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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2020 (27.02.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/037665 A1

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

(21) International Application Number:
PCT/CN2018/102305

(22) International Filing Date:
24 August 2018 (24.08.2018)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(72) Inventors; and

(71) Applicants *(for US only)*: **GUAN, Xuepan** [CN/CN]; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). **PANT, Nitin** [US/US]; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). **UMATT, Bhupesh** [US/US]; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). **TSAI, Shiau-He** [US/US]; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). **GUO, Jiming** [CN/CN]; 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(74) Agent: **NTD PATENT & TRADEMARK AGENCY LIMITED**; 10th Floor, Tower C, Beijing Global Trade Center, 36 North Third Ring Road East, Dongcheng District, Beijing 100013 (CN).

(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).

(54) **Title:** TECHNIQUES FOR USE IN IDENTIFYING A BASE STATION AS AN UNTRUSTED RESOURCE

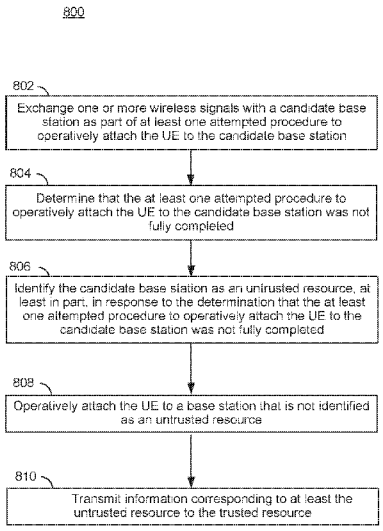

FIG. 8

(57) **Abstract:** Various techniques are provided herein which may be implemented as methods, apparatuses, and/or items of manufacture. In an example, a user equipment (UE) may be configured to exchange one or more wireless signals with a candidate base station as part of at least one attempted procedure to operatively attach the UE to the candidate base station, determine that the attempted procedure to operatively attach the UE to the candidate base station was not fully completed, and identify the candidate base station as an untrusted resource, at least in part, in response to the determination that the attempted procedure was not fully completed. The UE may, subsequently, operatively attach to another base station, e.g., that is not identified as an untrusted resource, and transmit information corresponding to at least the untrusted resource to the base station.

WO 2020/037665 A1

[Continued on next page]

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

TECHNIQUES FOR USE IN IDENTIFYING A BASE STATION AS AN UNTRUSTED RESOURCE

INTRODUCTION

Field of the Disclosure

[0001] Aspects of the disclosure relate generally to methods, apparatuses and items of manufacture for use in wireless communication devices, and more particularly to techniques for identifying a base station as an untrusted resource based, at least in part, on one or more wireless signals exchanged between the base station and at least one user equipment at part of an attempted procedure to operatively attach the user equipment and the base station.

Background

[0002] Attackers may deploy one or more fake base stations (BSs) in mobile communication networks to make unauthorized connections to UEs (e.g., user equipments (UEs), such as smartphones). Such connections may result in theft of valuable information from users, destruction/corruption of data, loss of privacy, and/or unauthorized control of UEs just to name a few concerns.

[0003] Hence, there is a continuing need for techniques to deal with fake BSs.

SUMMARY

[0004] The following presents a simplified summary of some aspects of the disclosure to provide a basic understanding of such aspects. This summary is not an extensive overview of all contemplated features of the disclosure and is intended neither to identify key or critical elements of all aspects of the disclosure nor to delineate the scope of any or all aspects of the disclosure. Its sole purpose is to present various concepts of some aspects of the disclosure in a simplified form as a prelude to the more detailed description that is presented later.

[0005] In accordance with certain aspects, a method is provided for use by a user equipment (UE), the method comprising, at the UE: exchanging one or more wireless signals with a candidate base station as part of at least one attempted procedure to operatively attach the UE to the candidate base station; determining that the at least one attempted procedure to operatively attach the UE to the

candidate base station was not fully completed; identifying the candidate base station as an untrusted resource, at least in part, in response to the determination that the at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed; subsequently, operatively attaching the UE to a base station that is not identified as an untrusted resource; and transmitting, to the base station, information corresponding to at least the untrusted resource.

[0006] In certain implementations, such a UE may support at least a first mode and a second mode of wireless signal transmission and reception. For example, one mode may be UMTS and the other mode may be GSM. In another example, one mode may be 4G and the other mode may be 2G. In certain instances, a first mode may support communication with a trusted resource in a trusted manner but not an untrusted resource. The second mode may support communication with either a trusted resource or an untrusted resource in an untrusted manner. As part of certain techniques presented herein, such a UE, may be configured to (continue to) operate in the first mode rather than switching to the second mode in response to identifying a candidate base station as an untrusted resource.

[0007] In certain implementations, the method may include, at the UE, determining that a candidate base station failed to perform one or more trust-related activities as part of at least one attempted procedure to operatively attach the UE to the candidate base station. For example, a UE may determine that a message transmitted by the candidate base station was received without a security context activated, or without including a cipher, or without including an integrity check, or some combination thereof. In another example, a UE may receive an attachment rejection message from the candidate base station. In certain instances, a UE may receive at least a portion of a list of candidate base stations from at least one other device, identify a candidate base station using the list of candidate base stations at the UE; identify a candidate base station as an untrusted resource based, at least in part, on one or more criteria stored at the UE, maintain at least a portion of the list of candidate base stations at the UE, generate at least a portion of the list of candidate base stations at the UE, or some combination thereof. In certain instances, all or part of a list of candidate base stations may be indicative of a known trusted resource, or a known

untrusted resource, or one or more candidate base stations, or a combination thereof. In certain instances, a UE may identify a corresponding period of time during which the candidate base station is to be identified as an untrusted resource and wherein after the period of time is over the candidate base station may no longer be so identified as an untrusted resource. In certain instances, the one or more wireless signals comprise at least one of a Tracking Area Update (TAU) message, or a Location Area Update (LAU) message, or a Routing Area Update (RAU) message, or some combination thereof.

[0008] In accordance with certain other aspects, a UE may be provided which comprises memory, a transceiver, and a processing unit that is coupled to the memory and the transceiver. Here, for example, the processing unit may be configured to: initiate an exchange, via the transceiver, one or more wireless signals with a candidate base station as part of at least one attempted procedure to operatively attach the UE to the candidate base station; determine that the at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed; identify, in the memory, the candidate base station as an untrusted resource, at least in part, in response to the determination that the at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed; subsequently, operatively attach the UE to a base station that is not identified as an untrusted resource via the transceiver; and initiate transmission of information corresponding to at least the untrusted resource to the base station via the transceiver.

[0009] In accordance with certain other aspects, a method may be provided for use by a network resource, e.g., a base station or the like. The method may comprise: receiving, from a user equipment (UE), information corresponding to a candidate base station that the UE has identified as an untrusted resource based, at least in part, in response to a determination that at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed; maintaining a list of candidate base stations based, at least in part, on the received information; and transmitting at least a portion of the list of candidate base stations.

[0010] In certain implementations, received information may comprise information corresponding to the candidate base station received from a plurality of UEs, wherein the plurality of UEs comprises the UE. In certain

implementations, a network resource may comprise a base station identified by the UE as comprising a trusted network resource. In certain implementations, a least a portion of the list of candidate base stations is indicative of a known trusted resource, or a known untrusted resource, or both.

[0011] In accordance with still other aspects, a network resource may be provided which comprises memory, a transceiver, and a processing unit coupled to the memory and the transceiver. The processing unit of the network resource may be configured to: receive, via the transceiver from a user equipment (UE), information corresponding to a candidate base station that the UE has identified as an untrusted resource based, at least in part, in response to a determination that at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed; maintain a list of candidate base stations based, at least in part, on the received information; and initiate transmission of at least a portion of the list of candidate base stations to one or more other devices.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The accompanying drawings are presented to aid in the description of aspects of the disclosure and are provided solely for illustration of the aspects and not limitations thereof.

[0013] FIG. 1 is a conceptual diagram illustrating an example of a radio access network, in accordance with certain implementations.

[0014] FIG. 2 is a block diagram conceptually illustrating an example of a BS communicating with one or more UEs, in accordance with certain implementations.

[0015] FIG. 3 is a block diagram conceptually illustrating an example of a hardware implementation for a UE, in accordance with certain implementations.

[0016] FIG. 4 is a block diagram conceptually illustrating an example of a hardware implementation for a BS, in accordance with certain implementations.

[0017] FIG. 5 illustrates an example network configuration showing a man-in-the-middle attack, in accordance with certain implementations.

[0018] FIG. 6 illustrates an example network configuration showing a UE under attack by a fake BS, in accordance with certain implementations.

[0019] FIG. 7 illustrates an example attach procedure for a UE in a communication network, in accordance with certain implementations.

[0020] FIG. 8 illustrates an example process for a UE, in accordance with certain implementations.

[0021] FIG. 9 illustrates an example process for a UE, in accordance with certain implementations.

[0022] FIG. 10 illustrates an example process for a trusted resource (e.g., BS), in accordance with certain implementations.

[0023] FIG. 11 illustrates a call-flow diagram for UE and one or more BSs FIG. 8 illustrates an example process for a UE, in accordance with certain implementations.

DETAILED DESCRIPTION

[0024] The detailed description set forth below in connection with the appended drawings is intended as a description of various configurations and is not intended to represent the only configurations in which the concepts described herein may be practiced. The detailed description includes specific details for the purpose of providing a thorough understanding of various concepts. However, it will be apparent to those skilled in the art that these concepts may be practiced without these specific details. In some instances, well known structures and components are shown in block diagram form in order to avoid obscuring such concepts.

[0025] The various concepts presented throughout this disclosure may be implemented across a broad variety of telecommunication systems, network architectures, and communication standards. Referring now to FIG. 1, as an illustrative example without limitation, a schematic illustration of a radio access network 100 is provided.

[0026] The geographic region covered by the radio access network 100 may be divided into a number of cellular regions (cells) that may be uniquely identified by a UE based on an identification broadcasted over a geographical area from a base station (BS). FIG. 1 illustrates macrocells 102, 104, and 106, and a small cell 108, each of which may include one or more sectors. Hence, a sector may comprise a sub-area of a cell. In certain implementations, all sectors within a cell may be served by the same BS. A radio link within a sector may be identified by

a logical identification corresponding to that sector. In certain implementations, a sector may be served by one or more group(s) of antennas with the antennas responsible for communication with UEs in an applicable portion of the cell/sector.

[0027] A BS may comprise a network element in a radio access network responsible for radio transmission and reception (e.g., exchanging wireless signals) in one or more cells with one or more UEs. By way of some none limiting examples, a BS may also be referred to by those skilled in the art as base transceiver station (BTS), a radio base station, a radio transceiver, a transceiver function, a basic service set (BSS), an extended service set (ESS), an access point (AP), a Node B (NB), an eNode B (eNB), a gNode B (gNB), or some other suitable terminology.

[0028] In FIG. 1, two high-power BSs 110 and 112 are shown in cells 102 and 104; and a third high-power BS 114 is shown controlling a remote radio head (RRH) 116 in cell 106. That is, a BS may comprise an integrated antenna or may be coupled to an antenna or RRH, e.g., via feeder cables, etc. In the illustrated example, cells 102, 104, and 106 may be referred to as macrocells, as the high-power BSs 110, 112, and 114 may be configured to support cells having large size(s). Further, a low-power BS 118 is shown in the small cell 108 (e.g., a microcell, picocell, femtocell, home BS, home Node B, home eNode B, etc.) which may overlap with one or more macrocells. In this example, the cell 108 may be referred to as a small cell, as the low-power BS 118 may support a cell having a relatively small size. Cell sizing may vary according to system design as well as component constraints. It is to be understood that the radio access network 100 may include any number of wireless BSs and cells. Further, a relay node may be deployed to extend the size or coverage area of a given cell. The BSs 110, 112, 114, 118 provide wireless access points to a core network for any number of mobile apparatuses.

[0029] FIG. 1 further includes a quadcopter or drone 120, which may be configured to function as a BS. That is, in some examples, a cell may not necessarily be stationary, and the geographic area of the cell may move according to the location of a mobile BS such as the quadcopter 120.

[0030] In general, BSs may include a backhaul interface for communication with a backhaul portion of the network. The backhaul may provide a link between a BS and a core network, and in some examples, the backhaul may provide

interconnection between the respective BSs. The core network is a part of a wireless communication system that is generally independent of the radio access technology used in the radio access network. Various types of backhaul interfaces may be employed, such as a direct physical connection, a virtual network, or the like using any suitable transport network. Some BSs may be configured as integrated access and backhaul (IAB) nodes, where the wireless spectrum may be used both for access links (i.e., wireless links with UEs), and for backhaul links. This scheme is sometimes referred to as wireless self-backhauling. By using wireless self-backhauling, rather than requiring each new BS deployment to be outfitted with its own hard-wired backhaul connection, the wireless spectrum utilized for communication between the BS and UE may be leveraged for backhaul communication, enabling fast and easy deployment of highly dense small cell networks.

[0031] The radio access network 100 is illustrated supporting wireless communication for multiple mobile apparatuses (also referred to as UEs). A mobile apparatus is commonly referred to as user equipment (UE) in standards and specifications promulgated by the 3rd Generation Partnership Project (3GPP), but may also be referred to by those skilled in the art as a mobile station (MS), a subscriber station, a mobile unit, a subscriber unit, a wireless unit, a remote unit, a mobile device, a wireless device, a wireless communications device, a remote device, a mobile subscriber station, an access terminal (AT), a mobile terminal, a wireless terminal, a remote terminal, a handset, a terminal, a user agent, a mobile client, a client, or some other suitable terminology. A UE may be an apparatus that provides a user with access to network services.

