



(51) International Patent Classification:

H04L 29/08 (2006.01) **H04L 29/06** (2006.01)
H04L 9/32 (2006.01) **H04W 4/00** (2009.01)

(21) International Application Number:

PCT/FI2017/050307

(22) International Filing Date:

24 April 2017 (24.04.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **NOKIA TECHNOLOGIES OY** [FI/FI];
Karaportti 3, 02610 Espoo (FI).

(72) Inventors: **SAVOLAINEN, Teemu**; Manttaalimutka 18
B 4, 37120 Nokia (FI). **REUNAMÄKI, Jukka**; Pel-
tomäenkatu 14 A, 33820 Tampere (FI). **PALIN, Arto**;
Rantatie 39, 37830 Akaa (FI).

(74) Agent: **NOKIA TECHNOLOGIES OY** et al.; Ari Aarnio,
IPR Department, Karakaari 7, 02610 Espoo (FI).

(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, JP, KE, KG, KH, KN, KP, KR,
KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,
MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM,
PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every
kind of regional protection available*): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

(54) Title: METHOD AND SYSTEM FOR SERVER LOAD REDUCTION DURING HOST AND KEY IDENTIFICATION AND LOCATION IN A NETWORK ENVIRONMENT

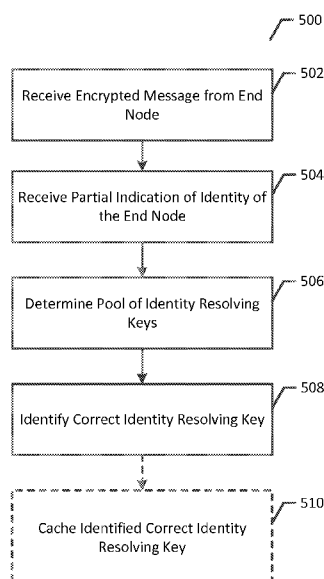


Figure 5

(57) Abstract: A method, apparatus and computer program product are provided in accordance with example embodiments in order to provide for the efficient determination of an identity resolving key associated with a device transmitting one more encrypted messages within a communication network environment. Some example implementations are directed to the use of partial indicators of a device identity to allow a server to reduce the pool of potential identity resolving keys such that the load placed on a server during the process of identifying the appropriate key is reduced.

METHOD AND SYSTEM FOR SERVER LOAD REDUCTION DURING HOST AND KEY IDENTIFICATION AND LOCATION IN A NETWORK ENVIRONMENT

TECHNICAL FIELD

[0001] An example embodiment relates generally to communications network technology, particularly in the context of systems where large numbers of end-nodes, such as sensors, send encrypted data frames to a central server in a connectionless fashion within a given network environment.

BACKGROUND

[0002] As modern communications networks have become increasingly ubiquitous, reliable, and useful, an ever-increasing number of devices and types of devices that are capable of interacting with such communications networks have been introduced. Sensors that are capable of wirelessly transmitting information are one such type of device that has become increasingly popular, to the extent that large numbers of such sensors have been built and deployed.

[0003] While networks and their operators are typically able to meet the demands associated with limited groups of sensors, the ever-increasing sensor population, and the attendant computing and processing resources consumed by a network seeking to service such sensors, can place strains on finite network resources and raises a number of technical challenges. Many of these technical challenges are compounded in situations where a network is tasked with determining the identity of a given sensor within a large pool of sensors, and where the information transmitted by a sensor is encrypted. The inventors of the invention disclosed herein have identified these and other technical challenges, and developed the solutions described and otherwise referenced herein.

BRIEF SUMMARY

[0004] A method, apparatus and computer program product are therefore provided in accordance with an example embodiment in order to provide methods, apparatuses, and/or systems that provide for the use by a server of partial indications of an identity of a network device to reduce the pool of decryption keys to be tested by the server when attempting to resolve the public address of the device and decrypting messages received from the device.

[0005] In an example embodiment, a method is provided that includes receiving, at a server, a message transmitted by an end-node, wherein the message comprises an

encrypted payload and wherein the end-node is configured with a privacy-enabled address; receiving, at the server a partial indication of the identity of the end-node; determining, based at least in part on the partial indication of the identity of the end-node, a plurality of identity resolving keys to be tested against the message; and identifying a correct identity resolving key from amongst the plurality of identity resolving keys. In some example implementations of such a method, the message is a Bluetooth Low Energy advertisement messages or an Internet Protocol message.

