



(51) International Patent Classification:

H04W 48/18 (2009.01) *H04W 48/04* (2009.01)

(21) International Application Number:

PCT/US2018/048923

(22) International Filing Date:

30 August 2018 (30.08.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **CISCO TECHNOLOGY, INC.** [US/US]; 170 West Tasman Drive, San Jose, California 95134 (US).

(72) Inventors: **OBSTFELD, Joel Abraham**; 2, Rockingham Gate, Bushey Hertfordshire WD23 4DQ (GB). **BRINCKMAN, Bart**; Wallenbulk 11, 9850 Nevele (BE).

(74) Agent: **MONAJEMI, Babak**; Polsinelli, Three Embarcadero Center, Suite 2400, San Francisco, California 94111 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, SZ, TZ,

(54) Title: GEO-LOCATION BASED IDENTITY SELECTION FOR WIRELESS CONNECTIONS

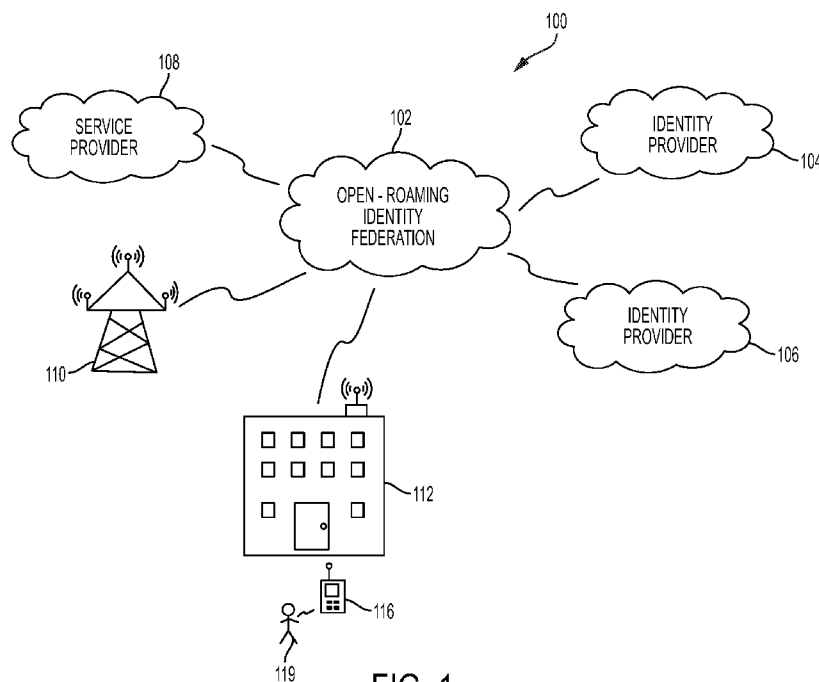


FIG. 1

(57) Abstract: Systems, methods, and computer-readable media are provided for a geo-location based selection of an identity for a mobile device to attach to a nearby network of an access provider. In one aspect of the present disclosure, a method includes determining, by one or more processors, a location of a mobile device; identifying, by the one or more processors, an access provider having a network for the mobile device to connect to; selecting, by the one or more processors, one of a plurality of identities associated with the mobile device for authorizing connection to the network of the access provider, the selection being based on the location of the mobile device and connection parameters specified by the access provider; and establishing, by the one or more processors, the connection of the mobile device to the network of the access provider using the one of the plurality of identities.



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:

— *of inventorship (Rule 4.17(iv))*

Published:

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

GEO-LOCATION BASED IDENTITY SELECTION FOR WIRELESS CONNECTIONS

TECHNICAL FIELD

[0001] The present technology pertains in general to providing a dynamic selection process for selecting an identity for a mobile device to connect to a wireless access provider based on a geographical location of the mobile device among other factors.

BACKGROUND

[0002] When a mobile device is 'roaming' on/connecting to third party-provided WiFi networks, a cumbersome procedure needs to be followed where by the mobile device needs to register with the owner/operator of the third-party provided WiFi network and/or an identity provider needs to be selected, such as a native network operator, in order to validate and verify user credentials. Once validated, the mobile device is then able to use that third-party provided WiFi network.

[0003] The above illustrates that many steps are involved in establishing connection to a third-party provided WiFi networks. With the ever increasing availability of various identities and access providers, the above heavily user-involved process is inconvenient and far from seamless.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] In order to describe the manner in which the above-recited and other advantages and features of the disclosure can be obtained, a more particular description of the principles briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only exemplary embodiments of the disclosure and are not therefore to be considered to be limiting of its scope, the principles herein are described and explained with additional specificity and detail through the use of the accompanying drawings in which:

[0005] FIG. 1 illustrates an example of network architecture and associated components, according to an aspect of the present disclosure;

[0006] FIG. 2 describes an example process for generation a database to be used for geo-location based identity selection for wireless connections, according to an aspect of the present disclosure;

[0007] FIG. 3 describes an example process for geo-location based identity selection for wireless connections, according to an aspect of the present disclosure; and

[0008] FIG. 4 illustrates an example system including various hardware computing components, according to an aspect of the present disclosure.

DETAILED DESCRIPTION

[0009] Various example embodiments of the disclosure are discussed in detail below. While specific implementations are discussed, it should be understood that this is done for illustration purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without parting from the spirit and scope of the disclosure. Thus, the following description and drawings are illustrative and are not to be construed as limiting. Numerous specific details are described to provide a thorough understanding of the disclosure. However, in certain instances, well-known or conventional details are not described in order to avoid obscuring the description. References to one or an embodiment in the present disclosure can be references to the same embodiment or any embodiment; and, such references mean at least one of the embodiments.

[0010] Reference to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the disclosure. The appearances of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Moreover, various features are described which may be exhibited by some embodiments and not by others.

[0011] Without intent to limit the scope of the disclosure, examples of instruments, apparatus, methods and their related results according to the embodiments of the

present disclosure are given below. Note that titles or subtitles may be used in the examples for convenience of a reader, which in no way should limit the scope of the disclosure. Unless otherwise defined, technical and scientific terms used herein have the meaning as commonly understood by one of ordinary skill in the art to which this disclosure pertains. In the case of conflict, the present document, including definitions will control.

[0012] Additional features and advantages of the disclosure will be set forth in the description which follows, and in part will be obvious from the description, or can be learned by practice of the herein disclosed principles. The features and advantages of the disclosure can be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. These and other features of the disclosure will become more fully apparent from the following description and appended claims, or can be learned by the practice of the principles set forth herein.

[0013] A client can include a device and/or application seeking to execute a function on an Execution Endpoint. Non-limiting examples of a client can include a mobile phone, a laptop, a tablet, etc.

OVERVIEW

[0014] Disclosed are systems, methods, and computer-readable media for a geo-location based selection of an identity for a mobile device to attach to a nearby network of an access provider.

