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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 June 2019 (13.06.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/112923 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04W 4/70* (2018.01)
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2018/063544

(22) International Filing Date:
03 December 2018 (03.12.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/594,333 04 December 2017 (04.12.2017) US

(71) Applicant: **CONVIADA WIRELESS, LLC** [US/US]; 200 Bellevue Parkway, Suite 300, Wilmington, DE 19809-3727 (US).

(72) Inventors: **STARSINIC, Michael, F.**; 200 Bellevue Parkway, Suite 300, Wilmington, DE 19809-3727 (US). **LI, Hongkun**; 200 Bellevue Parkway, Suite 300, Wilmington, DE 19809-3727 (US). **DI GIROLAMO, Rocco**; 200 Bellevue Parkway, Suite 300, Wilmington, DE 19809-3727 (US). **MLADIN, Catalina, Mihaela**; 200 Bellevue Parkway, Suite 300, Wilmington, DE 19809-3727 (US). **LY, Quang**; 200 Bellevue Parkway, Suite 300, Wilmington, DE 19809-3727 (US). **CHEN, Zhuo**; 200 Bellevue Parkway, Suite 300, Wilmington, DE 19809-3727 (US). **SEED, Dale, N.**; 200 Bellevue Parkway, Suite 300, Wilmington, DE 19809-3727 (US).

(74) Agent: **SAMUELS, Steven, B.** et al.; Baker & Hostetler LLP, 2929 Arch Street, Cira Centre, 12th Floor, Philadelphia, PA 19104-2891 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

(54) Title: IMPROVING SECURITY VIA AUTOMATED SIDEBAND COMMUNICATION FOR M2M/IOT

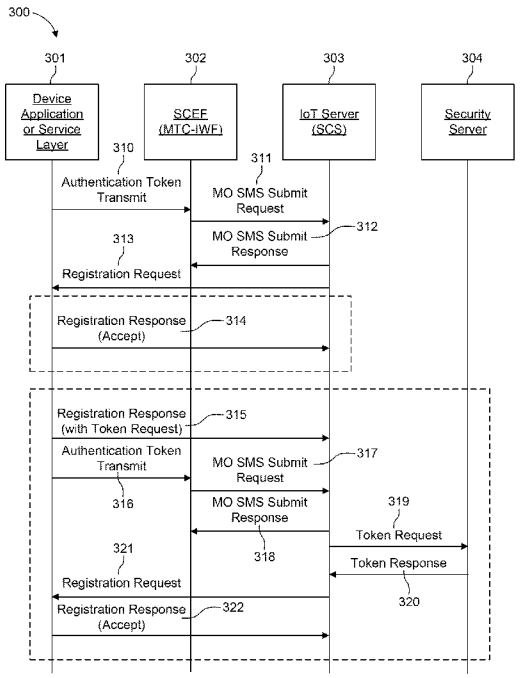


Fig. 3

(57) Abstract: Methods and apparatuses for improving security via sideband communications (i.e. secondary channels) are described herein. An apparatus may detect an initiation event on a primary channel of a communication network. The primary channel may be a user plane channel communicating via Internet Protocol (IP). The apparatus may transmit, to a server via a secondary channel of the communication network, a sideband message that includes an authentication token and a transaction reference identifier. The secondary channel may be a control plane channel communicating via short message service (SMS) or Non-IP Data Delivery. The apparatus may receive, from the server via the primary channel, a registration request message. If the registration request message includes the authentication token and the transaction reference identifier, the apparatus may transmit, to the server via the primary channel, a registration acceptance message. The apparatus may otherwise reject registration.

WO 2019/112923 A1

[Continued on next page]

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

IMPROVING SECURITY VIA AUTOMATED SIDEBAND COMMUNICATION FOR M2M/IOT

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 62/594,333, filed December 4, 2017, which is hereby incorporated by reference in its entirety.

BACKGROUND

[0002] Narrowband LTE Radio or Internet of Things (NB-IoT) sensors may be deployed throughout city centers and be accessed by a plurality of Internet of Things (IoT) servers. NB-IoT sensors or many other IoT devices are lightweight and require long battery lifetimes.

[0003] Multi-Factor authentication is process in which a party is only considered to be authenticated after providing multiple pieces of evidence of their identity. Multi-factor authentication mechanisms are inherently more secure than a single factor authentication mechanism because an actor, who is impersonating another actor, would have to defeat multiple authentication mechanisms in order to defeat the authentication procedure.

[0004] One example of multi-factor authentication is when a user is logging onto a web site and a message pops up asking the user to enter a token that was sent via short message service (SMS). This type of multi-factor authentication requires human interaction to either click a button or type in the token, and accordingly it is not automated. This type of use case requires advanced I/O, such as an LCD display and/or keypad, which may not typically be found on machine to machine (M2M) or IoT constrained devices. An I/O or keypad would be needed in order for the user to enter the received token. Accordingly, there is a need to enable IoT devices, applications, and servers to authenticate without human interaction. Existing service layer protocols do not support such device authentication methods.

SUMMARY

[0005] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter. Furthermore, the claimed subject matter is not limited to limitations that solve any or all disadvantages noted in any part of this disclosure.

[0006] Methods and apparatuses for improving security via sideband communications (i.e. secondary channels) are described herein. Sideband communication or sideband messages may be communication that takes a path that is different than the main IP traffic (i.e. the primary channel) and may be secured via different means (i.e. a secondary channel). In accordance with various embodiments, an apparatus may detect an initiation event on a primary channel of a communication network. The primary channel may be a user plane channel communicating via Internet Protocol (IP). The apparatus may transmit, to a server via a secondary channel of the communication network, a sideband message that includes an authentication token and a transaction reference identifier. The secondary channel may be a control plane channel communicating via short message service (SMS) or Non-IP Data Delivery. The sideband message may be transmitted to the server via a service capability exposure function (SCEF). The apparatus may receive, from the server via the primary channel, a registration request message. On a condition that the registration request message includes the authentication token and the transaction reference identifier, the apparatus may transmit, to the server via the primary channel, a registration acceptance message. On a condition that the registration request message does not include the authentication token and the transaction reference identifier, the apparatus may transmit, to the server via the primary channel, a registration response message that indicates that authentication is not accepted.

[0007] In accordance with another embodiment, the apparatus may receive, from a server via a primary channel of a communication network, a registration request message. The primary channel may be a user plane channel communicating via IP. On a condition that the registration request message includes an authentication token and a transaction reference identifier, the apparatus may transmit, to the server via the primary channel, a registration acceptance message. On a condition that the registration request message does not include the authentication token and

the transaction reference identifier, the apparatus may transmit, to the server via the primary channel, a registration response message that indicates that authentication is not accepted. On a condition that authentication was not accepted, the apparatus may transmit, to the server via a secondary channel of the communication network, a sideband message that includes the authentication token and the transaction reference identifier. The secondary channel may be a control plane channel communicating via SMS or Non-IP Data Delivery.

[0008] In accordance with another embodiment, the apparatus may receive from a first server a request message. The apparatus may determine whether a policy is associated with the request message that indicates that a sideband warning message should be transmitted. The sideband warning message may be transmitted via SMS or non-IP data delivery. On a condition that the policy indicates that the sideband warning message should be transmitted, the apparatus may transmit, to a second server, the sideband warning message that includes a transaction reference identifier and a description of the request message. The apparatus may receive from the second server a sideband message that indicates that the request message is associated with unauthorized activity and that includes the transaction reference identifier and a remedial action.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] In order to facilitate a more robust understanding of the application, reference is now made to the accompanying drawings, in which like elements are referenced with like numerals. These drawings should not be construed to limit the application and are intended only to be illustrative.

[0010] Fig. 1 depicts an example architectural reference model of the Service Capability Exposure Framework (SCEF);

[0011] Fig. 2 depicts an example scenario in which a legitimate SCS/IoT Server or network application communicates with an IoT Device;

[0012] Fig. 3 depicts an example procedure for use in an IoT device for automated sideband communication for authentication of an IoT Server in accordance with one embodiment;

[0013] Fig. 4 depicts an example procedure for use in an IoT device for automated sideband communication for authentication of an IoT Server in accordance with another embodiment;

[0014] Fig. 5 depicts an example procedure for use in an IoT device for using sideband communication to detect network intrusion in accordance with another embodiment;

[0015] Fig. 6 is a diagram of an example graphic user interface (GUI) that may be provided by an IoT Device;

[0016] Fig. 7 is a diagram of another example GUI that may be provided by an IoT Device;

[0017] Fig. 8A is a system diagram of an example machine-to-machine (M2M) or Internet of Things (IoT) communication system in which one or more disclosed embodiments may be implemented;

[0018] Fig. 8B is a system diagram of an example architecture that may be used within the M2M / IoT communications system illustrated in Fig. 8A;

[0019] Fig. 8C is a system diagram of an example M2M / IoT terminal or gateway device that may be used within the communications system illustrated in Fig. 8A; and

[0020] Fig. 8D is a block diagram of an example computing system in which aspects of the communication system of Fig. 8A may be embodied

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0021] The Third Generation Partnership Project (3GPP) provides a Service Capability Exposure Framework (SCEF) that exposes core network services to, for example, Internet of Things (IoT) Servers. A SCEF may have an integrated Machine Type Communication Interworking Function (MTC-IWF) that performs the functions that are described as being performed by the SCEF, or the functions that are described as being performed by the SCEF may be performed by the MTC-IWF. The SCEF may also be referred to as a 5G Network Exposure Function (NEF). The NEF may provide the same services that are provided by the SCEF. An IoT Server may also be referred to herein as a Service Capability Server (SCS), an Application Server (AS), or an Application Function (AF).

[0022] Fig. 1 depicts an example architectural reference model of the SCEF 100. As shown in the example of Fig. 1, the SCEF 103 has application programming interfaces (APIs) defined that provide access to 3GPP interfaces and capabilities. In the example of Fig. 1, API 1 102a, API 2 102b, API 3 102c ... API n 102d provide access to 3GPP interfaces and capabilities. The expose services by the network creates a "toolbox" of capabilities that, with proper authorization, may be used by the 3rd Party Servers (SCS/AS) 101a, 101b, 101c to retrieve information, to request specific services, to receive notifications, to request the setting of specific parameters, etc. Referring to the example of Fig. 1, the SCEF may have access to the following 3GPP network entities and interfaces in the trust domain 104: the Home Subscriber Server (HSS) 105 via a S6t 106 interface, the Policy Control and Charging Rules Function (PCRF) 107 via a Rx, Nt 108 interface, the Packet Flow Description Function (PFDF) 109 via a Nu 110 interface, the Mobility Management Entity and Serving GPRS Support Node (MME/SGSN) 111 via a T6a/T6b 112 interface, the Broadcast-Multicast Service Centre (BM-SC) 113 via a MB2 114 interface, the Serving – Call State Control Function (S-CSCF) 115 via a ISC 116 interface, and the RAN Congestion Awareness Function (RCAF) 117 via a Ns 118 interface. The SCEF 103 may abstract services from these underlying 3GPP network interfaces and protocols, which may allow access by each SCS/AS 101a, 101b, 101c to services via a RESTful interface referred to as the T8 119 interface.

[0023] The following is a list of acronyms relating to technologies that may be used in the architecture depicted in Fig. 1 and in the examples described herein:

AF Application Function

APN Access Point Name

AS Application Server

IoT Server Internet of Things Server

MSISDN Mobile Station International Subscriber Directory Number

NEF Network Exposure Function

NIDD Non-IP Data Delivery

PoA Point of Access

MO Mobile Originated

MT Mobile Terminated

MTC-IWF Machine Type Communication Interworking Function

SCEF Service Capability Exposure Function

SCS Service Capability Server

SMS Short Message Service

[0024] A UE may send SMS messages to an SCS/IoT Server. 3GPP defines a procedure referred to as Mobile Station International Subscriber Directory Number (MSISDN)-less mobile originated (MO)-SMS via the T8 interface. In this procedure, an SMS message may be sent from a UE and delivered to an SCS/IoT Server via a T8 interface API of the SCEF. This procedure does not require the UE or the SCS/IoT Server to have an MSISDN. When the SMS message is sent to the SCS/IoT Server by the SCEF, the SCEF provides the SCS/IoT Server with an External Identifier of the UE. The UE may be provisioned with an SMS Service Centre Address that may be used to reach the SCS/IoT Server. When the SMS Service Centre receives the SMS message, it may be provisioned to know that SMS messages from that UE should be routed towards the SCS/IoT Server based on the SMS Service Centre Address. The SMS Service Centre may will use the SMS Application port identifier field of the message to determine to which SCS/IoT Server the message should be sent.

[0025] A SCS/IoT Server may send SMS messages to a UE. 3GPP defines a procedure referred to as Device Triggering via the T8 interface. In this procedure, an SMS message is sent from the SCS/IoT Server and is delivered to the UE. An application on the UE may be listening on the SMS port number that the SCS/IoT Server specifies in the trigger request.

[0026] Internet Protocol (IP) based communication protocols are often used to communicate between an IoT Device and an SCS/IoT Server. Sideband communication or sideband messages may be referred to herein as communication that takes a path that is different than the main IP traffic (i.e. the primary channel) between the UE and SCS/IoT Server and may be secured via different means (i.e. a secondary channel). SMS and Non-IP Data Delivery (NIDD) are two examples of sideband communication. Other examples of sideband communication include but are not limited to: routing traffic through a different network slice, through a different PDN connection, or towards a different IP Address.

[0027] A procedure is needed in which IoT Applications and Servers authenticate via sideband communication channels without human interaction. Thus, multi-factor authentication

procedures may be improved by enabling applications to associate tokens with requests, or transactions, in an automated manner. This enables applications and servers to know with which transaction a token is associated.

[0028] A security mechanism that may be referred to as a honey pot is often used in information technology (IT) networks to detect unauthorized use of the IT network. For example, a network administrator may set up a server on his network referred to as the honey pot server, which is made to appear to have interesting information but has no useful information. Furthermore, this server may send warning messages to an IT administrator whenever a user accesses it. The network administrator may conclude that a user accessing the honey pot server is an indication that network security may have been breached and an unauthorized user is accessing the network. The network administrator would then go on to further investigate the suspicious activity.

