



(51) International Patent Classification:

H04W 48/14 (2009.01) H04W 48/02 (2009.01)

H04W 48/10 (2009.01)

(21) International Application Number:

PCT/US2017/038875

(22) International Filing Date:

22 June 2017 (22.06.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: INTEL IP CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95054 (US).

(72) Inventors: GUPTA, Vivek; 4945 Bridgeview Lane, San Jose, California 95138 (US). CANPOLAT, Necati; 20978 NW Swire Lane, Beaverton, Oregon 97006 (US).

(74) Agent: KACVINSKY, John F.; KACVINSKY DAISAK BLUNI PLLC, 430 Davis Drive, Suite 150, Morrisville, North Carolina 27560 (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, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

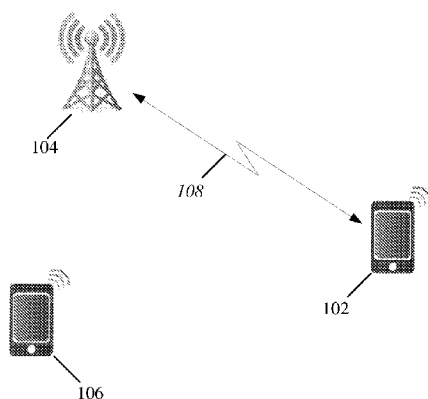
Published:

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

(54) Title: GUEST ACCESS FOR NEUTRAL HOST NETWORK MODE

FIG. 1

100



(57) Abstract: Techniques for enabling guest access to a service provider of a neutral host network are provided. A MulteFire enabled wireless device can obtain guest access to a MulteFire network. The wireless device can determine that the service provider provides guest access. The wireless device can determine parameters controlling the guest access. The wireless device can request guest access based on the determined parameters. After the wireless device agrees to guest access restrictions, the wireless device can be granted guest access. Other embodiments are described and claimed.



GUEST ACCESS FOR NEUTRAL HOST NETWORK MODE**TECHNICAL FIELD**

Embodiments described herein generally relate to wireless communications between devices in wireless networks.

5

BACKGROUND

MulteFire networks can operate within unlicensed frequency bands to provide high-speed and reliable wireless communications. However, MulteFire networks do not provide a mechanism to enable guest access to the network such that a guest wireless device can establish a relationship with a service provider and access host services in a secure manner. Accordingly,
10 new techniques may be needed to provide guest access to MulteFire network resources.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an embodiment of a first operating environment.
FIG. 2 illustrates an embodiment of a second operating environment.
FIG. 3 illustrates an embodiment of a first message flow.
15 FIG. 4 illustrates an embodiment of a second message flow.
FIG. 5 illustrates first exemplary data message formats.
FIG. 6 illustrates a second exemplary data message format.
FIG. 7 illustrates an embodiment of a first logic flow.
FIG. 8 illustrates an embodiment of a storage medium.
20 FIG. 9 illustrates an embodiment of a device.
FIG. 10 illustrates an embodiment of a first wireless network.
FIG. 11 illustrates an embodiment of a first wireless network.

DETAILED DESCRIPTION

Various embodiments may be generally directed to techniques for enabling guest access to
25 a service provider of a neutral host network (NHN). Various embodiments provide a MulteFire enabled wireless device to obtain guest access to a MulteFire network. The wireless device can determine that the service provider provides guest access. The wireless device can determine parameters controlling the guest access. The wireless device can request guest access based on the determined parameters. After the wireless device agrees to guest access restrictions, the
30 wireless device can be granted guest access.

Various embodiments may comprise one or more elements. An element may comprise any structure arranged to perform certain operations. Each element may be implemented as hardware, software, or any combination thereof, as desired for a given set of design parameters or performance constraints. Although an embodiment may be described with a limited number
35 of elements in a certain topology by way of example, the embodiment may include more or less

elements in alternate topologies as desired for a given implementation. It is worthy to note that any 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. The appearances of the phrases “in one embodiment,” “in some
5 embodiments,” and “in various embodiments” in various places in the specification are not necessarily all referring to the same embodiment.

Various embodiments herein are generally directed to wireless communications systems. Various embodiments may be directed to wireless communications over any frequency band or range. Various embodiments may involve wireless communications according to one or more
10 wireless communication standards. Some embodiments may involve wireless communications performed according to one or more broadband wireless communication standards. For example, various embodiments may involve wireless communications performed according to one or more 3rd Generation Partnership Project (3GPP), 3GPP Long Term Evolution (LTE), and/or 3GPP LTE-Advanced (LTE-A) technologies and/or standards, including their
15 predecessors, revisions, progeny, and/or variants. Various embodiments may be directed to wireless communications performed in accordance with one or more 3GPP standards over one or more unlicensed frequency bands including, for example, the MulteFire (MF) standard. Additional examples of broadband wireless communication technologies/standards that may be utilized in some embodiments may include – without limitation – Global System for Mobile
20 Communications (GSM)/Enhanced Data Rates for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS)/High Speed Packet Access (HSPA), and/or GSM with General Packet Radio Service (GPRS) system (GSM/GPRS), IEEE 802.16 wireless broadband standards such as IEEE 802.16m and/or IEEE 802.16p, International Mobile Telecommunications Advanced (IMT-ADV), Worldwide Interoperability for Microwave Access
25 (WiMAX) and/or WiMAX II, Code Division Multiple Access (CDMA) 2000 (e.g., CDMA2000 1xRTT, CDMA2000 EV-DO, CDMA EV-DV, and so forth), High Performance Radio Metropolitan Area Network (HIPERMAN), Wireless Broadband (WiBro), High Speed Downlink Packet Access (HSDPA), High Speed Orthogonal Frequency-Division Multiplexing (OFDM) Packet Access (HSOPA), High-Speed Uplink Packet Access (HSUPA) technologies
30 and/or standards, including their predecessors, revisions, progeny, and/or variants.

Further examples of wireless communications technologies and/or standards that may be used in various embodiments may include – without limitation – other IEEE wireless communication standards such as the IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11u, IEEE 802.11ac, IEEE 802.11af, and/or IEEE 802.11ah
35 standards, High-Efficiency Wi-Fi standards developed by the IEEE 802.11 High Efficiency

WLAN (HEW) Study Group and/or IEEE 802.11 Task Group (TG) ax, Wi-Fi Alliance (WFA) wireless communication standards such as Wi-Fi, Wi-Fi Direct, Wi-Fi Direct Services, WiGig Display Extension (WDE), WiGig Bus Extension (WBE), WiGig Serial Extension (WSE) standards and/or standards developed by the WFA Neighbor Awareness Networking (NAN) Task Group, machine-type communications (MTC) standards such as those embodied in 3GPP Technical Report (TR) 23.887, 3GPP Technical Specification (TS) 22.368, and/or 3GPP TS 23.682, and/or near-field communication (NFC) standards such as standards developed by the NFC Forum, including any predecessors, revisions, progeny, and/or variants of any of the above. The embodiments are not limited to these examples.

FIG. 1 illustrates an exemplary operating environment 100 such as may be representative of various embodiments in which techniques for guest network access are implemented. The operating environment 100 can include a first mobile device 102, an access point 104, and a second mobile device 106. The access point 104 can be part of a 3GPP wireless network. In various embodiments, the access point 104 can be an access point of a MulteFire network and can be part of and/or can be associated with a neutral host network (NHN) providing external network access through a service provider.

The first mobile device 102 can be any type of wireless device. In various embodiments, the first mobile device 102 can be a User Equipment (UE). In various embodiments, the first mobile device can be a MF UE (e.g., a MF capable or enabled UE).

The MF UE 102 and the access point 104 can communicate over a wireless communications interface 108. The wireless communications interface 108 can provide the MF UE 102 with connectivity to other devices and/or networks coupled to the access point 104. The wireless communications interface 108 can be, for example, a wireless interface for any of the wireless networks or standards described herein including, for example, any 3GPP standard, including any MF technology or standard. In various embodiments, the wireless communications interface 108 may operate within or over any frequency band including any unlicensed frequency band. The access point 104 can be part of a MF network enabling access to the MF UE 102 over the wireless communications interface 108. In particular, the MF UE 102 can be provided access to external networks and/or the Internet through a service provider.

The second mobile device 106 can also be any type of wireless device. In various embodiments, the second mobile device 106 can be a User Equipment (UE). In various embodiments, the second mobile device 106 can be a MF UE (e.g., a MF capable or enabled UE). The second mobile device 106 can be new to the operating environment 100. The second mobile device 106 can be, for example, a guest of the operating environment 100 and can be desirous of being able to communicate with the access point 104 over the wireless

communications interface 108. Prior to obtaining guest access, the second mobile device 106 can be restricted to not using the MF network accessible through the access point 104.

Accordingly, the second mobile device 106 can attempt to obtain guest access with the service provider of the NHN to obtain NHN services by way of the AP 104.

5 Techniques described herein can provide the second mobile device 106, for example, as a MF UE, with guest or courtesy access to the MF network through the access point 104. The embodiments are not limited in this context.

Various embodiments provide techniques to provide the second mobile device 106 with guest access to an MF network (and/or other 3GPP networks) accessible through the AP 104.

10 Accordingly, the techniques described herein allow the second mobile device 106 to establish a relationship with a service provider coupled to the AP 104 and to access host network services in a secure manner. Various embodiments enable the NHN to indicate to second mobile device 106 that guest access services are available and for the second mobile device 106 to be allowed access without any pre-provisioned credentials with the NHN or the service provider. Guest
15 access techniques described herein can be provided to the second mobile device 106 automatically without any operator interaction, such that guest access provisioning can be done quickly and efficiently.

FIG. 2 illustrates an exemplary operating environment 200 for providing MulteFire guest access. The operating environment 200 can include a MF UE 202, a certificate authority 204, a
20 MF neutral host network (NHN) 206, and a MF service provider network 208. The MF UE 202 can represent the second mobile device 106 depicted in FIG. 1 that can attempt to obtain guest access to a MF network – for example, access to the MF NHN 206.

The MF UE 202 can include a number of components. In various embodiments, the MF UE 202 can include a device discovery for guest access and credential management component
25 210 and a MF modem for network access server (NAS) and extensible authentication protocol (EAP) component 212.

The MF NHN 206 can include a number of components. In various embodiments, the MF NHN 206 can include a neutral host (NH) gateway (GW) (NH-GW) 214 and a NH-mobility management entity (MME) (NH-MME) 216. The MF NHN 206 can also include a MF access
30 point (AP) 218. In various embodiments, the MF AP 218 can be considered to be separate and/or distinct from the MF NHN 206 and can be communicatively coupled to the MF NHN 206. The MF AP 218 can represent the AP 104 depicted in FIG. 1.

The MF service provider network 208 can include a number of components. In various embodiments, the MF service provider network 208 can include a terms and conditions (T&C)
35 server 220, an authentication, authorization, and accounting (AAA) server 222, and a billing

and/or charging component 224. The billing and/or charging component 224 can be a server and/or database or other entity for tracking billing operations. In various embodiments, the AAA server 222 can be part of the MF NHN 206.

The certificate authority (CA) 204 can represent any entity that can provide a unique
5 identifier for the MF UE 202 and/or can provide a mechanism such that the MF UE 202 can be uniquely identified. In general, it is desired for the MF service provider network 208 to be able to identify each device that is provided service including, for example, the MF UE 202. To provide this capability, device certificates can be issued by the CA 204.