[0032] In certain instances, a UE may comprise a “mobile” apparatus which may be moved about continuously, or from time to time, or may be provisioned in a more stationary state. The term mobile apparatus or mobile device may broadly refer to a diverse array of devices and technologies. For example, some non-limiting examples of a mobile apparatus include a mobile, a cellular (cell) phone, a smart phone, a session initiation protocol (SIP) phone, a laptop, a personal computer (PC), a notebook, a netbook, a smartbook, a tablet, a personal digital assistant (PDA), and a broad array of embedded systems, e.g., corresponding to an “Internet of things” (IoT). A mobile apparatus may additionally be an automotive or other transportation vehicle, a remote sensor or actuator, a robot

or robotics device, a satellite radio, a global positioning system (GPS) device, an object tracking device, a drone, a multi-copter, a quad-copter, a remote control device, a consumer and/or wearable device, such as eyewear, a wearable camera, a virtual reality device, a smart watch, a health or fitness tracker, a digital audio player (e.g., MP3 player), a camera, a game console, etc. A mobile apparatus may additionally be a digital home or smart home device such as a home audio, video, and/or multimedia device, an appliance, a vending machine, intelligent lighting, a home security system, a smart meter, etc. A mobile apparatus may additionally be a smart energy device, a security device, a solar panel or solar array, a municipal infrastructure device controlling electric power (e.g., a smart grid), lighting, water, etc.; an industrial automation and enterprise device; a logistics controller; agricultural equipment; military defense equipment, vehicles, aircraft, ships, and weaponry, etc. Still further, a mobile apparatus may provide for connected medicine or telemedicine support, i.e., health care at a distance. Telehealth devices may include telehealth monitoring devices and telehealth administration devices, whose communication may be given preferential treatment or prioritized access over other types of information, e.g., in terms of prioritized access for transport of critical service data, and/or relevant QoS for transport of critical service data.

[0033] Within the radio access network 100, the cells may include UEs that may be in communication with one or more sectors of each cell. For example, UEs 122 and 124 may be in communication with BS 110; UEs 126 and 128 may be in communication with BS 112; UEs 130 and 132 may be in communication with BS 114 by way of RRH 116; UE 134 may be in communication with low-power BS 118; and UE 136 may be in communication with mobile BS 120. Here, each BS 110, 112, 114, 118, and 120 may be configured to provide an access point to a core network (not shown) for all the UEs in the respective cells. Transmissions from a BS (e.g., BS 110) to one or more UEs (e.g., UEs 122 and 124) may be referred to as downlink (DL) transmission, while transmissions from a UE (e.g., UE 122) to a BS may be referred to as uplink (UL) transmissions. In accordance with certain aspects of the present disclosure, the term downlink may refer to a point-to-multipoint transmission originating at a BS 202 (see FIG. 2). Another way to describe this scheme may be to use the term broadcast channel multiplexing.

In accordance with further aspects of the present disclosure, the term uplink may refer to a point-to-point transmission originating at UE.

[0034] In some examples, a mobile network node (e.g., quadcopter 120) may be configured to function as a UE. For example, the quadcopter 120 may operate within cell 102 by communicating with BS 110. In some aspects of the disclosure, two or more UEs (e.g., UEs 126 and 128) may communicate with each other using peer to peer (P2P) or sidelink signals 127 without relaying that communication through a BS (e.g., BS 112).

[0035] In the radio access network 100, the ability for a UE to communicate while moving, independent of its location, is referred to as mobility. The various physical channels between the UE and the radio access network are generally set up, maintained, and released under the control of an access and mobility management function (AMF), which may include a security context management function (SCMF) that manages the security context for both the control plane and the user plane functionality, and a security anchor function (SEAF) that performs authentication. In various aspects of the disclosure, a radio access network 100 may utilize DL-based mobility or UL-based mobility to enable mobility and handovers (i.e., the transfer of a UE's connection from one radio channel to another). In a network configured for DL-based mobility, during a call with a BS, or at any other time, a UE may monitor various parameters of the signal from its serving cell as well as various parameters of neighboring cells. Depending on the quality of these parameters, the UE may maintain communication with one or more of the neighboring cells. During this time, if the UE moves from one cell to another, or if signal quality from a neighboring cell exceeds that from the serving cell for a given amount of time, the UE may undertake a handoff or handover from the serving cell to the neighboring (target) cell. For example, UE 124 (illustrated as a vehicle, although any suitable form of UE may be used) may move from the geographic area corresponding to its serving cell 102 to the geographic area corresponding to a neighbor cell 106. When the signal strength or quality from the neighbor cell 106 exceeds that of its serving cell 102 for a given amount of time, the UE 124 may transmit a reporting message to its serving BS 110 indicating this condition. In response, the UE 124 may receive a handover command, and the UE may undergo a handover to the cell 106.

[0036] In a network configured for UL-based mobility, UL reference signals from each UE may be utilized by the network to select a serving cell for each UE. In some examples, the BSs 110, 112, and 114/116 may broadcast unified synchronization signals (e.g., unified Primary Synchronization Signals (PSSs), unified Secondary Synchronization Signals (SSSs) and unified Physical Broadcast Channels (PBCH)). The UEs 122, 124, 126, 128, 130, and 132 may receive the unified synchronization signals, derive the carrier frequency and slot timing from the synchronization signals, and in response to deriving timing, transmit an uplink pilot or reference signal. The uplink pilot signal transmitted by a UE (e.g., UE 124) may be concurrently received by two or more cells (e.g., BSs 110 and 114/116) within the radio access network 100. Each of the cells may measure a strength of the pilot signal, and the radio access network (e.g., one or more of the BSs 110 and 114/116 and/or a central node within the core network) may determine a serving cell for the UE 124. As the UE 124 moves through the radio access network 100, the network may continue to monitor the uplink pilot signal transmitted by the UE 124. When the signal strength or quality of the pilot signal measured by a neighboring cell exceeds that of the signal strength or quality measured by the serving cell, the network 100 may handover the UE 124 from the serving cell to the neighboring cell, with or without informing the UE 124.

[0037] Although the synchronization signal transmitted by the BSs 110, 112, and 114/116 may be unified, the synchronization signal may not identify a particular cell, but rather may identify a zone of multiple cells operating on the same frequency and/or with the same timing. The use of zones in 5G networks or other next generation communication networks may enable an uplink-based mobility framework that may improve the efficiency of the UE and the network. For example, in certain instances the number of mobility messages that may need to be exchanged between a UE and the network may be reduced at times.

[0038] In various implementations, the air interface in the radio access network 100 may utilize licensed spectrum, unlicensed spectrum, or shared spectrum. Licensed spectrum provides for exclusive use of a portion of the spectrum, generally by virtue of a mobile network operator purchasing a license from a government regulatory body. Unlicensed spectrum provides for shared use of a portion of the spectrum without need for a government-granted license. While compliance with some technical rules is generally still required to access

unlicensed spectrum, generally, any operator or device may gain access. Shared spectrum may fall between licensed and unlicensed spectrum, wherein technical rules or limitations may be required to access the spectrum, but the spectrum may still be shared by multiple operators and/or multiple RATs. For example, the holder of a license for a portion of licensed spectrum may provide licensed shared access (LSA) to share that spectrum with other parties, e.g., with suitable licensee-determined conditions to gain access.

[0039] In some examples, access to the air interface may be scheduled, wherein a BS allocates resources for communication among some or all devices and equipment within its service area or cell. Within the present disclosure, as discussed further below, the BS may be responsible for scheduling, assigning, reconfiguring, and releasing resources for one or more UEs. That is, for scheduled communication, UEs or scheduled entities utilize resources allocated by the BS.

[0040] In some examples, a given UE may be capable, to at least some extent, to function as a BS, e.g., possibly scheduling resources for one or more scheduled entities (e.g., one or more other UEs). In other examples, sidelink signals may be used between UEs (e.g., either with scheduling from a BS or without necessarily relying on scheduling or control information from a BS). For example, UE 138 is illustrated communicating with UEs 140 and 142. In some examples, the UE 138 is functioning as a BS or a primary sidelink device, and UEs 140 and 142 may function as a UE or a non-primary (e.g., secondary) sidelink device. In still another example, a UE may function as a BS in a device-to-device (D2D), peer-to-peer (P2P), or vehicle-to-vehicle (V2V) network, and/or in a mesh network. In a mesh network example, UEs 140 and 142 may optionally communicate directly with one another in addition to communicating with the BS 138.

[0041] Thus, in a wireless communication network with scheduled access to time–frequency resources and having a cellular configuration, a P2P configuration, or a mesh configuration, a BS and one or more UEs may communicate utilizing the scheduled resources. Referring now to FIG. 2, a block diagram illustrates a BS 202 and a plurality of UEs 204 (e.g., 204a and 204b). Here, the BS 202 may correspond to a BS 110, 112, 114, and/or 118. In additional examples, the BS 202 may correspond to a UE 138, the quadcopter

120, or any other suitable node in the radio access network 100. Similarly, in various examples, the UE 204 may correspond to the UE 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, and 142, or any other suitable node in the radio access network 100.

[0042] As illustrated in FIG. 2, the BS 202 may broadcast traffic 206 to one or more UEs 204 (the traffic may be referred to as downlink traffic). Broadly, the BS 202 is a node or device responsible for scheduling traffic in a wireless communication network, including the downlink transmissions and, in some examples, uplink traffic 210 from one or more UEs to the BS 202. Broadly, the UE 204 is a node or device that receives control information, including but not limited to scheduling information (e.g., a grant), synchronization or timing information, or other control information from another entity in the wireless communication network such as the BS 202.

[0043] In some examples, UEs such as a first UE 204a and a second UE 204b may utilize sidelink signals for direct D2D communication. Sidelink signals may include sidelink traffic 214 and sidelink control 216. In some aspects, the sidelink traffic 214 and/or sidelink control 216 may be communicated via a PC5 interface. In such aspects, the PC5 interface may support multicarrier transmissions and/or carrier aggregation (CA). For example, when LTE-based vehicle-to-everything (V2X) communication protocols are implemented by the first UE 204a, the first UE 204a may be allowed to use multiple carriers for the transmission of V2X messages.

[0044] Sidelink control information 216 may in some examples include a request signal, such as a request-to-send (RTS), a source transmit signal (STS), and/or a direction selection signal (DSS). The request signal may provide for a UE 204 to request a duration of time to keep a sidelink channel available for a sidelink signal. Sidelink control information 216 may further include a response signal, such as a clear-to-send (CTS) and/or a destination receive signal (DRS). The response signal may provide for the UE 204 to indicate the availability of the sidelink channel, e.g., for a requested duration of time. An exchange of request and response signals (e.g., handshake) may enable different UEs performing sidelink communications to negotiate the availability of the sidelink channel prior to communication of the sidelink traffic information 214.

[0045] The air interface in the radio access network 100 may utilize one or more duplexing algorithms. Duplex refers to a point-to-point communication link where both endpoints may communicate with one another in both directions. Full duplex means both endpoints may simultaneously communicate with one another. Half duplex means only one endpoint may send information to the other at a time. In a wireless link, a full duplex channel generally relies on physical isolation of a transmitter and receiver, and suitable interference cancellation technologies. Full duplex emulation is frequently implemented for wireless links by utilizing frequency division duplex (FDD) or time division duplex (TDD). In FDD, transmissions in different directions operate at different carrier frequencies. In TDD, transmissions in different directions on a given channel are separated from one another using time division multiplexing. That is, at some times the channel is dedicated for transmissions in one direction, while at other times the channel is dedicated for transmissions in the other direction, where the direction may change very rapidly, e.g., several times per slot.

[0046] In order for transmissions over the radio access network 100 to obtain a low block error rate (BLER) while still achieving very high data rates, channel coding may be used. That is, wireless communication may generally utilize a suitable error correcting block code. In a typical block code, an information message or sequence is split up into code blocks (CBs), and an encoder (e.g., a CODEC) at the transmitting device then mathematically adds redundancy to the information message. Exploitation of this redundancy in the encoded information message may improve the reliability of the message, enabling correction for any bit errors that may occur due to the noise.

[0047] In 5G NR specifications, user data may be coded using quasi-cyclic low-density parity check (LDPC) with two different base graphs: one base graph is used for large code blocks and/or high code rates, while the other base graph is used otherwise. Control information and the physical broadcast channel (PBCH) are coded using Polar coding, based on nested sequences. For these channels, puncturing, shortening, and repetition are used for rate matching.

[0048] However, those of ordinary skill in the art will understand that aspects of the present disclosure may be implemented utilizing any suitable channel code. Various implementations of BS 202 and UE 204 may include suitable hardware

and capabilities (e.g., an encoder, a decoder, and/or a CODEC) to utilize one or more of these channel codes for wireless communication.

[0049] The air interface in the radio access network 100 may utilize one or more multiplexing and multiple access algorithms to enable simultaneous communication of the various devices. For example, 5G NR specifications provide multiple access for uplink (UL) or reverse link transmissions from UEs 122 and 124 to BS 110, and for multiplexing for downlink (DL) or forward link transmissions from BS 110 to one or more UEs 122 and 124, utilizing orthogonal frequency division multiplexing access (OFDM) with a cyclic prefix (CP). In addition, for UL transmissions, 5G NR specifications provide support for discrete Fourier transform-spread-OFDM (DFT-s-OFDM) with a CP (also referred to as single-carrier FDMA (SC-FDMA)). However, within the scope of the present disclosure, multiplexing and multiple access are not limited to the above schemes and may be provided utilizing time division multiple access (TDMA), code division multiple access (CDMA), frequency division multiple access (FDMA), sparse code multiple access (SCMA), resource spread multiple access (RSMA), or other suitable multiple access schemes. Further, multiplexing downlink (DL) or forward link transmissions from the BS 110 to UEs 122 and 124 may be provided utilizing time division multiplexing (TDM), code division multiplexing (CDM), frequency division multiplexing (FDM), orthogonal frequency division multiplexing (OFDM), sparse code multiplexing (SCM), or other suitable multiplexing schemes.

[0050] FIG. 3 is a block diagram illustrating an example of a hardware implementation for a UE 300 employing a processing system 314. For example, the UE 300 may be representative of a UE as illustrated in any one or more of drawings herein.

[0051] UE 300 may be implemented with a processing system 314 that includes one or more processing units represented by processors 304. Examples of processors 304 include microprocessors, microcontrollers, digital signal processors (DSPs), field programmable gate arrays (FPGAs), programmable logic devices (PLDs), state machines, gated logic, discrete hardware circuits, and other suitable hardware configured to perform the various functionality described throughout this disclosure. In various examples, the UE 300 may be configured to perform any one or more of the functions described herein. That is, the processor 304, as utilized in the UE 300, may be used to implement any one or

more of the processes and procedures described below and illustrated in FIG. 21.