[0029] In the embodiments described herein, an IoT Device may leverage the services of a mobile core network to more reliably authenticate SCS/IoT Servers or the Network Applications that it communicates with. When an SCS/IoT server attempts to establish communication with an IoT device, there are authentication mechanisms that allow the remote device to authenticate the SCS/IoT Server. For example, the oneM2M standard defines authentication mechanisms that are based on provisioned keys and/or certificates. However, keys and certificates may be compromised in a similar way that a username and password may be compromised. In a scenario where keys and/or certificates are the only thing that is relied on for authentication, it would be useful to have a secondary authentication method available. It would be preferable that any such secondary authentication mechanism use, as a much as possible, secondary communication channels that are separate from the communication channels that are used by the primary authentication method. Thus, any hacker, or impersonator, would be required to defeat additional layers of security to successfully defeat the authentication procedure and make themselves appear as a legitimate IoT Server. Similarly, when an IoT device attempts to register with, or establish communication with, an SCS/IoT Server, the IoT device may verify that it is communicating with a legitimate SCS/IoT Server and that its traffic has not been redirected to a malicious actor.

[0030] Fig. 2 depicts an example scenario in which a legitimate SCS/IoT Server or network application communicates with an IoT Device 200. In the example of Fig. 2, there are

two possible access paths. In path 1 211, the network application 206 has access to an SCS/IoT Server 205 but communicates directly with the remote IoT sensor 201 via the Internet 204, mobile core network 203, and radio access network 202. In path 2 210, the network application 206 does not directly communicate with the remote IoT sensor 201, but instead the SCS/IoT Server 205 communicates directly with the remote IoT sensor via the Internet 204, mobile core network 203, and radio access network 202. In both scenarios, the authentication issues are the same.

[0031] Mutual authentication is the process where the IoT Device authenticates the SCS/IoT Server, and the SCS/IoT Server authenticates the IoT Device. In accordance with the embodiments described herein, the IoT Device may leverage the services of the mobile core network to more reliably authenticate the SCS/IoT Servers, or network applications with which it communicates.

[0032] In the embodiments described herein, services of the mobile core network may be used by IoT Service Providers to detect malicious activity such as a malicious actor gaining access in their IoT Network (i.e. on their IoT Devices). For example, a malicious actor may be someone who stole a legitimate set of login credentials or may be someone who has legitimate login credentials but is intent on stealing information or harming the network. As aforementioned, honeypots may be set up in IT network to help detect network intrusion. However, as described above, there is a need in service layer standards for support of network intrusion detection.

[0033] In the embodiments described herein, sideband communication (i.e. SMS or NIDD) via a secondary channel may be used to improve the reliability of the procedure that the device application, or service layer, uses to authenticate the IoT Server.

[0034] In an example, a device may send authentication tokens to an SCS/IoT Server via a sideband communication channel (also referred to herein as a secondary channel), thus taking advantage of mobile core network services including but not limited to SMS and NIDD. The SCS/IoT Server may then provide the device application with the token that was received via SMS. As a result, any hacker who may have compromised the key, certificate, user name, and/or password would also need to have intercepted the SMS messages directed to the IoT Server in order to authenticate with the device. Thus, it is much more difficult for the hacker to circumvent the authentication procedure. The IoT Device and SCS/IoT Server may also coordinate their use of the sideband authentication mechanism. The IoT Device may also obtain the information in

order to address the SCS/IoT Server so that the sideband message is properly routed to the SCS/IoT Server.

[0035] In another example, a device application may be configured with a policy such that whenever a resource, or memory location, or setting, is accessed (read or write) a sideband alarm or warning message is sent to the SCS/IoT Server. The IoT Device may be configured with polices to control these sideband alarm messages. When the SCS/IoT Server receives the warning message the IoT Server may analyze the warning message and determine if action needs to be taken or not. For example, the SCS/IoT Server may determine that the warning message describes that a different, unauthorized SCS/IoT Server attempted to access the device application. The SCS/IoT Server may then send a warning message to an administrative monitoring application, for example, to warn the network administrator of the potential network intrusion.

[0036] Figs. 3 to 7 (described hereinafter) illustrate various embodiments associated with improving security via sideband communications. In these figures, various steps or operations are shown being performed by one or more nodes, apparatuses, devices, servers, functions, or networks. For example, the apparatuses may operate singly or in combination with each other to effect the methods described herein. As used herein, the terms apparatus, network apparatus, node, server, device, entity, network function, and network node may be used interchangeably. It is understood that the nodes, devices, servers, functions, or networks illustrated in these figures may represent logical entities in a communication network and may be implemented in the form of software (e.g., computer-executable instructions) stored in a memory of, and executing on a processor of, a node of such network, which may comprise one of the general architectures illustrated in Figs. 8A or 8B described below. That is, the methods illustrated in Figs. 3 to 7 may be implemented in the form of software (e.g., computer-executable instructions) stored in a memory of a network node, such as for example the node or computer system illustrated in Figs. 8C or 8D, which computer executable instructions, when executed by a processor of the node, perform the steps illustrated in the figures. It is also understood that any transmitting and receiving steps illustrated in these figures may be performed by communication circuitry (e.g., circuitry 34 or 97 of Figs. 8C and 8D, respectively) of the node under control of the processor of the node and the computer-executable instructions (e.g., software) that it executes. It is further understood that

the nodes, devices, and functions described herein may be implemented as virtualized network functions.

[0037] Fig. 3 depicts an example procedure 300 for use in an IoT device for automated sideband communication for authentication of an IoT Server in accordance with one embodiment, which may be used in combination with any of the embodiments described herein. In the example of Fig. 3, the IoT device transmits and receives messages using the sideband communication mechanisms (e.g. SMS of NIDD) that are provided by the 3GPP mobile core network to improve the reliability of the authentication of an SCS/IoT Server performed by the device application or service layer. This procedure 300 may be part of various other processes including but not limited to registration process, a standalone authentication procedure, a resource read or write procedure, a boot strapping procedure, or an on-boarding procedure. In Fig. 3, messages that are sent to/from a core network node such as the SCEF 302 may be considered sideband messages. Messages that are shown as going directly between the device application or service layer 301 and SCS/IoT Server 303 are not sideband messages.

[0038] Referring to Fig. 3, the device application or service layer 301 may detect an initiation event on a primary channel of a communication network and then in response to detection of the initiation event transmit, to the SCS/IoT Server 303 via the SCEF 302, a sideband message via a secondary channel of the communication network (e.g. SMS message) that includes an authentication token 310. The primary channel may be a user plane channel communicating via Internet Protocol (IP). The secondary channel is a control plane channel communicating via SMS or Non-IP Data Delivery. Initiation events include but are not limited to the following: when the device application or service layer detects that it is not registered to any SCS/IoT Server; there is a suspicious access from an SCS/IoT Server that it does not recognize; at the expiration of a timer; after device power up; after the device losing and reestablishing IP connectivity with the network; after the device denied an attempt to access data; by a request from a user that may be initiated by a button push, a command line entry, or a GUI; when starting to access a new server/domain; when receiving requests from a new server/domain; etc.

[0039] The payload of the sideband message (e.g. SMS message) may contain information in addition to the authentication token that includes but is not limited to the following: a device application or service layer identifier; a time-stamp for the token; an expiration time for

the token or a lifetime for the token; a storage location for the token; a cause; a reference identifier; and an initiation vector (IV).

[0040] The storage location may be a resource name or URI, for example. The cause may be an indication of why the device application is sending the sideband message. For example, the cause may indicate that the sideband message was initiated because of any of the initiation events described above.

[0041] The reference identifier (i.e. transaction identifier) may be included in the sideband message (e.g. SMS message) if the sideband message (e.g. SMS message) is initiated based on a transaction or request from the SCS/IoT Server. The reference identifier may be a value that was provided by the SCS/IoT Server that the sideband message (e.g. SMS message) may include to enable the SCS/IoT Server to correlate the sideband message (e.g. SMS message) with the original transaction or request. This correlation of sideband communication with the original transaction or request enables automation of the authentication process.

[0042] The Initiation Vector (IV) may be used in an encryption algorithm. The encryption algorithm may be used to encrypt messages that are sent directly between the device application or service layer and IoT Server. This mechanism may be triggered in the IoT Server if suspicious activity is detected.

[0043] The device application may be provisioned with an MSISDN and application port identifier that may be used to send the message to the SCS/IoT Server. The MSISDN and application port identifier fields are included in the header of the SMS message. This provisioning may be in the code that is preloaded on the device, provided via a command line entry from a user, or provided by the user via a GUI. The SCS/IoT Server might have no assigned MSISDN. If the SCS/IoT Server has no MSISDN, the device application may be provisioned with an SMS Service Centre Address that may be used to send the message to the SCS/IoT Server. The SMS Service Centre Address is another field that is in the header of the SMS message. For example, the SMS message may be sent to a dummy MSISDN, and the SMS Service Centre would be provisioned to know that all SMS messages from the UE with a particular application port identifier should be routed towards a particular SCS/IoT Server.

[0044] The sideband message may then be sent 311 by the SCEF 302 to the SCS/IoT Server 303 via, for example, an MO SMS Submit Request message of the T8 interface. The MO

SMS Submit Request may include the external identifier of the device, the SMS payload, and the application port identifier. The SMS payload may include the information described above with respect to step 310. The IoT Server may interpret this request from the Device Application as a request for the IoT Server to initiate contact with the Device Application. The SCS/IoT Server 303 may store the token and its expiration time, and the value may be stored in a location indicated in the payload.

[0045] The SCS/IoT Server 303 may acknowledge the request by sending an MO SMS Submit Response message of the T8 interface 312 to the SCEF 302.

[0046] When the SCS/IoT Server 303 registers or communicates with the device application or service layer 301, the same authentication token may be provided back to the device application or service layer 301. If the same authentication token is not provided, the device application or service layer 301 may choose to disallow the registration request. The server initiated (i.e. registration, communication, bootstrapping, or onboarding) procedure that is initiated may comprise an additional authentication mechanism that is based on a key, certificate, user name, and/or password. By the SCS/IoT Server 303 providing the device application or service layer 301 with the token that was received via a sideband channel (i.e. secondary channel) such as SMS of NIDD, a hacker who may have compromised the key, certificate, user name, and/or password would also need the ability to intercept sideband channel messages (e.g. SMS messages) directed to the SCS/IoT Server 303 in order to authenticate with the device application or service layer 301. Thus, it would be a lot more difficult for the hacker to circumvent the authentication procedure.

[0047] Referring to FIG. 3, the SCS/IoT Server 303 may send via the primary channel a registration request message 313 to the device application or service layer 301. The request may include an authentication token that was previously received from the device application or service layer 301 and stored in a resource on the SCS/IoT Server 303. For example, the token may have been received as described above from the device application or service layer 301 via the SCEF 302. The SCS/IoT Server 303 may hash or perform some other pre-determined mathematical operation on the token before sending it back to the device application or service layer 301. The registration request message may also include an identifier associated with the SCS/IoT Server 303 and the reference identifier. It should be appreciated that although this procedure describes the

registration request, the same concepts could be applied to other types of requests, such as requests to read or write a resource or data.

[0048] The device application or service layer 301 may respond to the SCS/IoT Server 303. If the registration request message from the SCS/IoT Server 303 included an authentication token and the device application or service layer 301 has verified that the token is correct, the device application or service layer 301 may respond by indicating that the registration request message (or read or write) has been accepted 314. The procedure 300 may stop at this point.

[0049] The device application or service layer 301 may respond to the registration request message with an indication that the SCS/IoT Server 303 needs to provide an additional token, or value, in order to be considered successfully authenticated. For example, the device application or service layer 301 may provide the token to the SCS/IoT Server 303. The SCS/IoT Server 303 may then complete the authentication process by providing the token value to the device application or service layer 301. Thus, the following steps depicted in Fig. 3 may be needed if the device application or service layer 301 responds to the registration request message with an indication that the SCS/IoT Server 303 needs to provide an additional token or value, in order to be considered successfully authenticated. Referring to Fig. 3, the device application or service layer 301 may respond 315 via the primary channel to the SCS/IoT Server 303 indicating that the registration (or read or write) has been rejected or conditionally accepted and indicating a request for an authentication token in order to proceed in communicating. The response 315 may indicate that a token has already been sent (as described above) or that a token will be sent. This response message may indicate a type of communication used to send the message (e.g. SMS or NIDD) and where the token has been stored (e.g. a resource name).

[0050] The device application or service layer 301 may map the identifier associated with the SCS/IoT Server 303 identifier that was received the registration request message to an MSISDN and application port identifier or an SMS Service Centre Address and port identifier. The device application or service layer 301 may then send an authentication token 316 to the SCS/IoT Server 303 via a sideband message on the secondary channel as described above. The payload of the message may also include the reference identifier that may have been received from the SCS/IoT Server 303 in the registration request. The storage location for the token that is indicated in the payload may have been provided to the device application. The sideband message

may then be sent 317 by the SCEF 302 to the SCS/IoT Server 303 via an MO SMS Submit Request message of the T8 interface as described above. The SCS/IoT Server 303 may acknowledge the request 318 by sending an MO SMS Submit Response message of the T8 interface.

[0051] The sideband communications of Fig. 3 may also include a communication path to a known IP address. This known IP address may be referred to as a logical security server 304 whose role is to store tokens and supply the tokens to valid requesting entities. The device application or service layer 301 and the SCS/IoT server 303 may both have a priori knowledge of the security server 304 (i.e. the IP address of this device). The device application or service layer 301 may store the token in the security server 304 using an authentication token transmit request. This request may contain the information included in the payload of the sideband message described above and also information including but not limited to the following: a list of whitelisted IoT servers and network applications (those IoT servers and network application that are allowed to access the token); a list of blacklisted IoT servers and network applications (those IoT servers and network application that are not allowed to access the token); and time windows when such access lists are active.