[0015] In one aspect of the present disclosure, a method includes determining, by one or more processors, a location of a mobile device; identifying, by the one or more processors, an access provider having a network for the mobile device to connect to; selecting, by the one or more processors, one of a plurality of identities associated with the mobile device for authorizing connection to the network of the access provider, the selection being based on the location of the mobile device and connection parameters specified by the access provider; and establishing, by the one or more processors, the connection of the mobile device to the network of the access provider using the one of the plurality of identities.

[0016] In one aspect of the present disclosure, a network component has one or more identity providers and one or more access providers registered therewith. The network component includes memory having computer-readable instructions stored therein and one or more processors. The one or more processors configured to execute the computer-readable instructions to determine a location of a mobile device; identify an access provider from the one or more access providers having a network for the mobile device to connect to; select an identity provided by one of the one or more identity providers, the identity being associated with the mobile device for authorizing connection to the network and being selected based on the location of the mobile device and connection parameters specified by the access provider and connect the mobile device to the network using the selected identity.

[0017] In one aspect of the present disclosure, one or more non-transitory computer-readable medium have computer-readable instructions stored therein, which when executed by one or more processors of a network component, cause the one or more processors to determine a location of a mobile device; identify a plurality of access providers each having a network for the mobile device to connect to; based on corresponding connection parameters associated with each of the plurality of access providers and the location of the mobile device, select one of the plurality of access providers and an identity associated with the mobile device for attaching the mobile device to a network of the one of the plurality of access providers; and attaching the mobile device to the network of the one of the plurality of access providers.

DETAILED DESCRIPTION

[0018] As indicated above, the availability of third-party network access providers are continuously increasing. As an example, at any point in time a user who is roaming through a geographical area is likely to receive several options on WiFi providers to connect to. Furthermore, users may have a variety of different identities such as user credentials with different social network providers, a business credential, etc. Accordingly, the process of selecting an identity and connecting to any one such provider is tedious and cumbersome as the user needs to input user credentials.

[0019] One idea for making the above process less tedious is referred to as roaming exchange. According to roaming exchange, there may be a centralized service

provider referred to as a roaming identity federation provider (ID federation provider) to which various service providers and identity providers can subscribe/register with.

[0020] Examples of service providers can include, but are not limited to, entities providing internet access (e.g., a WiFi access). This can be any known or to be developed access provider. For example, a business entity may provide a WiFi access for its patrons and customers to connect to. A wireless carrier can be another example of an access provider.

[0021] Examples of identity providers can include, but is not limited to, any known or to be developed social service provider with which users can set up accounts having associated user names and passwords (user credentials). Examples include email service providers, social platform providers (e.g., Google and Facebook), etc. Other examples of identity providers include businesses that provide user credentials to their employees. Such identities may be referred to as business identities.

[0022] A user having an associated mobile device may have multiple registered identities each provided by a different identity provider. when roaming, whenever the user and the associated mobile device is detected within a coverage area of a service provider that is part of the consortium (roaming exchange), the ID federation provider may retrieve various identities associated the user, present the available identities to the user on the mobile device, receive a selection of one of the identities via the mobile device, authenticate the user's selected identity with a corresponding identity provider and enable the mobile device to roam on the service provider's access network.

[0023] While the ID federation provider simplifies the process of mobile devices establishing a connection to a nearby access provider, there is still a level of interaction and user intervention required, as described above (e.g., the user needs to select an identity to be used for authenticating user's access to the access provider's network). Hereinafter, example embodiments will be described that further simplify the above process by providing a geo-location based identity selection for connecting to an access point, which eliminates any need for user intervention and provides a seamless (from the user perspective) process for connecting to an access provider's network.

[0024] The disclosure begins with a description of a setting in which geo-location based identity selection for seamless connection to an access network can be implemented.

[0025] FIG. 1 illustrates an example of network architecture and associated components, according to an aspect of the present disclosure. As shown in FIG. 1, architecture 100 includes a cloud hosted open roaming identity federation provider 102 (ID federation provider 102). ID federation provider 102 may be hosted on or more servers operated by a provider such as Cisco Technology, Inc. of San Jose, CA.

[0026] FIG. 1 further shows identity providers 104 and 106. Identity providers 104 and 106 may be different private or public platforms, outlets or organizations which users register and have a profile and associated authentication credentials. Examples of identity providers include, but are not limited to, those described above.

[0027] FIG. 1 also shows service providers 108, 110 and 112, examples of which include, but are not limited to, those described above. In FIG. 1, service provider 108 and 112 may be different WiFi Access providers while service provider 110 is a wireless carrier access provider. For example, service provider 110 can be an LTE nodeB, to which a mobile device may attach. Service provider 110 can provide any known or to be developed wireless technology to its subscribers including, but not limited to, Long Term Evolution (LTE) access network, a 5th Generation (5G) network, etc.

[0028] In one example, all or some of access providers 108, 110 and 112 can be part of the same 5G network. In one example, a single entity can be both an identity provider and an access provider.

[0029] FIG. 1 further shows a user 114 having an associated mobile device 116. Furthermore, user 114 and mobile device 116 are shown to be present within coverage area of access provider 112. In this example, access provider 112 provides wireless access to devices within a physical building, location, etc. The present disclosure is not limited to mobile device 116 being in the coverage area of only a single access provider at any time but may be within coverage areas of multiple access providers, simultaneously.

[0030] Examples of mobile device 116 include, but are not limited to, any portable device capable of establishing a wireless connection with a service provider such as a

smart phone, a mobile device, a laptop, a tablet, a personal digital assistant (PDA), etc.

[0031] Communications between various components of architecture 100 described above, can be based on any known, or to be developed, method of wireless (and/or wired) communication scheme. Furthermore, while certain components have been shown and described with reference to architecture 100, architecture 100 is not limited thereto. Architecture 100 and its components may include any additional component or element necessary and ordinary to their operations and functionalities.

[0032] While FIG. 1 illustrates a certain number of access providers, identity providers and mobile devices, the present disclosure is not limited thereto. There can be more or less identity providers and access providers registered with ID federation provider 102. Furthermore, there can be more than one user and associated mobile devices attempting to gain access to an access provider's network.

[0033] In one example, when mobile device 116 is present in the coverage area of access provider 112 and assuming that user 114 has multiple identities (e.g., one identity with each of identity providers 104 and 106), a list of two identities will be presented to user 114 on mobile device 116. User 114 then selects one of the presented identities. Upon receiving the selected identity, access provider 112 authenticates user 114, using known or to be developed authentication procedures, via ID federation provider 102 and the corresponding identity provider (e.g., one of identity providers 104 and 106) before providing mobile device 116 access to access provider 112's network.

[0034] In one example, the identity selected on mobile device 116 by user 114 will be used as the default identity for user 114 whenever an access provider's network that is associated with ID federation provider 102 is detected on mobile device 116 until user 114 selects another identity.