[0052] In this example, the processing system 314 may be implemented with a bus architecture, represented generally by the bus 302. The bus 302 may include any number of interconnecting buses and bridges depending on the specific application of the processing system 314 and the overall design constraints. The bus 302 communicatively couples together various circuits including one or more processors (represented generally by the processor 304), a memory 305, and computer-readable media (represented generally by the computer-readable medium 306). The bus 302 may also link various other circuits such as timing sources, peripherals, voltage regulators, and power management circuits, which are well known in the art, and therefore, will not be described any further. A bus interface 308 provides an interface between the bus 302 and a transceiver 310. The transceiver 310 provides a communication interface or means for communicating with various other apparatus over a transmission medium. Depending upon the nature of the apparatus, a user interface 312 (e.g., keypad, display, touch screen, speaker, microphone, joystick, camera, biometric interface, etc.) may also be provided.

[0053] In some aspects of the disclosure, the processor 304 may, at times, be configured to provide a fake cell detection function 340 that may be configured, at least in part, to implement all or part of the various techniques presented herein, for example, to possibly identify a candidate BS as an untrusted resource, and to act in some manner based on such an identification. For example, a candidate BS may be identified as an untrusted resource in response, at least in part, to a determination that one or more attempted procedures to operatively attach the UE to the candidate BS way not fully completed for some reason. Thus, in certain instances, a malfunctioning or busy candidate BS may be identified as an untrusted resource following a failed attach procedure or the like. In another example, a rogue or otherwise intentionally provisioned fake BS may by identified as an untrusted resource following a failed attach procedure or the like. As described in greater detail herein, in certain example implementations, an indication that a candidate BS is an untrusted resource may eventually be communicated in some manner to another base station (e.g., a trusted resource) and possibly considered by that or other network resources in managing the

network. For example, a list of candidate BSs (e.g., "white-list," "black-list," "neighborhood list," or the like or some combination thereof, may be actively or periodically maintained, and such list(s) or portions thereof may be shared in some manner, e.g., with one or more UEs. Hence, by way of example, a list of candidate BSs 342 is illustrated within processor 304 to represent that all or part of such may be accessible or otherwise obtained by processor 304, e.g., possibly via a memory 305, possibly via a transceiver 310, and/or a computer-readable medium 306. In some example implementations, all or part of a list of candidate BSs 342 may be received by the UE from one or more other devices. In some example implementations, all or part of a list of candidate BSs 342 may be maintained, modified, generated, or otherwise affected by the UE, e.g., as part of face cell detection function 340.

[0054] In certain implementations, a list of candidate BSs 342 may be employed to by a network resource to inform UEs about one or more untrusted cells that a UE should avoid or may be restricted from using, e.g., to camp-on, for handover, and/or possibly for signal measurements, or reselection, or redirection, etc. By way of an example, in certain instances, a network resource may apply/adjust a penalty value or the like indicated in a list of candidates that may affect a UE's behavior with regard to untrusted resources and/or possibly untrusted signaling frequencies, or the like. Conversely, after some period of time, or perhaps based on a lack of further reports, a network resource may remove an untrusted resource from a list of candidate BSs identified as untrusted resources. In certain instances, altering a trust-related status may comprise altering a penalty value or the like that may be indicated in a list of candidates.

[0055] In certain aspects of the disclosure, processor 304 may include detection criteria 344 that may comprise information that may be considered by fake cell detection function 340 in determining whether to identify a candidate BS as an untrusted resource. In certain instances, detection criteria 344 may comprise data and/or instructions, and may be obtained via memory 305, computer-readable medium 306, transceiver 310, a user interface 312, or the like or some combination thereof. In certain instances, all or part of detection criteria 344 may be obtained from one or more other devices. Detection criteria 344 may comprise one or more criterion for consideration. For example, a detection criterion may correspond to an event that may be detectable, at least in part, by fake cell

detection function 340 as part of an attempted attachment procedure between the UE 304 and a candidate BS (not shown). A detection criterion may be indicative in some manner that a particular event may or may not be considered proper as part of an attempted and/or successful attachment procedure. Thus, for example, information conveyed in one or more wireless signals received from a candidate base station as part of one or more attempted procedures to operatively attach the UE to the candidate base station may inform decision logic of fake cell detection function 340, at least in part, whether or not the candidate base station may be operating as a trusted resource or an untrusted resource. Several potential examples for detection criteria 344 are described in greater detail herein. For example, detection criteria 344 may be indicative of all or part of an expected (proper) call flow and/or protocol process that may be indicative of a trusted resource. Hence, detection criteria 344 may be used to detect a deviation or other anomalous behavior of a candidate BS by detection criteria 344. In certain instances, detection criteria 344 may determine that a candidate BS failed to perform one or more trust-related activities as part of at least one attempted procedure to operatively attach the UE to the candidate base station. For example, if a candidate BS transmits the wrong information in a message, or fails to transmit a particular message or response therein, or transmits an unexpected message, or transmits a message without a security context activated (e.g., including cipher, integrity check, etc.), then the candidate BS may be identified as an untrusted resource.

[0056] In some aspects of the disclosure, the processor 304 may include detection information 346 corresponding to fake cell detection function 340, and possibly list of candidate base stations 342. All or part of detection information 346 may be stored in memory 305, computer-readable medium 306, or both, and accessed or otherwise obtained by processor 304. Detection information 344 may, for example, be indicative of a candidate BS identified as an untrusted resource by fake cell detection function 340. Hence, detection information 344 may comprise one or more (possibly unique) identifiers used by the untrusted resource, signal-related information for signals transmitted by the untrusted resource (e.g., RSRP, RSRQ,, RSSI, EARFCN, frequency, etc.), position/location information corresponding to the untrusted resource and/or UE (e.g., TAC, LAC, TA, coordinates, PCID, sector ID, beam ID, etc.), timing-related information

(detection time, timer or period of time information, etc.), previous BS connectivity information (e.g., relating to one or more other BSs identified as trusted resource(s), other logged network access information, specific UE related information (e.g., capabilities, make/model, etc.), and/or the like or some combination thereof just to name a few examples.

[0057] With such examples and others in mind, in certain implementations, detection information 346 may comprise some information that may be used by the UE, at least in part, to possibly affect its behavior in some manner (e.g., avoid accessing an untrusted resource), affect list of candidate BSs 342 (e.g., add an untrusted resource to a "blacklist", add a trusted resource to a "whitelist", etc.), transmit a report to one or more other devices (e.g., another BS that is identified as a trusted resource) based upon and/or comprising all or part of the detection information 346 regarding one or more untrusted resources (and/or possibly one or more trusted resources), or the like or some combination thereof, just to name a few examples.

[0058] In some example implementations, processor 304 may also be responsible, at least in part, for managing the bus 302 and general processing, including the execution of software stored on the computer-readable medium 306. The software, when executed by the processor 304, causes the processing system 314 to perform the various functions described below for any particular apparatus. The computer-readable medium 306 and the memory 305 may also be used for storing data that is manipulated by the processor 304 when executing software.

[0059] One or more processors 304 in the processing system may execute software. Software shall be construed broadly to mean instructions, instruction sets, code, code segments, program code, programs, subprograms, software modules, applications, software applications, software packages, routines, subroutines, objects, executables, threads of execution, procedures, functions, etc., whether referred to as software, firmware, middleware, microcode, hardware description language, or otherwise. The software may reside on a computer-readable medium 306. The computer-readable medium 306 may be a non-transitory computer-readable medium. A non-transitory computer-readable medium includes, by way of example, a magnetic storage device (e.g., hard disk, floppy disk, magnetic strip), an optical disk (e.g., a compact disc (CD) or a digital

versatile disc (DVD)), a smart card, a flash memory device (e.g., a card, a stick, or a key drive), a random access memory (RAM), a read only memory (ROM), a programmable ROM (PROM), an erasable PROM (EPROM), an electrically erasable PROM (EEPROM), a register, a removable disk, and any other suitable medium for storing software and/or instructions that may be accessed and read by a computer. The computer-readable medium 306 may reside in the processing system 314, external to the processing system 314, or distributed across multiple entities including the processing system 314. The computer-readable medium 306 may be embodied in a computer program product. By way of example, a computer program product may include a computer-readable medium in packaging materials. Those skilled in the art will recognize how best to implement the described functionality presented throughout this disclosure depending on the particular application and the overall design constraints imposed on the overall system.

[0060] In one or more examples, the computer-readable storage medium 306 may comprise detection capability 350 that may comprise instructions and/or data for use, at least in part, in configuring processor 340 to provide fake cell detection function 340, or access and/or affect list of candidate BSs 342, or access and/or affect detection criteria 344, to access and/or affect detection information 346, or access, affect and/or implement all or part of BS selection function 348.

[0061] Although not illustrated in FIG. 3 for simplification purposes, it should be understood that UE 300 may comprise additional components that may be of use in some other context of the UE. For example, UE 300 may comprise a position location capability, such as, may be provided by a global navigation satellite system (GNSS) receiver (not shown) or the like. A GNSS or other like capability may, in certain implementations, provide UE-related location information that may be useful to UE 300 (e.g., to processor 304, processing system 314, etc.) to affect fake cell detection function 340, or list of candidate BSs 342, or detection criteria 344, or detection information 346, or BS selection function 348, or some combination thereof.

[0062] FIG. 4 is a conceptual diagram illustrating an example of at least a partial hardware implementation for an exemplary BS 400 employing a processing system 414. In accordance with various aspects of the disclosure, an element, or any portion of an element, or any combination of elements may be implemented

with a processing system 414 that includes one or more processors 404 (e.g., one or more processing units). For example, the BS 400 may be a BS or candidate BS as illustrated in any of the other drawing presented by way of example herein.

[0063] The processing system 414 while appearing similar to processing system 314 illustrated in FIG. 3, e.g., by including a bus interface 408, a bus 402, memory 405, a processor 404, and a computer-readable medium 406, will actually be significantly different in certain implementations. This of course is well known. However, as mentioned there may be implementations wherein some UE may be configured to act as a BS in some fashion, and hence processing system 414 may be more similar to processing system 314. Furthermore, as shown in this example, BS 400 may include a user interface 412, or a transceiver 410. That is, the processor 404, as utilized in the BS 400, may be used to implement or support all or part of one or more of the techniques presented herein.

[0064] In some aspects of the disclosure, the processor 404 may include a circuit 440 configured for various functions. The circuit 440 may be configured to implement one or more of the techniques described herein.

[0065] 3G mobile communication networks have brought mutual authentication, stronger and well-analyzed cryptographic algorithms as compared to 2G/GSM networks. 4G/LTE networks further strengthened the security features, giving a belief that LTE provides strong privacy and security to mobile users. Attacks, such as man-in-the-middle (MITM) attacks using fake BSs (also referred to as fake BSs or fake base stations), have become more difficult in 3G/UMTS networks and 4G/LTE networks and which is continuing via developing 5G NR standards, as compared to 2G/Global System for Mobile (GSM) networks. FIG. 5 illustrates an example network configuration 500 showing a man-in-the-middle attack. As shown in FIG. 5, a UE 502 may be communicating with one or more of the authentic BSs 504, 506, and 508 of a mobile communication network (e.g., LTE). As further shown in FIG. 5, for example, a fake BS 510 may be deployed by an attacker to control the UE 500 and/or the authentic BS 506.

[0066] However, LTE may be vulnerable to newer attacks, such as privacy info leaks, location tracking, denial of service, fake SMS messages with phishing attacks, eavesdropping on phone calls and text messages, spam with malicious links that inject malware/spyware onto phones, and downgrade attacks to 2G with

weak or no encryption. FIG. 6 illustrates an example network configuration 600 showing a UE under attack by a fake BS. As shown in FIG. 6, a UE 602 may be communicating with an authentic BS 604 of a mobile communication network (e.g., LTE, NR). As further shown in FIG. 6, a fake BS 606 may be deployed by an attacker and may cause the UE 602 to establish a connection with the fake BS 606. The fake BS 606 may then trick the UE 602 into providing identity information (e.g., an International Mobile Subscriber Identity (IMSI)) and/or may limit the UE 602 to particular radio access network (e.g., a downgraded radio access network, such as a 2G network). In some cases, the fake BS 606 may prevent the UE 602 from connecting to a mobile communication network (e.g., a denial of service (DOS) attack).

[0067] The fourth-generation (4G) cellular network, although significantly improved it security over previous generations, still has the vulnerability that a user-equipment (UE) cannot actively validate the network under certain scenarios. For example, when a UE updates its presence upon entering a new tracking area (TA) and receives a network response indicating anomaly, the UE is not able to authenticate its counterpart. Another example is that there appears no existing UE mechanism to determine reliability of system configuration for mobility towards previous generations (albeit not essential for acquiring 4G services). One potential detrimental effect from accessing an untrusted resource may be lead to a UEs loss of 4G service (downgrade attack), and the subsequent UE exposure to rogue 2G BSs that may operate without security and may attempt to gain illicit control or otherwise affect the UE on some way. One way for a fake BS to accomplish such may be by a denial-of-service (DoS) attack at the non-access-stratum (NAS) which may lead the UE to change from a 4G mode to a 2G mode; another way is through extremely biased 4G-to-2G reselection configuration in a system broadcast information. Some example NAS DoS attacks may include a fake BS failing to respond to a NAS tracking area update (TAU) request (e.g., possibly no lower-layer connection setup or a bare connection setup without any NAS signaling) from the UE. Some example NAS DoS attacks may include a fake BS sending an identity request in response to NAS TAU followed by a rejection (or possibly lower-layer redirect). In response to such NAS Dos attacks, an example UE may be configured per 4G standards to remove a 4G mode from its radio access technology (RAT) list or the like after

a certain number (e.g., 5) failed TAUs in a row, and/or possibly to down-grade and redirect to a 2G mode.