[0052] The whitelist of SCS/IoT servers and network applications may contain one or more of the following: identifier of IoT Server/Network Application, IP address of IoT Server/Network Application, type of IoT Server/Network Application, the requested operation to be performed on the Device Application/Service layer, etc.

[0053] The blacklist of SCS/IoT servers may contain one or more of the following: identifier of IoT Server/Network Application, IP address of IoT Server/Network Application, type of IoT Server/Network Application, the requested operation to be performed on the Device Application/Service layer, etc.

[0054] Referring to Fig. 3, upon receiving an access (registration, write, delete, etc.) registration request message 313, the device application or service layer 301 may respond with an access response telling the IoT server to obtain a valid token. Subsequently, the SCS/IoT server 303 may retrieve the token from the security server 304 using an authentication token retrieve request 319. This request may include the device application or service layer 301 identifier, the identifier associated with the SCS/IoT Server 303, the SCS/IoT Server type, the type of request the IoT intends to perform on the device application or service layer, etc. The identity of the

security server 304 may be stored in the SCS/IoT Server 303 or it may have been provided to the SCS/IoT Server 303 by, for example, the device application or service layer 301 in the registration response. The security server 304 may then check if the SCS/IoT server 303 is allowed to access the token for the device application or service layer 301, and if allowed, the authentication token may be provided 320 to the SCS/IoT Server 303 in an authentication token retrieve response. The SCS/IoT server 30 may then use the token when it re-sends the access request. For added security, the token may be pseudo-randomly moved between security servers. This movement is known to both the device application or service layer 301 and the allowed SCS/IoT Servers.

[0055] The SCS/IoT Server 303 may then send a registration, communication, read, or write request 321 to the device application or service layer 301. The request message may include the authentication token that was previously received. The request message may also include the identifier associated with the SCS/IoT Server 303 identifier and reference identifier. It should be appreciated that although this procedure describes the registration request, the same concepts could be applied to other types of requests, such as requests to read or write a resource or data. The request message may alternatively include a token or value that is the result of a mathematical operation that was performed on the tokens that were received in the other steps in the procedure. The device application or service layer 301 may respond 322 to the SCS/IoT Server 303 with an indication that the registration (or read or write) has been allowed. The procedure may stop at this point.

[0056] Fig. 4 depicts an example procedure 400 for use in an IoT device for automated sideband communication for authentication of an IoT Server in accordance with another embodiment, which may be used in combination with any of the embodiments described herein. In the example of Fig. 4, the device application or service layer 401 may authenticate the SCS/IoT Server 403 when initiating a request and may authenticate response from the SCS/IoT Server 404. The device application or service layer 401 may send a sideband message 410 (e.g. SMS message or NIDD) including a token and a reference identifier (i.e. transaction identifier) to the SCS/IoT Server 403. The sideband message may be then be sent 411 by the SCEF 402 to the SCS/IoT Server 403 via, for example, an MO SMS Submit Request message of the T8 interface. The SCS/IoT Server 403 may acknowledge the request by sending an MO SMS Submit Response message of the T8 interface 412 to the SCEF 402.

[0057] When the SCS/IoT Server 403 receives the token, it may send a request 413 to verify the token to a security server 404 to verify that the token is legitimate The request may include the token, a reference identifier (i.e. transaction identifier), device application identifier, device identifier, identifier associated with the SCS/IoT Server 403, and any of the information that was sent to the SCS/IoT Server 403. The Security Server 404 may perform a mathematical function, or hash on the token and respond to the IoT Server with a new hash. The mathematical function, or hash, maybe based on the identity of the device, device application, the reference identifier (i.e. transaction identifier), and/or the identifier associated with the SCS/IoT Server 403. The security server 404 may respond 414 to the SCS/IoT Server 403 and provide an indication of whether or not the token is valid and may include a new token.

[0058] The device application or service layer 401 may send a request 415 to the SCS/IoT Server 403 that includes a reference identifier (i.e. transaction identifier). The reference identifier (i.e. transaction identifier) may be the same or different than the reference identifier (i.e. transaction identifier) that was included in the sideband message 410. If it is different, then it might be the result of the same mathematical function that the security server 404 may have performed.

[0059] The SCS/IoT Server 403 may respond 416 to the request, and the response may include the reference identifier (i.e. transaction identifier), the token, and/or the value that was provided by the security server 404 to the device application or service layer 401 to enable the device application or service layer 401 to be sure that the response came from a legitimate SCS/IoT Server.

[0060] An IoT service provider may detect unauthorized access to a device or an IoT network in accordance with another embodiment. Further, activity on the IoT Device may be recorded and reports may be sent to the SCS/IoT Server that may be used for charging purposes or for detecting device or network level problems. A device application or service layer may be configured with a policy such that whenever a resource, or memory location, or setting, is accessed (read or write) a sideband alarm or warning message is sent to the IoT Server. The policy may be provided by the IoT Server and attached, as an attribute, to the resource.

[0061] However, it might not be preferable to allow the IoT Server to configure this policy because the policy may influence how authentication of the IoT Server is performed.

Instead, the policy that dictates when a device sends a sideband alarm may be provisioned by the user (i.e. the device owner or operator) via a GUI or command line interface. Alternatively, the policy may be configured via a Mobile Terminated SMS (or NIDD or a device management procedure) message. When the IoT Server receives the warning message, the IoT Server may analyze the warning message and determine if action needs to be taken or not. For example, the IoT Server may determine that the warning message describes that a different, unauthorized IoT Server attempted to access the device application or service layer. The IoT Server may then send a warning message to the administrative monitoring application to warn the network administrator of the potential network intrusion.

[0062] Fig. 5 depicts an example procedure 500 for use in an IoT device for using sideband communication to detect network intrusion in accordance with another embodiment, which may be used in combination with any of the embodiments described herein. In the example of Fig. 5, messages that are transmitted to/from a core network node such as the SCEF may be considered a sideband message. Messages that are shown as going directly between the device application or service layer and the SCS/IoT Server are not sideband messages. Sideband alarm messages may also be triggered by other conditions. For example, the device application or service layer may detect that its battery is dying. In another example, it may determine, based on input from a GUI or a vibration detector that the device is being tampered with, turned off, or decommissioned.

[0063] Referring to Fig. 5, the device application or service layer 501 may receive requests 510 or 511, which may have been sent from legitimate SCS/IoT Server 503 or illegitimate SCS/IoT Server 504 (i.e. a hacker), respectively. The requests may include, for example, registration requests, login requests, read requests, write requests, etc. The device application or service layer 501 may respond 512, 513 to the requesting SCS/IoT Server, which in the example of Fig. 5 may be legitimate SCS/IoT Server 503 or illegitimate SCS/IoT Server 504. The device application or service layer 501 may check if there is a policy 514 associated with the request or resource that the request message targets. For example, a policy may indicate for example:

[0064] That a sideband warning message should be sent whenever a request is rejected because the requestor does not have access rights to a requested resource or command, or the request is for a restricted resource.

[0065] That a sideband warning message should be sent whenever a request is rejected because the requestor attempted to access a non-existent resource or attempted an invalid command.

[0066] That a sideband warning message should be sent whenever a certain command is received or if a certain resource is accessed. The policy could further dictate that the warning should be sent after the resource or command is accessed a certain number of times or at a certain rate.

[0067] That a sideband warning message should be sent whenever the device application detects that the device is physically re-located, shaken, etc.

[0068] That a sideband warning message should be sent whenever the device application updates certain resources or detects new operating conditions.

[0069] That a sideband warning message should be sent whenever the request message is from a certain originator, region or a location.

[0070] Dummy resources, memory locations, or commands may be made available on the IoT device or device application. The dummy resources, memory locations, or commands may be made to appear real or interesting so that an unauthorized user would be enticed to access them, thus causing a sideband warning message to be sent to a legitimate SCS/IoT Server.

[0071] The device application or service layer 501 may transmit a sideband warning message 515 (e.g. an SMS message) to the SCS/IoT Server 503 via SCEF 502. The sideband message may be transmitted whenever policies dictate, as described above. The device application, or UE, may be provisioned with an MSISDN and application port identifier that may be used to send the message to the SCS/IoT Server. The MSISDN and Application port identifier are fields in the header of the SMS message. This provisioning may be in the code that is preloaded on the device, provided via a command line entry from the user, or provided by the user via a GUI. The IoT Server might have no assigned MSISDN. If the SCS/IoT Server has no MSISDN, the device application, or UE, may be provisioned with an SMS Service Centre Address that could be used to send the message to the SCS/IoT Server. SMS Service Centre Address is another field that is in the header of the SMS. The SMS message may be sent to a dummy MSISDN, and the SMS Service Centre may be provisioned to know that all SMS messages from the UE with a particular application port identifier should be routed towards a particular SCS/IoT Server. The payload of

the sideband message (e.g. SMS message) may contain information including but not limited to the following: device application or service layer identifier; a time-stamp for the warning report; a description of the event; the IP Address that initiated the request that caused the warning; the command or resource that was accessed, or attempted to be accessed; what triggered the report (e.g. too many accesses, denied access rights, etc.); whether or not the attempted access was successful; reference identifier (i.e. transaction identifier) such as any reference identifier that was provided by the requestor; the credentials that were provided by the requestor; and a sideband reply port.

[0072] The sideband warning message may be transmitted by the SCEF 502 to the SCS/IoT Server 503 via, for example, an MO SMS Submit Request message of the T8 interface 516. The MO SMS Submit Request message may include the external identifier of the UE, the SMS payload, and application port identifier. The SMS payload in the MO SMS Submit Request message may include the fields that were listed above.

[0073] The SCS/IoT Server 503 may acknowledge the request by sending an MO SMS Submit Response message of the T8 interface 517 to the SCEF 502. The SCS/IoT Server 503 may analyze 518 the sideband warning message and determine if the behavior that is described in the sideband warning message is legitimate or not. For example, it may check charging records or resources and determine that the IoT Server previously generated the requests(s) that are described in the warning report.

[0074] If the SCS/IoT Server 503 determines that the warning message describes illegitimate or possible illegitimate activity, it may send a warning message to a network application or administrative monitoring application 505 that may transmit a warning message 519 to the network administrator that network security may have been compromised. The network administrator may then examine the situation more closely and possibly decide to take action such as, for example, changing passwords or credentials within the network.

[0075] If the SCS/IoT Server 503 determines that the description of the transaction is not acceptable, or is suspicious, the SCS/IoT Server 503 may transmit a sideband remedy message 520 to the device application or service layer 501 that for example, may command it to shut down, change its security credentials, invalidate its security credentials, stop communicating with a particular client/IoT Server, reverse, or undo a transaction, or disallow a transaction. A sideband

remedy message 520 may include the same reference identifier (i.e. transaction identifier) that was transmitted by the device application or service layer 501 so that the device application or service layer 501 knows which transaction has been determined to be not acceptable, or suspicious, by the SCS/IoT Server 503. The a sideband remedy message 520 may be transmitted via Mobile Terminated SMS (i.e. a device trigger) or a mobile terminated non-IP message, and it may be directed to the sideband reply port that was provided by the device application or service layer 501 in sideband warning message 515.

[0076] The procedure of Fig. 5 may also be used by the device application or service layer to record transactions via sideband messages that are sent to a SCS/IoT Server. For example, the SCS/IoT Server that sends the messages 510 or 511 may be different than the SCS/IoT Server that receives the sideband warning message 515 and analyzes 518 the warning, which may be an SCS/IoT Server that is used for receiving sideband reports from IoT Devices. The reports may be records or logs of device activity for the purpose of charging the SCS/IoT Servers that access the device via messages 510 or 511 rather than warnings.

[0077] The procedures in the examples of Fig. 3, Fig. 4, and Fig. 5 may apply to other forms of sideband communication other than SMS. For example, the procedures of Fig. 3, Fig. 4, and Fig. 5 may be modified to show that non-IP Data Delivery may be used to send sideband messages to the SCS/IoT Server. For example, the procedures of Fig. 3, Fig. 4, and Fig. 5 may reference the Mobile Originated NIDD Procedure that may be used instead of the procedure for MSISDN-less MO-SMS via T8.

[0078] When NIDD is used instead of SMS, the device application may not be provisioned with an MSISDN and application identifier or SMS Service Centre Address and application port identifier for contacting the IoT Server. Instead, the IoT device application, or IoT device, may need to be provisioned with an Access Point Name (APN) that may be used to send the port to the IoT Server. If the Reliable Data Service is used to send the non-IP packet, then the IoT device application, or IoT device, may also need to be provisioned with a source and destination application port identifier that may be used to route the message to the SCS/IoT Server and indicate what Device Application sent the message.

[0079] The procedures in the examples of Fig. 3, Fig. 4, and Fig. 5 may apply to authenticating the IoT device application instead of the SCS/IoT Server. For example, the

procedures of Fig. 3, Fig. 4, and Fig. 5 may be modified for the case where the IoT device application initiates contact with the SCS/IoT Server. Instead of using Mobile Originated SMS or NIDD procedures to send messages, as described above, the SCS/IoT Server may use the Device Triggering Procedure via the T8 interface to send SMS messages to the device application or the Mobile Terminated NIDD Procedure to send non-IP data packets to the IoT device application.

[0080] For example, steps 310, 311, and 312 of Fig. 3 may be replaced by the SCS/IoT Server sending a device trigger, SMS, or Non-IP message to the UE with all the information that is listed in step 310 of Fig. 3. Steps 313 and 314 of Fig. 3 may be replaced by the device application initiating contact with the SCS/IoT Server to register, refresh its PoA, read a resource, write a resource, etc. The message from the device application may include the fields that are listed in step 313 of Fig. 3. Step 315 may be replaced by the SCS/IoT Server sending a response to the device application that indicates that the device application needs to reattempt the request and provide a token. Steps 316, 317, and 318 may be replaced by the SCS/IoT Server sending a device trigger, SMS, or Non-IP message to the UE with all the information that is listed in step 316 of Fig 3. Steps 319 and 320 of Fig. 3 may be replaced by the device application contacting a Security Server. Steps 321 and 322 of Fig. 3 may be replaced by the device application initiating contact with the SCS/IoT Server to register, refresh its PoA, read a resource, write a resource, etc.