[0035] This default use of a selected identity and the still existing level of interaction required from user 114 presents two challenges. First, due to various issues (e.g., security, privacy, etc.), user 114 may not want to use one identity to gain access to all different access providers' networks. For example, when user 114 is within coverage area of a WiFi network provided by a coffee shop, user 114 may not wish and/or be allowed to use his or her business identity to connect to the coffee shop's WiFi

network. Furthermore, due to user 114's personal privacy concerns, user 114 may not wish to use a particular identity provided by a social media platform such as Facebook at the coffee shop but may instead wish to use another identity of user 114.

[0036] Therefore, depending on user's location and/or the available access networks, users may wish to use different identities for connecting to each different access network. Furthermore, different access providers may specify different restrictions for type of devices and users that may connect to their networks.

[0037] The identity selection process can be made more seamless by eliminating the need for selection of an identity on a user's mobile device. As will be described below, geo-location based identity selection addresses the above described challenges.

[0038] FIG. 2 describes a process for generation a database to be used for geo-location based identity selection for wireless connections, according to an aspect of the present disclosure. FIG. 2 will be described from the perspective of ID federation provider 102. However, it will be understood that ID federation provider 102 has one or more processors execution computer-readable instructions stored on one or more memories thereof to perform the process of FIG. 2.

[0039] FIG. 2 described an example process according to which ID federation provider 102 constructs (generates) databases, which will be used for geo-location based identity selection as will be described below with reference to FIG. 3.

[0040] At S200, ID federation provider 102 receives a registration request from an access provider (which can also be an identity provider). The registration request can include information such as, but not limited to, access providers identification information and connection parameters. Connection parameters can specify conditions according to which a mobile device may attach or connect to access provider's network. For example, access provider can be a corporation or a business entity that only allows access to its network when a business identity issued by the corporation is used. In another example, access provider can also specify other business identities (3rd party business identities) that may be used for attachment to its network. This can, for example, be business identities issued by business partners of the corporation, a client of the corporation, etc. In another example, an access provider can specify a category of identities that may be used to for attachment to its network (e.g., any registered social network provided identity, any registered business

identity, etc., where the registration is with ID federation provider 102 as part of the roaming exchange mentioned above).

[0041] Connection parameters can also specify times and days according to which certain identities can be used to attach to its network. For example, the corporation in this example can specify that 3rd party business identities can access its network during business hours (e.g., 8AM to 5PM) from Monday to Friday but not on Saturdays and Sundays.

[0042] Connection parameters can also specify different privileges for different identities. For example, devices that attach to the corporation's network using business identities issued by the corporation can be allowed to access a different network (e.g., with more access privileges) than devices that attach using 3rd party business identities (with less access privileges).

[0043] In another example, the corporation of example above can allow limited access to any valid identity during certain times (e.g., outside business hours). This will also be specified as a connection parameter.

[0044] Connection parameters can also specify one or more geo-locations where roaming or access to provider's network is permitted. For example, access to those logging in with 3rd party business identities may be limited to within a certain distance (e.g., 200ft, a mile, etc.) of physical premises of the corporation. In another example, access to all valid identities outside business hours can be limited to a different geographical location (e.g., one corresponding to a parking lot of the corporation or a certain distance outside the physical premise of the corporation such as a perimeter of 100ft to half a mile surrounding the corporation's building.

[0045] The above are a few examples of different connection parameters, which are non-limiting of the scope of the present disclosure.

[0046] At S202, ID federation provider 102 process the registration request and registers the access/identity provider.

[0047] At S204, ID federation provider 102 stores connection parameters and the identification of the access provider from which the request is received at S200 in a database associated with ID federation provider 102.

[0048] The registration request and example connection parameters described with reference to S200, S202 and S204 have been described with respect to a request received from an access provider.

[0049] However, the request received at S200 can also be a registration request received from an identity provider. As part of the registration request, ID federation provider 102 receives information regarding credentials of particular user, information identifying user's associated devices such a mobile device 116, etc.

[0050] ID federation provider 102 completes the registration of an identity provider and stores the data in the database in the same manner as described above with reference to S202 and S204.

[0051] With a database of access providers and identity providers, examples will be described below for enabling geo-location based identity selection for a mobile device attempting to gain access to an access provider's network.

[0052] FIG. 3 describes an example process for geo-location based identity selection for wireless connections, according to an aspect of the present disclosure. FIG. 3 will be described from the perspective of ID federation provider 102. However, it will be understood that ID federation provider 102 can have one or more processors executing computer-readable instructions stored on one or more memories thereof to perform the process of FIG. 3. Furthermore, FIG. 3 will be described with reference to example embodiments of FIG. 1.

[0053] At S300, ID federation provider 102 determines/detects that mobile device 116 is within coverage area of access provider 112. This determination may be based on any known or to be developed method. For example, access provider 112 may detect the presence of mobile device 116 in its coverage area based on exchange of beacon information, a response to a "hello" message transmitted by one or more access points of service provider 116, etc. More specifically, access provider 112 may detect MAC address of mobile device 116 and transmit the same to ID federation 102. At S300, ID federation provider 102 may detect that mobile device 116 is within the coverage area of multiple access providers (e.g., access provider 110 and 112). Accordingly, the process described below can be carried out with respect to every detected access provider for selection of one for mobile device 116 to connect to.

[0054] At S302, ID federation provider 102 determines, by referencing a table of identity providers stored as described with reference to FIG. 2, identities of user 114 associated with mobile device 116 (using mobile device 116's MAC address).

[0055] At S303, ID federation provider 112 determines geo-location of mobile device 116.

[0056] A geo-location of mobile device 116 may be determined according to any known, or to be developed method such as using Global Positioning System (GPS) signals, cell tower triangulation as well as WiFi positioning systems. GPS can offer position accuracy of between 8 and 3 meters, subject to a number of known variables. Cell towers triangulation accuracy can vary widely, subject to the density of cell towers and features within the landscape. Cell tower accuracies can vary between, for example, 400 to 1400 meters. Some device operating systems used on devices include background location services that can collect WiFi access point details along with the GPS or cell tower triangulation-derived location, send the collected information to the operating system vendor or another operating entity to derive location information of a mobile device. The accuracy of such methods can vary widely, subject to the coverage of WiFi access points. Such variation can be between 10 to 100 meters.

[0057] In another example, the above mentioned methods can be used in conjunction with on-device location determination sensors. For example, mobile device 116 can have known or to be developed on-board accelerometers, gyroscopes, magnetometers, etc. which can record, at a finer grain, movement of mobile device 116, which can then be used to augment location information derived from GPS signals, cell tower triangulation, etc.

[0058] In another example, a device's IP address assignment can also be used in further refining a device's location information.