Other forms of identification can also be used to uniquely identify the MF UE 202 such as,
10 for example, a phone number or a medium access control (MAC) address. The unique identifier for the MF UE 202 can be provisioned for the MF UE 202 during manufacture (e.g., factory provisioned). For example, the unique identifier can include an International Mobile Equipment Identity (IMEI) or a Mobile Subscriber Integrated Services Digital Network Number (MSISDN) or other identifier issued by a service provider or manufacturer.

15 As part of a process for providing guest access, the MF service provider network 208 can validate the MF UE 202 by verifying its unique identifier (e.g., its provisioned certificate from the CA 204) before provisioning subscription information to the MF UE 202 to establish guest access.

The MF UE 202 can interact with the MF AP 218 for guest access discovery 228. In
20 various embodiments, the device discovery for guest access and credential management component 210 can interact with the MF AP 218 for guest access discovery 228. The MF UE 202 can determine that guest access on the MF NHN 206 is available through a number of mechanisms. In various embodiments, the MF UE 202 can discover guest access is available based on information (e.g., a specific bit sequence or message) provided in system broadcast
25 information transmitted by the MF AP 218 – for example, in a system information block (SIB) broadcast by the MF AP 218.

In various embodiments, the MF UE 202 can use access network query protocol (ANQP)
methods or service discovery protocol (SDP) based methods to query guest access capabilities of the MF NHN 206 and/or MF service provided network 208. In various embodiments, the MF
30 UE 202 can obtain the name of the service provider of the MF service provider network 208 using these query methods – for example, using an SDP query request and receiving SPD responses to obtain a participating service provider (PSP) identification (ID).

After guest access discovery 228, the MF UE 202 can interact with the MF service
provider network 208 through the MF NHN 206 to obtain guest access. In various embodiments,
35 the MF modem for NAS and EAP component 212 can interact with the AAA server 222 through

the NH-MME 216. For example, the MF modem for NAS and EAP component 212 can interact with the NH-MME 216 to request guest access and the NH-MME 216 can interact with the AAA server 222 to authenticate the MF UE 202.

5 The MF UE 202 can interact with the MF service provider network 208 to provision guest access credentials 232. In various embodiments, the device discovery for guest access and credential management component 210 can interact with the T&C server 220 through the NH-GW 214 to provision guest access credentials 232. In various embodiments, the provision of guest access credentials 232 can be implemented using, for example, open mobile alliance (OMA) device management (DM) (OMA-DM) or simple object access protocol (SOAP) 10 extensible markup language (XML) (SOAP-XML) over hypertext transfer protocol secure (HTTPS). The T&C server can store requirements and terms for use that the MF UE 202 must agree to before guest access is provided. Once access is provided, the billing/charging component 224 can track for any billing or expenses associated with the provided guest access to either the MF UE 202 and/or the MF NHN 206.

15 The techniques for providing guest access to the MF UE 202 described herein can allow the MF UE 202 to retrieve any stored terms, conditions, or requirements related to guest access from the T&C server 220 (e.g., through a webpage retrieval) while restricting access to the Internet or other services until any terms of use have been accepted. Further, the provided guest access can restrict packet routing options available to entities provided with guest or courtesy 20 access. Server certificates can also be used and/or anonymous authentication using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) can be used for provisioning guest access.

FIG. 3 illustrates an exemplary embodiment of a message flow 300, which may be representative of the operations executed by one or more embodiments described herein. The message flow 300 illustrates exemplary messages and/or communications exchanged between 25 multiple network elements. As shown in FIG. 3, the message flow 300 illustrates communications between a UE 302, a MF AP 304, and a NHN MME 306. The UE 302 can represent the MF UE 202 depicted in FIG. 2 and/or the second mobile device 106 depicted in FIG. 1. The MF AP 304 can represent the MF AP 218 depicted in FIG. 2 and/or the AP 104 depicted in FIG. 1. The NHN MME 306 can represent the NH-MME 216 depicted in FIG. 2. The message flow 300 can represent operations performed and/or messages or communications exchanged to provide the UE 302 with guest access to a MF network.

The message flow 300 can begin with guest access capability being discovered. For example, at 308, the UE 302 can receive system broadcast information transmitted by the MF AP 304. The system broadcast information can include an indication that guest access is available 35

and/or possible. As an example, the UE 302 can receive a SIB at 308 indicating that guest access is available. As an alternative, the UE 302 can use ANQP methods and/or SDP based methods to query the NHN MME 306 regarding guest access (e.g., regarding capabilities for guest access). Further, as an example, at 310, the UE 302 can prepare and transmit a SDP query request for the PSP ID. In response, at 312, the NHN MME 306 can prepare and transmit a SDP query response with the PSP ID and/or other information regarding the service provider of the network for which the UE 302 may be desirous of obtaining guest access.

Next, the UE 302 can select a service provider for guest access and can obtain credentials relating to obtaining guest access. For example, at 314, the UE 302 can prepare and transmit a SDP query request seeking credentials and/or other required parameters related to guest access. In response, at 316, the NHN MME 306 can prepare and send a SDP query response providing the credentials and/or other required parameters for guest access. In various embodiments, the NHN MME 306 can provide the UE 302 with the network access identifier (NAI) to use for an attach procedure. The NHN MME 306 can also provide the UE 302 with the uniform resource identifier (URI) that can be used by the UE 302 to access any stored terms and conditions information relating to guest access. Further, the NHN MME 306 can provide the UE 302 with information about the access point name (APN) to be used for the attach procedure as well as any additional required guest access credentials.

The UE 302 can subsequently initiate a guest access process. For example, at 318, the UE 302 can prepare and transmit an attach request for guest access to the packet data network (PDN). The UE 302 may initiate an attach request with an “attach type” set to a normal attach. For cellular Internet of Things (CIoT) devices, the UE 302 can initiate an attach request without a PDN connection and instead can attach to an APN obtained earlier.

In response to the attach request at 318, the NHN MME 306 can initiate EAP authentication with the guest network (e.g., service provider network) based on obtained NAI and guest credentials (e.g., from the UE 302). If authentication and authorization is successful, then at 320 the NHN MME 306 can respond to the attach request at 318. The UE 302 can then establish a PDN connection with the guest network with default bearers. Accordingly, after 320, the attach procedure can be completed and successful and a PDN connection between the UE 302 and the guest network can be established.

Once the attach process is successful and a PDN connection has been established, the UE 302 can obtain the URI that can be used to access any specific terms and conditions that govern guest access. The terms and conditions can be indicated or provided through a secure webpage for example. The terms and conditions can be a set of requirements that must be agreed to before access to the guest network may be provided. For example, unless the UE 302 accepts the

terms and conditions, access may be restricted by use of a captive portal and the selected APN may not allow packet access beyond the guest network. Further, no Internet link can be provided until the requirements for access are reviewed and agreed to for access. The UE 302 can access the terms and conditions at 322 by, for example, by using a HTTPS-GET request. The terms and
5 conditions can then be provided to the UE 302 for review. If accepted fully, the guest network can determine to provide the UE 302 with guest access as specified in the terms and conditions information. The UE 302 can then subsequently operate while using the guest access to the guest network.

At 324, after using the guest access, the UE 302 can implement a detach procedure to
10 detach from the guest network.

In various embodiments, when the UE 302 revisits a guest network that it has already discovered and/or a guest network to which it was provided access previously, one or more of the steps shown in FIG. 3 may be skipped or not implemented when the UE 302 attempts to seek guest access again. That is, one or more of the steps depicted in FIG. 3 may not be implemented
15 when the UE 302 seeks guest access again to a network where it previously obtained guest access.

Further, in various embodiments, the UE 302 at 322 can store a copy of the terms and conditions it agrees to in order to obtain guest access. If the terms and conditions for guest access have not changed since the UE 302 last agreed to the terms and conditions, then the UE
20 302 may not be required to seek the terms and conditions at step 322. Instead, a verification that the terms and conditions are the same or substantially the same may be implemented to verify that the UE 302 has already agreed to the terms and conditions. This can be accomplished by, for example, tracking a date and/or version of the terms and conditions or by checking a hash value associated with the terms and conditions.

FIG. 4 illustrates an exemplary embodiment of a message flow 400, which may be representative of the operations executed by one or more embodiments described herein. The message flow 400 illustrates exemplary messages and/or communications exchanged between multiple network elements. As shown in FIG. 4, the message flow 400 illustrates communications between a UE 302, a MF AP 304, and a NHN MME 306. The UE 302 can
25 represent the MF UE 202 depicted in FIG. 2 and/or the second mobile device 106 depicted in FIG. 1. The MF AP 304 can represent the MF AP 218 depicted in FIG. 2 and/or the AP 104 depicted in FIG. 1. The NHN MME 306 can represent the NH-MME 216 depicted in FIG. 2. The message flow 400 can represent operations performed and/or messages or communications exchanged to provide the UE 302 with guest access to a MF network that the UE 302 has already
30

previously been given guest access to and/or to a MF network where the terms and conditions for access have not changed since the last time the UE 302 gained guest access to the network.

As shown in FIG. 4, the message flow 400 can largely track the message flow 300. After a PDN connection is established, for example, the UE 302 may be required to agree to the terms and conditions of the guest network. If the terms and conditions for guest access have not changed (e.g., since the last time the UE 302 agreed to the terms and conditions governing access to the guest network), then the UE 302 may not be required to submit a HTTPS request for any terms and conditions page. Instead, at 402, the UE 302 and the NHN MME 306 may exchange messages verifying that the terms and conditions have not changed and/or that the UE 302 has already agreed to the current terms and conditions. In various embodiments, the UE 302 and the NHN MME 306 can exchange messages verifying a version and/or date of the terms and conditions. In various embodiments, a hash value associated with the terms and conditions can be verified and/or exchanged.

FIG. 5 illustrates a format of SDP container type elements. The SDP container type elements can specify the type of the SDP container included into a query or response message container for a NAS information element (IE). As shown in FIG. 5, a first column 502 identifies the SDP container type and a second column 504 specifies a bit sequence corresponding to the SDP container type such that each SDP container type can be uniquely identified. A guest query SDP container type 506 can have a first corresponding bit sequence 508 and guest response SDP container type 510 can have a second corresponding bit sequence 512 as shown.

In general, a guest query container can be generated and transmitted in an uplink query NAS transport message. Likewise, a guest response container can be generated and transmitted in a downlink NAS transport message. The SDP containers for guest query and response messages can include various information. FIG. 6 illustrates an exemplary embodiment of an SDP response message container for a guest response 600. The SDP container for guest response 600 can be generated and transmitted by the guest network and received and processed by a MF UE. FIG. 6 illustrates an example coding of the SDP container for guest response.

As shown in FIG. 6, the SDP container for guest response 600 can include a number of fields (602-618) with each field containing, indicating, or providing specific information while occupying or using a certain amount of bits. The fields can contain any information or message and can be of any size. In various embodiments, as shown in FIG. 6, the SDP container for guest response 600 can first include a length of container field 602. The length of container field 602 can have a size of two octets. Next, a length of guest APN field 604 can be provided. The length of guest APN field 604 can have a length of one or more octets. A guest APN field 606 can then be provided. The guest APN field 606 can have a length of one or more octets. After

the guest APN field 606, a length of terms and conditions server URI field 608 can be provided. The length of terms and conditions server URI field 608 can have a length of one or more octets. Next, a terms and conditions server URI field 610 can be provided that can have a length of one or more octets.