[0081] In another example, the SCS/IoT Server may authenticate the device application and, as part of the authentication procedure, provide a token to the UE. The UE may use a sideband communication channel to send the token back to the SCS/IoT Server as described in step 310 or 315 of Fig. 3. The SCS/IoT Server may not consider the UE authenticated until after receiving the token via the sideband communication channel. Unlike the example in Fig. 3, the token that is provided to the SCS/IoT Server is based on the token that was received from the SCS/IoT Server. The device application may hash or perform some other pre-determined mathematical operation on the token before sending it back to the SCS/IoT Server.

[0082] Fig. 6 is a diagram of an example graphic user interface (GUI) 600 that may be provided by an IoT Device. The GUI 600 may be used to configure whether the UE is permitted to send sideband warning messages. The GUI 600 may allow the user to select what type of sideband methods should be used to send sideband messages and what events should be used to trigger a sideband warning message. The GUI 600 may be used to configure where sideband

messages are sent. For example, it may be used to provision the device with contact information for the IoT Server (MSISDN, SMS Service Address, and SMS Application Port Number for SMS and APN and NIDD Application Port number for NIDD). As shown in Fig. 6, the GUI 600 may provide the capability to allow sideband messages 601 via the yes/no 608 selection and configure sideband message types 602 SMS or NIDD 609. The GUI 600 may also enable the configuration of allowing SMS messages for the following events 603: when not registered 604, after loss of PS connection 605, after change of location 606, and after attempted access rights violations 607 via each of their respective allow selections 610, 611, 612, and 613.

[0083] Fig. 7 is a diagram of another example GUI 700 that may be provided by an IoT Device. The GUI 700 may be used, for example, in the case when multiple applications on the device use a feature. The GUI 700 may enable each application to be configured to use a different port number. In the example of Fig. 7, the GUI 700 may allow sideband warning message configuration 701. The GUI 700 may also enable an SMS Service Center Address 702 port number 707 to be configured, an MSISDN 703 port number to be configured 708, an NIDD APN 704 port number 709 to be configured, and device application 1 port number 705 – device application n 706 application port number to be configured with their respective port numbers 710 and 711.

[0084] Fig. 8A is a diagram of an example machine-to-machine (M2M), Internet of Things (IoT), or Web of Things (WoT) communication system 10 in which one or more disclosed embodiments may be implemented. Generally, M2M technologies provide building blocks for the IoT/WoT, and any M2M device, M2M gateway or M2M service platform may be a component of the IoT/WoT as well as an IoT/WoT service layer, etc. Any of the devices, functions, nodes, or networks illustrated in any of Figs. 1 to 7 may comprise a node of a communication system such as the one illustrated in Figs. 8A-B.

[0085] As shown in Fig. 8A, the M2M/IoT/WoT communication system 10 includes a communication network 12. The communication network 12 may be a fixed network (e.g., Ethernet, Fiber, ISDN, PLC, or the like) or a wireless network (e.g., WLAN, cellular, or the like) or a network of heterogeneous networks. For example, the communication network 12 may comprise multiple access networks that provides content such as voice, data, video, messaging, broadcast, or the like to multiple users. For example, the communication network 12 may employ one or more channel access methods, such as code division multiple access (CDMA), time division

multiple access (TDMA), frequency division multiple access (FDMA), orthogonal FDMA (OFDMA), single-carrier FDMA (SC-FDMA), and the like. Further, the communication network 12 may comprise other networks such as a core network, the Internet, a sensor network, an industrial control network, a personal area network, a fused personal network, a satellite network, a home network, or an enterprise network for example.

[0086] As shown in Fig. 8A, the M2M/ IoT/WoT communication system 10 may include the Infrastructure Domain and the Field Domain. The Infrastructure Domain refers to the network side of the end-to-end M2M deployment, and the Field Domain refers to the area networks, usually behind an M2M gateway. The Field Domain and Infrastructure Domain may both comprise a variety of different nodes (e.g., servers, gateways, devices, of the network. For example, the Field Domain may include M2M gateways 14 and terminal devices 18. It will be appreciated that any number of M2M gateway devices 14 and M2M terminal devices 18 may be included in the M2M/ IoT/WoT communication system 10 as desired. Each of the M2M gateway devices 14 and M2M terminal devices 18 are configured to transmit and receive signals via the communication network 12 or direct radio link. A M2M gateway device 14 allows wireless M2M devices (e.g. cellular and non-cellular) as well as fixed network M2M devices (e.g., PLC) to communicate either through operator networks, such as the communication network 12 or direct radio link. For example, the M2M devices 18 may collect data and send the data, via the communication network 12 or direct radio link, to an M2M application 20 or M2M devices 18. The M2M devices 18 may also receive data from the M2M application 20 or an M2M device 18. Further, data and signals may be sent to and received from the M2M application 20 via an M2M service layer 22, as described below. M2M devices 18 and gateways 14 may communicate via various networks including, cellular, WLAN, WPAN (e.g., Zigbee, 6LoWPAN, Bluetooth), direct radio link, and wireline for example. Exemplary M2M devices include, but are not limited to, tablets, smart phones, medical devices, temperature and weather monitors, connected cars, smart meters, game consoles personal digital assistants, health and fitness monitors, lights, thermostats, appliances, garage doors and other actuator-based devices, security devices, and smart outlets.

[0087] Referring to Fig. 8B, the illustrated M2M service layer 22 in the field domain provides services for the M2M application 20, M2M gateway devices 14, and M2M terminal devices 18 and the communication network 12. It will be understood that the M2M service layer

22 may communicate with any number of M2M applications, M2M gateway devices 14, M2M terminal devices 18, and communication networks 12 as desired. The M2M service layer 22 may be implemented by one or more servers, computers, or the like. The M2M service layer 22 provides service capabilities that apply to M2M terminal devices 18, M2M gateway devices 14 and M2M applications 20. The functions of the M2M service layer 22 may be implemented in a variety of ways, for example as a web server, in the cellular core network, in the cloud, etc.

[0088] Similar to the illustrated M2M service layer 22, there is the M2M service layer 22' in the Infrastructure Domain. M2M service layer 22' provides services for the M2M application 20' and the underlying communication network 12' in the infrastructure domain. M2M service layer 22' also provides services for the M2M gateway devices 14 and M2M terminal devices 18 in the field domain. It will be understood that the M2M service layer 22' may communicate with any number of M2M applications, M2M gateway devices and M2M terminal devices. The M2M service layer 22' may interact with a service layer by a different service provider. The M2M service layer 22' may be implemented by one or more servers, computers, virtual machines (e.g., cloud/compute/storage farms, etc.) or the like.

[0089] Still referring to Fig. 8B, the M2M service layer 22 and 22' provide a core set of service delivery capabilities that diverse applications and verticals can leverage. These service capabilities enable M2M applications 20 and 20' to interact with devices and perform functions such as data collection, data analysis, device management, security, billing, service/device discovery, etc. Essentially, these service capabilities free the applications of the burden of implementing these functionalities, thus simplifying application development and reducing cost and time to market. The service layer 22 and 22' also enables M2M applications 20 and 20' to communicate through various networks 12 and 12' in connection with the services that the service layer 22 and 22' provide.

[0090] The M2M applications 20 and 20' may include applications in various industries such as, without limitation, transportation, health and wellness, connected home, energy management, asset tracking, and security and surveillance. As mentioned above, the M2M service layer, running across the devices, gateways, and other servers of the system, supports functions such as, for example, data collection, device management, security, billing, location

tracking/geofencing, device/service discovery, and legacy systems integration, and provides these functions as services to the M2M applications 20 and 20'.

[0091] Generally, a service layer (SL), such as the service layers 22 and 22' illustrated in Figs. 8A and 8B, defines a software middleware layer that supports value-added service capabilities through a set of application programming interfaces (APIs) and underlying networking interfaces. Both the ETSI M2M and oneM2M architectures define a service layer. ETSI M2M's service layer is referred to as the Service Capability Layer (SCL). The SCL may be implemented in a variety of different nodes of the ETSI M2M architecture. For example, an instance of the service layer may be implemented within an M2M device (where it is referred to as a device SCL (DSCL)), a gateway (where it is referred to as a gateway SCL (GSCL)) and/or a network node (where it is referred to as a network SCL (NSCL)). The oneM2M service layer supports a set of Common Service Functions (CSFs) (i.e. service capabilities). An instantiation of a set of one or more particular types of CSFs is referred to as a Common Services Entity (CSE), which can be hosted on different types of network nodes (e.g. infrastructure node, middle node, application-specific node). The Third Generation Partnership Project (3GPP) has also defined an architecture for machine-type communications (MTC). In that architecture, the service layer, and the service capabilities it provides, are implemented as part of a Service Capability Server (SCS). Whether embodied in a DSCL, GSCL, or NSCL of the ETSI M2M architecture, in a Service Capability Server (SCS) of the 3GPP MTC architecture, in a CSF or CSE of the oneM2M architecture, or in some other node of a network, an instance of the service layer may be implemented in a logical entity (e.g., software, computer-executable instructions, and the like) executing either on one or more standalone nodes in the network, including servers, computers, and other computing devices or nodes, or as part of one or more existing nodes. As an example, an instance of a service layer or component thereof may be implemented in the form of software running on a network node (e.g., server, computer, gateway, device, or the like) having the general architecture illustrated in Fig. 8C or 8D described below.

[0092] Further, the methods and functionalities described herein may be implemented as part of an M2M network that uses a Service Oriented Architecture (SOA) and/or a resource-oriented architecture (ROA) to access services, such as the above-described Network and Application Management Service for example.

[0093] Fig. 8C is a block diagram of an example hardware/software architecture of a node of a network, such as one of the nodes, devices, functions, or networks illustrated in Figs. 1 to 7, which may operate as an M2M server, gateway, device, or other node in an M2M network such as that illustrated in Figs. 8A and 8B. As shown in Fig. 8C, the node 30 may include a processor 32, a transceiver 34, a transmit/receive element 36, a speaker/microphone 38, a keypad 40, a display/touchpad 42, non-removable memory 44, removable memory 46, a power source 48, a global positioning system (GPS) chipset 50, and other peripherals 52. The node 30 may also include communication circuitry, such as a transceiver 34 and a transmit/receive element 36. It will be appreciated that the node 30 may include any sub-combination of the foregoing elements while remaining consistent with an embodiment. This node may be a node that implements the notifications and triggers related thereto described herein.

[0094] The processor 32 may be a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Array (FPGAs) circuits, any other type of integrated circuit (IC), a state machine, and the like. The processor 32 may perform signal coding, data processing, power control, input/output processing, and/or any other functionality that enables the node 30 to operate in a wireless environment. The processor 32 may be coupled to the transceiver 34, which may be coupled to the transmit/receive element 36. While Fig. 8C depicts the processor 32 and the transceiver 34 as separate components, it will be appreciated that the processor 32 and the transceiver 34 may be integrated together in an electronic package or chip. The processor 32 may perform application-layer programs (e.g., browsers) and/or radio access-layer (RAN) programs and/or communications. The processor 32 may perform security operations such as authentication, security key agreement, and/or cryptographic operations, such as at the access-layer and/or application layer for example.

[0095] As shown in Fig. 8C, the processor 32 is coupled to its communication circuitry (e.g., transceiver 34 and transmit/receive element 36). The processor 32, through the execution of computer executable instructions, may control the communication circuitry in order to cause the node 30 to communicate with other nodes via the network to which it is connected. In particular,

the processor 32 may control the communication circuitry in order to perform the transmitting and receiving steps described herein (e.g., in Figs. 1-7) and in the claims. While Fig. 8C depicts the processor 32 and the transceiver 34 as separate components, it will be appreciated that the processor 32 and the transceiver 34 may be integrated together in an electronic package or chip.

[0096] The transmit/receive element 36 may be configured to transmit signals to, or receive signals from, other nodes, including M2M servers, gateways, devices, and the like. For example, in an embodiment, the transmit/receive element 36 may be an antenna configured to transmit and/or receive RF signals. The transmit/receive element 36 may support various networks and air interfaces, such as WLAN, WPAN, cellular, and the like. In an embodiment, the transmit/receive element 36 may be an emitter/detector configured to transmit and/or receive IR, UV, or visible light signals, for example. In yet another embodiment, the transmit/receive element 36 may be configured to transmit and receive both RF and light signals. It will be appreciated that the transmit/receive element 36 may be configured to transmit and/or receive any combination of wireless or wired signals.

[0097] In addition, although the transmit/receive element 36 is depicted in Fig. 8C as a single element, the node 30 may include any number of transmit/receive elements 36. More specifically, the node 30 may employ MIMO technology. Thus, in an embodiment, the node 30 may include two or more transmit/receive elements 36 (e.g., multiple antennas) for transmitting and receiving wireless signals.

[0098] The transceiver 34 may be configured to modulate the signals that are to be transmitted by the transmit/receive element 36 and to demodulate the signals that are received by the transmit/receive element 36. As noted above, the node 30 may have multi-mode capabilities. Thus, the transceiver 34 may include multiple transceivers for enabling the node 30 to communicate via multiple RATs, such as UTRA and IEEE 802.11, for example.

[0099] The processor 32 may access information from, and store data in, any type of suitable memory, such as the non-removable memory 44 and/or the removable memory 46. The non-removable memory 44 may include random-access memory (RAM), read-only memory (ROM), a hard disk, or any other type of memory storage device. The removable memory 46 may include a subscriber identity module (SIM) card, a memory stick, a secure digital (SD) memory card, and the like. In other embodiments, the processor 32 may access information from, and store

data in, memory that is not physically located on the node 30, such as on a server or a home computer. The processor 32 may be configured to control lighting patterns, images, or colors on the display or indicators 42 to reflect the status of a node or configure a node (e.g., nodes in Figs.1-7), and in particular underlying networks, applications, or other services in communication with the UE. The processor 32 may receive power from the power source 48, and may be configured to distribute and/or control the power to the other components in the node 30. The power source 48 may be any suitable device for powering the node 30. For example, the power source 48 may include one or more dry cell batteries (e.g., nickel-cadmium (NiCd), nickel-zinc (NiZn), nickel metal hydride (NiMH), lithium-ion (Li-ion), etc.), solar cells, fuel cells, and the like.