[0068] By way of applicable techniques provided herein, a UE may be configured to detect a fake BS, and identify the fake BS as an untrusted resource, perhaps for at least for a period of time. Information corresponding to (e.g., identifying) an untrusted resource may subsequently be reported to a network entity via one or more subsequently accessed trusted resources. For example, information corresponding to an untrusted resource may be shared via an RRC/NAS message. For example, an RRC/NAS message may report a candidate cell identified as an untrusted resource to a trusted resource via one or more message with a security context properly activated. In response to the information provided in such a report or as otherwise obtained by one or more network entities, list of candidate BSs may be affected in some manner to indicate to a BS that an untrusted resource may exist and preferably avoided (possibly just for some determined period of time) by UEs. For example, a list of candidate BSs may comprise a "whitelist" section corresponding to candidate BSs, and/or trusted resources. Here, for example, it may be that an untrusted resource may simply be removed from or otherwise not included in such a whitelist. For example, a list of candidate BSs may comprise a "blacklist" section corresponding to untrusted resources. Here, for example, it may be that an untrusted resource may be included in such a blacklist. In another example, a list of candidate BSs may comprise a combination of candidate BSs some of which may have been identified as (known) trusted resources, or (known) untrusted resources, or candidate BSs that presently lack such a trust indication. In affecting a list of candidate BSs, a network entity may consider a plurality of reports from one or more UEs, a period of time relating to the detection/indication of an untrusted or trusted resource, known network configurations, and/or the like or some combination thereof.

[0069] FIG. 7 illustrates an example attach procedure for a UE 702 in a communication network that includes at least a BS 704 and an MME 706. As shown in FIG. 7, the UE 702 may power on 708, and may perform a cell search operation 710 and a random-access procedure 712. The UE 702 and the MME 706 may enter an EMM deregistered state and an ECM idle state 714, 716. The UE 702 and the BS 704 may enter an RRC idle mode 718, 720. The UE 702 may

perform network selection 722 and initial cell selection 724, followed by a connection based random access 725 and an RRC connection setup 726. The UE 702 and the BS 704 may enter an RRC connected mode 728, 730. The UE 702, BS 704, and MME 706 may perform an attach procedure 732. In general, an attach procedure may be specified by a standard corresponding to the network arrangement and RAT as supported by the UE and BS, e.g., 4G/LTE, 5G NR, 2G, 3G, GSM, UMTS, etc.

[0070] The UE 702 and the MME 706 may enter an EMM registered state and an ECM connected state 734, 736. As shown in FIG. 7, as per 3GPP specifications there may be a few reasons that may lead to deregistering (e.g., indicated with arrow 742 in FIG. 7) of the UE 702 while in the EMM registered state and an ECM connected state 734, leading the UE 702 to enter the EMM deregistered state and ECM idle state 714. Also shown in FIG. 7, when an idle timer of the UE 702 expires (e.g., indicated with arrow 740 in FIG. 7) while in the RRC Connected State 728, the UE 702 may enter RRC idle state 718. The UE 702 may then perform an idle mode cell reselection operation (e.g., at least performing operation 724).

[0071] FIG. 8 is a flow diagram illustrating an example process 800 that be implemented, at least in part, in a UE, in accordance with certain aspects of the present description.

[0072] At example block 802, the UE may exchange one or more wireless signals with a candidate BS, e.g., as part of at least one attempted procedure to operatively attach the UE to the candidate BS. In certain instances, block 802 may correspond, at least in part, to attach procedure 732 (see FIG. 7), and/or an attach procedure as initiated at block 1102 (see FIG. 11).

[0073] At example block 804, the UE may determine that the at least one attempted procedure to operatively attach the UE to the candidate BS was not fully completed. By way of example, in certain implementations an attach procedure (e.g., defined by a protocol) corresponding to at least some of the signaling performed/attempted at block 802 may comprise certain message/data exchanges between the UE and the candidate BS. In such an implementation, at block 804, it may be determined that the attach procedure was not fully completed based, at least in part, on the signaling at block 802.

[0074] Thus, for example, certain types of anomalies and/or deviations from such expected signaling and procedures may, at times, support a determination by the UE that the procedure was not fully completed (e.g., as might be expected when dealing with a trusted resource). For example, if a particular response is expected from the candidate BS and a different response is received, a UE may determine that the attach procedure has not fully completed. In another example, if a particular response is expected from the candidate BS and no response is timely received, a UE may determine that the attach procedure has not fully completed. Some additional, non-limiting, examples are provided is later sections.

[0075] At example block 806, the UE may identify the candidate base station as an untrusted resource, at least in part, in response to the determination that at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed. In certain instances, blocks 802 and 804 may be performed one or more times before process 800 continues to block 806. In certain instances, a decision at block 806 may consider the results of one or more determinations made at block 804 in determining that at least one attempted procedure to operatively attach the UE to the candidate BS was not fully completed. To the contrary, had an attempted procedure to operatively attach the UE to the candidate BS been fully completed at block 802, then process 800 may end.

[0076] In response to identifying that a candidate BS is an untrusted resource, the UE may affect its operation in some manner. For example, a UE may gather detection information corresponding to the candidate base station, such as, for example, BS device-related identification information or lack thereof, BS service-related information, BS transmission/signal-related information or lack thereof, BS security-related information or lack thereof, BS standards-related information, location-related information, time-related information, and/or the like or some combination. In another example, in response to identifying that a candidate BS is an untrusted resource, the UE may inform/affect one or more other functions, capabilities, etc. In certain instances, the UE may provide some form of indication to a user of the UE, e.g., via display, sound, haptic mechanism, etc.

[0077] At example block 808, the UE may, e.g., subsequent to block 806, operatively attach to at least one other base station that is not identified as an untrusted resource. At example block 810, the UE may transmit information

corresponding to at least the untrusted resource to the base station, e.g., via one or more wireless signals/messages. By way of example, information transmitted to the base station at block 810 may comprise or otherwise correspond to all or part of detection information gathered at part of process 800.

[0078] Attention is drawn next to FIG. 9, which is a is a flow diagram illustrating an example process 900 that be implemented, at least in part, in a UE, in accordance with certain aspects of the present description. Process 900 includes some further example activities that may be provided, at least in a part, by one or more of the blocks in process 800. More specifically, in this example, some additional/optional activities are illustrated with regard to blocks 804 and 806 from process 800.

[0079] As shown, in process 900, example block 804 may further comprise example block 902. At block 902, a UE may determine that the candidate base station failed to perform one or more trust-related activities as part of at least one attempted procedure to operatively attach the UE to the candidate base station. A trust-related activity may, for example, comprise one or more security contexts/processes, one or more authentication processes, or one or more encryption processes, and/or the like or some combination thereof. An attach procedure may comprise one or more trust-related activities.

[0080] In a particular example, at example block 904 (which is shown as being optional as denoted by the dashed-lines), a UE may determine that a message transmitted by the candidate BS was received without a security context activated, or without including a cipher, or without including an integrity check, or some combination thereof. A decision at block 902 may be based, at least in part, on the determination of block 904. Thus, for example, an attempted procedure to operatively attach the UE to the candidate BS at block 802 may be determined at block 804 as having not been fully completed based, at least in part, on the activities at block 904.

[0081] In another example, at example block 906 (optional) a UE may receive an attachment rejection message or the like from a candidate BS. Note, the actual reception may occur at block 802. A decision at block 902 may be based, at least in part, on the determination of block 906. Thus, for example, an attempted procedure to operatively attach the UE to the candidate BS at block 802 may be

determined at block 804 as having not been fully completed based, at least in part, on the attachment rejection message or the like per block 906.

[0082] Example block 806 is further illustrated in FIG. 9 as potentially including one or more of (optional) blocks 908, 910 or 912. Thus, in certain implementations, identifying the candidate BS as an untrusted resource at block 806 may further include a decision at block 908 to identify a corresponding period of time during which the candidate BS is to be identified as an untrusted resource. By way of example, in certain implementations, a timer, time-stamp, etc., may be provided to indicate a lifespan or other measure to correspond to the identification of being an untrusted resource. Such information may be included, at least in part, in corresponding gathered/generated detection information. The span of such a period of time may vary by network, device, situation, environment, security concerns, location, etc. Thus, in certain instances, a period of time may extend from several seconds, to minutes, to hours, days, etc. In certain instances, a period of time may increase or decrease based on how often a particular candidate BS is identified as being an untrusted resource. In certain instances, the UE may determine a period of time dynamically or apply a more static value. In certain instances, the UE may receive a period of time or other like information from one or more other devices. For example, in certain implementations, a period of time corresponding to an untrusted resource may be indicated via a list of candidate base stations or the like, which may be received from time to time by the UE from one or more network resources (e.g., a trusted BS). Here, for example, a list of candidate base stations may comprise a blacklist identifying that one or more base stations may comprise untrusted resources. Such a blacklist may, for example, identify an untrusted resource in some manner (e.g., via an ID, etc.) possibly along with some indication of an applicable period of time for such resource to be considered untrusted. Conversely, a list of candidate base stations may comprise a whitelist, which may, for example, identify a trusted resource in some manner (e.g., via an ID, etc.) possibly along with some indication of an applicable period of time for such resource to be considered trusted. A list of candidate base stations may comprise a list of candidate base stations that the UE may consider for processes 800 and/or 900, wherein a given BS may be identified by the UE as an untrusted resource or perhaps as a trusted resource (again, possibly for some period of

time). As mentioned, in certain instances a UE may maintain, generate, alter, or otherwise affect a list of candidate base stations stored at the UE. All or part of a list of candidate base stations may be received by the UE from one or more other devices, in certain implementations. All or part of a list of candidate base stations may be based, as least in part, on information provided by the UE as part of processes 800 and/or 900 (e.g., at block 810).

[0083] At example (optional) block 910, shown in FIG. 9 within block 806, in certain instances a UE may (continue) to operate the UE in a first mode of wireless signal transmission and reception rather than switching to a second mode of wireless signal transmission and reception upon identifying the candidate base station as an untrusted resource. By way of an example, a UE may determine (e.g., at blocks 804, 902, 904, 906) that a given candidate BS has not been able to fully complete an attach procedure, and at block 806 the given candidate BS may be identified as an untrusted resource at block 806. However, there may also be another process in place at the UE, wherein some of the responses or lack thereof (at block 802) from the given candidate BS during an attach procedure may indicate the UE should attempt to switch from a first mode to a second mode of wireless signal transmission and reception and to re-attempt to attach to the given candidate BS. For example, as mentioned, a UE having been unable to fully complete an attach procedure in a first mode (e.g., a 4G mode) may switch to a second mode (e.g., 2G) and attempt to attach using the second mode of wireless signal transmission and reception. However, such a switch (e.g., from a more secure mode (4G, 5G) to a less secure mode (2G)) may be just the response intended by a person or entity via a rogue or fake BS. Example block 910 may prevent such a fallback or other like process from occurring at times.

[0084] At example (optional) block 912, shown within block 806, to help identify a candidate base station as an untrusted resource, a UE may consider/apply at least one criterion. By way of example, in certain instances detection criteria may correspond to one or more results that may come from trust-related activities associated with blocks 804, 902, 904, and 906, just to name a few examples. Hence, detection criteria may correspond to an expected response from a trusted resource, or conversely an expected response from an untrusted resource, or some combination thereof. In certain instances, all or part of the detection criteria

may be stored by the UE, possibly generated, maintained, or otherwise affected by the UE. In certain instances, all or part of the detection criteria may be received by the UE from another device. In certain instances, one or more threshold values may be provided as detection criteria. For example, design criteria may specify how many times or how often/when, etc., a UE may attempt to fully complete an attach procedure before possibly identifying a candidate BS as an untrusted resource. Indeed, while some examples are mentioned, it should be understood that a variety of criterion may be included in detection criteria for use at one or more of the example blocks in methods 800 and/or 900.

[0085] FIG. 10 is a flow diagram illustrating an example process 1000 that be implemented, at least in part, in one or more network resources, in accordance with certain aspects of the present description. By way of an example, all or part of process 1000 may be implemented at a base station, or other like network device, or a cloud computing resource, etc.

[0086] At example block 1002, information corresponding to a candidate base station that the UE has identified as an untrusted resource may be received. The information may be based, at least in part, in response to a determination that at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed. For example, at a UE, such information may result from all or part of processes 800 and/or 900, or other like techniques provided herein.

[0087] At example block 1004, a list of candidate base stations may be maintained in some manner, based, at least in part, on the received information. For example, the received information may indicate that a UE identified a particular candidate BS as an untrusted resource and at block 1004 a list of candidate base stations may be affected in some manner based on such information. Hence, in certain implementations, a lust of candidate base stations may comprise a blacklist or the like which may be affected at block 1004 in some manner based on the received information (e.g., possibly added to the blacklist or the like). In certain instances, at block 1004, received information from two or more UEs may be considered before affecting a list of candidate base stations. For example, a particular candidate BS may not be included in a blacklist or the like until reported as an untrusted resource by some threshold number or UEs, or

some threshold number of reports, possibly corresponding to some window of time, etc.

[0088] At example block 1006, at least a portion of the list of candidate base stations may be transmitted, e.g., to one or more UEs, or other network devices. By way of example, a transmission in accord with block 1006 may occur from time to time, e.g., per some schedule, or in response to a request, or as needed (e.g., when an update us ready), or at some other point(s) in time, just to name a few examples.

[0089] FIG. 11 is a flow diagram illustrating an example call-flow process 1100 in accordance with some aspects of the present disclosure. Call-flow process 1100 illustrates certain process blocks and signaling/messaging relating to a UE and a candidate BS (which is assumed to for this example to represent a rogue or fake BS), and also the UE and a trusted resource. It should be understood, however, that an actual call-flow applying at least a portion of the techniques provided herein may include additional signaling/messaging not shown in this brief example. Call-flow process 1100 is further intended to illustrate certain aspects of all or part of one or more of the example processes 800, 900, and/or 1000. Thus, by way of example, in certain instances blocks 1102, 1110 and 1112 from call-flow process 1100 may relate to blocks 802, 804, 806, 902, 904, 906, 908, 910, and/or 912 in some manner.

[0090] With this in mind, as shown in call-flow process 1100, a UE may initiate at least one attach procedure with the candidate BS, e.g., beginning at block 1102. As described, however, the attach procedure in this example may end at block 1110 without being fully completed as per certain aspects of the present description.

[0091] As part of an example attach procedure, the UE may transmit one or more attach request messages or the like to the candidate BS, as represented by a request message 1104. By way of some examples, request message 1104 may relate to a TAU request, a LAU request, a RAU request, and/or the like or some combination thereof.