5 Continuing, the SDP container for guest response 600 can further include a length of guest access NAI field 612 that can have a length of one or more octets. A guest NAI field 614 can then be provided having a length of one or more octets. Finally, a length of guest credentials field 616 can be provided having a length of one or more octets. A corresponding guest credentials field 618 can then be provided having a length of one or more octets.

10 FIG. 7 illustrates an example of a logic flow 700 that may be representative of operations of an MF enabled wireless device for obtaining guest access to a service provider of a NHN according to various embodiments. For example, logic flow 700 may be representative of operations that may be performed in various embodiments by the mobile devices 102 and/or 106 in operating environment 100 of FIG. 1, MF UE 202 of operating environment 200 of FIG. 2,
15 and/or UE 302 depicted in FIGs. 3 and 4,

At 702, an MF enabled wireless device can determine that a service provider of a NHN can provide guest access. The MF enabled wireless device can determine that the service provider provides guest access based on system broadcast information. In various embodiments, the MF enabled wireless device can determine that the service provider provides guest access based on
20 processing a SIB. The MF enabled wireless device can determine that the service provider provides guest access based on ANQP methods or SDP based methods for receiving responses to queries regarding network capabilities and/or guest access capabilities.

At 704, the MF enabled wireless device can determine various parameters controlling or governing operation of the MF network and/or guest access. In various embodiments, the
25 MF enabled wireless device can generate and transmit SDP queries requesting the parameters and can receive and process responses that indicate or provide the parameters controlling guest access.

At 706, the MF enabled wireless device can request guest access based on the determined parameters controlling guest access. The MF enabled wireless device can generate and transmit
30 a data message indicating or providing a unique identifier of the MF enabled wireless device. The unique identifier can be used to verify and authenticate the MF enabled wireless device.

At 708, the MF enabled wireless device can be provided limited guest access. The MF enabled wireless device can agree to guest access restrictions in order to be granted full guest access capabilities. The guest access restrictions can be stored or hosted by a server of the
35 service provider and can represent terms and conditions governing guest access (e.g., access

restrictions). After accepting the terms and conditions, the MF enabled wireless device can be given guest access that can include access to the Internet through the service provider.

Various embodiments of the invention may be implemented fully or partially in software and/or firmware. This software and/or firmware may take the form of instructions contained in
5 or on a non-transitory computer-readable storage medium. Those instructions may then be read and executed by one or more processors to enable performance of the operations described herein. The instructions may be in any suitable form, such as but not limited to source code, compiled code, interpreted code, executable code, static code, dynamic code, and the like. Such a computer-readable medium may include any tangible non-transitory medium for storing
10 information in a form readable by one or more computers, such as but not limited to read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; a flash memory, etc. The embodiments are not limited in this context.

FIG. 8 illustrates an embodiment of a storage medium 800. Storage medium 800 may comprise any non-transitory computer-readable storage medium or machine-readable storage
15 medium, such as an optical, magnetic or semiconductor storage medium. In various embodiments, storage medium 800 may comprise an article of manufacture. In some embodiments, storage medium 800 may store computer-executable instructions, such as computer-executable instructions to implement logic flow 700 of FIG. 7. Examples of a computer-readable storage medium or machine-readable storage medium may include any
20 tangible media capable of storing electronic data, including volatile memory or non-volatile memory, removable or non-removable memory, erasable or non-erasable memory, writeable or re-writeable memory, and so forth. Examples of computer-executable instructions may include any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, object-oriented code, visual code, and the like. The embodiments are
25 not limited in this context.

FIG. 9 illustrates an embodiment of a communications device 900 that may implement one or more of wireless devices 102, 106, 202, 302, logic flow 700, and storage medium 800. In various embodiments, device 900 may comprise a logic circuit 928. The logic circuit 928 may include physical circuits to perform operations described for one or more of wireless devices
30 102, 106, 202, 302, logic flow 700, and storage medium 800, for example. As shown in FIG. 9, device 900 may include a radio interface 910, baseband circuitry 920, and computing platform 930, although the embodiments are not limited to this configuration.

The device 900 may implement some or all of the structure and/or operations for one or more of wireless devices 102, 106, 202, 302, logic flow 700, and storage medium 800, and logic
35 circuit 928 in a single computing entity, such as entirely within a single device. Alternatively,

the device 900 may distribute portions of the structure and/or operations for one or more of wireless devices 102, 106, 202, 302, logic flow 700, and storage medium 800, and logic circuit 928 across multiple computing entities using a distributed system architecture, such as a client-server architecture, a 3-tier architecture, an N-tier architecture, a tightly-coupled or clustered
5 architecture, a peer-to-peer architecture, a master-slave architecture, a shared database architecture, and other types of distributed systems. The embodiments are not limited in this context.

In one embodiment, radio interface 910 may include a component or combination of components adapted for transmitting and/or receiving single-carrier or multi-carrier modulated
10 signals (e.g., including complementary code keying (CCK), orthogonal frequency division multiplexing (OFDM), and/or single-carrier frequency division multiple access (SC-FDMA) symbols) although the embodiments are not limited to any specific over-the-air interface or modulation scheme. Radio interface 910 may include, for example, a receiver 912, a frequency synthesizer 914, and/or a transmitter 916. Radio interface 910 may include bias controls, a
15 crystal oscillator and/or one or more antennas 918-*f*. In another embodiment, radio interface 910 may use external voltage-controlled oscillators (VCOs), surface acoustic wave filters, intermediate frequency (IF) filters and/or RF filters, as desired. Due to the variety of potential RF interface designs an expansive description thereof is omitted.

Baseband circuitry 920 may communicate with radio interface 910 to process receive
20 and/or transmit signals and may include, for example, an analog-to-digital converter 922 for down converting received signals, a digital-to-analog converter 924 for up converting signals for transmission. Further, baseband circuitry 920 may include a baseband or physical layer (PHY) processing circuit 926 for PHY link layer processing of respective receive/transmit signals. Baseband circuitry 920 may include, for example, a medium access control (MAC) processing
25 circuit 727 for MAC/data link layer processing. Baseband circuitry 920 may include a memory controller 932 for communicating with MAC processing circuit 727 and/or a computing platform 930, for example, via one or more interfaces 934.

In some embodiments, PHY processing circuit 926 may include a frame construction and/or detection module, in combination with additional circuitry such as a buffer memory, to
30 construct and/or deconstruct communication frames. Alternatively or in addition, MAC processing circuit 927 may share processing for certain of these functions or perform these processes independent of PHY processing circuit 926. In some embodiments, MAC and PHY processing may be integrated into a single circuit.

The computing platform 930 may provide computing functionality for the device 900. As
35 shown, the computing platform 930 may include a processing component 940. In addition to, or

alternatively of, the baseband circuitry 920, the device 900 may execute processing operations or logic for one or more of wireless devices 102, 106, 202, 302, logic flow 700, and storage medium 800, and logic circuit 928 using the processing component 940. The processing component 940 (and/or PHY 926 and/or MAC 727) may comprise various hardware elements, software elements, or a combination of both. Examples of hardware elements may include devices, logic devices, components, processors, microprocessors, circuits, processor circuits, circuit elements (e.g., transistors, resistors, capacitors, inductors, and so forth), integrated circuits, application specific integrated circuits (ASIC), programmable logic devices (PLD), digital signal processors (DSP), field programmable gate array (FPGA), memory units, logic gates, registers, semiconductor device, chips, microchips, chip sets, and so forth. Examples of software elements may include software components, programs, applications, computer programs, application programs, system programs, software development programs, machine programs, operating system software, middleware, firmware, software modules, routines, subroutines, functions, methods, procedures, software interfaces, application program interfaces (API), instruction sets, computing code, computer code, code segments, computer code segments, words, values, symbols, or any combination thereof. Determining whether an embodiment is implemented using hardware elements and/or software elements may vary in accordance with any number of factors, such as desired computational rate, power levels, heat tolerances, processing cycle budget, input data rates, output data rates, memory resources, data bus speeds and other design or performance constraints, as desired for a given implementation.

The computing platform 930 may further include other platform components 950. Other platform components 950 include common computing elements, such as one or more processors, multi-core processors, co-processors, memory units, chipsets, controllers, peripherals, interfaces, oscillators, timing devices, video cards, audio cards, multimedia input/output (I/O) components (e.g., digital displays), power supplies, and so forth. Examples of memory units may include without limitation various types of computer readable and machine readable storage media in the form of one or more higher speed memory units, such as read-only memory (ROM), random-access memory (RAM), dynamic RAM (DRAM), Double-Data-Rate DRAM (DDRAM), synchronous DRAM (SDRAM), static RAM (SRAM), programmable ROM (PROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), flash memory, polymer memory such as ferroelectric polymer memory, ovonic memory, phase change or ferroelectric memory, silicon-oxide-nitride-oxide-silicon (SONOS) memory, magnetic or optical cards, an array of devices such as Redundant Array of Independent Disks (RAID) drives, solid state memory devices (e.g., USB memory, solid state drives (SSD) and any other type of storage media suitable for storing information.

Device 900 may be, for example, an ultra-mobile device, a mobile device, a fixed device, a machine-to-machine (M2M) device, a personal digital assistant (PDA), a mobile computing device, a smart phone, a telephone, a digital telephone, a cellular telephone, user equipment, eBook readers, a handset, a one-way pager, a two-way pager, a messaging device, a computer, a
5 personal computer (PC), a desktop computer, a laptop computer, a notebook computer, a netbook computer, a handheld computer, a tablet computer, a server, a server array or server farm, a web server, a network server, an Internet server, a work station, a mini-computer, a main frame computer, a supercomputer, a network appliance, a web appliance, a distributed computing system, multiprocessor systems, processor-based systems, consumer electronics, programmable
10 consumer electronics, game devices, display, television, digital television, set top box, wireless access point, base station, node B, subscriber station, mobile subscriber center, radio network controller, router, hub, gateway, bridge, switch, machine, or combination thereof. Accordingly, functions and/or specific configurations of device 900 described herein, may be included or omitted in various embodiments of device 900, as suitably desired.

15 Embodiments of device 900 may be implemented using single input single output (SISO) architectures. However, certain implementations may include multiple antennas (e.g., antennas 918-f) for transmission and/or reception using adaptive antenna techniques for beamforming or spatial division multiple access (SDMA) and/or using MIMO communication techniques.

 The components and features of device 900 may be implemented using any combination of
20 discrete circuitry, application specific integrated circuits (ASICs), logic gates and/or single chip architectures. Further, the features of device 900 may be implemented using microcontrollers, programmable logic arrays and/or microprocessors or any combination of the foregoing where suitably appropriate. It is noted that hardware, firmware and/or software elements may be collectively or individually referred to herein as “logic” or “circuit.”

25 It should be appreciated that the exemplary device 900 shown in the block diagram of FIG. 9 may represent one functionally descriptive example of many potential implementations. Accordingly, division, omission or inclusion of block functions depicted in the accompanying figures does not infer that the hardware components, circuits, software and/or elements for implementing these functions would be necessarily be divided, omitted, or included in
30 embodiments.

 In various embodiments, device 900 can operate according to one or more 3GPP standards including, for example, MulteFire related standards and technologies.