[0059] At S304, ID federation provider 102 determines if mobile device 116 is attempting to connect to access provider 112's network for the first time. For example, ID federation provider 102 determines if, in a database described with reference to FIG. 2, there is a record of past connections/attachments of mobile device 116 to access provider 112's network. If there is, the answer in S304 is no. If there is none, the answer in S304 is yes.

[0060] If at S304, ID federation provider 102 determines that mobile device 116 is attempting to connect to access provider 112's network for the first time, then at S306, ID federation provider 102 selects one of the identities associated with user 114 of mobile device 116 determined at S302. In one example, ID federation provider 102 makes this determination, in part based on connection parameters specified by access provider 102 and stored in the database of ID federation provider 102, as described above. For example, access provider 112 may be that of Company X and at the time of registering with ID federation provider 102, Company X may have specified several connection parameters. One is that user identities associated with customers (e.g., Company Y) can access/attach to access provider 112's network, if they visit access provider 112's premise between the hours of 8 AM and 5PM Mondays through Fridays. Another connection parameter may be that mobile devices seeking access to access provider 112's network should be within 100 feet of access provider 112's physical location(s).

[0061] In this example, it is assumed that user 114 is an employee of Company Y visiting Company X's premise (access provider 112's premise) at 11AM on a Tuesday. Therefore, at S306, ID federation provider 102 determines that user 114 has an identity provided by Company Y and is at the location of Company X (service provider 112) at 11 AM on a Tuesday. Accordingly, ID federation provider 102 selects user 114's business identity with Company Y as the identity to attach to access provider 112's network.

[0062] At S308, ID federation provider 102 determines if an identity is selected at S306. For example, user 114 may not have any identity that matches connection parameters of access provider 112. If not, at S310, ID federation provider 102 generates and sends a notification to mobile device 116 indicating that mobile device 116 cannot access/attach to access provider 112's network (access denial).

[0063] However, if at S308, ID federation provider 102 determines that an identity is selected, then at S312, ID federation provider 102 authenticates/confirm user 114's selected identity with a corresponding identity provider (e.g., one of identity providers 104 and 106 of FIG. 1). For example, ID federation provider 102 communicates with Company Y's database that has provided user 114's business identity selected at S306 to confirm user 114's identity (according to any known, or to be developed, authentication process).

[0064] At S314, ID federation provider 102 determines if user 114's selected identity is confirmed. If not, the process reverts back to S310, where ID federation provider 102 denies mobile device 116's attempted access to access provider 112's network and sends a notification of denial to mobile device 116.

[0065] However, if at S314, ID federation provider 102 determines that user 114's identity has been confirmed, then at S316, ID federation provider 102 attaches mobile device 116 to access provider 112's network and records details on mobile device 116's connection to access provider 112's network. Details can include, but are not limited to, geo-location information of mobile device 116, time stamp and duration of attachment to access provider 112's network, etc.

[0066] Referring back to S304, if ID federation provider 102 determines that mobile device 116's attempt to attach to access provider 112's network is not a first attempt to do so, at S320, ID federation provider 102, retrieves connection parameters of access provider 112 stored in a database.

[0067] At S322 and based on the connection parameters and geo-location information of mobile device 116, ID federation provider 102 selects an identity for attaching mobile device 116 to access provider 112's network. For example, ID federation provider 102 determines if geo-location information of mobile device 116 matches those specified by connection parameters of access provider 112 and/or corresponds to (e.g., within a margin of error of/deviates from) a record of previous geo-location of mobile device 116 during a prior attachment to the network of access provider 112. The margin of error may be a configurable parameter determined based on empirical studies and can be for example +/- 10%.

[0068] As an example and per the description of FIG. 2, access provider 112 may specify connection parameters that limit access to its network based on a geographical location of a mobile device. For example, while access provider 112's network coverage may extend out from a physical location of access provider 112 to its surrounding areas or adjacent roads, streets, parking lots, adjacent buildings, etc., access provider 112 may wish to only allow access to its network when a mobile device is within access provider 112's building and not, for example, in the parking lot.

[0069] Therefore, even if user 114 of device 116 has a business identity that matches corresponding connection parameters specified by access provider 112, if mobile device 116 is not within the specified geographical location, access provider 112 would deny mobile device 116 access to its network.

[0070] At S324, ID federation provider 102 determines if an identity is selected at S324. For example, user 114 may not have any identity that matches connection parameters and specified geo-location limitations of access provider 112. If not, at S326, ID federation provider 102 generates and sends a notification to mobile device 116 indicating that mobile device 116 cannot access/attach to access provider 112's network (access denial message).

[0071] However, if at S324, ID federation provider 102 determines that an identity is selected, then at S328, ID federation provider 102 authenticates/confirmes the selected identity with a corresponding identity provider (e.g., one of identity providers 104 and 106 of FIG. 1), in a similar manner as described above with reference to S312.

[0072] At S330, ID federation provider 102 determines if user 114's selected identity is confirmed. If not, the process reverts to S326, where ID federation provider 102 denies mobile device 116's attempted access to access provider 112's network and sends a notification of access denial to mobile device 116.

[0073] However, if at S330, ID federation provider 102 determines that user 114's identity has been confirmed, then at S332, ID federation provider 102 attaches mobile device 116 to access provider 112's network and records details on mobile device 116's connection to access provider 112's network. Details can include, but are not limited to, geo-location information of mobile device 116, time stamp and duration of attachment to access provider 112's network, etc. Thereafter, the process ends.

[0074] Accordingly, a seamless process is provided by ID federation provider 102 to select an identity for network connection based on geo-location information of mobile device 116. In other words, every time a mobile device is detected in coverage area of an access provider that is registered with ID federation provider 102 and has an identity (provided by an identity provider that is also registered with ID federation provider 102) and if the geo-location of mobile device 116 as well as any one of the associated identities match connection parameters of a nearby access provider, ID

federation provider 102 seamlessly establishes a connection to said access provider's network using the appropriate identity associated with mobile device 116.

[0075] In one example and upon selection of an identity for mobile device 116 to attach to access provider 112's network with, there may be an optional step according to which a notification may be provided on mobile device 116 to confirm or deny the attachment (connection to) service provider 112's network and/or to select an alternative profile to be used for the connection.

[0076] While with reference to FIG. 3, a specific example of Company X and Y was described. However, the present disclosure is not limited to the example of a business entity specifying access to its network using certain business identities during certain business hours at certain geographical locations.

[0077] As another example, assume that after visiting Company X's physical site and connecting to access provider 112's network using the identity provided by Company Y, as described above, user 114 exits Company X's physical site and proceeds to a local restaurant. The local restaurant may be another example of an access provider providing WiFi access to its patrons and customers, who is registered with ID federation provider 102. Furthermore, assume that user 114 had previously visited the local restaurant and used one of user's social/public identities to gain access to the local restaurant's WiFi network. Moreover, assume that connection parameters specified by the local restaurant and stored in a database by ID federation provider 102 indicates that all verified identities (e.g., registered with ID federation provider 102) can be used to access its WiFi network as long as a customer is physically located inside the local restaurant.