[0006] In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with an end-node group context identifier. In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with a forwarding gateway identity. In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with a forwarding gateway end-node identity. In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with a time at which a message is expected to be received.

[0007] In some such example implementations, and in other example implementations, the method further comprises caching the correct identity resolving key from amongst the plurality of identity resolving keys for use with a subsequent message received from the end-node.

[0008] In another example embodiment, an apparatus is provided that includes at least one processor and at least one memory that includes computer program code with the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to at least receive, at a server, a message transmitted by an end-node, wherein the message comprises an encrypted payload and wherein the end-node is configured with a privacy-enabled address; receive, at the server a partial indication of the identity of the end-node; determine, based at least in part on the partial indication of the identity of the end-node, a plurality of identity resolving keys to be tested against the message; and identify a correct identity resolving key from amongst the plurality of identity resolving keys. In some example implementations of such an apparatus, the

message is a Bluetooth Low Energy advertisement message or an Internet Protocol message.

[0009] In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with an end-node group context identifier. In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with a forwarding gateway identity. In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with a forwarding gateway end-node identity. In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with a time at which a message is expected to be received.

[0010] In some such example implementations, and in other example implementations, the at least one memory and the computer program code are further configured to, with the processor, cause the apparatus to at least cache the correct identity resolving key from amongst the plurality of identity resolving keys for use with a subsequent message received from the end-node.

[0011] In a further example embodiment, a computer program product is provided that includes at least one non-transitory computer-readable storage medium having computer-executable program code instructions stored therein with the computer-executable program code instructions including program code instructions configured to receive, at a server, a message transmitted by an end-node, wherein the message comprises an encrypted payload and wherein the end-node is configured with a privacy-enabled address; receive, at the server a partial indication of the identity of the end-node; determine, based at least in part on the partial indication of the identity of the end-node, a plurality of identity resolving keys to be tested against the message; and identify a correct identity resolving key from amongst the plurality of identity resolving keys. In some example implementations of such a computer program product, the message is a Bluetooth Low Energy advertisement message or an Internet Protocol message.

[0012] In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with an end-node group context identifier. In some such example implementations, and in other

example implementations, the partial indication of the identity of the end-node is associated with a forwarding gateway identity. In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with a forwarding gateway end-node identity. In some such example
5 implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with a time at which a message is expected to be received.

[0013] In some such example implementations, and in other example implementations, the computer-executable program code instructions further comprise
10 program code instructions configured to cache the correct identity resolving key from amongst the plurality of identity resolving keys for use with a subsequent message received from the end-node.

[0014] In yet another example embodiment, an apparatus is provided that includes means for receiving, at a server, a message transmitted by an end-node, wherein the
15 message comprises an encrypted payload and wherein the end-node is configured with a privacy-enabled address; receiving, at the server a partial indication of the identity of the end-node; determining, based at least in part on the partial indication of the identity of the end-node, a plurality of identity resolving keys to be tested against the message; and
20 identifying a correct identity resolving key from amongst the plurality of identity resolving keys. In some example implementations of such an apparatus, the message is a Bluetooth Low Energy advertisement message or an Internet Protocol message.

[0015] In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with an end-node group context identifier. In some such example implementations, and in other
25 example implementations, the partial indication of the identity of the end-node is associated with a forwarding gateway identity. In some such example implementations, and in other example implementations, the partial indication of the identity of the end-node is associated with a forwarding gateway end-node identity. In some such example implementations, and in other example implementations, the partial indication of the
30 identity of the end-node is associated with a time at which a message is expected to be received.

[0016] In some such example implementations, and in other example implementations, the apparatus further comprises means for caching the correct identity resolving key from amongst the plurality of identity resolving keys for use with a subsequent message received from the end-node.

5

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] Having thus described certain example embodiments of the present disclosure in general terms, reference will hereinafter be made to the accompanying drawings, which are not necessarily drawn to scale, and wherein:

10 [0018] Figure 1 depicts an example system environment in which implementations in accordance with an example embodiment of the present invention may be performed;

[0019] Figure 2 is a block diagram of an apparatus that may be specifically configured in accordance with an example embodiment of the present invention;

15 [0020] Figure 3 is a block diagram depicting an example address structure that illustrates aspects of an example embodiment of the present invention;

[0021] Figure 4 is a block diagram depicting an example system environment in which implementations in accordance with an example embodiment of the present invention may be performed; and

20 [0022] Figure 5 is a flowchart illustrating a set of operations performed, such as by the apparatus of Figure 2, in accordance with an example embodiment of the present invention.