[0092] In response to request message 1104 the candidate BS, in one example, may transmit a response message 1106, wherein message 1106 may be transmitted without an expected security context activated. Hence, the candidate BS may have intentionally or unintentionally failed to perform one or more trust-

related activities as expected in response to request message 1104. For example, response message 1106 may lack an expected cipher, integrity check, etc., associated with a security context.

[0093] In another example, in response to request message 1104 the candidate BS may intentionally transmit a reject message 1108 (e.g., possibly for nefarious reasons). In this example, reject message 1108 may be transmitted by the candidate BS without an expected security context activated. Again, for example, reject message 1108 may lack an expected cipher or integrity check, etc., associated with a security context.

[0094] At example block 1110, the UE may end the attach procedure without completion, e.g., based, at least in part, on response message 1106, rejection message 1108, and/or the like. At example block 1112, the UE may gather or otherwise provide information (e.g., detection information or the like), which may relate to the attempted attach procedure, the UE, the candidate BS, one or more responses or other signaling/message exchanges, etc.

[0095] At example block 1120, at a time subsequent to block 1110, the UE may fully complete an attach procedure with another BS or the like, represented here by the trusted resource. Here, as shown, the UE may transmit one or more messages to the trusted resource, as represented by report message 1122. In certain example implementations, report message 1122 may comprise all or part of one or more messages via which ma convey information associated with the attach procedure that ended at block 1110. Thus, for example, report message 1122 may comprise all or part of the detection information as gathered at block 1112. In this example, report message 1122 may indicate that the candidate BS has been identified by the UE as an untrusted resource.

[0096] In accordance with certain further aspects and represented by message 1124, the trusted resource may, at times, provide all or part of a list of candidate BSs to the UE. As presented herein, in certain instances, information provided via one or more report messages 1122 may be used to affect all or part of such a list of candidate BSs. For example, the trusted resource or other network resources may be configured to compare report message information with known network configuration(s) to update or otherwise maintain a list of candidate BSs that may be useful to UE network access.

[0097] Some of the techniques presented herein may be implemented in a UE to possibly detect, identify, and report a fake BS. The information provided in a report to the network by the UE may lead to further analysis of the BS and/or dissemination of such knowledge to other UEs. The information provided to the network may, for example, comprise or correspond to a RAT, a cell ID, an ARFCN, a PCID, AC/LAC GPS info, information regarding a previous camped-on cell, a time elapsed, a period of time, a time stamp, and/or the like or some combination thereof, just to name a few examples.

[0098] As shown and described by way of several non-limiting examples herein, a network (e.g., one or more resources/devices therein) may use the information reported by one or more UEs regarding one or more BSs identified by the UE(s) as an untrusted resources to inform UEs about the network. By way of further example, an untrusted resource may be added to otherwise included in a blacklist or the like in the network's system information, which may inform a UE to avoid such untrusted resources (e.g., don't select such BS for attachment), at least for a period of time (specified or inherent). In certain instances, a network may remove an untrusted resource from a blacklist through a system information change in idle, or blackCellsToRemoveList or other like in a measurement object in a connected state, or reconfigure a blacklist in a connected state, just to name a few examples.

[0099] Several aspects of a wireless communication network have been presented with reference to an exemplary implementation. As those skilled in the art will readily appreciate, various aspects described throughout this disclosure may be extended to other telecommunication systems, network architectures and communication standards.

[0100] The examples set forth herein are provided to illustrate certain concepts of the disclosure. Those of ordinary skill in the art will comprehend that these are merely illustrative in nature, and other examples may fall within the scope of the disclosure and the appended claims. Based on the teachings herein those skilled in the art should appreciate that an aspect disclosed herein may be implemented independently of any other aspects and that two or more of these aspects may be combined in various ways. For example, an apparatus may be implemented or a method may be practiced using any number of the aspects set forth herein. In addition, such an apparatus may be implemented or such a method may be

practiced using other structure, functionality, or structure and functionality in addition to or other than one or more of the aspects set forth herein.

[0101] As those skilled in the art will readily appreciate, various aspects described throughout this disclosure may be extended to any suitable telecommunication system, network architecture, and communication standard. By way of example, various aspects may be applied to wide area networks, peer-to-peer network, local area network, other suitable systems, or any combination thereof, including those described by yet-to-be defined standards.

[0102] Many aspects are described in terms of sequences of actions to be performed by, for example, elements of a computing device. It will be recognized that various actions described herein can be performed by specific circuits, for example, central processing units (CPUs), graphic processing units (GPUs), digital signal processors (DSPs), application specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), or various other types of general purpose or special purpose processors or circuits, by program instructions being executed by one or more processors, or by a combination of both. Additionally, sequences of actions described herein can be considered to be embodied entirely within any form of computer readable storage medium having stored therein a corresponding set of computer instructions that upon execution would cause an associated processor to perform the functionality described herein. Thus, the various aspects of the disclosure may be embodied in a number of different forms, all of which have been contemplated to be within the scope of the claimed subject matter. In addition, for each of the aspects described herein, the corresponding form of any such aspects may be described herein as, for example, "logic configured to" perform the described action.

[0103] Further, those of skill in the art will appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the aspects disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the

described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the disclosure.

[0104] It is to be understood that the specific order or hierarchy of steps in the methods disclosed is an illustration of example processes. Based upon design preferences, it is understood that the specific order or hierarchy of steps in the methods may be rearranged. The accompanying method claims present elements of the various steps in a sample order and are not meant to be limited to the specific order or hierarchy presented unless specifically recited therein.

[0105] The terminology used herein is for the purpose of describing particular aspects only and is not intended to be limiting of the aspects. As used herein, the singular forms "a," "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises," "comprising," "includes" or "including," when used herein, specify the presence of stated features, integers, steps, operations, elements, or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, or groups thereof. Moreover, it is understood that the word "or" has the same meaning as the Boolean operator "OR," that is, it encompasses the possibilities of "either" and "both" and is not limited to "exclusive or" ("XOR"), unless expressly stated otherwise. It is also understood that the symbol "/" between two adjacent words has the same meaning as "or" unless expressly stated otherwise. Moreover, phrases such as "connected to," "coupled to" or "in communication with" are not limited to direct connections unless expressly stated otherwise.

[0106] While the foregoing disclosure shows illustrative aspects, it should be noted that various changes and modifications could be made herein without departing from the scope of the appended claims. The functions, steps or actions of the method claims in accordance with aspects described herein need not be performed in any particular order unless expressly stated otherwise. Furthermore, although elements may be described or claimed in the singular, the plural is contemplated unless limitation to the singular is explicitly stated.

CLAIMS

What is Claimed is:

1. A method for use by a user equipment (UE), the method comprising, at the UE:

exchanging one or more wireless signals with a candidate base station as part of at least one attempted procedure to operatively attach the UE to the candidate base station;

determining that the at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed;

identifying the candidate base station as an untrusted resource, at least in part, in response to the determination that the at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed;

subsequently, operatively attaching the UE to a base station that is not identified as an untrusted resource; and

transmitting, to the base station, information corresponding to at least the untrusted resource.

2. The method as recited in Claim 1, and wherein the UE supports at least a first mode and a second mode of wireless signal transmission and reception, and wherein the first mode supports communication with a trusted resource in a trusted manner but not an untrusted resource, and wherein the second mode supports communication with either a trusted resource or an untrusted resource in an untrusted manner, and further comprising, at the UE, continuing to operate the UE in the first mode rather than switching to the second mode upon identifying the candidate base station as an untrusted resource.

3. The method as recited in Claim 1, wherein determining that the at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed comprises:

determining that the candidate base station failed to perform one or more trust-related activities as part of at least one attempted procedure to operatively attach the UE to the candidate base station.

4. The method as recited in Claim 3, wherein determining that the candidate base station failed to perform one or more trust-related activities further comprises:

determining that a message transmitted by the candidate base station was received without a security context activated, or without including a cipher, or without including an integrity check, or some combination thereof.

5. The method as recited in Claim 1, wherein determining that the at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed comprises:

receiving an attachment rejection message from the candidate base station.

6. The method as recited in Claim 1, wherein subsequently, operatively attaching the UE to the base station comprises:

determining that the base station performed one or more trust-related activities as part of a procedure to operatively attach the UE to the base station.

7. The method as recited in Claim 1, and further comprising, at the UE:

receiving at least a portion of a list of candidate base stations from at least one other device; or

identify the candidate base station using the list of candidate base stations at the UE; or

wherein identifying the candidate base station as an untrusted resource is based, at least in part, on one or more criteria stored at the UE; or

maintaining at least a portion of the list of candidate base stations at the UE; or

generating at least a portion of the list of candidate base stations at the UE, or

some combination thereof.

8. The method as recited in Claim 7, wherein the list of candidate base stations is indicative of a known trusted resource, or a known untrusted resource, or one or more candidate base stations, or a combination thereof.

9. The method as recited in Claim 1, wherein identifying the candidate base station as an untrusted resource comprises identifying a corresponding period of time during which the candidate base station is to be identified as an untrusted resource and wherein after the period of time is over the candidate base station is no longer identified as an untrusted resource.

10. The method as recited in Claim 1, wherein the one or more wireless signals comprise at least one of a Tracking Area Update (TAU) message, or a Location Area Update (LAU) message, or a Routing Area Update (RAU) message, or some combination thereof.

11. A user equipment (UE) comprising:

memory;

a transceiver; and

a processing unit coupled to the memory and the transceiver, and configured to:

initiate an exchange, via the transceiver, one or more wireless signals with a candidate base station as part of at least one attempted procedure to operatively attach the UE to the candidate base station;

determine that the at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed;

identify, in the memory, the candidate base station as an untrusted resource, at least in part, in response to the determination that the at

least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed;

subsequently, operatively attach the UE to a base station that is not identified as an untrusted resource via the transceiver; and

initiate transmission of information corresponding to at least the untrusted resource to the base station via the transceiver.

12. The UE as recited in Claim 11, and wherein the UE supports at least a first mode and a second mode of wireless signal transmission and reception, and wherein the first mode supports communication with a trusted resource in a trusted manner but not an untrusted resource, and wherein the second mode supports communication with either a trusted resource or an untrusted resource in an untrusted manner, and wherein the processing unit is further configured to:

operate the UE in the first mode rather than switching to the second mode upon identifying the candidate base station as an untrusted resource.

13. The UE as recited in Claim 11, wherein the processing unit is further configured to determine that the candidate base station failed to perform one or more trust-related activities as part of the attempted procedure to operatively attach the UE to the candidate base station.

14. The UE as recited in Claim 13, wherein the processing unit is further configured to determine that a message transmitted by the candidate base station that and received via the transceiver without a security context activated, or without including a cipher, or without including an integrity check, or some combination thereof.

15. The UE as recited in Claim 11, wherein the processing unit is further configured to:

receive, via the transceiver, an attachment rejection message from the candidate base station.

16. The UE as recited in Claim 11, wherein the processing unit is further configured to operatively attach the UE to the base station in response to a determination that the base station successfully performed one or more trust-related activities as part of the procedure to operatively attach the UE to the base station.

17. The UE as recited in Claim 11, wherein the processing unit is further configured to:

receive, via the transceiver, at least a portion of a list of candidate base stations from at least one other device; or

identify the candidate base station using the list of candidate base stations at the UE; or

identify the base station using the list of candidate base stations at the UE;

identify the candidate base station as an untrusted resource is based, at least in part, on at least information representing one or more criteria stored in the memory; or

maintain at least a portion of the list of candidate base stations at the UE in the memory; or

generate at least a portion of the list of candidate base stations at the UE in the memory, or

some combination thereof.

18. The UE as recited in Claim 17, wherein the list of candidate base stations is indicative of a known trusted resource, or a known untrusted resource, or one or more candidate base stations, or a combination thereof.

19. The UE as recited in Claim 17, wherein the processing unit is further configured to identify a corresponding period of time during which the candidate base station is to be identified as an untrusted resource and wherein after the period of time is over the candidate base station is no longer identified as an untrusted resource.

20. The UE as recited in Claim 17, wherein the one or more wireless signals comprise at least one of a Tracking Area Update (TAU) message, or a Location Area Update (LAU) message, or a Routing Area Update (RAU) message, or some combination thereof.

21. A method for use by a network resource, the method comprising, at the network resource:

receiving, from a user equipment (UE), information corresponding to a candidate base station that the UE has identified as an untrusted resource based, at least in part, in response to a determination that at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed;

maintaining a list of candidate base stations based, at least in part, on the received information; and

transmitting at least a portion of the list of candidate base stations.

22. The method as recited in Claim 21, wherein the received information comprises information corresponding to the candidate base station received from a plurality of UEs, wherein the plurality of UEs comprises the UE.

23. The method as recited in Claim 21, wherein the network resource comprises a base station identified by the UE as comprising a trusted network resource.

24. The method as recited in Claim 21, wherein the candidate base station is identified via the at least a portion the list of candidate base stations as an

untrusted resource during a period of time and wherein after the period of time is over the candidate base station is no longer identified as an untrusted resource.

25. The method as recited in Claim 21, wherein a least a portion of the list of candidate base stations is indicative of a known trusted resource, or a known untrusted resource, or both.

26. A network resource comprising:

memory;

a transceiver; and

a processing unit coupled to the memory and the transceiver, and configured to:

receive, via the transceiver from a user equipment (UE), information corresponding to a candidate base station that the UE has identified as an untrusted resource based, at least in part, in response to a determination that at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed;

maintain a list of candidate base stations based, at least in part, on the received information; and

initiate transmission of at least a portion of the list of candidate base stations to one or more other devices.

27. The network resource as recited in Claim 26, wherein the received information comprises information corresponding to the candidate base station received from a plurality of UEs, wherein the plurality of UEs comprises the UE.

28. The network resource as recited in Claim 26, wherein the network resource comprises a base station identified by the UE as comprising a trusted network resource.

29. The network resource as recited in Claim 26, wherein the candidate base station is identified via the at least a portion the list of candidate base stations as an untrusted resource during a period of time and wherein after the period of time is over the candidate base station is no longer identified as an untrusted resource.

30. The network resource as recited in Claim 26, wherein a least a portion of the list of candidate base stations is indicative of a known trusted resource, or a known untrusted resource, or both.