 FIG. 10 illustrates an embodiment of a broadband wireless access system 1000. As shown in FIG. 10, broadband wireless access system 1000 may be an internet protocol (IP) type
35 network comprising an internet 1010 type network or the like that is capable of supporting

mobile wireless access and/or fixed wireless access to internet 1010. In one or more embodiments, broadband wireless access system 1000 may comprise any type of orthogonal frequency division multiple access (OFDMA)-based or single-carrier frequency division multiple access (SC-FDMA)-based wireless network, such as a system compliant with one or more of the 3GPP LTE Specifications and/or IEEE 802.13 Standards, and the scope of the claimed subject matter is not limited in these respects.

In the exemplary broadband wireless access system 1000, radio access networks (RANs) 1012 and 1018 are capable of coupling with evolved node Bs (eNBs) 1014 and 1020, respectively, to provide wireless communication between one or more fixed devices 1016 and internet 1010 and/or between one or more mobile devices 1022 and Internet 1010. One example of a fixed device 1016 and a mobile device 1022 is device 900 of FIG. 9, with the fixed device 1016 comprising a stationary version of device 900 and the mobile device 1022 comprising a mobile version of device 900. RANs 1012 and 1018 may implement profiles that are capable of defining the mapping of network functions to one or more physical entities on broadband wireless access system 1000. eNBs 1014 and 1020 may comprise radio equipment to provide RF communication with fixed device 1016 and/or mobile device 1022, such as described with reference to device 900, and may comprise, for example, the PHY and MAC layer equipment in compliance with a 3GPP LTE Specification or an IEEE 802.13 Standard. eNBs 1014 and 1020 may further comprise an IP backplane to couple to Internet 1010 via RANs 1012 and 1018, respectively, although the scope of the claimed subject matter is not limited in these respects.

Broadband wireless access system 1000 may further comprise a visited core network (CN) 1024 and/or a home CN 1026, each of which may be capable of providing one or more network functions including but not limited to proxy and/or relay type functions, for example authentication, authorization and accounting (AAA) functions, dynamic host configuration protocol (DHCP) functions, or domain name service controls or the like, domain gateways such as public switched telephone network (PSTN) gateways or voice over internet protocol (VoIP) gateways, and/or internet protocol (IP) type server functions, or the like. However, these are merely example of the types of functions that are capable of being provided by visited CN 1024 and/or home CN 1026, and the scope of the claimed subject matter is not limited in these respects. Visited CN 1024 may be referred to as a visited CN in the case where visited CN 1024 is not part of the regular service provider of fixed device 1016 or mobile device 1022, for example where fixed device 1016 or mobile device 1022 is roaming away from its respective home CN 1026, or where broadband wireless access system 1000 is part of the regular service provider of fixed device 1016 or mobile device 1022 but where broadband wireless access

system 1000 may be in another location or state that is not the main or home location of fixed device 1016 or mobile device 1022. The embodiments are not limited in this context.

Fixed device 1016 may be located anywhere within range of one or both of eNBs 1014 and 1020, such as in or near a home or business to provide home or business customer broadband
5 access to Internet 1010 via eNBs 1014 and 1020 and RANs 1012 and 1018, respectively, and home CN 1026. It is worthy of note that although fixed device 1016 is generally disposed in a stationary location, it may be moved to different locations as needed. Mobile device 1022 may be utilized at one or more locations if mobile device 1022 is within range of one or both of eNBs 1014 and 1020, for example. In accordance with one or more embodiments, operation support
10 system (OSS) 1028 may be part of broadband wireless access system 1000 to provide management functions for broadband wireless access system 1000 and to provide interfaces between functional entities of broadband wireless access system 1000. Broadband wireless access system 1000 of FIG. 10 is merely one type of wireless network showing a certain number of the components of broadband wireless access system 1000, and the scope of the claimed
15 subject matter is not limited in these respects.

FIG. 11 illustrates an embodiment of a wireless network 1100. As shown in FIG. 11, wireless network comprises an access point 1102 and wireless stations 1104, 1106, and 1108. In various embodiments, wireless network 1100 may comprise a wireless local area network (WLAN), such as a WLAN implementing one or more Institute of Electrical and Electronics
20 Engineers (IEEE) 1102.11 standards (sometimes collectively referred to as “Wi-Fi”). In some other embodiments, wireless network 1100 may comprise another type of wireless network, and/or may implement other wireless communications standards. In various embodiments, for example, wireless network 1100 may comprise a WWAN or WPAN rather than a WLAN. In various embodiments, the wireless network 1100 may comprise a wireless network operating
25 according to one or more 3GPP standards or technologies. In various embodiments, the wireless network 1100 can be a MF or MF-enabled wireless network. The embodiments are not limited to this example.

In some embodiments, wireless network 1100 may implement one or more broadband wireless communications standards, such as 3G or 4G standards, including their revisions,
30 progeny, and variants. Examples of 3G or 4G wireless standards may include without limitation any of the IEEE 802.16m and 802.16p standards, 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE) and LTE-Advanced (LTE-A) standards, and International Mobile Telecommunications Advanced (IMT-ADV) standards, including their revisions, progeny and variants. Other suitable examples may include, without limitation, Global System for Mobile
35 Communications (GSM)/Enhanced Data Rates for GSM Evolution (EDGE) technologies,

Universal Mobile Telecommunications System (UMTS)/High Speed Packet Access (HSPA) technologies, Worldwide Interoperability for Microwave Access (WiMAX) or the WiMAX II technologies, Code Division Multiple Access (CDMA) 2000 system technologies (e.g., CDMA2000 1xRTT, CDMA2000 EV-DO, CDMA EV-DV, and so forth), High Performance
5 Radio Metropolitan Area Network (HIPERMAN) technologies as defined by the European Telecommunications Standards Institute (ETSI) Broadband Radio Access Networks (BRAN), Wireless Broadband (WiBro) technologies, GSM with General Packet Radio Service (GPRS) system (GSM/GPRS) technologies, High Speed Downlink Packet Access (HSDPA) technologies, High Speed Orthogonal Frequency-Division Multiplexing (OFDM) Packet Access
10 (HSOPA) technologies, High-Speed Uplink Packet Access (HSUPA) system technologies, 3GPP Rel. 8-12 of LTE/System Architecture Evolution (SAE), and so forth. The embodiments are not limited in this context.

In various embodiments, wireless stations 1104, 1106, and 1108 may communicate with access point 1102 in order to obtain connectivity to one or more external data networks. In some
15 embodiments, for example, wireless stations 1104, 1106, and 1108 may connect to the Internet 1112 via access point 1102 and access network 1110. In various embodiments, access network 1110 may comprise a private network that provides subscription-based Internet-connectivity, such as an Internet Service Provider (ISP) network. The embodiments are not limited to this example.

20 In various embodiments, two or more of wireless stations 1104, 1106, and 1108 may communicate with each other directly by exchanging peer-to-peer communications. For example, in the example of FIG. 11, wireless stations 1104 and 1106 communicate with each other directly by exchanging peer-to-peer communications 1114. In some embodiments, such peer-to-peer communications may be performed according to one or more Wi-Fi Alliance
25 (WFA) standards. For example, in various embodiments, such peer-to-peer communications may be performed according to the WFA Wi-Fi Direct standard, 2010 Release. In various embodiments, such peer-to-peer communications may additionally or alternatively be performed using one or more interfaces, protocols, and/or standards developed by the WFA Wi-Fi Direct Services (WFDS) Task Group. The embodiments are not limited to these examples.

30 Various embodiments may be implemented using hardware elements, software elements, or a combination of both. Examples of hardware elements may include processors, microprocessors, circuits, circuit elements (e.g., transistors, resistors, capacitors, inductors, and so forth), integrated circuits, application specific integrated circuits (ASIC), programmable logic devices (PLD), digital signal processors (DSP), field programmable gate array (FPGA), logic
35 gates, registers, semiconductor device, chips, microchips, chip sets, and so forth. Examples of

software may include software components, programs, applications, computer programs, application programs, system programs, machine programs, operating system software, middleware, firmware, software modules, routines, subroutines, functions, methods, procedures, software interfaces, application program interfaces (API), instruction sets, computing code, computer code, code segments, computer code segments, words, values, symbols, or any combination thereof. Determining whether an embodiment is implemented using hardware elements and/or software elements may vary in accordance with any number of factors, such as desired computational rate, power levels, heat tolerances, processing cycle budget, input data rates, output data rates, memory resources, data bus speeds and other design or performance constraints.

One or more aspects of at least one embodiment may be implemented by representative instructions stored on a machine-readable medium which represents various logic within the processor, which when read by a machine causes the machine to fabricate logic to perform the techniques described herein. Such representations, known as “IP cores” may be stored on a tangible, machine readable medium and supplied to various customers or manufacturing facilities to load into the fabrication machines that actually make the logic or processor. Some embodiments may be implemented, for example, using a machine-readable medium or article which may store an instruction or a set of instructions that, if executed by a machine, may cause the machine to perform a method and/or operations in accordance with the embodiments. Such a machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware and/or software. The machine-readable medium or article may include, for example, any suitable type of memory unit, memory device, memory article, memory medium, storage device, storage article, storage medium and/or storage unit, for example, memory, removable or non-removable media, erasable or non-erasable media, writeable or re-writeable media, digital or analog media, hard disk, floppy disk, Compact Disk Read Only Memory (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewriteable (CD-RW), optical disk, magnetic media, magneto-optical media, removable memory cards or disks, various types of Digital Versatile Disk (DVD), a tape, a cassette, or the like. The instructions may include any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, encrypted code, and the like, implemented using any suitable high-level, low-level, object-oriented, visual, compiled and/or interpreted programming language.

The following examples pertain to further embodiments:

Example 1 is an apparatus, comprising a memory, and logic, at least a portion of the logic implemented in circuitry coupled to the memory, the logic to determine a service provider of a neutral host network (NHN) provides a guest access service, determine parameters controlling the guest access service, generate a data message for transmission to the NHN requesting the guest access service based on the determined parameters, and generate a data message for transmission to the service provider indicating acceptance of guest access restrictions to obtain the guest access service.

Example 2 is an extension of Example 1 or any other example disclosed herein, the apparatus to comprise a MulteFire (MF) enabled wireless device.

Example 3 is an extension of Example 2 or any other example disclosed herein, the MF enabled wireless device to comprise a user equipment (UE).

Example 4 is an extension of Example 1 or any other example disclosed herein, the logic to process system broadcast information to determine the service provider provides the guest access service.

Example 5 is an extension of Example 4 or any other example disclosed herein, the logic to process a system information block (SIB) indicating the service provider provides the guest access service.

Example 6 is an extension of Example 1 or any other example disclosed herein, the logic to process a response to an access network query protocol (ANQP) message indicating the service provider provides the guest access service.

Example 7 is an extension of Example 1 or any other example disclosed herein, the logic to process a response to a service discovery protocol (SDP) message indicating the service provider provides the guest access service.

Example 8 is an extension of Example 1 or any other example disclosed herein, the logic to process a response to a service discovery protocol (SDP) message to determine the parameters controlling the guest access service.

Example 9 is an extension of Example 8 or any other example disclosed herein, the response indicating a guest access point name (APN).

Example 10 is an extension of Example 8 or any other example disclosed herein, the response indicating a guest network access identifier (NAI).

Example 11 is an extension of Example 8 or any other example disclosed herein, the response indicating guest access credentials.

Example 12 is an extension of Example 8 or any other example disclosed herein, the response indicating a uniform resource indicator (URI) of a server hosting the guest service access restrictions.

Example 13 is an extension of Example 1 or any other example disclosed herein, the data message for transmission to the NHN to comprise an attach request.