DETAILED DESCRIPTION

[0023] Some embodiments will now be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all, embodiments of the invention are shown. Indeed, various embodiments of the invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. Like reference numerals refer to like elements throughout. As used herein, the terms “data,” “content,” “information,” and similar terms may be used interchangeably to refer to data capable of being transmitted, received and/or stored in accordance with embodiments of the present invention. Thus, use of any such terms should not be taken to limit the spirit and scope of embodiments of the present invention.

25

30

[0024] Additionally, as used herein, the term ‘circuitry’ refers to (a) hardware-only circuit implementations (e.g., implementations in analog circuitry and/or digital circuitry); (b) combinations of circuits and computer program product(s) comprising software and/or firmware instructions stored on one or more computer readable memories that work
5 together to cause an apparatus to perform one or more functions described herein; and (c) circuits, such as, for example, a microprocessor(s) or a portion of a microprocessor(s), that require software or firmware for operation even if the software or firmware is not physically present. This definition of ‘circuitry’ applies to all uses of this term herein, including in any claims. As a further example, as used herein, the term ‘circuitry’ also
10 includes an implementation comprising one or more processors and/or portion(s) thereof and accompanying software and/or firmware. As another example, the term ‘circuitry’ as used herein also includes, for example, a baseband integrated circuit or applications processor integrated circuit for a mobile phone or a similar integrated circuit in a server, a cellular network device, other network device, and/or other computing device.

15 [0025] As defined herein, a “computer-readable storage medium,” which refers to a non-transitory physical storage medium (e.g., volatile or non-volatile memory device), can be differentiated from a “computer-readable transmission medium,” which refers to an electromagnetic signal.

[0026] A method, apparatus and computer program product are provided in
20 accordance with example embodiments in order to provide for the use of partial indications of an identity of a network device to reduce the pool of decryption keys to be tested by a server when attempting to resolve the public address of the device and decrypting messages received from the device. Many implementations of example embodiments of the invention described and otherwise disclosed herein are directed to solving the technical
25 challenges associated with identifying a sending node and decrypting a message payload of inbound packets received from gateways forwarding unidirectional encrypted data frames sent by sensors.

[0027] Many example implementations of embodiments of the invention described and otherwise disclosed herein arise in the context of systems where large number of end-
30 nodes, such as sensors, send encrypted data frames to a central server in a connectionless fashion. In many such situations, the network environment may be configured such that there are untrusted and trusted forwarders – which may be referred to herein as “gateways”

– that are configured and/or otherwise structured to provide first hop connectivity to end-nodes and to forward encrypted data packets received from such sensors or other end-nodes to a server.

[0028] Many aspects of embodiments of the invention described and/or otherwise disclosed herein may be particularly advantageous in contexts that involve Bluetooth Low-Energy (LE) devices and gateways capable of forwarding Bluetooth LE Advertisement messages and/or similar messages to a cloud server. In many such contexts, these messages are sent from privacy-enabled addresses and may contain encrypted message payloads.

[0029] It will be appreciated that in many systems that involve Bluetooth LE-related technology, many of the Bluetooth LE (BLE) devices use resolvable private addresses in order to protect device privacy against eavesdroppers and other (passive) monitoring systems. In such situations, a device which knows the Identity Resolving Key (IRK) associated with the device can resolve the public address – which may be considered to be essentially and/or practically as the device identity - from the resolvable private address. Typically, the resolvable private address is generated with the IRK. In some such situations, the transmitted address (as transmitted from the end-node and/or gateway, for example) contains a randomly generated 24-bit number (which is referred to herein as a *prand*) and a *hash* (which may, in some situations be 24-bits in length or another length. In some example implementations, the *hash* may be generated using a random address function which may be expressed as

$$ah: hash = ah(IRK, prand).$$

[0030] In some example implementations, the *prand* and *hash* may be concatenated to generate a random address associated with a sensor or other end-node.