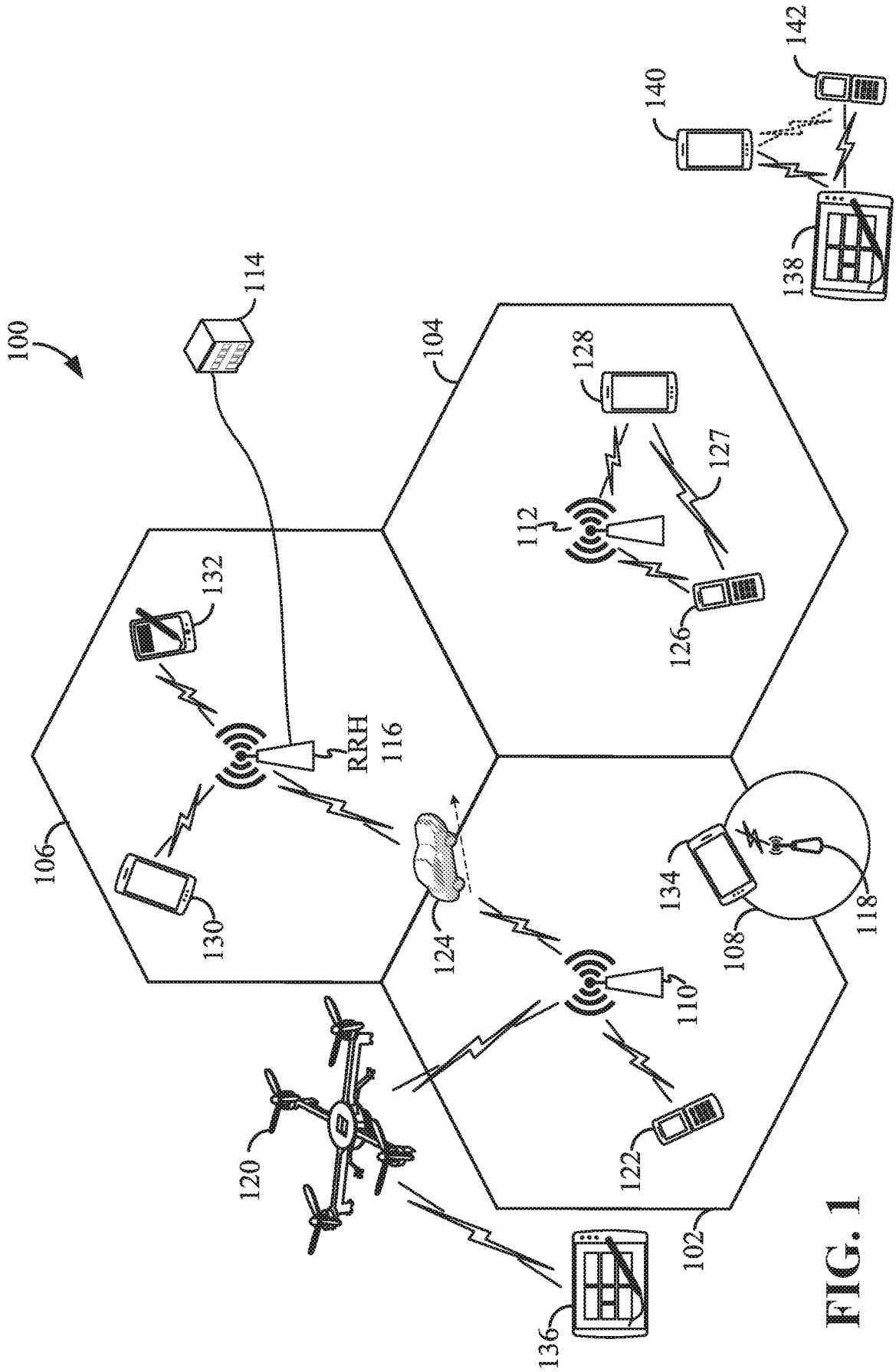
100
102
104
106
108
110
112
114
116
RRH
118
120
122
124
126
127
128
130
132
134
136
138
140
142

FIG. 1

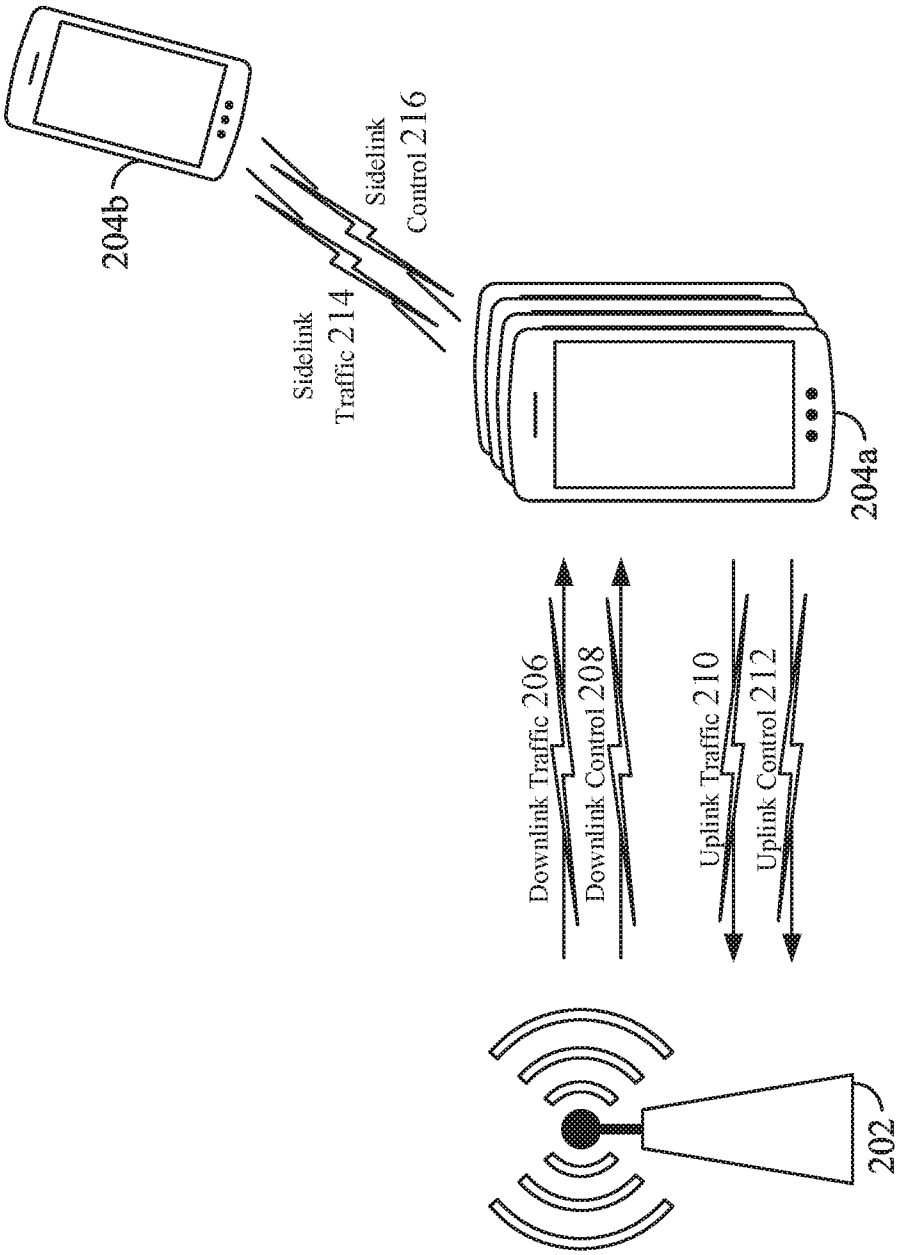
204b
Sidelink Control 216
Sidelink Traffic 214
204a
Downlink Traffic 206
Downlink Control 208
Uplink Traffic 210
Uplink Control 212
202

FIG. 2

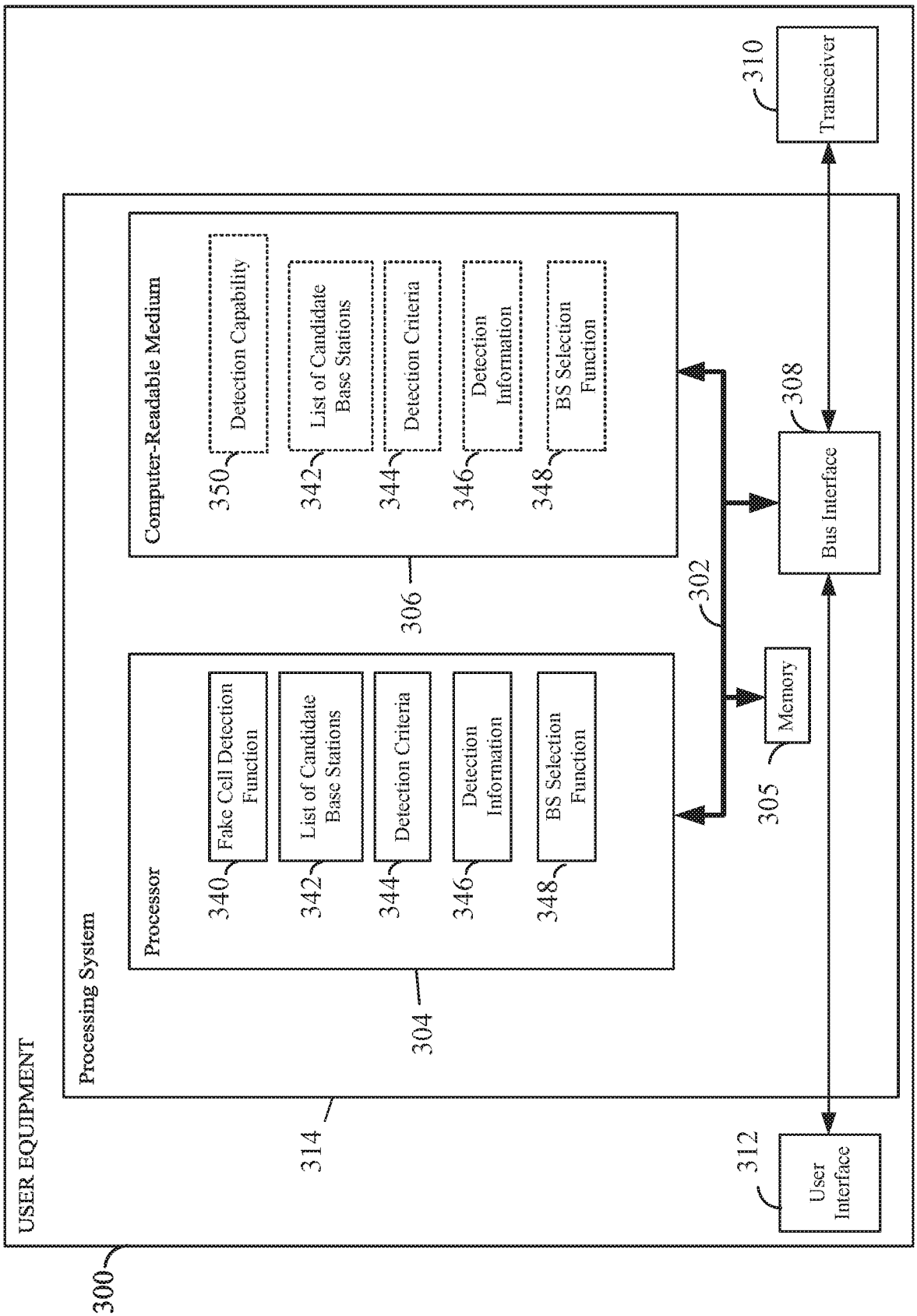
300
USER EQUIPMENT
314
Processing System
304
Processor
340
Fake Cell Detection Function
342
List of Candidate Base Stations
344
Detection Criteria
346
Detection Information
348
BS Selection Function
306
Computer-Readable Medium
350
Detection Capability
342
List of Candidate Base Stations
344
Detection Criteria
346
Detection Information
348
BS Selection Function
302
305
Memory
308
Bus Interface
310
Transceiver
312
User Interface

FIG. 3

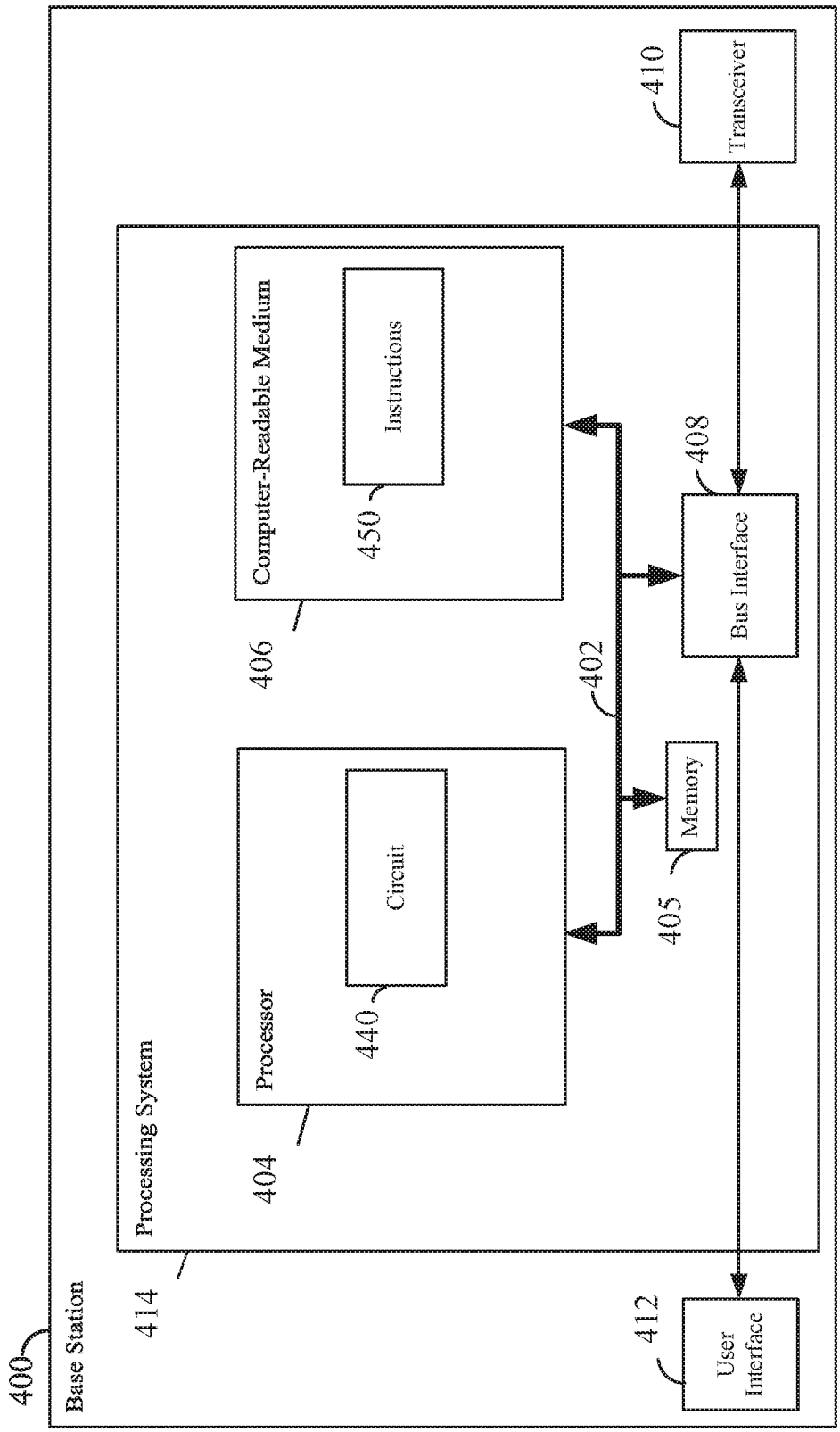
Base Station
400
Processing System
414
Processor
404
Circuit
440
Computer-Readable Medium
406
Instructions
450
Memory
405
Bus Interface
408
Transceiver
410
User Interface
412
402

