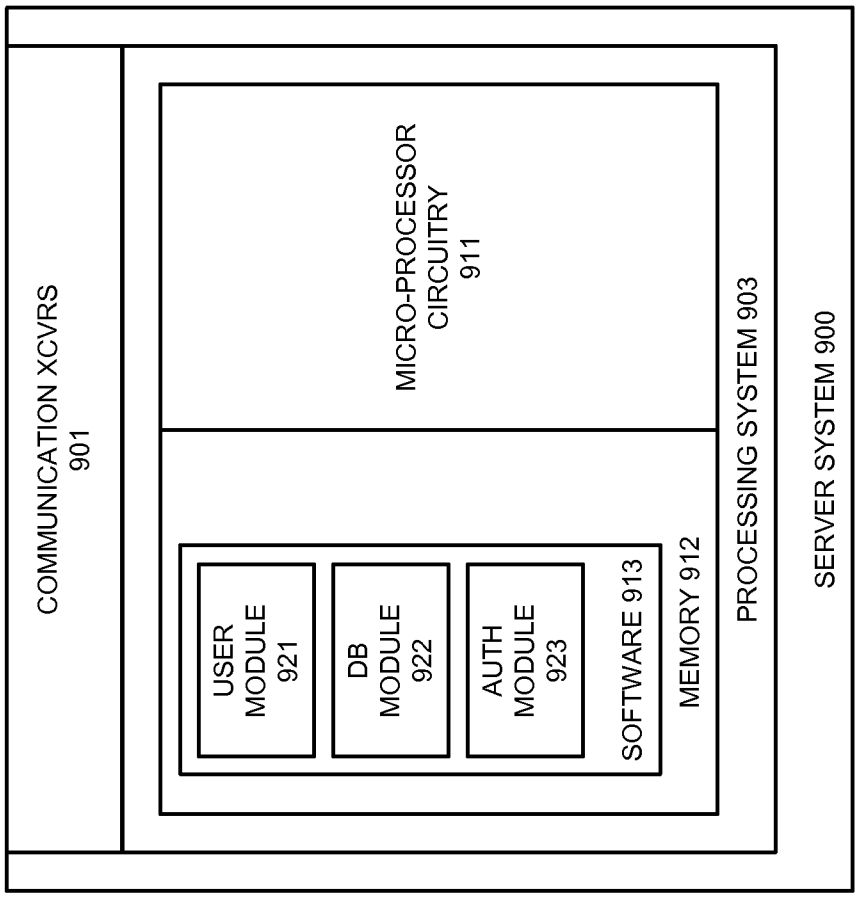

SERVER SYSTEM 900
COMMUNICATION XCVRS 901
PROCESSING SYSTEM 903
MICRO-PROCESSOR CIRCUITRY 911
MEMORY 912
SOFTWARE 913
USER MODULE 921
DB MODULE 922
AUTH MODULE 923