[00100] The processor 32 may also be coupled to the GPS chipset 50, which is configured to provide location information (e.g., longitude and latitude) regarding the current location of the node 30. It will be appreciated that the node 30 may acquire location information by way of any suitable location-determination method while remaining consistent with an embodiment.

[00101] The processor 32 may further be coupled to other peripherals 52, which may include one or more software and/or hardware modules that provide additional features, functionality, and/or wired or wireless connectivity. For example, the peripherals 52 may include various sensors such as an accelerometer, biometrics (e.g., fingerprint) sensors, an e-compass, a satellite transceiver, a digital camera (for photographs or video), a universal serial bus (USB) port or other interconnect devices, a vibration device, a television transceiver, a hands free headset, a Bluetooth® module, a frequency modulated (FM) radio unit, a digital music player, a media player, a video game player module, an Internet browser, and the like.

[00102] Fig. 8D is a block diagram of an exemplary computing system 90 which may also be used to implement one or more nodes of a network, such as nodes, devices, functions, or networks illustrated in Figs. 1-7, which may operate as an M2M server, gateway, device, or other node in an M2M network such as that illustrated in Figs. 8A and 8B. Computing system 90 may comprise a computer or server and may be controlled primarily by computer readable instructions, which may be in the form of software, wherever, or by whatever means such software is stored or accessed. Such computer readable instructions may be executed within central processing unit (CPU) 91 to cause computing system 90 to do work. In many known workstations, servers, and

personal computers, central processing unit 91 is implemented by a single-chip CPU called a microprocessor. In other machines, the central processing unit 91 may comprise multiple processors. Coprocessor 81 is an optional processor, distinct from main CPU 91, which performs additional functions or assists CPU 91. CPU 91 and/or coprocessor 81 may receive, generate, and process data related to the disclosed systems and methods for security protection.

[00103] In operation, CPU 91 fetches, decodes, and executes instructions, and transfers information to and from other resources via the computer's main data-transfer path, system bus 80. Such a system bus connects the components in computing system 90 and defines the medium for data exchange. System bus 80 typically includes data lines for sending data, address lines for sending addresses, and control lines for sending interrupts and for operating the system bus. An example of such a system bus 80 is the PCI (Peripheral Component Interconnect) bus.

[00104] Memory devices coupled to system bus 80 include random access memory (RAM) 82 and read only memory (ROM) 93. Such memories include circuitry that allows information to be stored and retrieved. ROMs 93 generally contain stored data that cannot easily be modified. Data stored in RAM 82 can be read or changed by CPU 91 or other hardware devices. Access to RAM 82 and/or ROM 93 may be controlled by memory controller 92. Memory controller 92 may provide an address translation function that translates virtual addresses into physical addresses as instructions are executed. Memory controller 92 may also provide a memory protection function that isolates processes within the system and isolates system processes from user processes. Thus, a program running in a first mode can access only memory mapped by its own process virtual address space; it cannot access memory within another process's virtual address space unless memory sharing between the processes has been set up.

[00105] In addition, computing system 90 may contain peripherals controller 83 responsible for communicating instructions from CPU 91 to peripherals, such as printer 94, keyboard 84, mouse 95, and disk drive 85.

[00106] Display 86, which is controlled by display controller 96, is used to display visual output generated by computing system 90. Such visual output may include text, graphics, animated graphics, and video. Display 86 may be implemented with a CRT-based video display, an LCD-based flat-panel display, gas plasma-based flat-panel display, or a touch-panel. Display

controller 96 includes electronic components required to generate a video signal that is sent to display 86.

[00107] Further, computing system 90 may contain communication circuitry, such as for example a network adaptor 97 that may be used to connect computing system 90 to an external communications network, such as network 12 of Fig. 8A and Fig. 8B, to enable the computing system 90 to communicate with other nodes of the network. The communication circuitry, alone or in combination with the CPU 91, may be used to perform the transmitting and receiving steps described herein (e.g., in Figs. 1-7) and in the claims.

[00108] In describing preferred embodiments of the subject matter of the present disclosure, as illustrated in the Figures, specific terminology is employed for the sake of clarity. The claimed subject matter, however, is not intended to be limited to the specific terminology so selected, and it is to be understood that each specific element includes all technical equivalents that operate in a similar manner to accomplish a similar purpose.

[00109] In describing preferred embodiments of the subject matter of the present disclosure, as illustrated in the Figures, specific terminology is employed for the sake of clarity. The claimed subject matter, however, is not intended to be limited to the specific terminology so selected, and it is to be understood that each specific element includes all technical equivalents that operate in a similar manner to accomplish a similar purpose.

What is Claimed:

1. An apparatus comprising a processor, a memory, and communication circuitry, the apparatus being connected to a network via its communication circuitry, the apparatus further comprising computer-executable instructions stored in the memory of the apparatus which, when executed by the processor of the apparatus, cause the apparatus to perform operations comprising:

detecting an initiation event on a primary channel of a communication network;

transmitting, to a server via a secondary channel of the communication network and in response to the initiation event, a sideband message that includes an authentication token and a transaction reference identifier;

receiving, from the server via the primary channel, a registration request message;

on a condition that the registration request message includes the authentication token and the transaction reference identifier, transmitting, to the server via the primary channel, a registration acceptance message; and

on a condition that the registration request message does not include the authentication token and the transaction reference identifier, transmitting, to the server via the primary channel, a registration response message that indicates that authentication is not accepted.

2. The apparatus as recited in claim 1, wherein the primary channel is a user plane channel communicating via Internet Protocol (IP).

3. The apparatus as recited in claim 1, wherein the secondary channel is a control plane channel communicating via short message service (SMS) or Non-IP Data Delivery.

4. The apparatus as recited in claim 1, wherein the sideband message is transmitted to the server via a service capability exposure function (SCEF).

5. The apparatus as recited in claim 1, wherein the detecting the initiation event includes detecting that the apparatus is not registered, detecting a suspicious access, expiration of a timer, power up, and losing Internet Protocol (IP) connectivity with the communication network.

6. The apparatus as recited in claim 1, further comprising:

on a condition that the apparatus transmitted the registration response message that indicates that authentication is not accepted, transmitting, to the server via the primary channel, an indication that the authentication token is required.

7. The apparatus as recited in claim 6, further comprising:

transmitting, to the server via the primary channel, an indication that the authentication token has been transmitted.

8. An apparatus comprising a processor, a memory, and communication circuitry, the apparatus being connected to a network via its communication circuitry, the apparatus further comprising computer-executable instructions stored in the memory of the apparatus which, when executed by the processor of the apparatus, cause the apparatus to perform operations comprising:

receiving, from a server via a primary channel of a communication network, a registration request message;

on a condition that the registration request message includes an authentication token and a transaction reference identifier, transmitting, to the server via the primary channel, a registration acceptance message;

on a condition that the registration request message does not include an authentication token and a transaction reference identifier, transmitting, to the server via the primary channel, a registration response message that indicates that authentication is not accepted; and

on a condition that authentication was not accepted, transmitting, to the server via a secondary channel of the communication network, a sideband message that includes the authentication token and the transaction reference identifier.

9. The apparatus as recited in claim 8, wherein the primary channel is a user plane channel communicating via Internet Protocol (IP).

10. The apparatus as recited in claim 8, wherein the secondary channel is a control plane channel communicating via short message service (SMS) or Non-IP Data Delivery.

11. The apparatus as recited in claim 8, wherein the sideband message is transmitted to the server via a service capability exposure function (SCEF).

12. The apparatus as recited in claim 8, further comprising:

on a condition that the apparatus transmitted the registration response message that indicates that authentication is not accepted, transmitting, to the server via the primary channel, an indication that an authentication token is required.

13. The apparatus as recited in claim 12, further comprising:

transmitting, to the server via the primary channel, an indication that an authentication token has been transmitted.

14. An apparatus comprising a processor, a memory, and communication circuitry, the apparatus being connected to a network via its communication circuitry, the apparatus further comprising computer-executable instructions stored in the memory of the apparatus which, when executed by the processor of the apparatus, cause the apparatus to perform operations comprising:

receiving, from a first server, a request message;

determining whether a policy is associated with the request message that indicates that a sideband warning message should be transmitted;

on a condition that the policy indicates that the sideband warning message should be transmitted, transmitting, to a second server, the sideband warning message that includes a transaction reference identifier and a description of the request message; and

receiving, from the second server a sideband message that indicates that the request message is associated with unauthorized activity and that includes the transaction reference identifier and a remedial action.

15. The apparatus as recited in claim 14, wherein the sideband warning message is transmitted via short message service (SMS) or non-IP data delivery.

16. The apparatus as recited in claim 14, wherein the sideband message includes a sideband reply port.

17. The apparatus as recited in claim 14, wherein the policy indicates that a sideband warning message should be transmitted if the first server does not have access rights to a requested resource or command associated with the request message, the first server attempted to access a non-existent resource or attempted an invalid command, or the first server attempted to access a restricted resource.

18. The apparatus as recited in claim 14, wherein the policy indicates that the sideband warning message should be transmitted whenever the apparatus detects that it has been physically re-located, the apparatus has updated certain resources, or the apparatus detects new operating conditions.

19. The apparatus as recited in claim 14, wherein the remedial action is to shut down, change security credentials, invalidate security credentials, stop communicating with the first server, reverse a transaction associated with the request message, or disallow a transaction associated with the request message.

20. The apparatus as recited in claim 14, wherein the sideband message is transmitted to the second server via a service capability exposure function (SCEF).

21. A method comprising:

detecting an initiation event on a primary channel of a communication network;

transmitting, to a server via a secondary channel of the communication network and in response to the initiation event, a sideband message that includes an authentication token and a transaction reference identifier;

receiving, from the server via the primary channel, a registration request message;

on a condition that the registration request message includes the authentication token and the transaction reference identifier, transmitting, to the server via the primary channel, a registration acceptance message; and

on a condition that the registration request message does not include the authentication token and the transaction reference identifier, transmitting, to the server via the primary channel, a registration response message that indicates that authentication is not accepted.

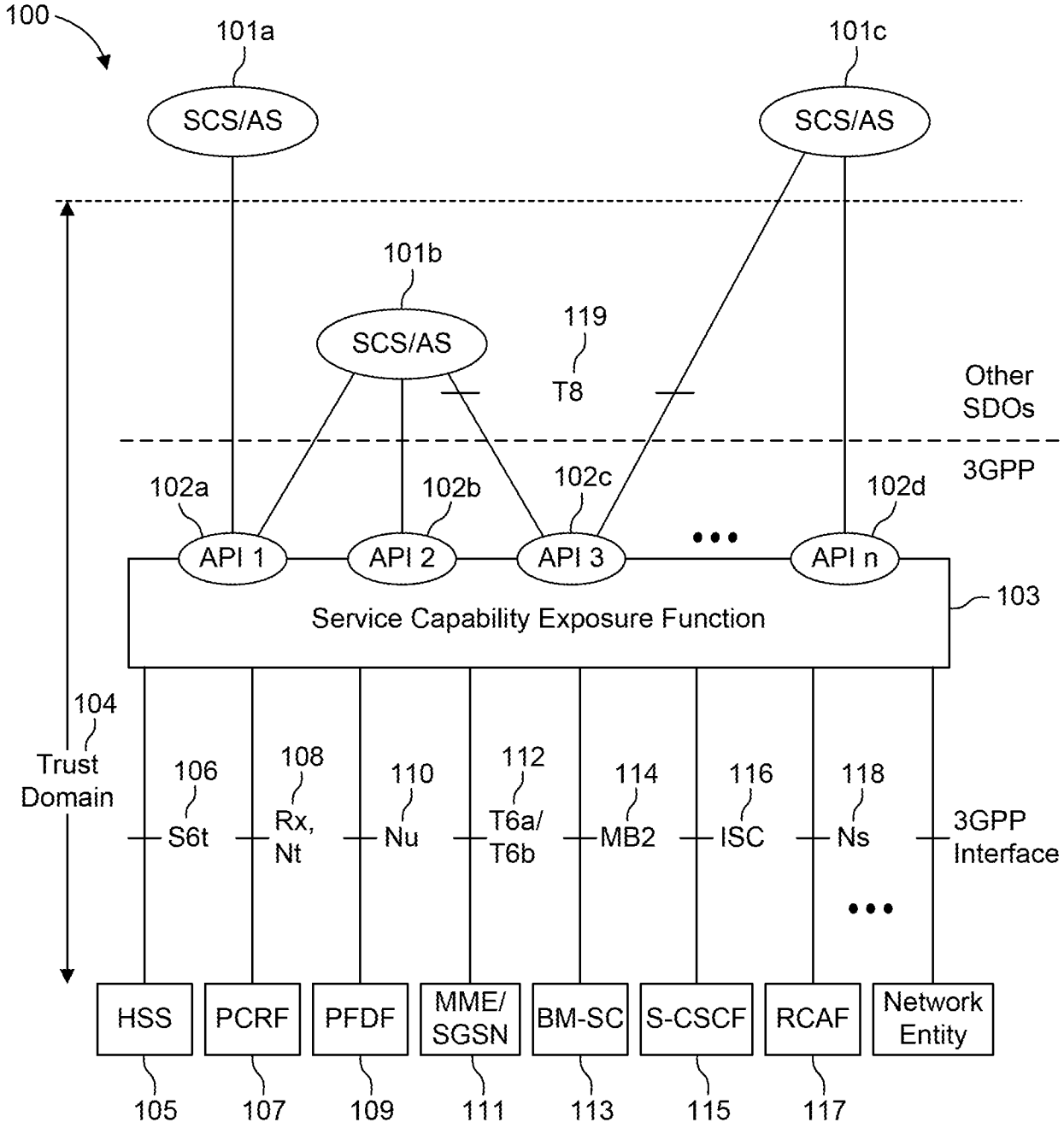

100
101a
SCS/AS
101c
SCS/AS
101b
SCS/AS
119
T8
Other SDOs
3GPP
102a
102b
102c
102d
API 1
API 2
API 3
API n
Service Capability Exposure Function
103
104
Trust Domain
106
S6t
108
Rx, Nt
110
Nu
112
T6a/ T6b
114
MB2
116
ISC
118
Ns
3GPP Interface
HSS
PCRF
PFDF
MME/ SGSN
BM-SC
S-CSCF
RCAF
Network Entity
105
107
109
111
113
115
117