FIG. 4

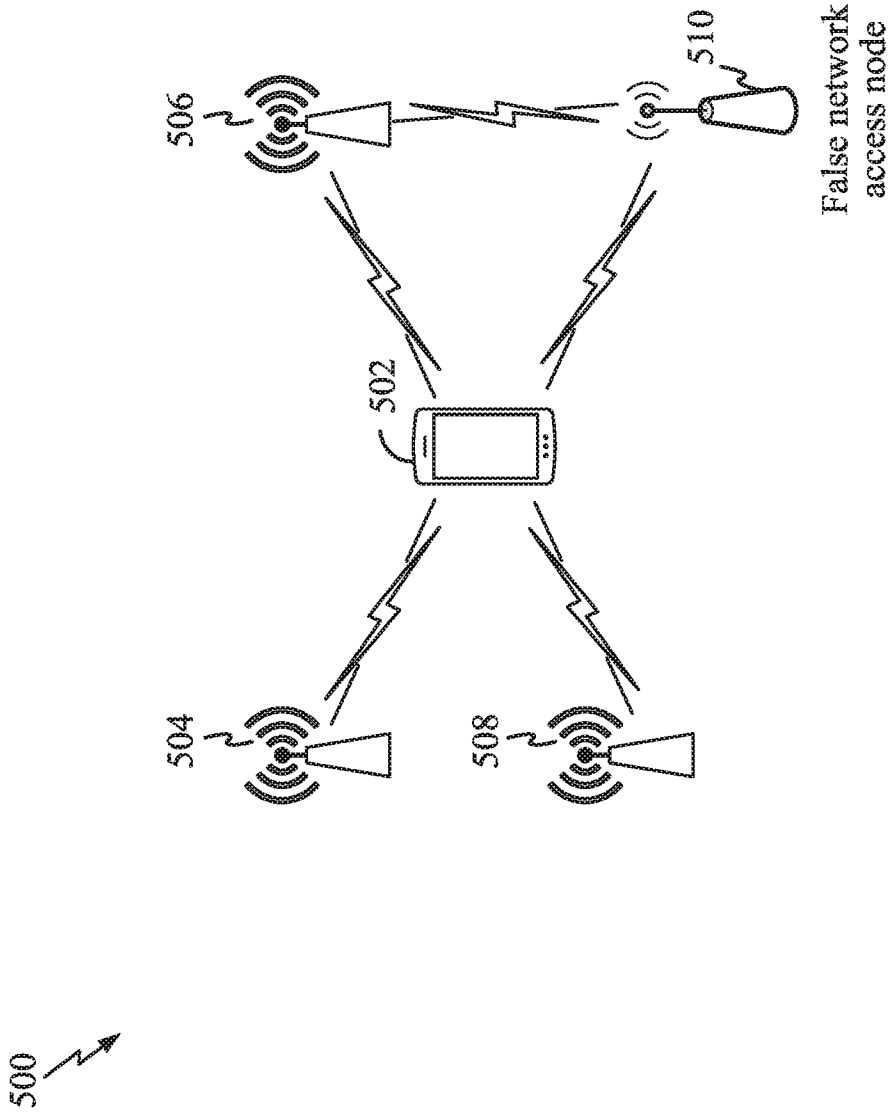

FIG. 5

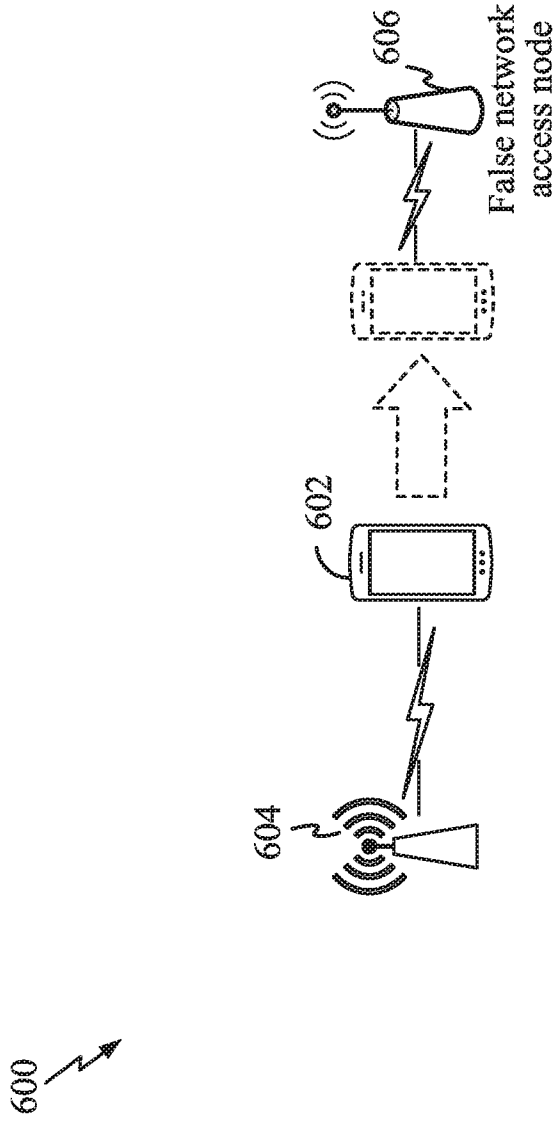

FIG. 6

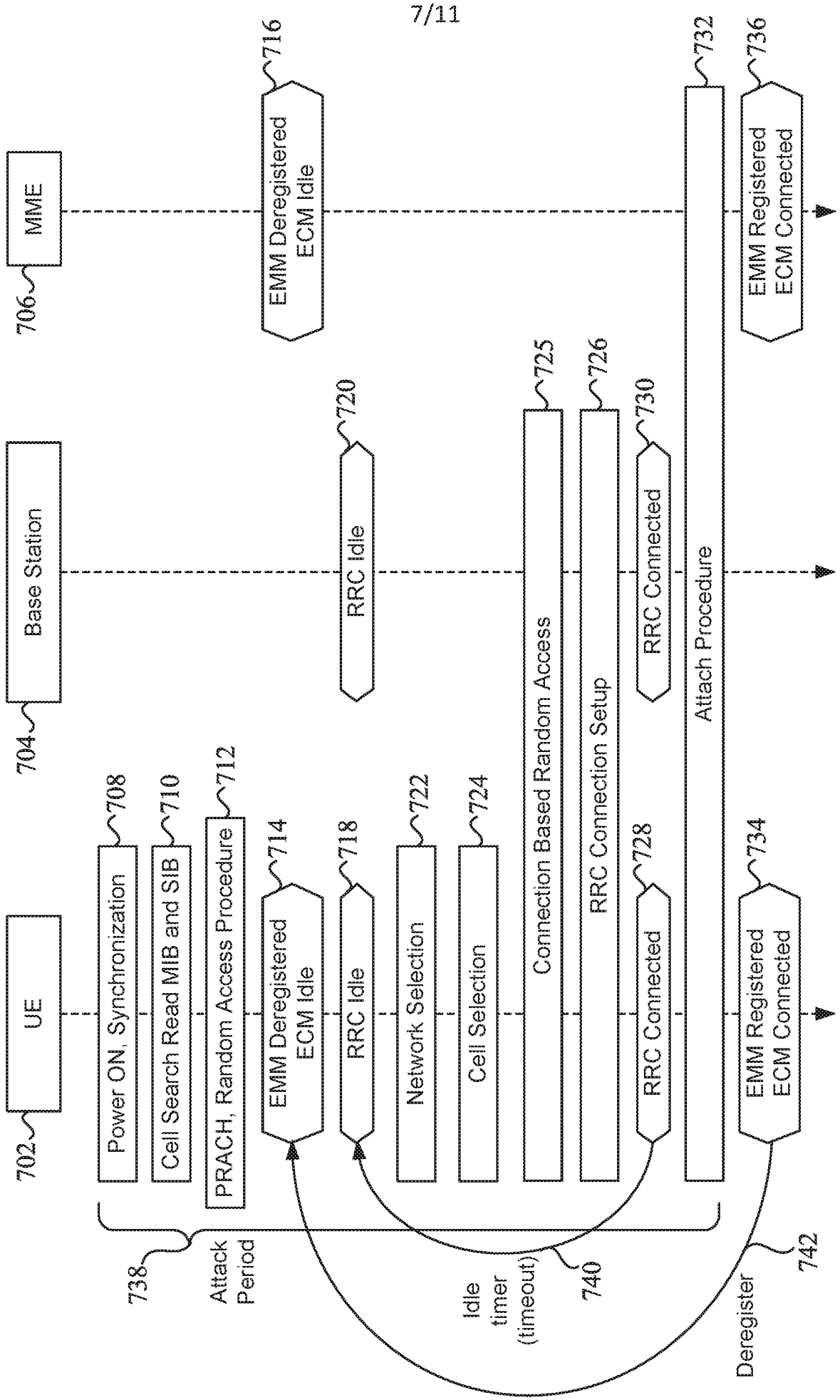
UE
Base Station
MME
702
704
706
Power ON, Synchronization
708
Cell Search Read MIB and SIB
710
PRACH, Random Access Procedure
712
EMM Deregistered ECM Idle
714
RRC Idle
718
Network Selection
722
Cell Selection
724
Connection Based Random Access
725
RRC Connection Setup
726
RRC Connected
728
EMM Registered ECM Connected
734
RRC Idle
720
RRC Connected
730
Attach Procedure
732
EMM Registered ECM Connected
736
EMM Deregistered ECM Idle
716
738
Attack Period
740
Idle timer (timeout)
742
Deregister

FIG. 7

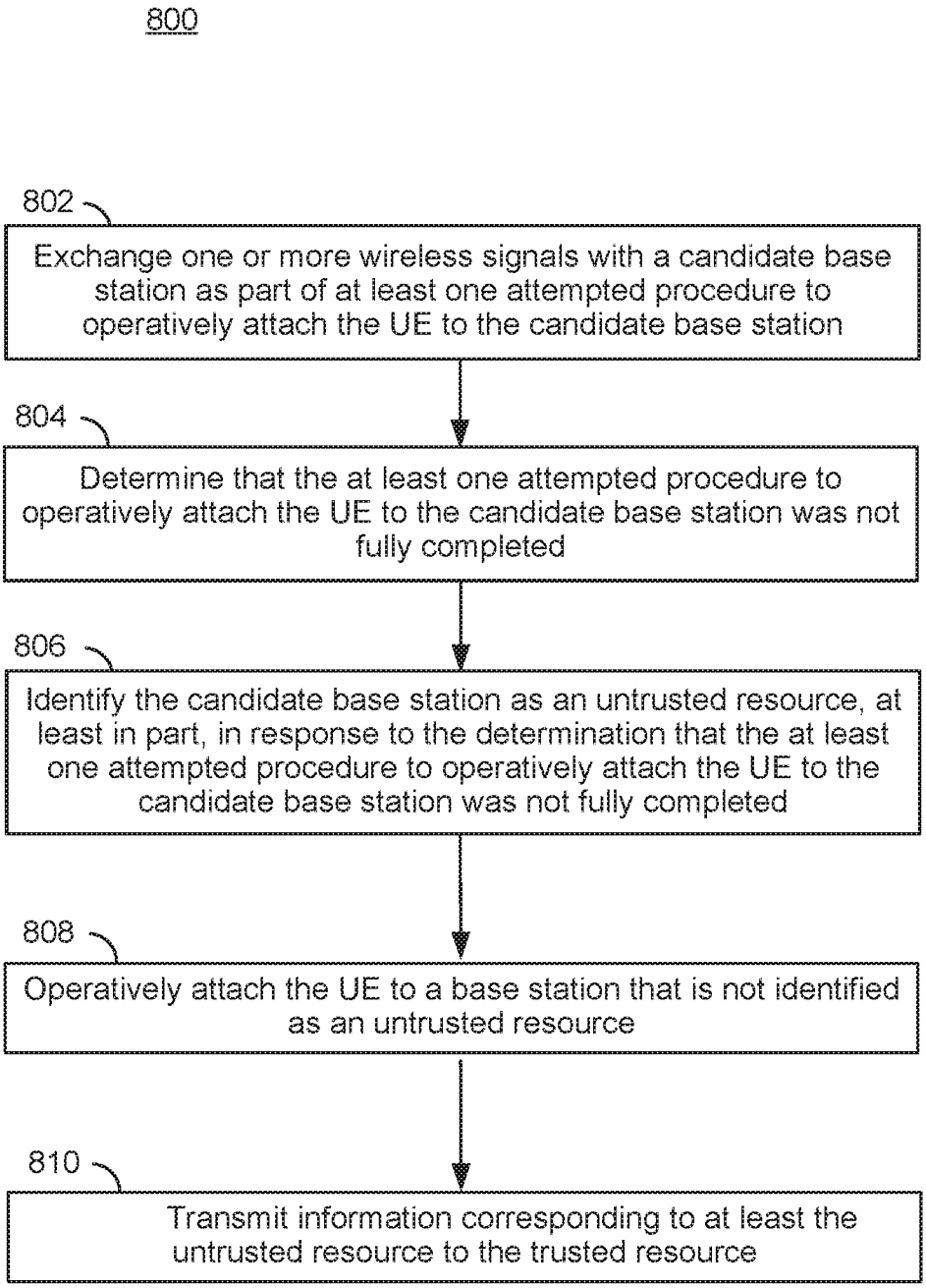
800
802
Exchange one or more wireless signals with a candidate base station as part of at least one attempted procedure to operatively attach the UE to the candidate base station
804
Determine that the at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed
806
Identify the candidate base station as an untrusted resource, at least in part, in response to the determination that the at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed
808
Operatively attach the UE to a base station that is not identified as an untrusted resource
810
Transmit information corresponding to at least the untrusted resource to the trusted resource