Example 14 is an extension of Example 13 or any other example disclosed herein, the attach request to comprise a normal attach request.

5 Example 15 is an extension of Example 13 or any other example disclosed herein, the attach request to include a request to establish a packet data network (PDN) connection.

Example 16 is an extension of Example 1 or any other example disclosed herein, the data message for transmission to the NHN to comprise a unique identifier of the apparatus.

10 Example 17 is an extension of Example 1 or any other example disclosed herein, the logic to process a data message indicating the guest access restrictions.

Example 18 is an extension of Example 17 or any other example disclosed herein, the logic to generate the data message for transmission to the service provider indicating acceptance of the guest access restrictions based on the processed data message indicating the guest access restrictions.

15 Example 19 is an extension of Example 1 or any other example disclosed herein, the data message for transmission to the service provider indicating acceptance by indicating a prior acceptance of the guest access restrictions.

Example 20 is an extension of Example 19 or any other example disclosed herein, the logic to verify a date of the guest access restrictions.

20 Example 21 is an extension of Example 19 or any other example disclosed herein, the logic to verify a version of the guest access restrictions.

Example 22 is an extension of Example 19 or any other example disclosed herein, the logic to verify a hash value associated with the guest access restrictions.

25 Example 23 is an extension of Example 1 or any other example disclosed herein, the logic to generate a data message for transmission to the NHN indicating termination of the guess access service.

Example 24 is an extension of Example 23 or any other example disclosed herein, the data message to comprise a detach procedure.

30 Example 25 is an extension of any of Examples 1 to 24 or any other example disclosed herein, comprising at least one radio frequency (RF) transceiver and at least one RF antenna.

Example 26 is a wireless communication method, comprising determining a service provider of a neutral host network (NHN) provides a guest access service, determining parameters controlling the guest access service, generating a data message for transmission to the NHN requesting the guest access service based on the determined parameters, and generating a

data message for transmission to the service provider indicating acceptance of guest access restrictions to obtain the guest access service.

Example 27 is an extension of Example 26 or any other example disclosed herein, the NHN to comprise a MulteFire (MF) enabled NHN.

5 Example 28 is an extension of Example 26 or any other example disclosed herein, comprising processing system broadcast information to determine the service provider provides the guest access service.

Example 29 is an extension of Example 28 or any other example disclosed herein, comprising processing a system information block (SIB) indicating the service provider provides
10 the guest access service.

Example 30 is an extension of Example 26 or any other example disclosed herein, further comprising processing a response to an access network query protocol (ANQP) message indicating the service provider provides the guest access service.

Example 31 is an extension of Example 26 or any other example disclosed herein, further
15 comprising processing a response to a service discovery protocol (SDP) message indicating the service provider provides the guest access service.

Example 32 is an extension of Example 26 or any other example disclosed herein, further comprising processing a response to a service discovery protocol (SDP) message to determine the parameters controlling the guest access service.

20 Example 33 is an extension of Example 32 or any other example disclosed herein, the response indicating a guest access point name (APN).

Example 34 is an extension of Example 32 or any other example disclosed herein, the response indicating a guest network access identifier (NAI).

Example 35 is an extension of Example 32 or any other example disclosed herein, the
25 response indicating guest access credentials.

Example 36 is an extension of Example 32 or any other example disclosed herein, the response indicating a uniform resource indicator (URI) of a server hosting the guest service access restrictions.

Example 37 is an extension of Example 26 or any other example disclosed herein, the data
30 message for transmission to the NHN to comprise an attach request.

Example 38 is an extension of Example 37 or any other example disclosed herein, the attach request to comprise a normal attach request.

Example 39 is an extension of Example 37 or any other example disclosed herein, the attach request to include a request to establish a packet data network (PDN) connection.

Example 40 is an extension of Example 37 or any other example disclosed herein, the data message for transmission to the NHN comprising a unique identifier of the apparatus.

Example 41 is an extension of Example 26 or any other example disclosed herein, comprising processing a data message indicating the guest access restrictions.

5 Example 42 is an extension of Example 41 or any other example disclosed herein, comprising generating the data message for transmission to the service provider indicating acceptance of the guest access restrictions based on the processed data message indicating the guest access restrictions.

10 Example 43 is an extension of Example 26 or any other example disclosed herein, the data message for transmission to the service provider indicating acceptance by indicating a prior acceptance of the guest access restrictions.

Example 44 is an extension of Example 43 or any other example disclosed herein, comprising verifying a date of the guest access restrictions.

15 Example 45 is an extension of Example 43 or any other example disclosed herein, comprising verifying a version of the guest access restrictions.

Example 46 is an extension of Example 43 or any other example disclosed herein, comprising verifying a hash value associated with the guest access restrictions.

20 Example 47 is an extension of Example 26 or any other example disclosed herein, comprising generating a data message for transmission to the NHN indicating termination of the guess access service.

Example 48 is an extension of Example 47 or any other example disclosed herein, the data message to comprise a detach procedure.

25 Example 49 is at least one non-transitory computer-readable medium comprising a set of instructions that, in response to being executed at a wireless communication device, cause the wireless communication device to determine a service provider of a neutral host network (NHN) provides a guest access service, determine parameters controlling the guest access service, generate a data message for transmission to the NHN requesting the guest access service based on the determined parameters and, generate a data message for transmission to the service provider indicating acceptance of guest access restrictions to obtain the guest access service.

30 Example 50 is an extension of Example 49 or any other example disclosed herein, the wireless communication device to comprise a MulteFire (MF) enabled wireless communication device.

Example 51 is an extension of Example 52 or any other example disclosed herein, the MF enabled wireless communication device to comprise a user equipment (UE).

Example 52 is an extension of Example 51 or any other example disclosed herein, the wireless communication device to process system broadcast information to determine the service provider provides the guest access service.

5 Example 53 is an extension of Example 52 or any other example disclosed herein, the wireless communication device to process a system information block (SIB) indicating the service provider provides the guest access service.

Example 54 is an extension of Example 51 or any other example disclosed herein, the wireless communication device to process a response to an access network query protocol (ANQP) message indicating the service provider provides the guest access service.

10 Example 55 is an extension of Example 54 or any other example disclosed herein, the wireless communication device to process a response to a service discovery protocol (SDP) message indicating the service provider provides the guest access service.

Example 56 is an extension of Example 51 or any other example disclosed herein, the wireless communication device to process a response to a service discovery protocol (SDP) message to determine the parameters controlling the guest access service.

Example 57 is an extension of Example 56 or any other example disclosed herein, the response indicating a guest access point name (APN).

Example 58 is an extension of Example 56 or any other example disclosed herein, the response indicating a guest network access identifier (NAI).

20 Example 59 is an extension of Example 56 or any other example disclosed herein, the response indicating guest access credentials.

Example 60 is an extension of Example 56 or any other example disclosed herein, the response indicating a uniform resource indicator (URI) of a server hosting the guest service access restrictions.

25 Example 61 is an extension of Example 49 or any other example disclosed herein, the data message for transmission to the NHN to comprise an attach request.

Example 62 is an extension of Example 61 or any other example disclosed herein, the attach request to comprise a normal attach request.

30 Example 63 is an extension of Example 61 or any other example disclosed herein, the attach request to include a request to establish a packet data network (PDN) connection.

Example 64 is an extension of Example 61 or any other example disclosed herein, the data message for transmission to the NHN comprising a unique identifier of the apparatus.

Example 65 is an extension of Example 49 or any other example disclosed herein, the wireless communication device to process a data message indicating the guest access restrictions.

Example 66 is an extension of Example 65 or any other example disclosed herein, the wireless communication device to generate the data message for transmission to the service provider indicating acceptance of the guest access restrictions based on the processed data message indicating the guest access restrictions.

5 Example 67 is an extension of Example 49 or any other example disclosed herein, the data message for transmission to the service provider indicating acceptance by indicating a prior acceptance of the guest access restrictions.

Example 68 is an extension of Example 67 or any other example disclosed herein, the wireless communication device to verify a date of the guest access restrictions.

10 Example 69 is an extension of Example 67 or any other example disclosed herein, the wireless communication device to verify a version of the guest access restrictions.

Example 70 is an extension of Example 67 or any other example disclosed herein, the wireless communication device to verify a hash value associated with the guest access restrictions.

15 Example 71 is an extension of Example 49 or any other example disclosed herein, the wireless communication device to generate a data message for transmission to the NHN indicating termination of the guess access service.

Example 72 is an extension of Example 71 or any other example disclosed herein, the data message to comprise a detach procedure.

20 Numerous specific details have been set forth herein to provide a thorough understanding of the embodiments. It will be understood by those skilled in the art, however, that the embodiments may be practiced without these specific details. In other instances, well-known operations, components, and circuits have not been described in detail so as not to obscure the embodiments. It can be appreciated that the specific structural and functional details disclosed
25 herein may be representative and do not necessarily limit the scope of the embodiments.

Some embodiments may be described using the expression "coupled" and "connected" along with their derivatives. These terms are not intended as synonyms for each other. For example, some embodiments may be described using the terms "connected" and/or "coupled" to indicate that two or more elements are in direct physical or electrical contact with each other.

30 The term "coupled," however, may also mean that two or more elements are not in direct contact with each other, but yet still co-operate or interact with each other.

Unless specifically stated otherwise, it may be appreciated that terms such as "processing," "computing," "calculating," "determining," or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulates and/or
35 transforms data represented as physical quantities (e.g., electronic) within the computing

system's registers and/or memories into other data similarly represented as physical quantities within the computing system's memories, registers or other such information storage, transmission or display devices. The embodiments are not limited in this context.

It should be noted that the methods described herein do not have to be executed in the order described, or in any particular order. Moreover, various activities described with respect to the methods identified herein can be executed in serial or parallel fashion.

Although specific embodiments have been illustrated and described herein, it should be appreciated that any arrangement calculated to achieve the same purpose may be substituted for the specific embodiments shown. This disclosure is intended to cover any and all adaptations or variations of various embodiments. It is to be understood that the above description has been made in an illustrative fashion, and not a restrictive one. Combinations of the above embodiments, and other embodiments not specifically described herein will be apparent to those of skill in the art upon reviewing the above description. Thus, the scope of various embodiments includes any other applications in which the above compositions, structures, and methods are used.

It is emphasized that the Abstract of the Disclosure is provided to comply with 37 C.F.R. § 1.72(b), requiring an abstract that will allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in a single embodiment for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separate preferred embodiment. In the appended claims, the terms "including" and "in which" are used as the plain-English equivalents of the respective terms "comprising" and "wherein," respectively. Moreover, the terms "first," "second," and "third," etc. are used merely as labels, and are not intended to impose numerical requirements on their objects.

Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

CLAIMS**What is claimed is:**

1. An apparatus, comprising:
a memory; and
- 5 logic, at least a portion of the logic implemented in circuitry coupled to the memory, the logic to:
determine a service provider of a neutral host network (NHN) provides a guest access service;
determine parameters controlling the guest access service;
- 10 generate a data message for transmission to the NHN requesting the guest access service based on the determined parameters; and
generate a data message for transmission to the service provider indicating acceptance of guest access restrictions to obtain the guest access service.
2. The apparatus of claim 1, the apparatus to comprise a MulteFire (MF) enabled wireless
- 15 device.
3. The apparatus of claim 1, the logic to process system broadcast information to determine the service provider provides the guest access service.
4. The apparatus of claim 1, the logic to process a response to an access network query protocol (ANQP) message indicating the service provider provides the guest access service.
- 20 5. The apparatus of claim 1, the logic to process a response to a service discovery protocol (SDP) message indicating the service provider provides the guest access service.
6. The apparatus of claim 1, the logic to process a response to a service discovery protocol (SDP) message to determine the parameters controlling the guest access service.
7. The apparatus of claim 6, the response indicating a guest access point name (APN).
- 25 8. The apparatus of claim 6, the response indicating a guest network access identifier (NAI).
9. The apparatus of claim 6, the response indicating guest access credentials.
10. The apparatus of claim 8, the response indicating a uniform resource indicator (URI) of a server hosting the guest service access restrictions.
11. The apparatus of claim 1, the data message for transmission to the NHN to comprise an
- 30 attach request.
12. The apparatus of claim 11, the attach request to include a request to establish a packet data network (PDN) connection.
13. The apparatus of claim 11, the data message for transmission to the NHN to comprise a unique identifier of the apparatus.

14. The apparatus of claim 1, the logic to process a data message indicating the guest access restrictions.
15. At least one non-transitory computer-readable medium comprising a set of instructions that, in response to being executed at a wireless communication device, cause the wireless communication device to:
- 5 determine a service provider of a neutral host network (NHN) provides a guest access service;
- determine parameters controlling the guest access service;
- generate a data message for transmission to the NHN requesting the guest access service
- 10 based on the determined parameters; and
- generate a data message for transmission to the service provider indicating acceptance of guest access restrictions to obtain the guest access service.
16. The at least one non-transitory computer-readable medium of claim 15, the wireless communication device to comprise a MulteFire (MF) enabled wireless communication device.
- 15 17. The at least one non-transitory computer-readable medium of claim 15, the wireless communication device to process system broadcast information to determine the service provider provides the guest access service.
18. The at least one non-transitory computer-readable medium of claim 15, the wireless communication device to process a response to an access network query protocol (ANQP)
- 20 message indicating the service provider provides the guest access service.
19. The at least one non-transitory computer-readable medium of claim 15, the wireless communication device to process a response to a service discovery protocol (SDP) message indicating the service provider provides the guest access service.
20. The at least one non-transitory computer-readable medium of claim 15, the wireless communication device to process a response to a service discovery protocol (SDP) message to
- 25 determine the parameters controlling the guest access service.
21. The at least one non-transitory computer-readable medium of claim 20, the response indicating guest access credentials.
22. The at least one non-transitory computer-readable medium of claim 20, the response
- 30 indicating a uniform resource indicator (URI) of a server hosting the guest service access restrictions.
23. The at least one non-transitory computer-readable medium of claim 20, the response indicating a guest access point name (APN) and a guest network access identifier (NAI).
24. The at least one non-transitory computer-readable medium of claim 20, the response
- 35 indicating guest access credentials.

25. The at least one non-transitory computer-readable medium of claim 20, the response indicating a uniform resource indicator (URI) of a server hosting the guest service access restrictions.