Fig. 1

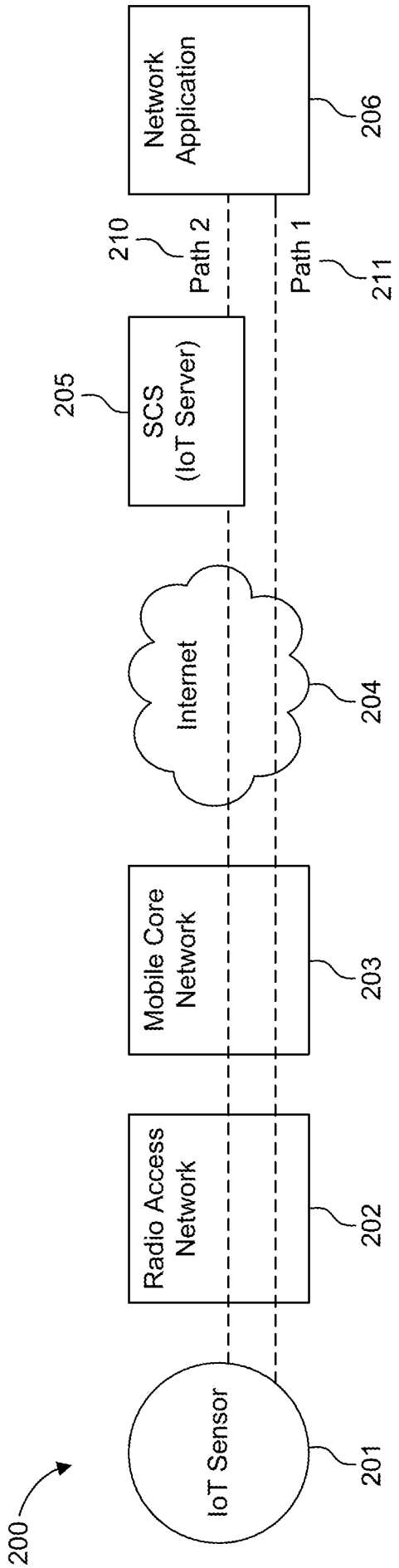

200
IoT Sensor
201
Radio Access Network
202
Mobile Core Network
203
Internet
204
SCS (IoT Server)
205
Network Application
206
Path 2
210
Path 1
211

Fig. 2

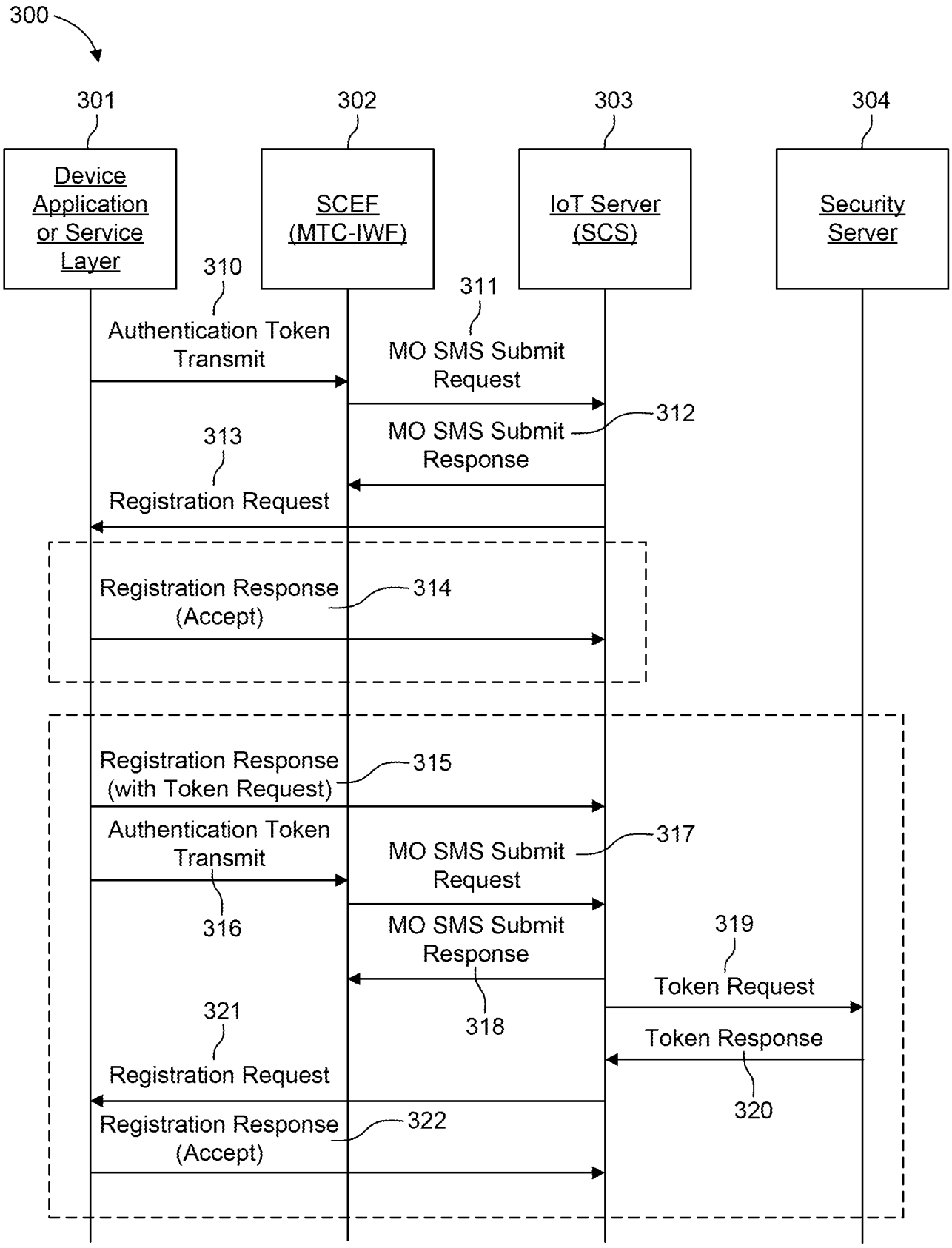

300
301
Device Application or Service Layer
302
SCEF (MTC-IWF)
303
IoT Server (SCS)
304
Security Server
310
Authentication Token Transmit
311
MO SMS Submit Request
312
MO SMS Submit Response
313
Registration Request
Registration Response (Accept)
314
Registration Response (with Token Request)
315
Authentication Token Transmit
316
MO SMS Submit Request
317
MO SMS Submit Response
318
319
Token Request
Token Response
320
321
Registration Request
Registration Response (Accept)
322

Fig. 3

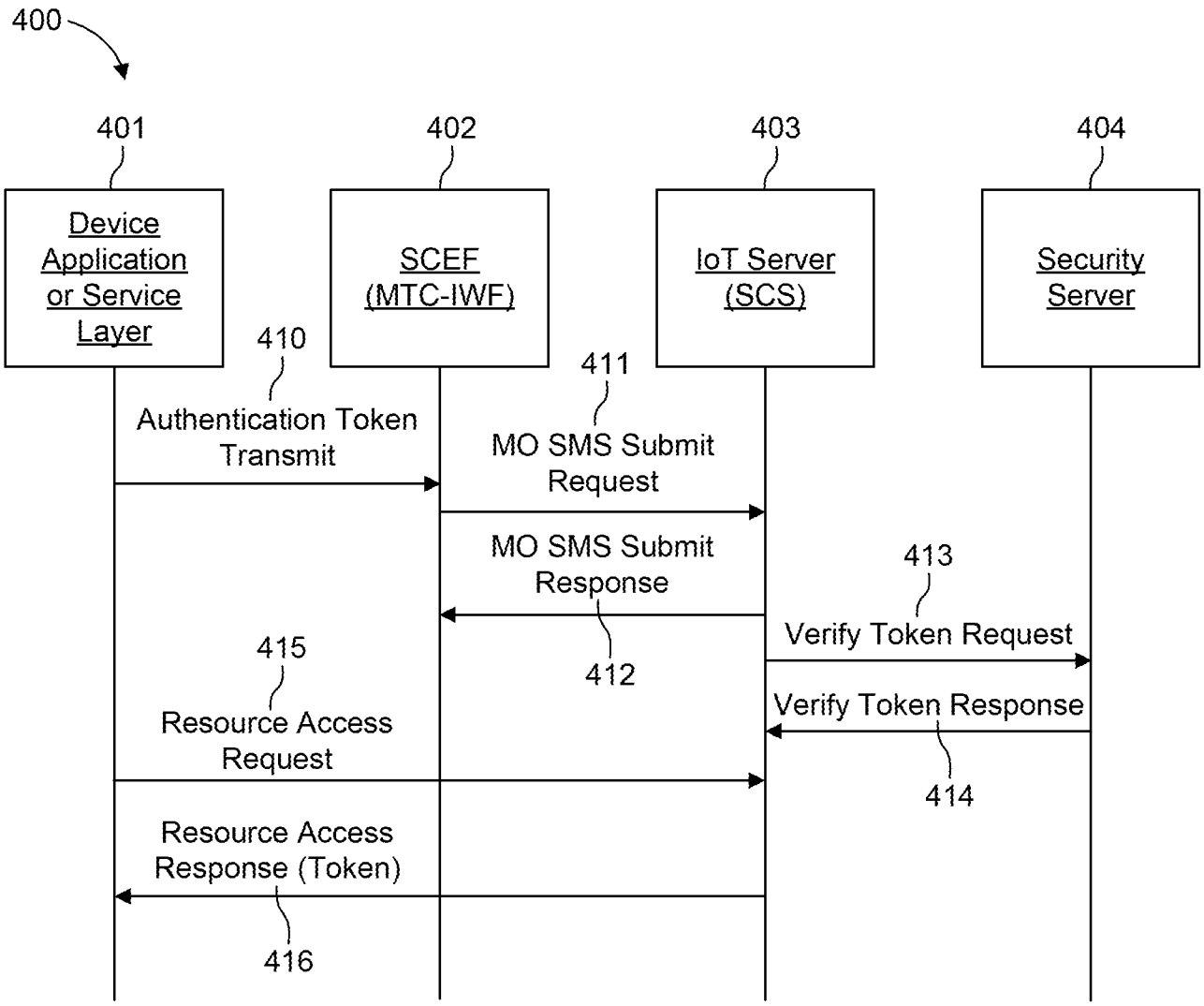

400
401
402
403
404
Device Application or Service Layer
SCEF (MTC-IWF)
IoT Server (SCS)
Security Server
410
Authentication Token Transmit
411
MO SMS Submit Request
MO SMS Submit Response
412
413
Verify Token Request
Verify Token Response
414
415
Resource Access Request
Resource Access Response (Token)
416

Fig. 4

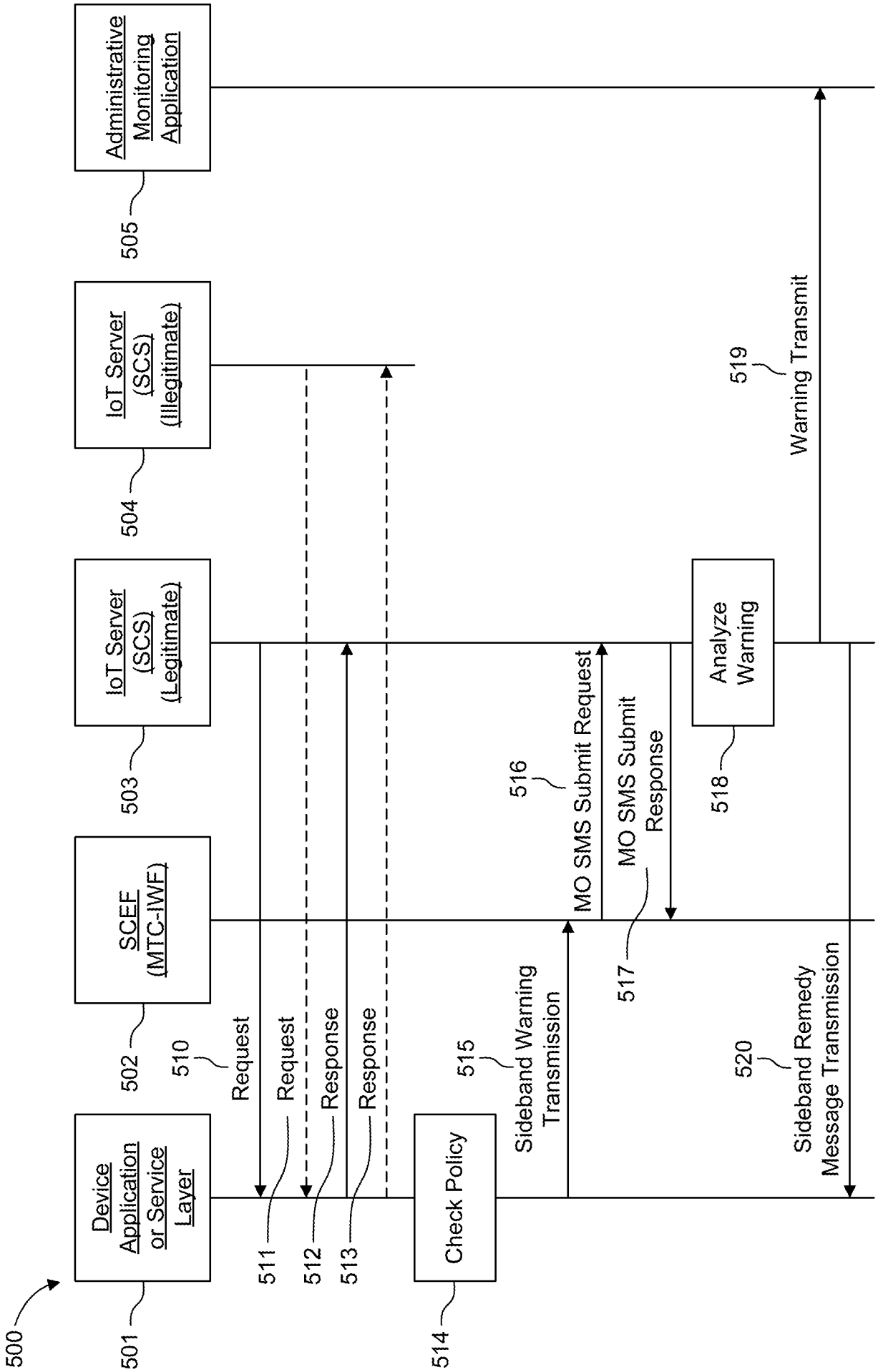

500
Device Application or Service Layer
501
SCEF (MTC-IWF)
502
IoT Server (SCS) (Legitimate)
503
IoT Server (SCS) (Illegitimate)
504
Administrative Monitoring Application
505
510
Request
511
Request
512
Response
513
Response
514
Check Policy
515
Sideband Warning Transmission
516
MO SMS Submit Request
517
MO SMS Submit Response
518
Analyze Warning
519
Warning Transmit
520
Sideband Remedy Message Transmission