[0078] In this case, after user 114 exits Company X's site and approaches the local restaurant, the WiFi access network of the local restaurant may be detected by mobile device 116 as soon as mobile device 116 enters a perimeter around the local restaurant. However, given the connection parameter that access is allowed only if a customer is physically inside the local restaurant, ID federation provider 102 would not select any of user 114's identities to connect to local restaurant's WiFi network, because geo-location information of mobile device 116 indicates that it is currently close to but still outside of the local restaurant. However, upon entering the local restaurant's building and given that ID federation provider 102 has a record of user

114 having previously used a social/public identity at the local restaurant, ID federation provider 102 automatically selects the same social/public identity of user 114, authenticates user 114's credentials with the corresponding identity provider (e.g., identity provider 104) and allows mobile device 116 to be seamlessly connected to the local restaurant's WiFi network.

[0079] Accordingly, movement of mobile device 116 from one location to another results in a dynamic and seamless switching of connections to different access providers depending on each access provider's connection parameters and geo-location of mobile device 116.

[0080] As mentioned above, after the connection is established, seamlessly, between mobile device 116 and the local restaurant's WiFi network, user 114 may be given a notification of the established connection and may have an option on a screen of mobile device 116 to reject (override) or modify (e.g., select another identity for connecting) the connection. In one example, the option to reject or modify may be time limited. For example, if no input is received on mobile device 116 to reject or modify the established connection, then ID federation provider 102 assumes that the connection is acceptable and records information about the connection in a database as described above.

[0081] Having described example embodiments for geo-location based identity selection for establishing network connection, the disclosure now turns to discussion of example devices that can be used as components such as ID federation provider 102, mobile device 116, any one of access providers 108, 110 and 112 and/or any one of identity providers 104 and 106.

[0082] FIG. 4 illustrates an example system including various hardware computing components, according to an aspect of the present disclosure. The more appropriate embodiment will be apparent to those of ordinary skill in the art when practicing the present technology. Persons of ordinary skill in the art will also readily appreciate that other system embodiments are possible.

[0083] FIG. 4 illustrates a system bus computing system architecture 400 wherein the components of the system are in electrical communication with each other using a connection 406. Exemplary system 400 includes a cache 402 and a processing unit (CPU or processor) 404 and a system connection 406 that couples various system

components including the system memory 420, such as read only memory (ROM) 418 and random access memory (RAM) 416, to the processor 404. The system 400 can include a cache of high-speed memory connected directly with, in close proximity to, or integrated as part of the processor 404. The system 400 can copy data from the memory 420 and/or the storage device 408 to the cache 402 for quick access by the processor 404. In this way, the cache can provide a performance boost that avoids processor 404 delays while waiting for data. These and other modules can control or be configured to control the processor 404 to perform various actions. Other system memory 420 may be available for use as well. The memory 420 can include multiple different types of memory with different performance characteristics. The processor 404 can include any general purpose processor and a service component, such as service 1 410, service 2 412, and service 3 414 stored in storage device 408, configured to control the processor 404 as well as a special-purpose processor where software instructions are incorporated into the actual processor design. The processor 404 may essentially be a completely self-contained computing system, containing multiple cores or processors, a bus, memory controller, cache, etc. A multi-core processor may be symmetric or asymmetric.

[0084] To enable user interaction with the computing device 400, an input device 422 can represent any number of input mechanisms, such as a microphone for speech, a touch-sensitive screen for gesture or graphical input, keyboard, mouse, motion input, speech and so forth. An output device 424 can also be one or more of a number of output mechanisms known to those of skill in the art. In some instances, multimodal systems can enable a user to provide multiple types of input to communicate with the computing device 400. The communications interface 426 can generally govern and manage the user input and system output. There is no restriction on operating on any particular hardware arrangement and therefore the basic features here may easily be substituted for improved hardware or firmware arrangements as they are developed.

[0085] Storage device 408 is a non-volatile memory and can be a hard disk or other types of computer readable media which can store data that are accessible by a computer, such as magnetic cassettes, flash memory cards, solid state memory devices, digital versatile disks, cartridges, random access memories (RAMs) 416, read only memory (ROM) 418, and hybrids thereof.

[0086] The system 400 can include an integrated circuit 428, such as an application-specific integrated circuit (ASIC) configured to perform various operations. The integrated circuit 428 can be coupled with the connection 406 in order to communicate with other components in the system 400.

[0087] The storage device 408 can include software services 410, 412, 414 for controlling the processor 404. Other hardware or software modules are contemplated. The storage device 408 can be connected to the system connection 406. In one aspect, a hardware module that performs a particular function can include the software component stored in a computer-readable medium in connection with the necessary hardware components, such as the processor 404, connection 406, output device 424, and so forth, to carry out the function.

[0088] For clarity of explanation, in some instances the present technology may be presented as including individual functional blocks including functional blocks comprising devices, device components, steps or routines in a method embodied in software, or combinations of hardware and software.

[0089] In some example embodiments the computer-readable storage devices, mediums, and memories can include a cable or wireless signal containing a bit stream and the like. However, when mentioned, non-transitory computer-readable storage media expressly exclude media such as energy, carrier signals, electromagnetic waves, and signals per se.

[0090] Methods according to the above-described examples can be implemented using computer-executable instructions that are stored or otherwise available from computer readable media. Such instructions can comprise, for example, instructions and data which cause or otherwise configure a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. Portions of computer resources used can be accessible over a network. The computer executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, firmware, or source code. Examples of computer-readable media that may be used to store instructions, information used, and/or information created during methods according to described examples include magnetic or optical disks, flash memory, USB devices provided with non-volatile memory, networked storage devices, and so on.

[0091] Devices implementing methods according to these disclosures can comprise hardware, firmware and/or software, and can take any of a variety of form factors. Typical examples of such form factors include laptops, smart phones, small form factor personal computers, personal digital assistants, rackmount devices, standalone devices, and so on. Functionality described herein also can be embodied in peripherals or add-in cards. Such functionality can also be implemented on a circuit board among different chips or different processes executing in a single device, by way of further example.

[0092] The instructions, media for conveying such instructions, computing resources for executing them, and other structures for supporting such computing resources are means for providing the functions described in these disclosures.

[0093] Although a variety of examples and other information was used to explain aspects within the scope of the appended claims, no limitation of the claims should be implied based on particular features or arrangements in such examples, as one of ordinary skill would be able to use these examples to derive a wide variety of implementations. Further and although some subject matter may have been described in language specific to examples of structural features and/or method steps, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to these described features or acts. For example, such functionality can be distributed differently or performed in components other than those identified herein. Rather, the described features and steps are disclosed as examples of components of systems and methods within the scope of the appended claims.