5

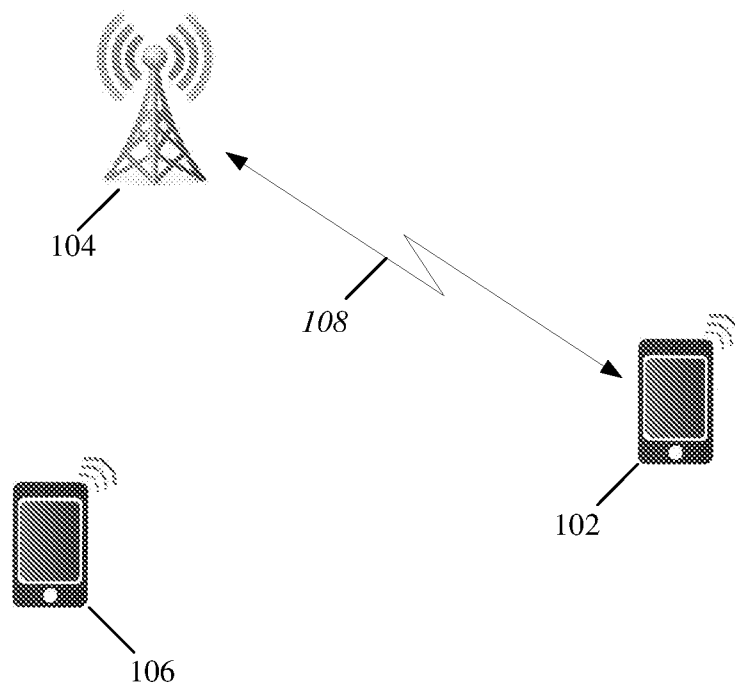
FIG. 1**100**

FIG. 2
200

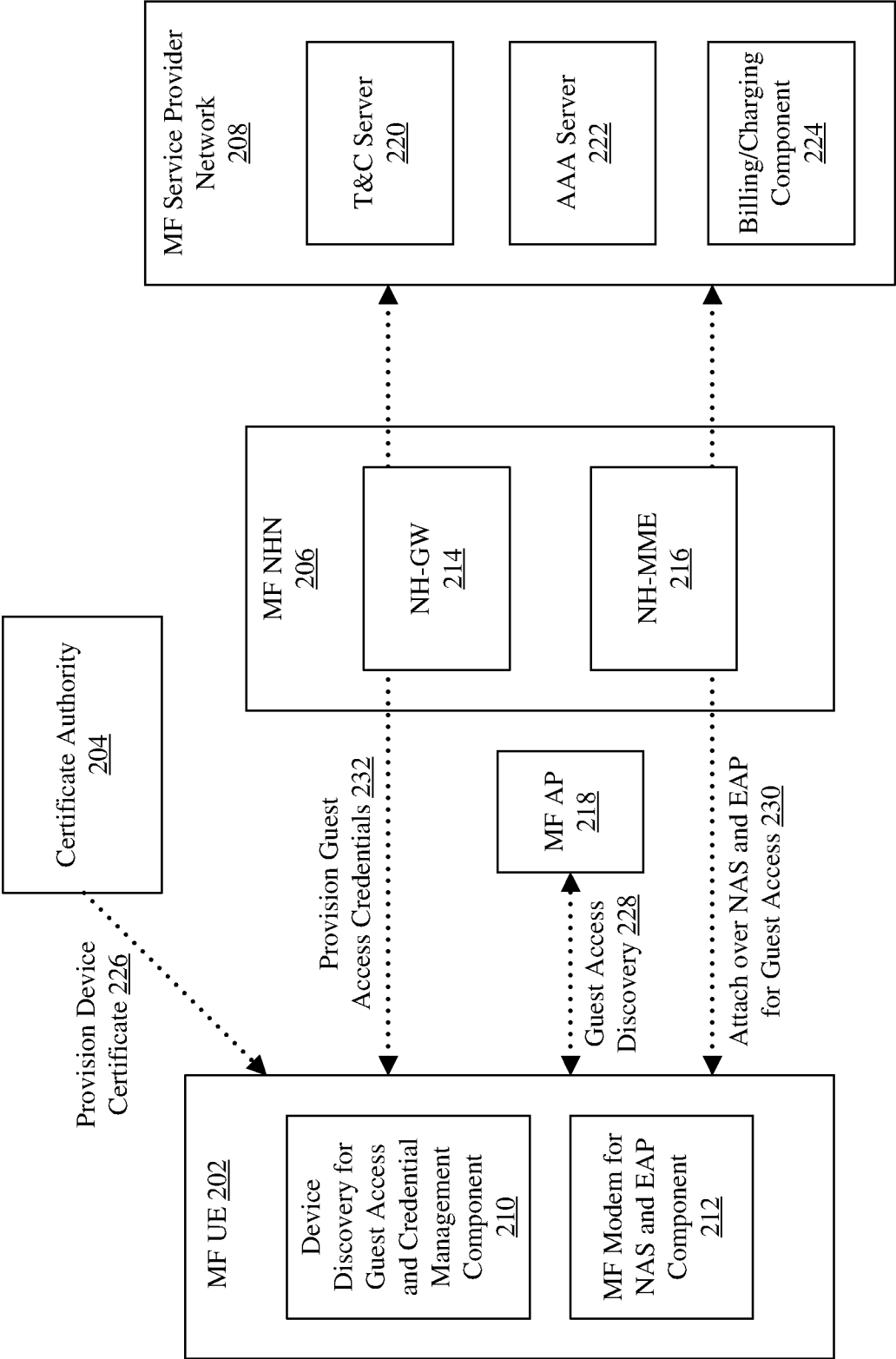


FIG. 3

300

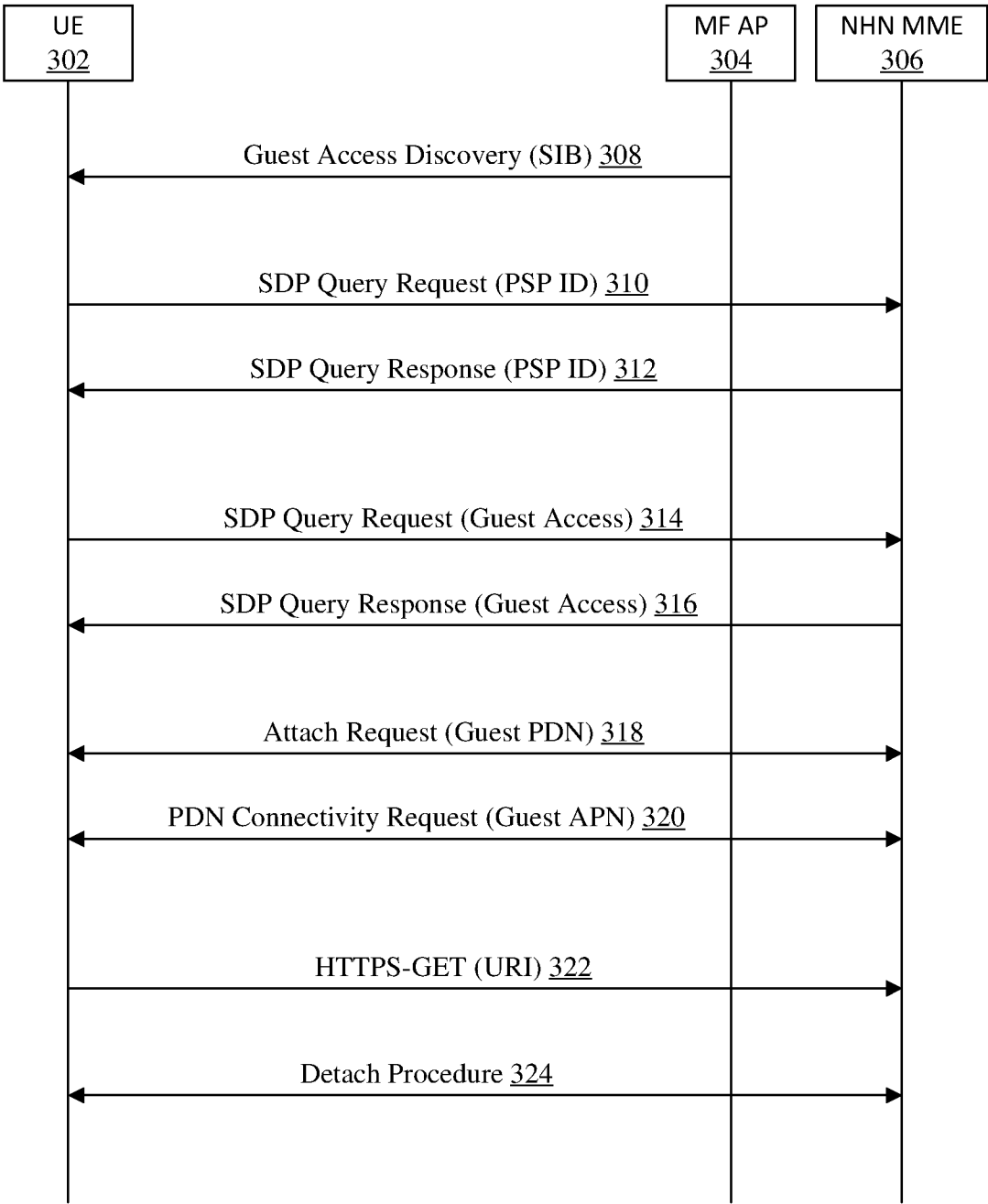


FIG. 4

400

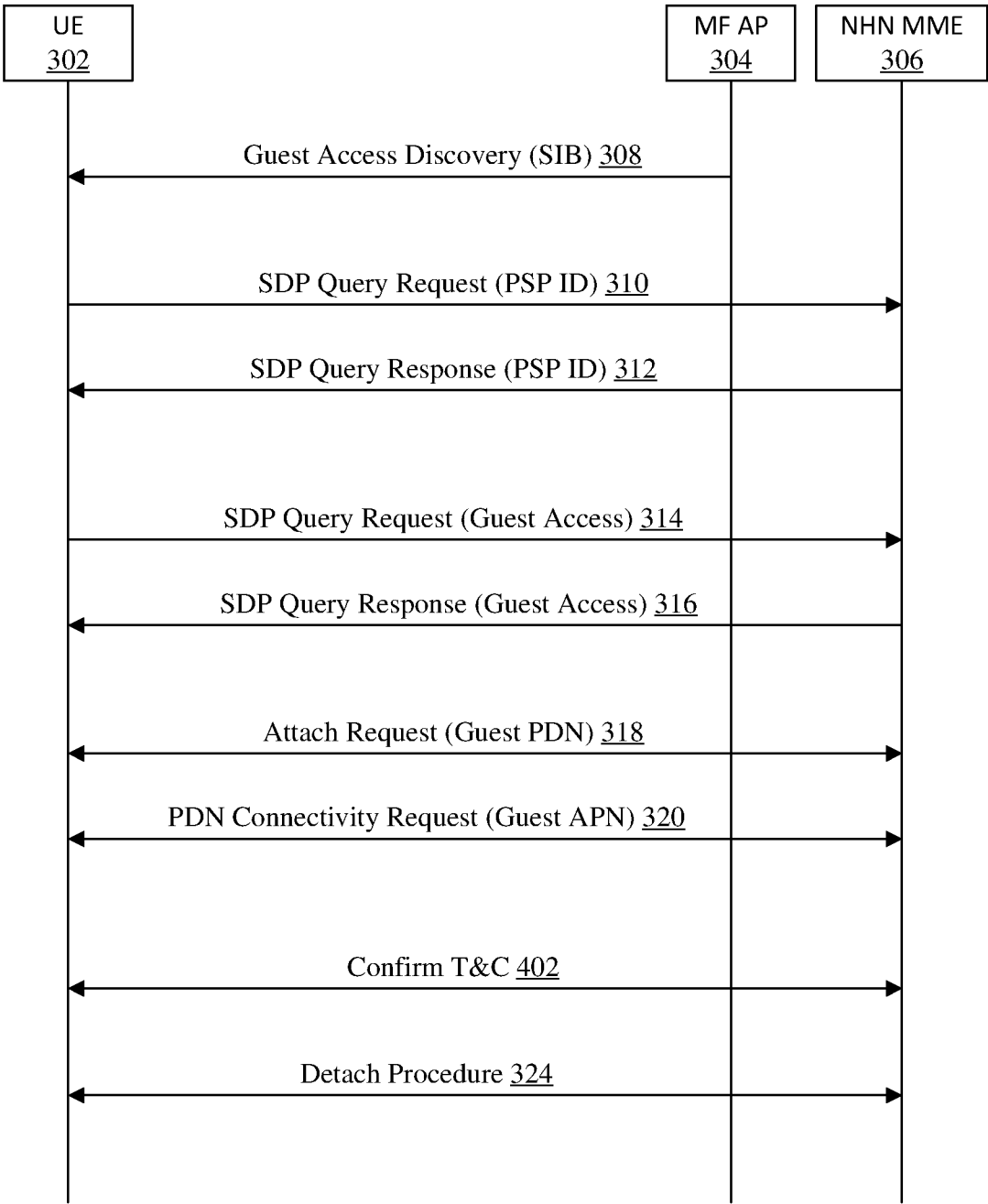


FIG. 5

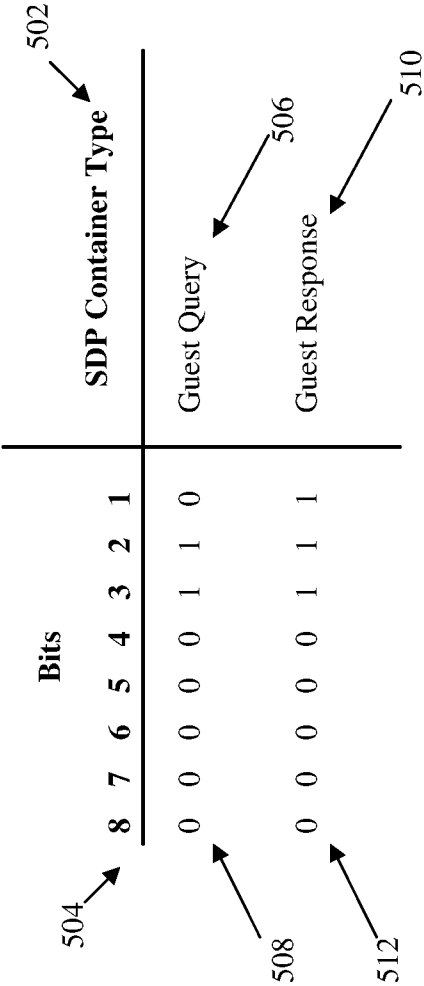


FIG. 6

600

Length of Container <u>602</u>
Length of Guest APN <u>604</u>
Guest APN <u>606</u>
Length of Terms and Conditions Server URI <u>608</u>
Terms and Conditions Server URI <u>610</u>
Length of Guest Access NAI <u>612</u>
Guest NAI <u>614</u>
Length of Guest Credentials <u>616</u>
Guest Credentials <u>618</u>