Fig. 5

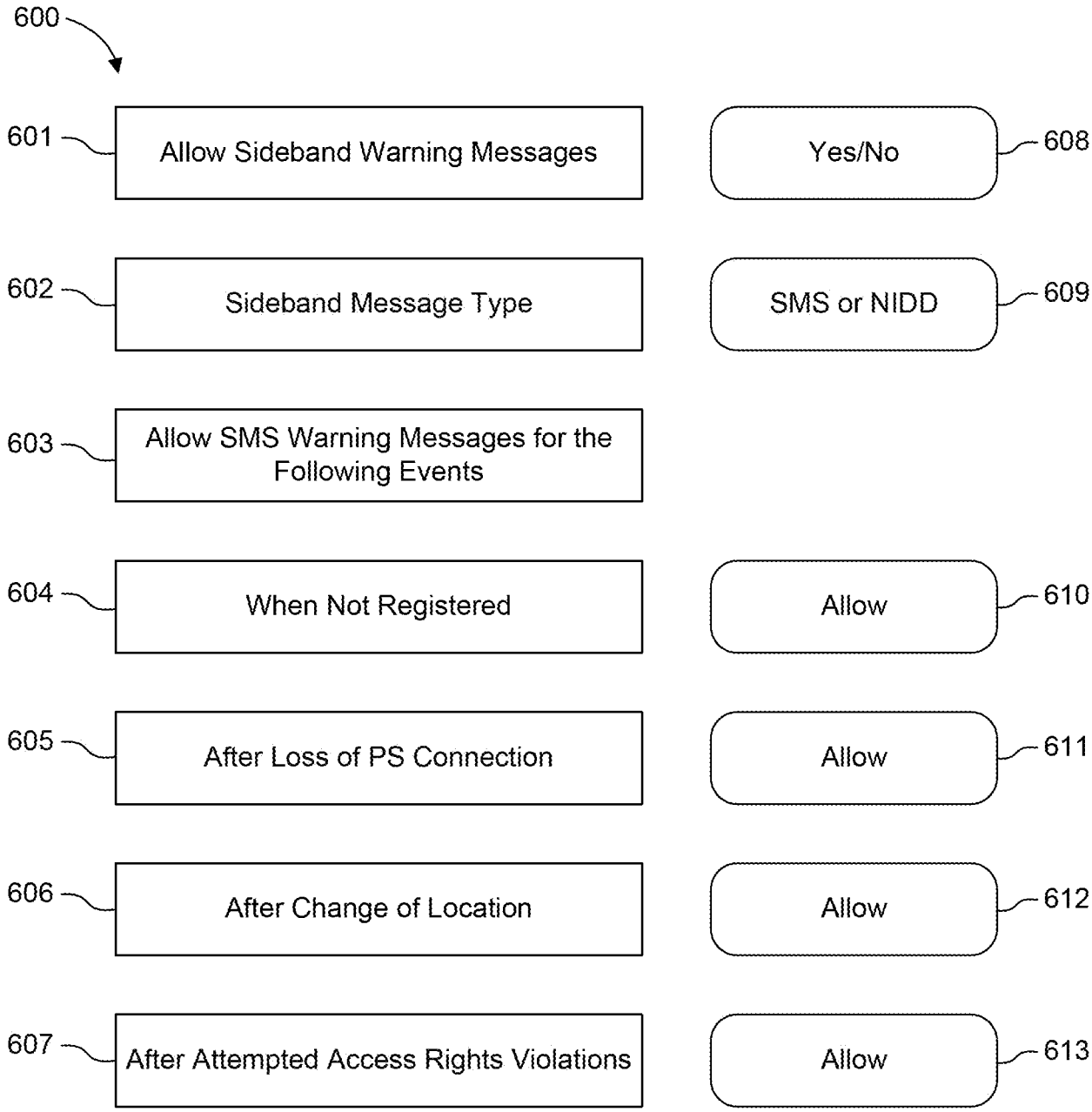

600
601
Allow Sideband Warning Messages
Yes/No
608
602
Sideband Message Type
SMS or NIDD
609
603
Allow SMS Warning Messages for the Following Events
604
When Not Registered
Allow
610
605
After Loss of PS Connection
Allow
611
606
After Change of Location
Allow
612
607
After Attempted Access Rights Violations
Allow
613

Fig. 6

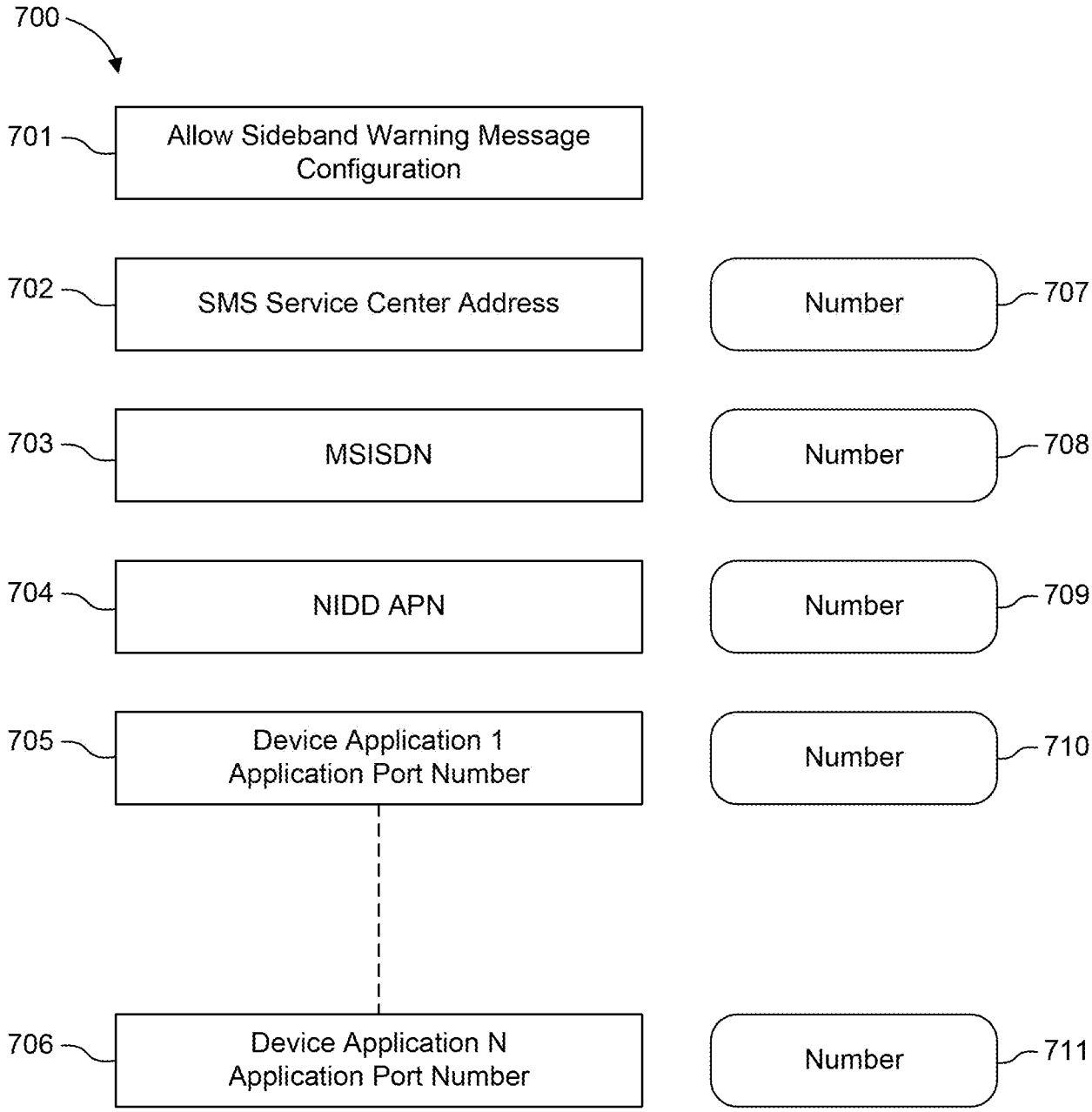

700
701
Allow Sideband Warning Message Configuration
702
SMS Service Center Address
Number
707
703
MSISDN
Number
708
704
NIDD APN
Number
709
705
Device Application 1 Application Port Number
Number
710
706
Device Application N Application Port Number
Number
711

Fig. 7

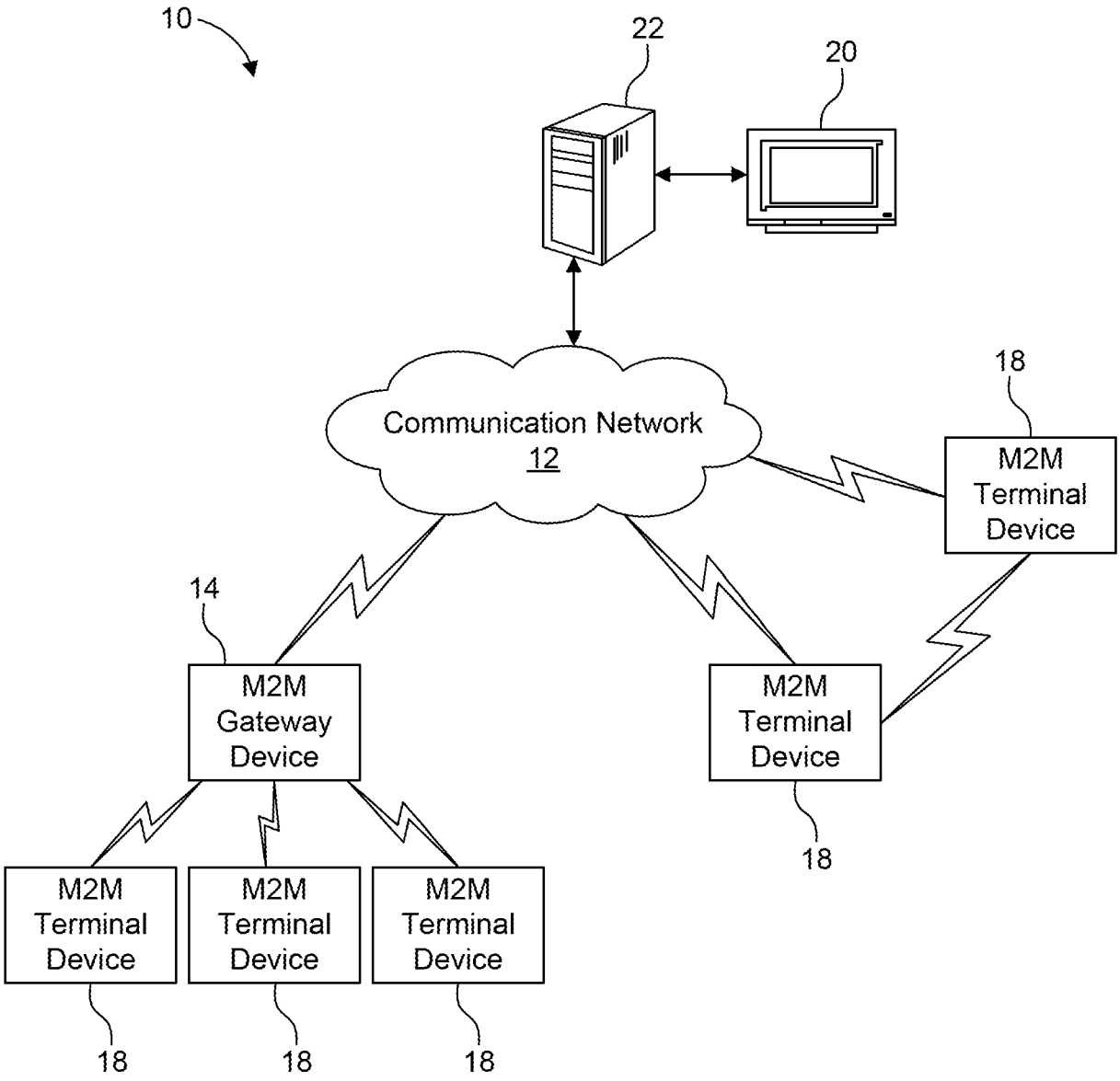

10
22
20
Communication Network
12
18
M2M
Terminal
Device
14
M2M
Gateway
Device
M2M
Terminal
Device
18
M2M
Terminal
Device
M2M
Terminal
Device
M2M
Terminal
Device
18
18
18