[0031] While many of the examples described herein involve the use of network environments that involve Bluetooth protocols, it will be appreciated that example embodiments of the invention described and otherwise disclosed herein may be implemented in system environments that incorporate other protocols. For example, some example embodiments involve systems that may utilize Internet Protocol version 6 (IPv6). In some example implementations of embodiments involving IPv6 aspects, Internet-of-Things (IoT) nodes may send unicast IPv6 packets to a cloud server, and use an IPv6 source address wherein the lower 64-bits may contain the same and/or similar types of information that may be contained and/or otherwise expressed in a Bluetooth LE privacy

address. In some example implementations involving such systems, and similar to systems involving Bluetooth LE privacy addresses, an IPv6 address may contain a 64-bit privacy-enabled interface identifier in a lower portion of a 128 bit IPv6 address. In some such example implementations, the privacy-enabled interface identifier may be composed
5 and/or otherwise structured in a manner to contain *hash* and *prand*, similar to the examples presented herein with respect to systems involving Bluetooth LE.

[0032] In Figure 3, an example random address 300 is depicted and arranged from a least-significant bit end 301b to a most significant bit end 301a. As shown in Figure 3, the example random address 300 includes a *prand* 302, which includes a leading bit set at
10 zero (shown as bit 302a) a subsequent bit set at 1 (shown as bit 302b) and a random portion of the *prand* 302c. Example random address 300 also includes a *hash* portion 304, which may be generated using the random address function disclosed herein, a similar function, or any other function suitable for generating a *hash* in connection with a random address. It will be appreciated that while many of the examples described and/or otherwise
15 disclosed herein may reference a *hash* and/or a *prand* as being 24 bits in length, some example implementations of example embodiments of the invention may be used in connection with address portions that have different and/or differing bit lengths. It will also be appreciated that some example implementations contemplate random addresses that include one or more additional portions beyond the *hash* and *prand* portions discussed
20 herein in connection with some of the example implementations.

[0033] In some example implementations of embodiments of the invention, the private address associated with a given sensor or other end-node may be resolved by first calculating a *localHash* value using the random address hash function *ah* for received address using one IRK, which may be expressed as follows:

$$\text{localhash} = ah(\text{IRK}, \text{prand}).$$

[0034] In some such example implementations, the *localHash* value may then be compared with the *hash* value extracted from the address. If the *localHash* value matches the extracted hash value, then the identity of the peer device can be considered to have been resolved. If a device has more than one stored IRK, the device may repeat the
30 process of calculating the hash value and the localhash value for each stored IRK to determine if the received resolvable private address is associated with a stored IRK, until an address resolution is successful for one of the IRKs, or all IRKs have been tried.

[0035] Many of the example implementations discussed and/or otherwise referenced herein arise in contexts where multiple sensors direct messages to a cloud server and/or other network entity through a plurality of gateways. For example, a number of generic gateways may be configured to forward unidirectional encrypted data frames sent by sensors using Bluetooth LE to a central cloud server.

[0036] One example system environment 400 that reflects such an arrangement of multiple sensors and gateways is depicted in Figure 4. As shown in Figure 4, example system environment 400 includes a number of sensors 402a-402n. In some example implementations, groups of sensors 402a-402n are each associated with one or a number of gateways 404a-404n, at least in the sense that each gateway 404a-404n is capable of receiving a unidirectional message (which may, for example, be encrypted) from its associated sensors from within the group of sensors 402a-402n and passing such messages to the cloud server 406.

[0037] In some situations arising in system environment 400 and/or similar environments, one or more of the sensors 402a-402n may use Bluetooth protocols and/or a similar approach to send BLE advertisements using privacy addresses. It will be appreciated that the use of a privacy address may be effective in defending against unauthorized device tracking and/or to otherwise maintain a degree of privacy regarding the location and movement of a particular device.

[0038] In typical uses of Bluetooth and similar protocols, a device (such as a sensor, an audio device, a mobile device, or the like, for example) may be paired with a limited number of peer devices. As such, and at least in part due to the limited number of peer devices, the resources necessary to try the set of known keys to determine which device sent a given message are relatively low. This low resource need is based at least in part on the limited number of keys to try out, such that a brute force approach (such as the iterative calculation of a *hash* and a *localhash* described above, for example) may be reasonable to perform.