[0094] Claim language reciting "at least one of" a set indicates that one member of the set or multiple members of the set satisfy the claim. For example, claim language reciting "at least one of A and B" means A, B, or A and B.

CLAIMS

1. A method comprising:
 - determining, by one or more processors, a location of a mobile device;
 - identifying, by the one or more processors, an access provider having a network for the mobile device to connect to;
 - selecting, by the one or more processors, one of a plurality of identities associated with the mobile device for authorizing connection to the network of the access provider, the selection being based on the location of the mobile device and connection parameters specified by the access provider; and
 - establishing, by the one or more processors, the connection of the mobile device to the network of the access provider using the one of the plurality of identities.
2. The method of claim 1, wherein no user input on the mobile device is required for establishing the connection to the network of the access provider.
3. The method of any preceding claim, wherein the one of the plurality of identities is selected if the location of the mobile device and the selected one of the plurality of identities match conditions specified in the connection parameters by the access provider.
4. The method of any preceding claim, wherein the connection parameters include one or more of:
 - geographical specifications for any mobile device attempting to connect to the network of the access provider;
 - one or more authorized identities permitted for use in authorizing the connection to the network of the access provider; and
 - time specifications indicative of days and hours during which attachment to the network of the access provider is allowed.
5. The method of claim 4, wherein selecting the one of the plurality of identities includes:

determining if the location of the mobile device matches the geographical specifications of the access provider;

determining if the one of the plurality of identities associated with the mobile device matches one of the one or more authorized identities;

determining if a time at which the mobile device is detected in a coverage area of the network of the access provider matches the time specifications provided by the access provider, wherein

the one of the plurality of identities is selected if (1) the location of the mobile device matches the geographical specifications of the access provider, (2) the one of the plurality of identities associated with the mobile device matches one of the one or more authorized identities, and (3) the time at which the mobile device is detected in a coverage area of the network of the access provider matches the time specifications provided by the access provider.

6. The method of any preceding claim, further comprising:

sending a notification to the mobile device indicating that the connection to the network of the access provider is established, the notification providing a time-limited option for one of rejecting or modifying the connection.

7. The method of any preceding claim, further comprising:

determining, by the one or more processors, if the mobile device is attempting the connection to the network of the access provider for a first time; and

recording, by the one or more processors, geographical coordinates of the mobile device after the connection is established, the record being used for automatic connection to the network of the access provider using the one of the plurality of identities selected.

8. The method of any preceding claim, further comprising:

detecting that the mobile device has moved to a new location that corresponds to a coverage area of another access provider; and

dynamically switching from the one of the plurality of identities to another one of the plurality of identities to connect to a network of the other access provider based on the new location of the mobile device and connection parameters specified by the other access provider.

9. A network component having one or more identity providers and one or more access providers registered therewith, the network component comprising:

memory having computer-readable instructions stored therein; and

one or more processors configured to execute the computer-readable instructions to:

determine a location of a mobile device;

identify an access provider from the one or more access providers having a network for the mobile device to connect to;

select an identity provided by one of the one or more identity providers, the identity being associated with the mobile device for authorizing connection to the network and being selected based on the location of the mobile device and connection parameters specified by the access provider; and

connect the mobile device to the network using the selected identity.

10. The network component of claim 9, wherein the one or more processors execute the computer-readable instructions to identify the access provider, to select the identity and to connect the mobile device without receiving any user input from mobile device.

11. The network component of any of claims 9 to 10, wherein the identity is selected if the location of the mobile device and the identity satisfy at least one condition specified in the connection parameters by the access provider.

12. The network component of any of claims 9 to 11, wherein the connection parameters include one or more of:

geographical specifications for any mobile device attempting to connect to the network of the access provider;

one or more authorized identity categories permitted for use in authorizing the connection to the network of the access provider; and

time specifications indicative of days and hours during which attachment to the network of the access provider is allowed.

13. The network component of claim 12, wherein the computer-readable instructions to select the identity includes instructions to:

determine if the location of the mobile device matches the geographical specifications of the access provider;

determine if the selected identity matches one of the one or more authorized identity categories;

determine if a time at which the mobile device is detected in a coverage area of the network of the access provider matches the time specifications provided by the access provider, wherein

the identity is selected if (1) if the location of the mobile device matches the geographical specifications of the access provider, (2) the identity matches one of the one or more authorized identity categories, and (3) the time at which the mobile device is detected in a coverage area of the network of the access provider matches the time specifications provided by the access provider.

14. The network component of any of claims 9 to 13, wherein the one or more processors are further configured to execute the computer-readable instructions to provide a notification to the mobile device indicating that the connection to the network of the access provider is established, the notification providing a time-limited option for one of rejecting or modifying the connection.

15. The network component of any of claims 9 to 14, wherein the one or more processors are further configured to execute the computer-readable instructions to:

determine if the mobile device is attempting the connection to the network of the access provider for a first time; and

record geographical coordinates of the mobile device after the connection is established, the record being used for automatic future connections to the network of the access provider using the selected identity.

16. The network component of any of claims 9 to 15, further comprising:

detecting that the mobile device has moved to a new location that corresponds to a coverage area of another access provider; and

dynamically switch from the selected identity to another one of the one or more identities for authorizing connection to a network of the other access provider

based on the new location of the mobile device and connection parameters specified by the other access provider.

17. One or more non-transitory computer-readable medium having computer-readable instructions stored therein, which when executed by one or more processors of a network component, cause the one or more processors to:

determine a location of a mobile device;

identify a plurality of access providers each having a network for the mobile device to connect to;

based on corresponding connection parameters associated with each of the plurality of access providers and the location of the mobile device, select one of the plurality of access providers and an identity associated with the mobile device for attaching the mobile device to a network of the one of the plurality of access providers; and

attaching the mobile device to the network of the one of the plurality of access providers.

18. The one or more non-transitory computer-readable medium of claim 17, wherein the mobile device has a plurality of identities associated therewith, each of the plurality of identities being provided by a different identity provider registered with the network component.

19. The one or more non-transitory computer-readable medium of claim 17 to 18, wherein the connection parameters of each of the plurality of access providers include one or more of:

geographical specifications for any mobile device attempting to connect to a corresponding network of each of the plurality of access providers;

one or more authorized identity categories permitted for use in authorizing the connection to the corresponding network of the access provider; and

time specifications indicative of days and hours during which attachment to the corresponding network is allowed.

20. The one or more non-transitory computer-readable medium of claim 17 to 19, wherein

the location of the mobile device is within a coverage area of each of the plurality of access providers; and

each of the plurality of access providers are registered with the network component.