FIGURE 9

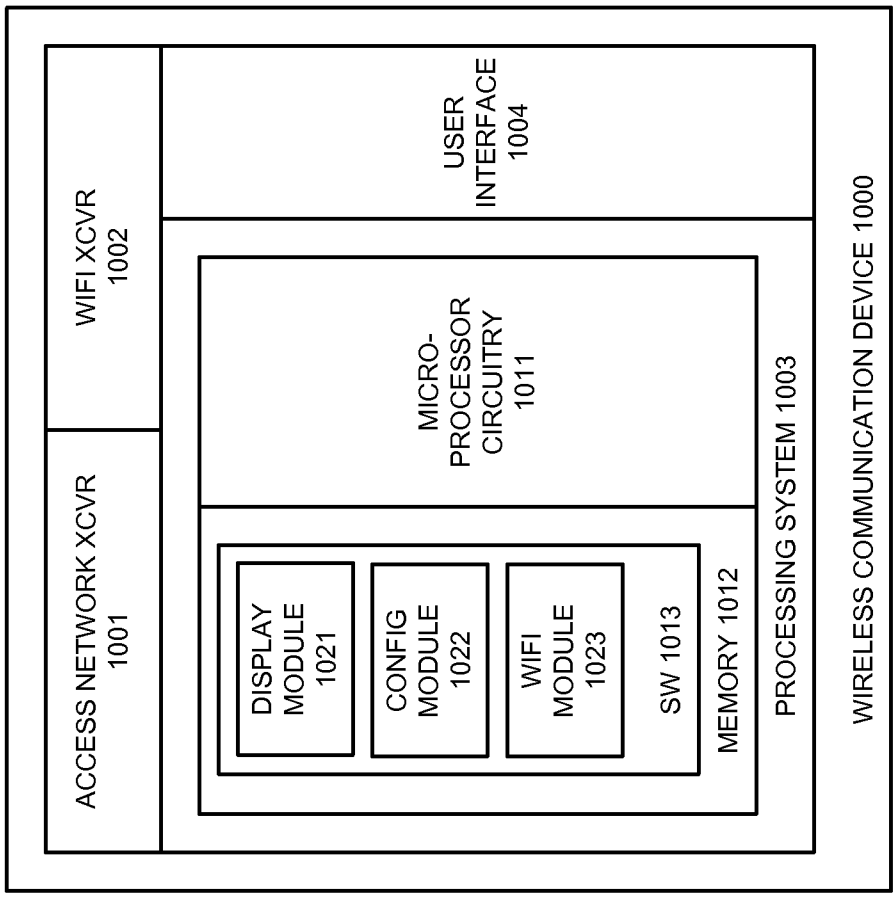

WIRELESS COMMUNICATION DEVICE 1000
ACCESS NETWORK XCVR 1001
WIFI XCVR 1002
USER INTERFACE 1004
PROCESSING SYSTEM 1003
MICRO-PROCESSOR CIRCUITRY 1011
MEMORY 1012
SW 1013
DISPLAY MODULE 1021
CONFIG MODULE 1022
WIFI MODULE 1023

FIGURE 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/050635

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06
ADD. H04W84/12

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

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2004/014024 A2 (WAVELINK CORP [US]) 12 February 2004 (2004-02-12) abstract; figures 1,2A page 7, line 7 - page 9, line 4 page 11, line 25 - page 14, line 10	1-20
Y	EP 2 200 223 A1 (PANASONIC CORP [JP]) 23 June 2010 (2010-06-23) abstract; figures 2,3,7,8 paragraphs [0009], [0010], [0020] - paragraph [0094]	1,3-11, 13-20
Y	US 2007/081496 A1 (KARGE RALF [DE] ET AL) 12 April 2007 (2007-04-12) abstract; figure 3 paragraphs [0011], [0012]	2,12

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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
31 October 2013	08/11/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Tozlovanu, Ana-Delia

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/050635

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ZHANG J ET AL: "Virtual operator based AAA in wireless LAN hot spots with ad-hoc networking support", MOBILE COMPUTING AND COMMUNICATIONS REVIEW, ACM, NEW YORK, NY, US, vol. 6, no. 3, 1 July 2002 (2002-07-01), pages 10-21, XP002390572, ISSN: 1091-1669 page 11 - page 14	1-20
A	US 2010/322123 A1 (LEE COOPER G [US]) 23 December 2010 (2010-12-23) abstract; figures 1A,9,10 paragraphs [0008], [0135]	1-20
A	EP 1 633 083 A1 (HUAWEI TECH CO LTD [CN]) 8 March 2006 (2006-03-08) paragraphs [0005], [0006], [0011] - paragraph [0014]	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/050635

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004014024 A2	12-02-2004	AU 2003258008 A1	23-02-2004
		EP 1527563 A2	04-05-2005
		US 2004198220 A1	07-10-2004
		WO 2004014024 A2	12-02-2004
EP 2200223 A1	23-06-2010	EP 2200223 A1	23-06-2010
		US 2010217881 A1	26-08-2010
		WO 2009034624 A1	19-03-2009
US 2007081496 A1	12-04-2007	AT 445170 T	15-10-2009
		DE 102005026788 A1	21-12-2006
		EP 1731919 A1	13-12-2006
		ES 2332460 T3	05-02-2010
		US 2007081496 A1	12-04-2007
US 2010322123 A1	23-12-2010	EP 2052499 A2	29-04-2009
		TW 200828853 A	01-07-2008
		US 2008042912 A1	21-02-2008
		US 2008043655 A1	21-02-2008
		US 2008043687 A1	21-02-2008
		US 2008125129 A1	29-05-2008
		US 2010284315 A1	11-11-2010
		US 2010322123 A1	23-12-2010
		WO 2008022272 A2	21-02-2008
EP 1633083 A1	08-03-2006	CA 2523416 A1	16-12-2004
		CN 1553656 A	08-12-2004
		EP 1633083 A1	08-03-2006
		JP 2006526917 A	24-11-2006
		RU 2316903 C2	10-02-2008
		US 2006109826 A1	25-05-2006
		US 2009158442 A1	18-06-2009
		WO 2004109980 A1	16-12-2004