[0039] However, in situations that arise in system environments similar to the example system environment 400 depicted in Figure 4, the relevant cloud server may potentially receive a very large number of encrypted Bluetooth LE advertisements from a very large end-node (such as a sensor, for example) pool through a set of gateways. Since, each sensor and/or other end-node (such as each of sensors 402a-402n, for example) is

associated with its own IRK, the arrangement of the system environment and the volume of sensors and gateways results in a scenario where the relevant cloud server may need to process a very large set of IRKs to ascertain the identity of a sensor associated with a given message.

5 **[0040]** In system environments similar to example system environment 400, since encrypted messages are flowing from end-nodes (such as sensors 402a-402n, for example) using privacy addresses to the relevant cloud server (such as server 406, for example), the server experiences a number of technical challenges associated with the use of significant time, system resources, and related effort for finding out which IRK from amongst the very
10 large set of keys must be used to resolve the identity of a sending node and to decrypt the message payload of each inbound packet. The time and effort spent results in heavy usage of computing resources and thus incurs potentially unwanted costs and potentially prevents system resources from being directed to other network activity.

[0041] It will be appreciated that the invention described and/or otherwise
15 disclosed herein, particularly when used in conjunction with a system environment similar to that shown in Figure 4, address a number of technical challenges associated with the processing of high volumes of sensor traffic in a network environment. In conventional Internet Protocol-based systems, the end-nodes create a bi-directional secure connection between each sensor and the relevant server. As such, when creating a connection, the
20 end-node explicitly identifies itself with a certificate to the server. This conventional approach allows the relevant server to use keys in a relatively efficient manner. However, this conventional approach requires the implementation of multiple bi-direction channels (such as one for each sensor, for example). This approach also results in a situation where the end-node is identified not only to the relevant server, but to the gateway and other
25 nodes on the path from the end-node to the relevant server, as the client certificate is sent in plaintext as part of a security handshake (such as a Transport Layer Security (TLS) handshake, for example).

[0042] In some other situations, end-nodes first explicitly communicate with a gateway, or forwarding entity, which then proxies the data to the relevant cloud server. In
30 such arrangements and situations, a conventional security setup, or pairing, is typically performed with the end-node and the gateway device. In such situations, the gateway device usually has only a very limited number of nodes paired, and hence it can easily use

brute force to find the correct keys. However, in addition to requiring the pairing of the end node (such as a sensor, for example) with the gateway, such arrangements also result in a system where the gateway then knows identity of communicating node – and content of communications - and each gateway that is used for forwarding has to be paired with the
5 end node. As such, significant technical challenges may arise when attempting to scale such arrangements to handle very large pools of sensors and/or other end-nodes.

[0043] Some approaches to handling very large pools of sensors involve the caching of data fetched through expensive operations. Such caching happens, for example, at web caches, such as HTTP proxies, that cache downloaded data so that follow-up
10 requests for the same resources could be provided locally. It will be appreciated that a Domain Name System resolver may cache results of DNS name queries for a period of time, such that follow-up requests for the same name could be locally processed at server with relatively low resource demands. It will also be appreciated that some central processing units (CPUs) cache results of RAM read operations so that follow-up requests
15 for the same data could be served from a local cache without the need to always perform read operations on a main RAM (which consumes time and/or other system resources).

[0044] To address these and other technical challenges associated with processing messages received in network environments that contain very large pools of sensors, some example implementations of embodiments of the invention described and/or otherwise
20 disclosed herein involve enabling and/or otherwise allowing a server to use a set of partial identifications of a device identity in order to reduce the pool of decryption keys that must be processed when attempting to detect the public address or other identity of a device and attempting to decrypt received encrypted messages that are sent from resolvable private addresses associated with a device. In some such example implementations, including but
25 not limited to some of the example described herein, such partial identifications may be identified and/or referred to as “hints” associated with a relevant device public address and/or other identity.

[0045] Some example implementations of embodiments of the invention contemplate the use of four different types of partial identifiers which may be used to
30 reduce the IRK and/or other key pool size needed for a given identification determination: (1) an explicit end-node group context identifier hint; (2) a forwarding gateway identity

hint; (3) a forwarding gateway provided end-node identity hint; and (4) a time correlation hint.