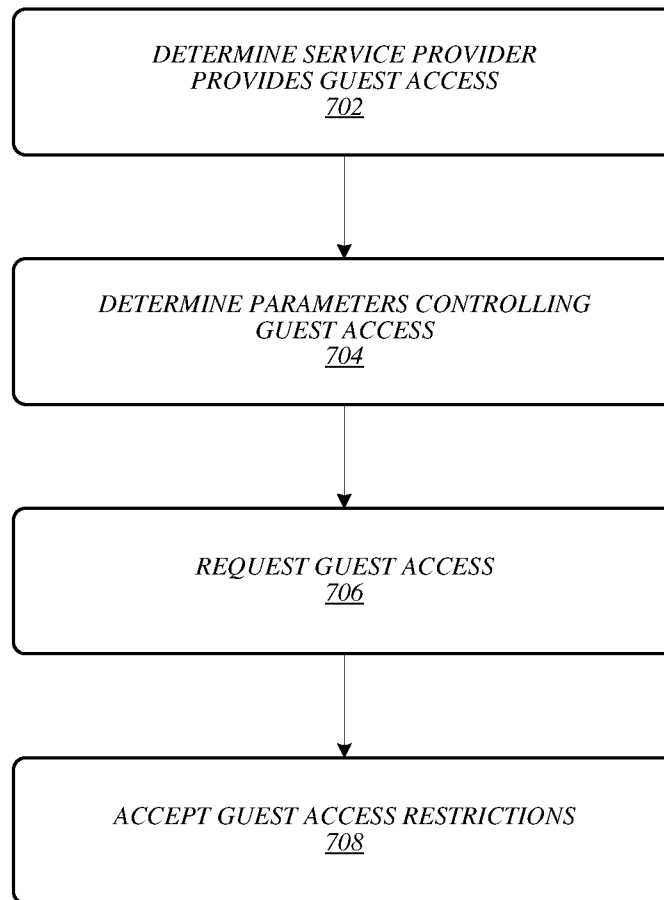
FIG. 7**700**

FIG. 8

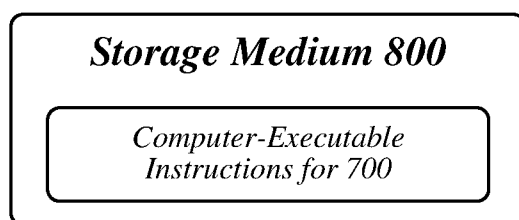


FIG. 9

Device 900

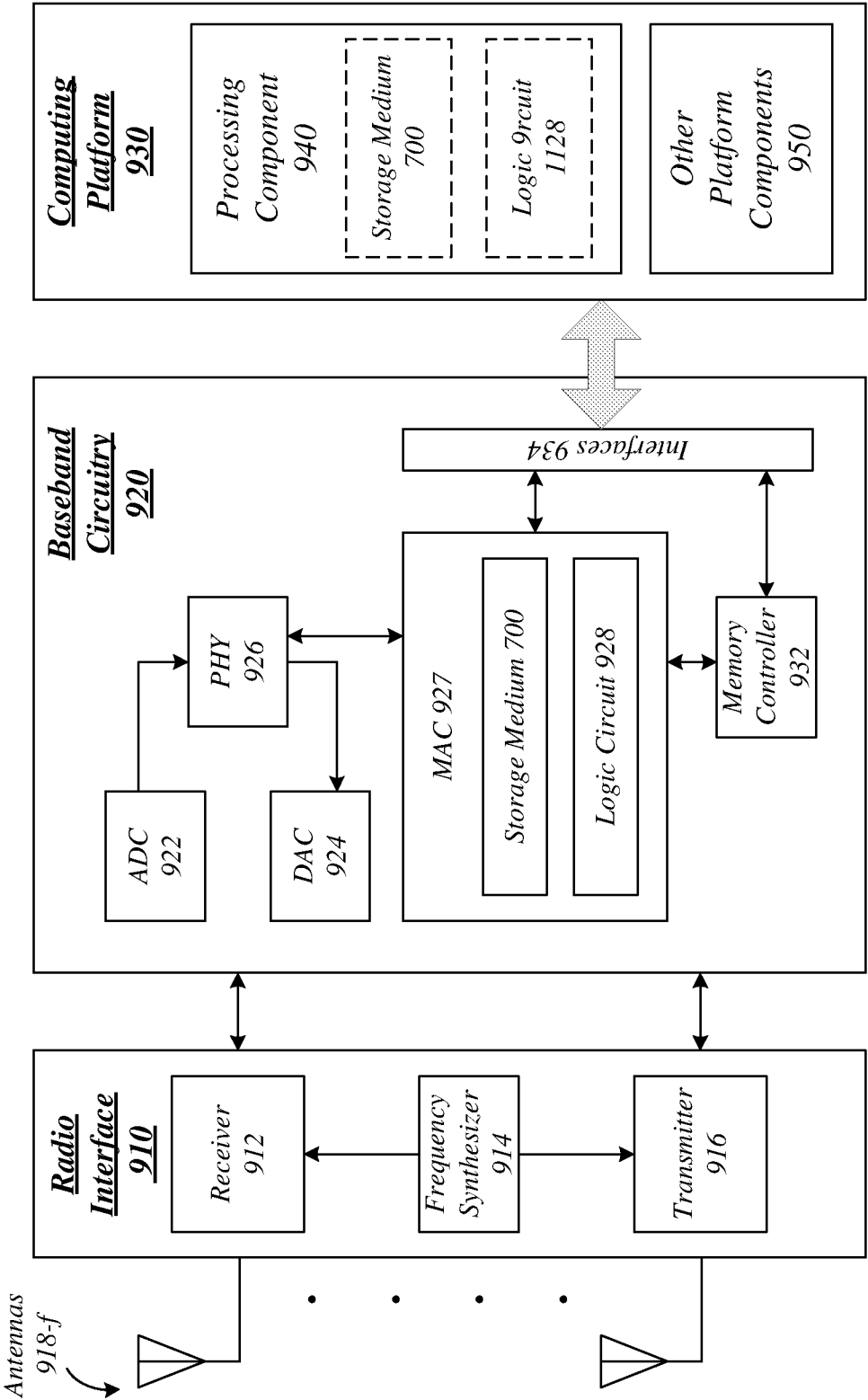


FIG. 10

Broadband Wireless Access System
1000

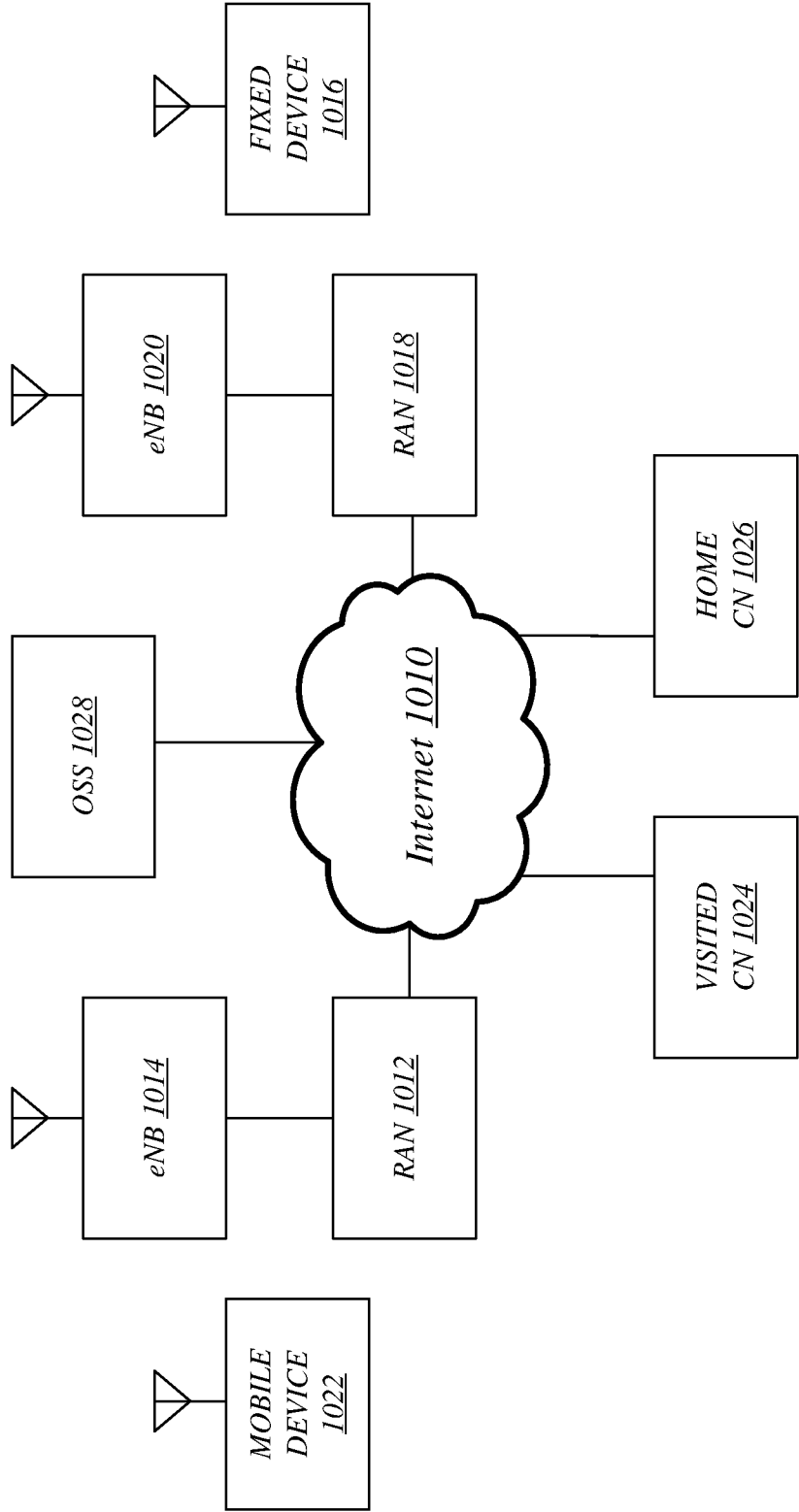
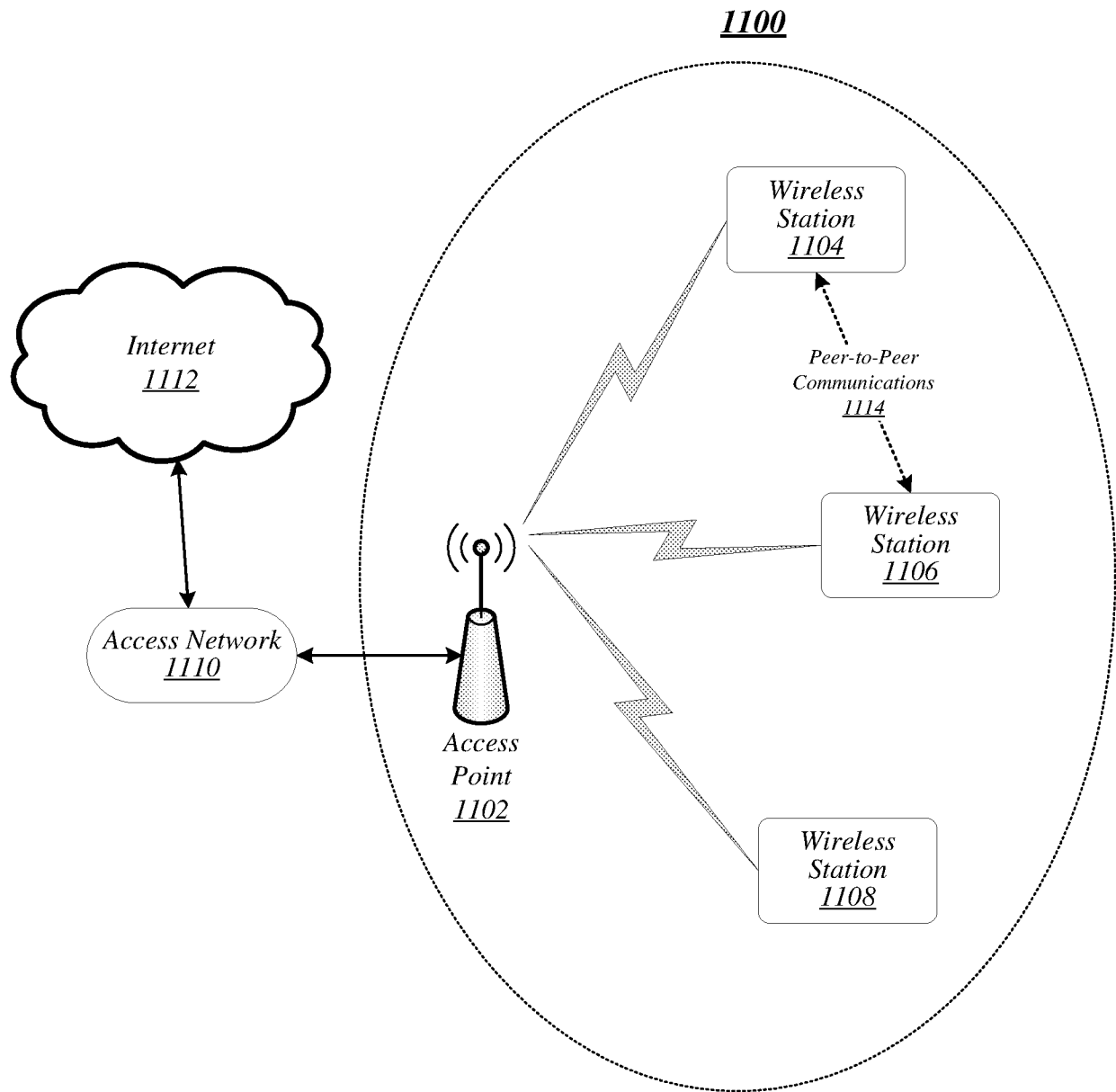


FIG. 11

A. CLASSIFICATION OF SUBJECT MATTER**H04W 48/14(2009.01)i, H04W 48/10(2009.01)i, H04W 48/02(2009.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W 48/14; H04W 28/08; H04W 76/02; H04W 48/16; H04L 29/06; H04W 4/02; H04W 48/10; H04W 48/02

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: neutral, host, network, guest, access, query, protocol, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2017-0034767 A1 (QUALCOMM INCORPORATED) 02 February 2017 See paragraphs [0028], [0035], [0058], [0076], [0078]; claim 14; and figures 1, 7-8.	1-25
Y	US 2016-0183169 A1 (QUALCOMM INCORPORATED) 23 June 2016 See paragraphs [0023], [0052]-[0053], [0087], [0135], [0186], [0188]; and figure 6.	1-25
A	WO 2017-082894 A1 (NOKIA SOLUTIONS AND NETWORKS OY et al.) 18 May 2017 See paragraphs [0027]-[0040]; and figures 1-2.	1-25
A	US 2014-0348062 A1 (REACH HOLDINGS LLC,) 27 November 2014 See paragraphs [0043]-[0068]; and figures 1-2.	1-25
A	US 2017-0164234 A1 (GOOGLE INC.) 08 June 2017 See paragraphs [0036]-[0065]; and figures 1-6D.	1-25



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

19 March 2018 (19.03.2018)

Date of mailing of the international search report

22 March 2018 (22.03.2018)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

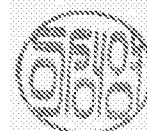


Facsimile No. +82-42-481-8578

Authorized officer

LEE, Seoung Young

Telephone No. +82-42-481-3535



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2017/038875

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2017-0034767 A1	02/02/2017	WO 2017-019285 A2 WO 2017-019285 A3	02/02/2017 20/07/2017
US 2016-0183169 A1	23/06/2016	CN 107113698 A EP 3238484 A1 KR 10-2017-0096121 A WO 2016-105980 A1	29/08/2017 01/11/2017 23/08/2017 30/06/2016
WO 2017-082894 A1	18/05/2017	None	
US 2014-0348062 A1	27/11/2014	US 9363708 B2	07/06/2016
US 2017-0164234 A1	08/06/2017	WO 2017-099961 A1	15/06/2017