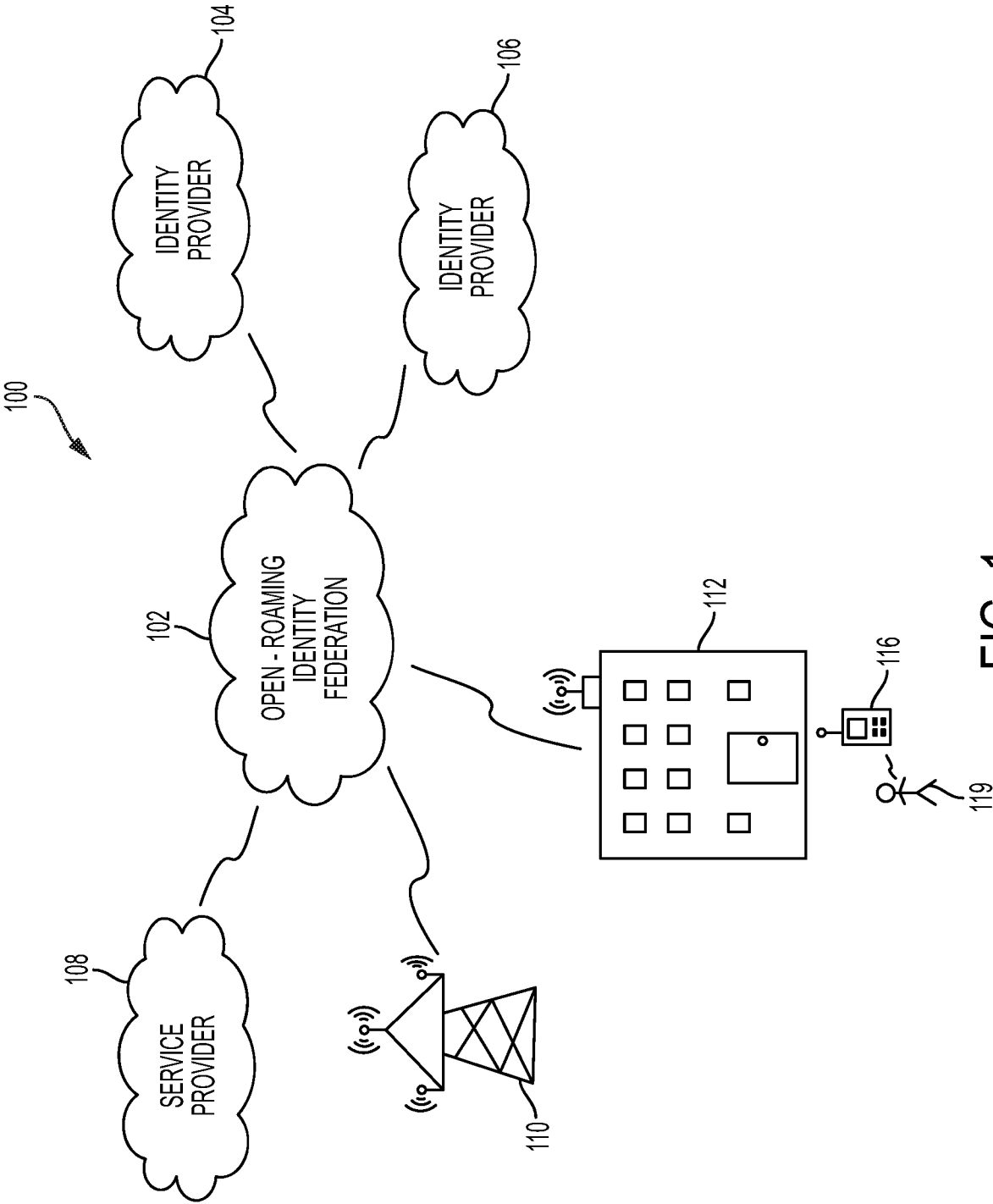


FIG. 1

2/4

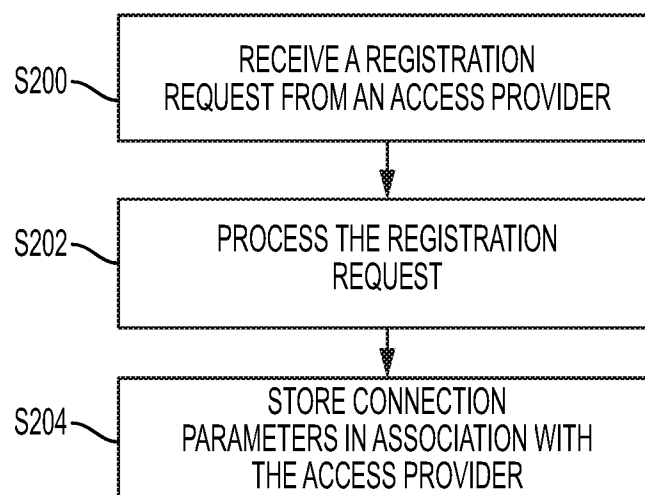


FIG. 2

3/4

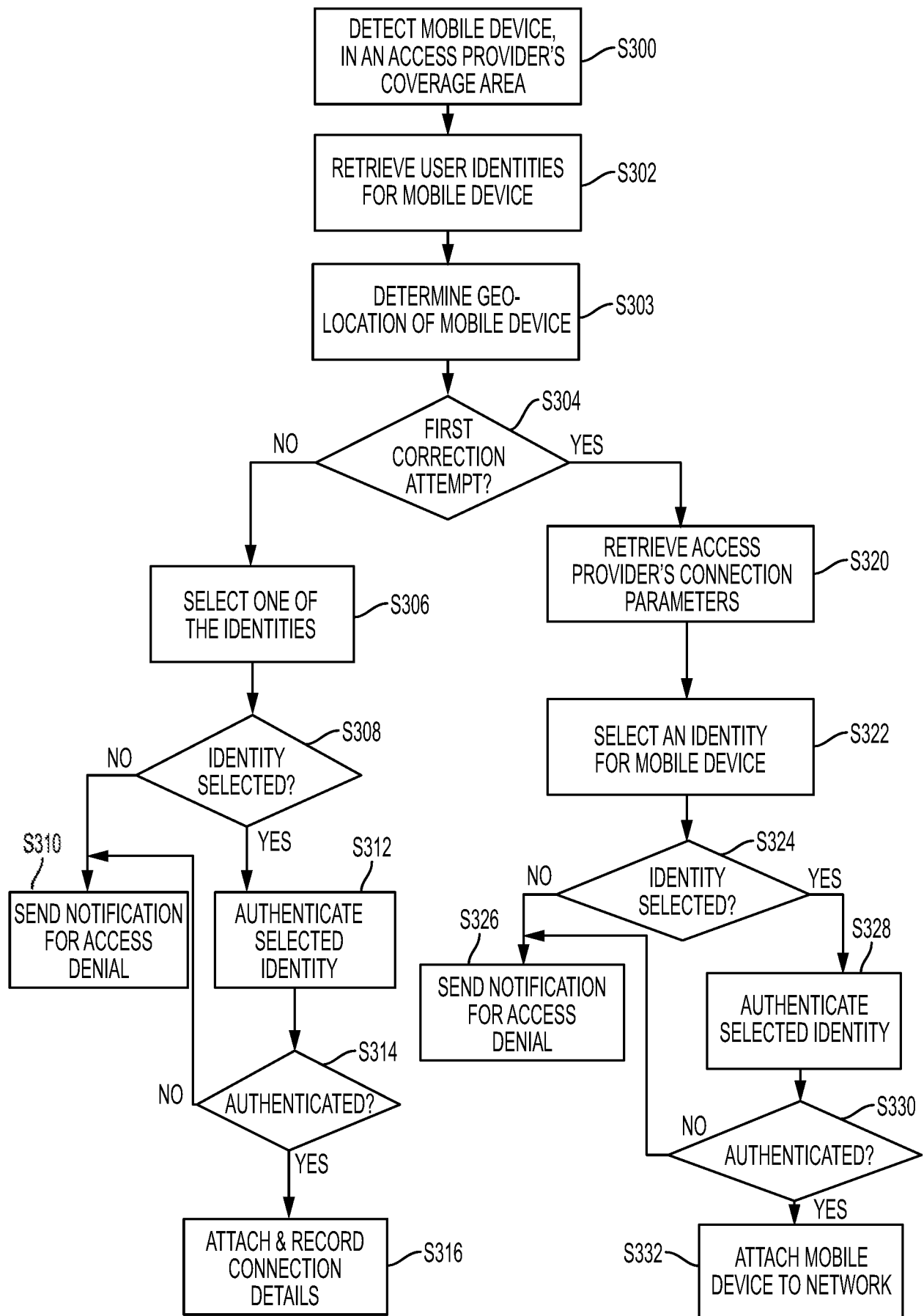


FIG. 3

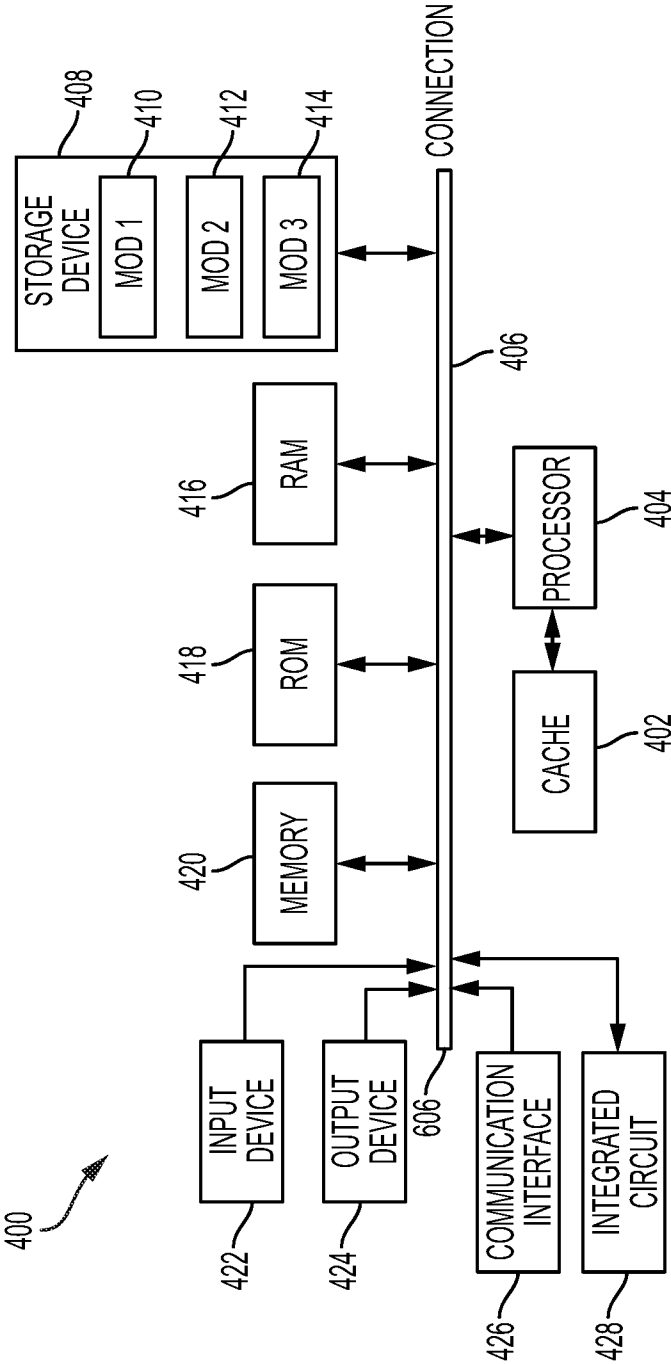


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 18/48923

A. CLASSIFICATION OF SUBJECT MATTER
 IPC(8) - H04W 48/18; H04W 48/04 (2018.01)
 CPC - H04W 48/18; H04W 4/02; H04W 8/06

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)

See Search History Document

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

See Search History Document

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

See Search History Document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/0116105 A1 (Frankel et al.) 01 June 2006 (01.06.2006); entire document, especially, abstract, FIG. 1-4, 6, para [0007], [0009], [0017], [0018], [0020], [0064], [0066], [0077], [0078], [0082] and claims 7 and 26	1-3, 9-11, 17-18
A	US 2011/0092185 A1 (Garskof) 21 April 2011 (21.04.2011); entire document	1-3, 9-11, 17-19
A	WO 2017/021787 A1 (Comviva Technologies Limited) 09 February 2017 (09.02.2017); entire document	1-3, 9-11, 17-19
A	CN 106658562 A (Shenzhen Youke Yunlian Tech Co Ltd) 10 May 2017 (10.05.2017); entire document,	1-3, 9-11, 17-19
A	EP 2282587 A1 (France Telecom) 09 February 2011 (09.02.2011); entire document	1-3, 9-11, 17-19
A	WO 2017/205715 A1 (Wandering WiFi LLC) 30 November 2017 (30.11.2017); entire document	1-3, 9-11, 17-19
A	US 2010/0330986 A1 (Rahman et al.) 30 December 2010 (30.12.2010); entire document	1-3, 9-11, 17-19
A	US 9,949,304 B1 (Sprint Communications Co. LP) 17 April 2018 (17.04.2018); entire document	1-3, 9-11, 17-19
A	US 2017/0194995 A1 (Evan et al.) 06 July 2017 (06.07.2017); entire document	1-3, 9-11, 17-19

☐ 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

18 January 2019 (18.01.2019)

Date of mailing of the international search report

08 FEB 2019

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
 P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-8300

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300
 PCT OSP: 571-272-7774

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 18/48923

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☒ Claims Nos.: 4-8; 12-16, 20
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.