[0046] In some example implementations of embodiments of the invention described and/or otherwise disclosed here, the server may utilize one or more of partial
5 identifiers or “hints”, either singly or in combination, and potentially at the same time or near same-time, in order to create a priority list of possible decryption keys (IRKs). When such a list of possible IRKs is composed, the server may test the keys (such as in priority order, for example) until the correct key is identified. In some example implementations, when a matching key is found, it is cached so that the cached key can be used with
10 subsequent messages until the device switches its source address and the key search and identification process needs to be repeated.

[0047] As discussed herein, many example implementations of embodiments of the present invention provide for the use by a server of partial indications of an identity of a network device to reduce the pool of decryption keys to be tested by the server when
15 attempting to resolve the public address of the device and decrypting messages received from the device. In particular, some example implementations of embodiments of the invention contemplate solutions that use one or more partial indications or “hints” associated with the identity of a sensor and/or other end-node to allow for a reduction in the number of IRKs to be tested in connection with a message received from a particular
20 sensor. Some example implementations also contemplate establishing a rank and/or priority order in which IRKs may be tested and the caching of successfully determined keys for use in connection with the receipt of subsequent messages.

[0048] While the method, apparatus and computer program product of an example embodiment may be deployed in a variety of different systems, one example of a system
25 that may benefit from the procedures discussed and contemplated herein in accordance with an example embodiment of the present invention is depicted in Figure 1. The depiction of system environment 100 in Figure 1 is not intended to limit or otherwise confine the embodiments described and contemplated herein to any particular configuration of elements or systems, nor is it intended to exclude any alternative
30 configurations or systems for the set of configurations and systems that can be used in connection with embodiments of the present invention. Rather, Figure 1, and the system environment 100 disclosed therein is merely presented to provide an example basis and

context for the facilitation of some of the features, aspects, and uses of the methods, apparatuses, and computer program products disclosed and contemplated herein. It will be understood that while many of the aspects and components presented in Figure 1 are shown as discrete, separate elements, other configurations may be used in connection with the methods, apparatuses, and computer programs described herein, including configurations that combine, omit, and/or add aspects and/or components.

[0049] As shown in Figure 1, the system environment includes one or more user equipment 102 configured to communicate wirelessly, such as via an access network, with a network 106. Although the user equipment may be configured in a variety of different manners, the user equipment may be embodied as a mobile terminal, such as a portable digital assistant (PDA), mobile phone, smartphone, pager, mobile television, gaming device, laptop computer, camera, tablet computer, communicator, pad, headset, touch surface, video recorder, audio/video player, radio, electronic book, positioning device (e.g., global positioning system (GPS) device), or any combination of the aforementioned, and other types of voice and text and multi-modal communications systems.

[0050] In addition to the more traditional types of user equipment 102 which may be present within a given system environment, system environment 100 also includes one or more sensors 110 that are capable of interacting with a system environment, such as through the use of unidirectional and/or bi-directional wireless communication. In some example implementations, one or more of the sensors 110 may be incorporated into and/or otherwise associated with an Internet-of-Things (IoT) user equipment device, which may be referred to as an IoT device. Although the sensor 110 may be configured in a variety of different manners, such an example sensor may be embodied as a sensor capable of communicating via a Bluetooth protocol, including but not limited to Bluetooth Low Energy (BLE) protocol, for example. The sensor 110 may also be incorporated into and/or configured as a cellular IoT (C-IoT) device, narrowband IoT (NB-IoT) device, and/or other IoT devices, including but not limited to those that may be associated with vehicles, appliances, mechanical equipment, HVAC equipment, wearable devices and/or other devices that have been configured to allow for communications and/or other interactions with a network environment.

[0051] System environment 100, as depicted in Figure 1, also includes one or more access points 104a and 104b, such as base stations (such as node Bs, evolved Node Bs

(eNB), or the like, for example). A cellular access point, such as a base station, may define and service one or more cells. The access points may, in turn, be in communication with a network 106, such as a core network via a gateway, such that the access points establish cellular radio access networks by which the user equipment 102 and/or sensors 110 may communicate with the network. The system environment 100 of Figure 1 may include a plurality of different cellular radio access networks including, for example, a 5G radio access network, an LTE radio access network, a UMTS (universal mobile telecommunications system) radio access network, etc. In some example implementations, equipment and other infrastructure associated with multiple different cellular radio access networks may be located at or near structures and/or other equipment associated with a particular access point, such as access point 104a and 104b.