Fig. 8A

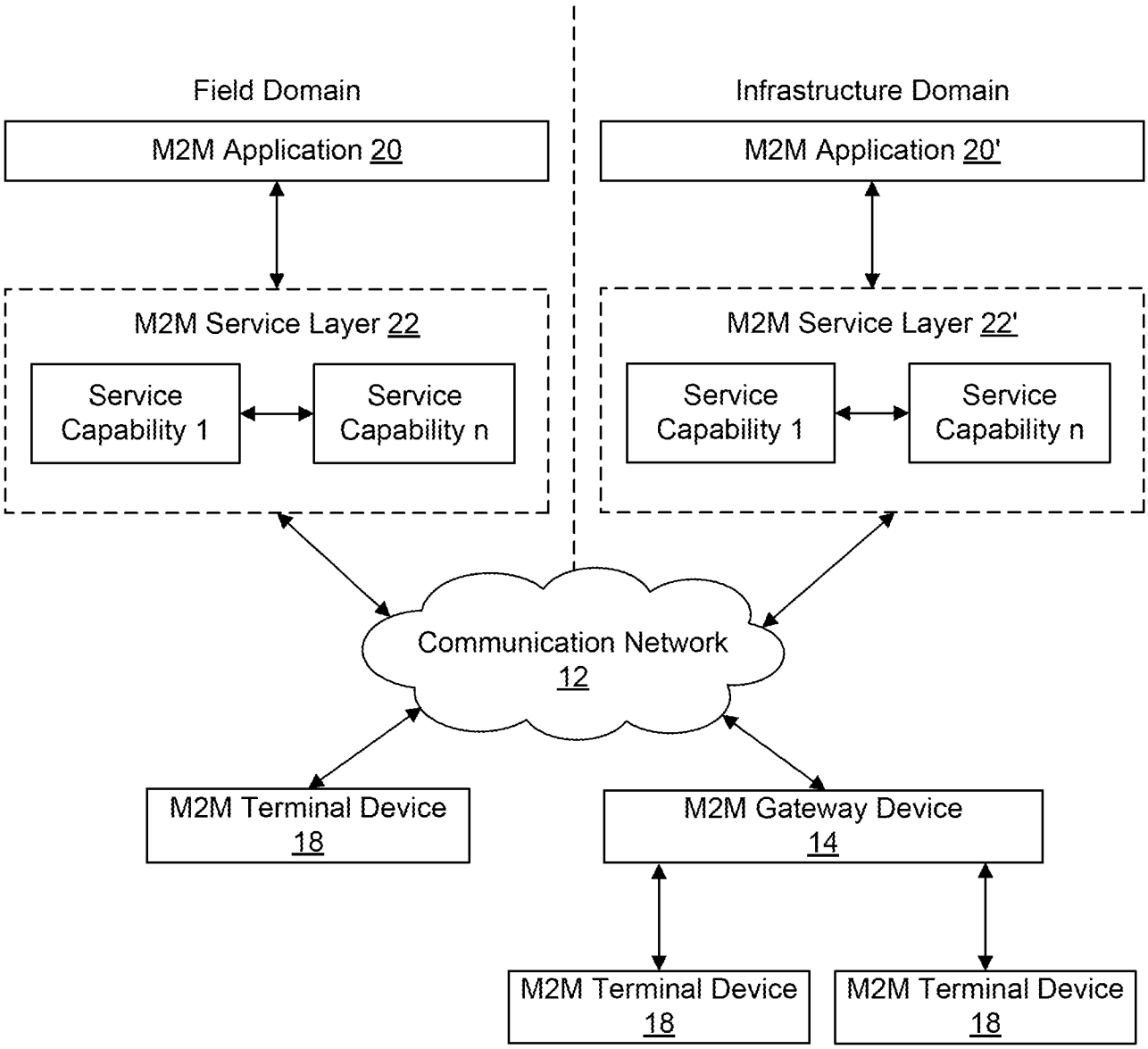

Field Domain
Infrastructure Domain
M2M Application 20
M2M Application 20'
M2M Service Layer 22
M2M Service Layer 22'
Service Capability 1
Service Capability n
Service Capability 1
Service Capability n
Communication Network 12
M2M Terminal Device 18
M2M Gateway Device 14
M2M Terminal Device 18
M2M Terminal Device 18

Fig. 8B

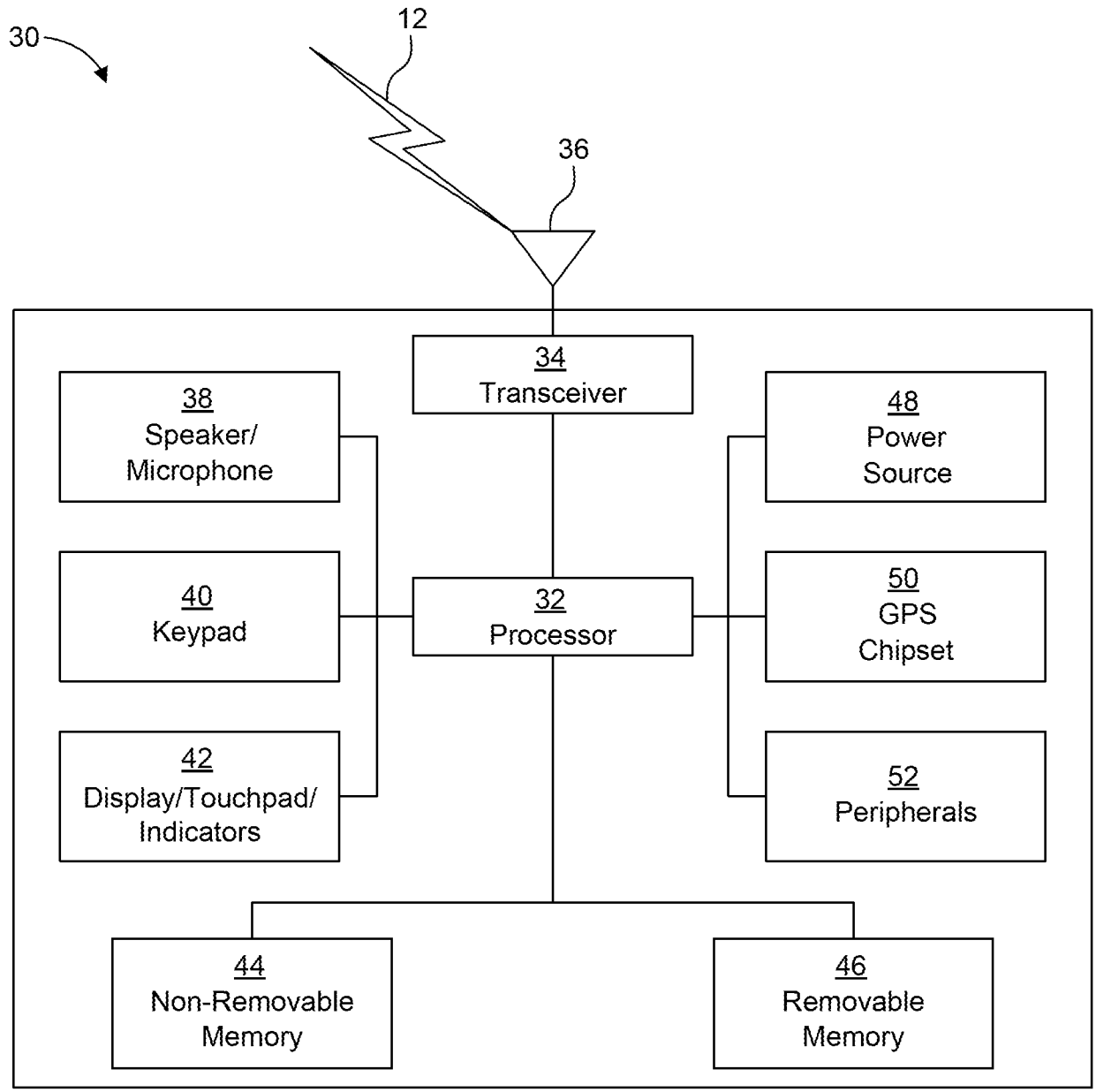

30
12
36
34
Transceiver
38
Speaker/
Microphone
40
Keypad
42
Display/Touchpad/
Indicators
32
Processor
48
Power
Source
50
GPS
Chipset
52
Peripherals
44
Non-Removable
Memory
46
Removable
Memory

Fig. 8C

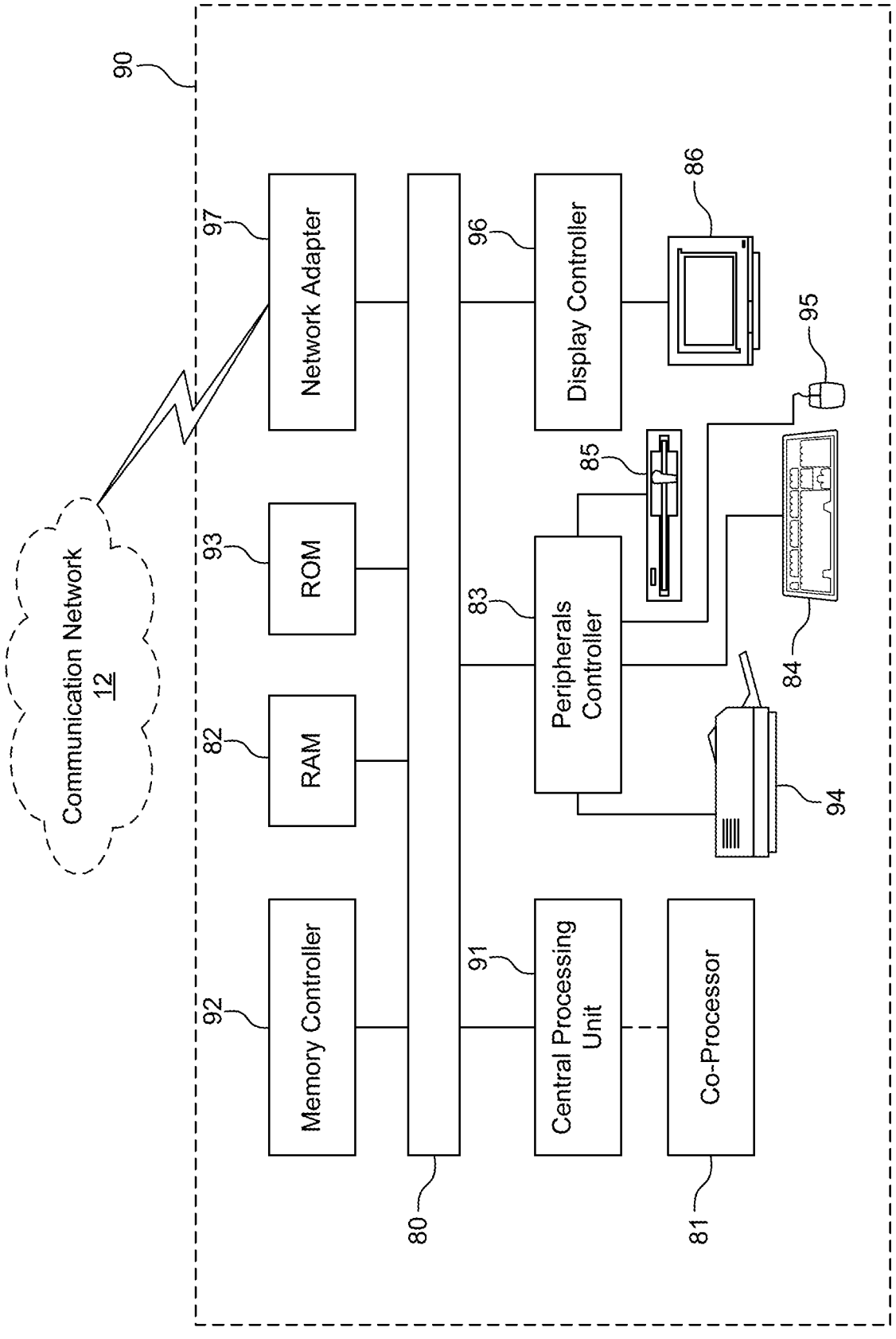

90
Communication Network
12
97
Network Adapter
93
ROM
82
RAM
92
Memory Controller
80
96
Display Controller
86
95
85
83
Peripherals Controller
84
94
91
Central Processing Unit
Co-Processor
81

Fig. 8D

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/063544

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06 H04L29/06 H04L9/32 H04W4/70 H04L29/08
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/226799 A1 (RAJ THANIGAIVEL ASHWIN [US]) 29 August 2013 (2013-08-29) figure 2 figure 5 paragraph [0047] paragraph [0071] - paragraph [0078] -----	1-21
A	US 2017/251329 A1 (BHALLA RAJESH [US]) 31 August 2017 (2017-08-31) figure 3 paragraph [0005] paragraph [0026] paragraph [0042] - paragraph [0043] paragraph [0065] ----- -/--	1-21

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 February 2019	13/02/2019

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

1

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

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HUAWEI ET AL: "Service Layer Security Bootstrapping Mechanism for IoT Devices", 3GPP DRAFT; S3-161142_PCR_SERVICE LAYER SECURITY BOOTSTRAPPING MECHANISM FOR IOT DEVICES, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA , vol. SA WG3, no. Chennai (India); 20160725 - 20160729 24 July 2016 (2016-07-24), XP051130994, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/Meetings_3GPP_SYNC/SA3/Docs/ [retrieved on 2016-07-24] Section 6.10.2.2.2. -----	1-21

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2018/063544

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013226799 A1	29-08-2013	US 2013226799 A1	29-08-2013
		WO 2013028901 A2	28-02-2013
US 2017251329 A1	31-08-2017	CN 107113529 A	29-08-2017
		EP 3198895 A1	02-08-2017
		US 2017251329 A1	31-08-2017
		WO 2016045602 A1	31-03-2016