FIG. 8

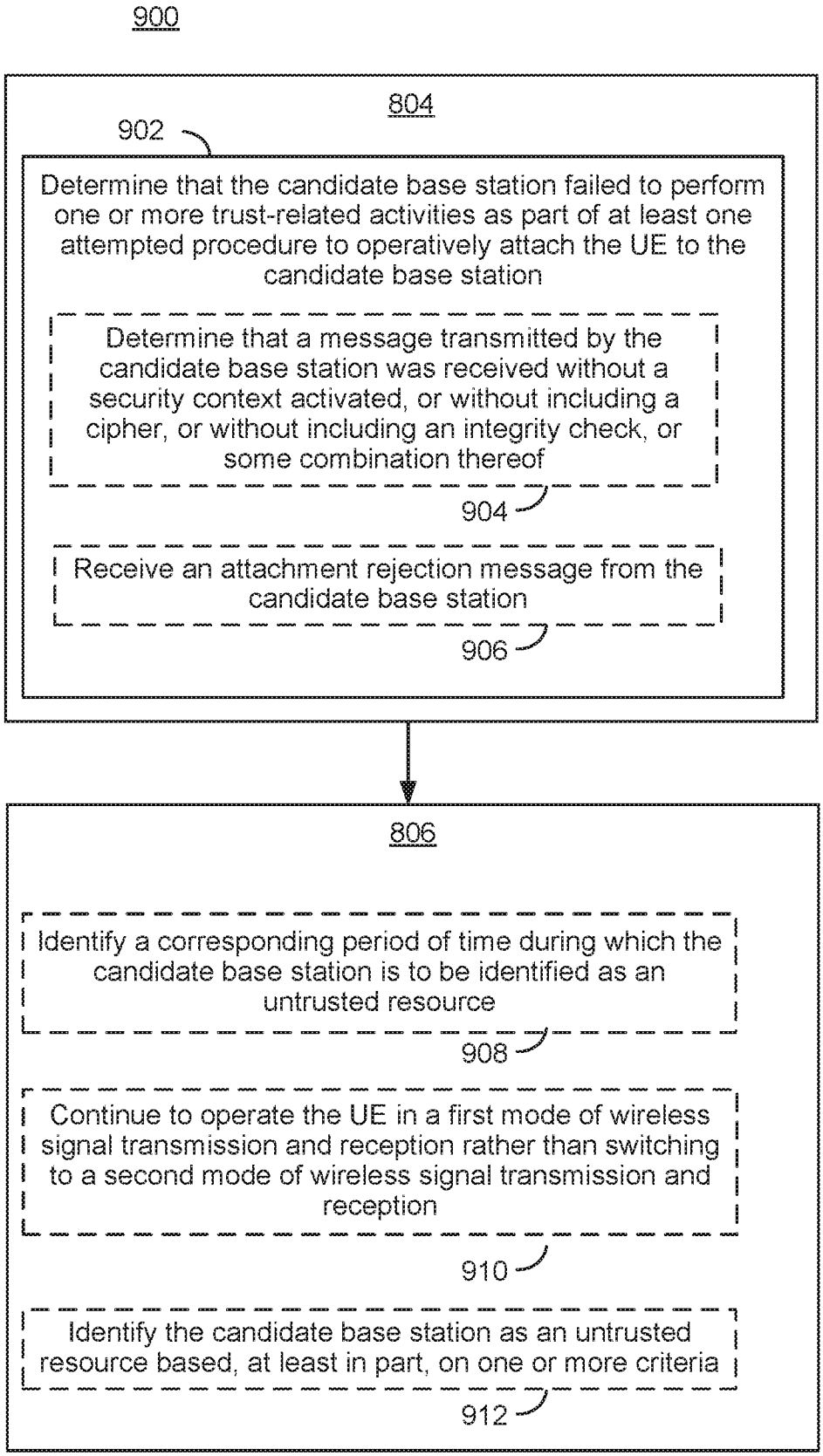
900
804
902
Determine that the candidate base station failed to perform one or more trust-related activities as part of at least one attempted procedure to operatively attach the UE to the candidate base station
Determine that a message transmitted by the candidate base station was received without a security context activated, or without including a cipher, or without including an integrity check, or some combination thereof
904
Receive an attachment rejection message from the candidate base station
906
806
Identify a corresponding period of time during which the candidate base station is to be identified as an untrusted resource
908
Continue to operate the UE in a first mode of wireless signal transmission and reception rather than switching to a second mode of wireless signal transmission and reception
910
Identify the candidate base station as an untrusted resource based, at least in part, on one or more criteria
912

FIG. 9

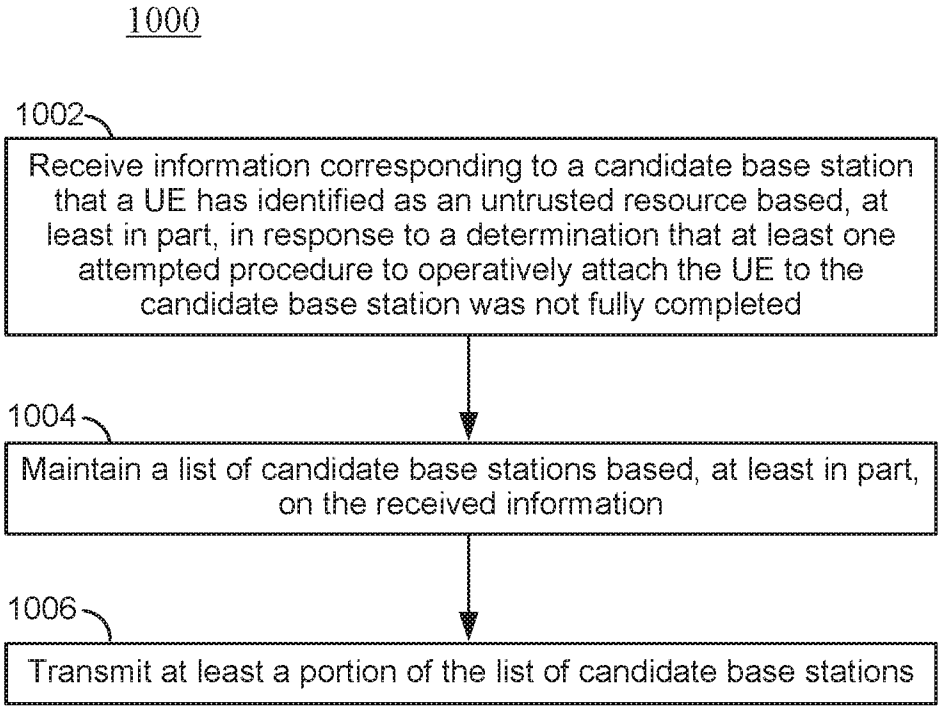
1000
1002
Receive information corresponding to a candidate base station that a UE has identified as an untrusted resource based, at least in part, in response to a determination that at least one attempted procedure to operatively attach the UE to the candidate base station was not fully completed
1004
Maintain a list of candidate base stations based, at least in part, on the received information
1006
Transmit at least a portion of the list of candidate base stations

FIG. 10

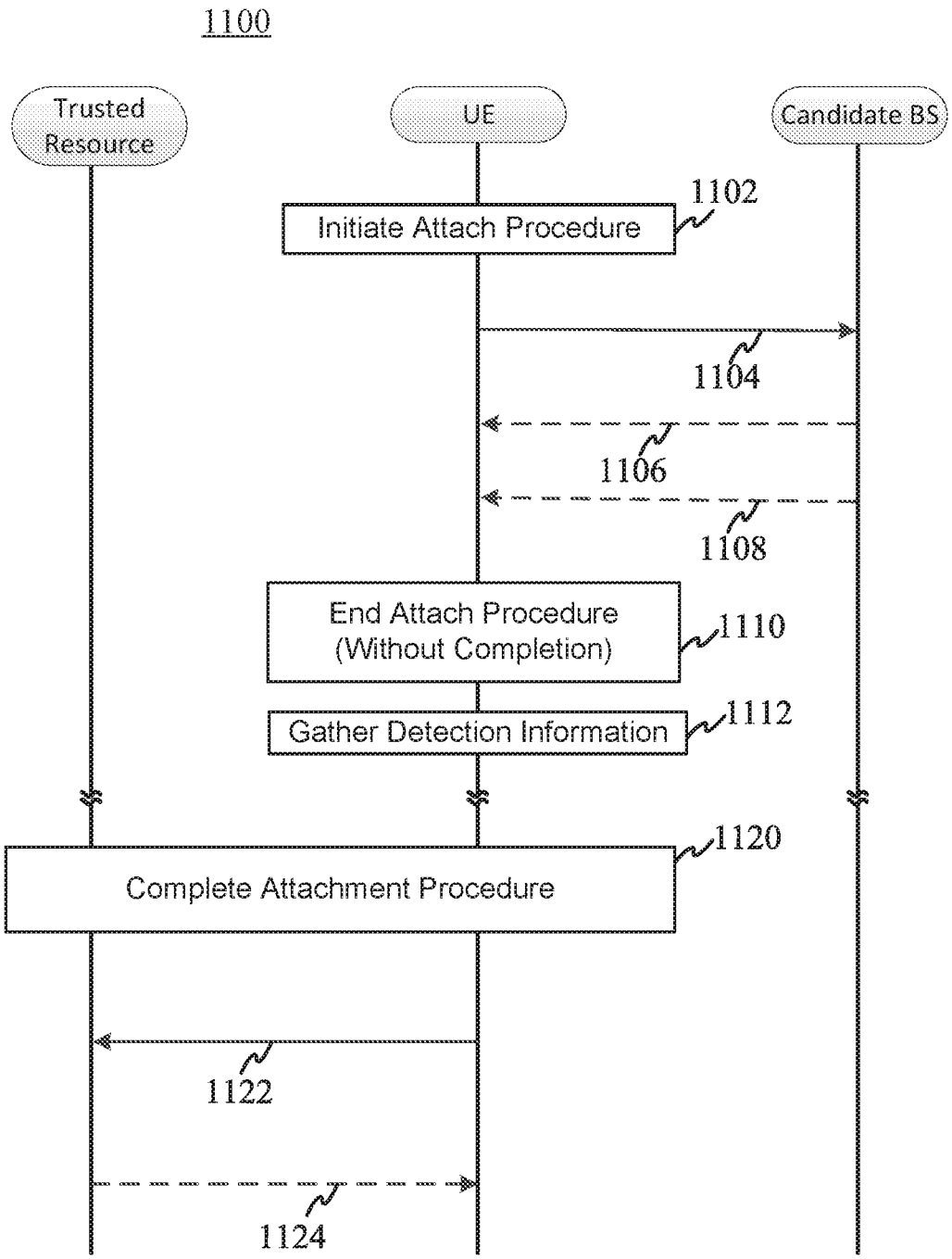
1100
Trusted Resource
UE
Candidate BS
1102
Initiate Attach Procedure
1104
1106
1108
End Attach Procedure (Without Completion)
1110
Gather Detection Information
1112
1120
Complete Attachment Procedure
1122
1124

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/102305

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/12(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)

H04L; H04W

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

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

CNABS;CNTXT;CNKI;VEN;USTXT;EPTXT;WOTXT: fake, untrusted, candidate, basestaion, base w station, attach???, security w context, integrity, TAU, LAU, RAU, denial 1w of 1w service, DOS, reselect???, 2G, GSM

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017215132 A1 (MEDIATEK SINGAPORE PTE LTD) 27 July 2017 (2017-07-27) see the description, paragraphs [0020]-[0067] and figures 1-5	1-30
X	CN 106572450 A (HUAWEI TECHNOLOGIES CO.) 19 April 2017 (2017-04-19) see the description, paragraphs [0101]-[0122] and figure 4	1-30
A	CN 107683617 A (HUAWEI TECHNOLOGIES CO.) 09 February 2018 (2018-02-09) see the whole document	1-30
A	US 2018109552 A1 (QUALCOMM INC) 19 April 2018 (2018-04-19) see the whole document	1-30

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 May 2019	**15 May 2019**

Name and mailing address of the ISA/CN	Authorized officer
National Intellectual Property Administration, PRC **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088** **China**	**ZOU,Feifei**
Facsimile No. **(86-10)62019451**	Telephone No. **86-(010)-62411263**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/102305

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2017215132 A1	27 July 2017	None	
CN 106572450 A	19 April 2017	None	
CN 107683617 A	09 February 2018	EP 3298814 A1	28 March 2018
		US 9867039 B2	09 January 2018
		EP 3298814 A4	11 April 2018
		WO 2016206610 A1	29 December 2016
		US 2016381545 A1	29 December 2016
US 2018109552 A1	19 April 2018	None	