[0052] In some implementations of system environment 100, the cellular radio access networks serviced by access points 104a, 104b, and any other access points in a given area are identical, in the sense that as user equipment 102 and/or sensor 110 moves from an area serviced by access point 104a to an area serviced by access point 104b, the user equipment 102 and/or sensor device 110 is able to access the network 106 via a radio access network provided by the same vendor across access points. Although not shown, the system may also include a controller associated with one or more of the cellular access points, (such as base stations for example), so as to facilitate operation of the access points and management of the user equipment 102 and/or sensor 110 in communication therewith. As shown in Figure 1, a system may also include one or more wireless local area networks (WLANs), each of which may be serviced by a WLAN access point 108 configured to establish wireless communications with the user equipment 102 and/or the sensor 110. As such, the user equipment 102 and/or the sensor 110 may communicate with the network via a WLAN access point as shown in solid lines in Figure 1, or, alternatively, via a cellular access point as shown in dashed lines. The radio access networks as well as the core networks may consist of additional network elements as routers, switches, servers, gateways, and/or controllers. For example, the system environment 100 may include, Bluetooth LE listening device and/or access points. Such network elements may be configured as stand-alone elements and/or be incorporated into one or more other network elements, and the inclusion of such Bluetooth LE listening devices and/or access points

may be advantageous in situations involving the transmission and other processing of Bluetooth LE advertisements and/or other messages.

[0053] In connection with the approaches to reduce the number of potential IRKs to be tested to determine the public address associated with a received message, some example implementations of embodiments of the invention disclosed and/or otherwise described herein contemplate the use of network entities such as servers (including but not limited to cloud servers, for example) and gateways. In this regard, using partial indications of a device identity and reducing the pool of potential IRKs can be accomplished by an apparatus 200 as depicted in Figure 2. The apparatus may be embodied by and/or incorporated into one or more servers, such as a server associated with network 106, or any of the other devices discussed with respect to Figure 1, such as access points 104a and/or 104b, one or more of WLAN access points 108, and/or devices that may be incorporated or otherwise associated with system environment 100. The apparatus may be embodied by and/or incorporated into any of the devices discussed in connection with Figure 4, including but not limited to the cloud server 406. Alternatively, the apparatus 200 may be embodied by another device, external to such devices. For example, the apparatus may be embodied by a computing device, such as a personal computer, a computer workstation, a server or the like, or by any of various mobile computing devices, such as a mobile terminal, (such as a smartphone, a tablet computer, or the like, for example). In some example implementations, it may be particularly advantageous to implement the apparatus 200 in connection with one or more network elements and/or functions.

[0054] Regardless of the manner in which the apparatus 200 is embodied, the apparatus of an example embodiment is configured to include or otherwise be in communication with a processor 202 and a memory device 204 and optionally the user interface 206 and/or a communication interface 208. In some embodiments, the processor (and/or co-processors or any other processing circuitry assisting or otherwise associated with the processor) may be in communication with the memory device via a bus for passing information among components of the apparatus. The memory device may be non-transitory and may include, for example, one or more volatile and/or non-volatile memories. In other words, for example, the memory device may be an electronic storage device (such as a computer readable storage medium, for example) comprising gates

configured to store data (such as bits, for example) that may be retrievable by a machine (such as a computing device like the processor, for example). The memory device may be configured to store information, data, content, applications, instructions, or the like for enabling the apparatus to carry out various functions in accordance with an example embodiment of the present invention. For example, the memory device could be configured to buffer input data for processing by the processor. Additionally or alternatively, the memory device could be configured to store instructions for execution by the processor.

[0055] As described above, the apparatus 200 may be embodied by a computing device. However, in some embodiments, the apparatus may be embodied as a chip or chip set. In other words, the apparatus may comprise one or more physical packages (such as chips, for example) including materials, components and/or wires on a structural assembly (such as a baseboard, for example). The structural assembly may provide physical strength, conservation of size, and/or limitation of electrical interaction for component circuitry included thereon. The apparatus may therefore, in some cases, be configured to implement an embodiment of the present invention on a single chip or as a single “system on a chip.” As such, in some cases, a chip or chipset may constitute means for performing one or more operations for providing the functionalities described herein.

[0056] The processor 202 may be embodied in a number of different ways. For example, the processor may be embodied as one or more of various hardware processing means such as a coprocessor, a microprocessor, a controller, a digital signal processor (DSP), a processing element with or without an accompanying DSP, or various other processing circuitry including integrated circuits such as, for example, an ASIC (application specific integrated circuit), an FPGA (field programmable gate array), a microcontroller unit (MCU), a hardware accelerator, a special-purpose computer chip, or the like. As such, in some embodiments, the processor may include one or more processing cores configured to perform independently. A multi-core processor may enable multiprocessing within a single physical package. Additionally or alternatively, the processor may include one or more processors configured in tandem via the bus to enable independent execution of instructions, pipelining and/or multithreading.

[0057] In an example embodiment, the processor 202 may be configured to execute instructions stored in the memory device 204 or otherwise accessible to the processor.

Alternatively or additionally, the processor may be configured to execute hard coded functionality. As such, whether configured by hardware or software methods, or by a combination thereof, the processor may represent an entity (such as by being physically embodied in circuitry, for example) capable of performing operations according to an embodiment of the present invention while configured accordingly. Thus, for example, when the processor is embodied as an ASIC, FPGA or the like, the processor may be specifically configured hardware for conducting the operations described herein.

Alternatively, as another example, when the processor is embodied as an executor of software instructions, the instructions may specifically configure the processor to perform the algorithms and/or operations described herein when the instructions are executed.

However, in some cases, the processor may be a processor of a specific device (such as a pass-through display or a mobile terminal, for example) configured to employ an embodiment of the present invention by further configuration of the processor by instructions for performing the algorithms and/or operations described herein. The processor may include, among other things, a clock, an arithmetic logic unit (ALU) and logic gates configured to support operation of the processor.

[0058] In some embodiments, the apparatus 200 may optionally include a user interface 206 that may, in turn, be in communication with the processor 202 to provide output to the user and, in some embodiments, to receive an indication of a user input. As such, the user interface may include a display and, in some embodiments, may also include a keyboard, a mouse, a joystick, a touch screen, touch areas, soft keys, a microphone, a speaker, or other input/output mechanisms. Alternatively or additionally, the processor may comprise user interface circuitry configured to control at least some functions of one or more user interface elements such as a display and, in some embodiments, a speaker, ringer, microphone and/or the like. The processor and/or user interface circuitry comprising the processor may be configured to control one or more functions of one or more user interface elements through computer program instructions (such as software and/or firmware, for example) stored on a memory accessible to the processor (such as memory device 204, and/or the like, for example).

[0059] The apparatus 200 may optionally also include the communication interface 208. The communication interface may be any means such as a device or circuitry embodied in either hardware or a combination of hardware and software that is configured

to receive and/or transmit data from/to a network and/or any other device or module in communication with the apparatus. In this regard, the communication interface may include, for example, an antenna (or multiple antennas) and supporting hardware and/or software for enabling communications with a wireless communication network.

- 5 Additionally or alternatively, the communication interface may include the circuitry for interacting with the antenna(s) to cause transmission of signals via the antenna(s) or to handle receipt of signals received via the antenna(s). In some environments, the communication interface may alternatively or also support wired communication. As such, for example, the communication interface may include a communication modem and/or
- 10 other hardware/software for supporting communication via cable, digital subscriber line (DSL), universal serial bus (USB) or other mechanisms.

[0060] As noted herein, many implementations of example embodiments of the invention described, contemplated, and/or otherwise disclosed herein are directed to solutions that allow for a server to use one or more partial indications of a device identity

15 to allow for a reduction in the size of the relevant IRK pool to be used when determining the identity of the device and decrypting a received message. As such, some example implementations are presented below to clarify how aspects of such example embodiments may be advantageous in certain situations. It will be appreciated that, while many of the following examples refer to a specific network entities and identify certain operations that

20 may be performed by such network entities, it should be appreciated that such references are done for the purposes of clarity, and example implementations conforming to those examples presented herein and/or otherwise contemplated by the invention disclosed herein may be performed in connection with other network entities, alone or in combination with one or more additional network entities, without departing from the spirit

25 and/or scope of the invention disclosed herein.

[0061] As noted herein, example implementations of embodiments of the invention involve the use, by a server, of a set of device identity partial indications or “hints” in order to reduce pool of decryption keys to be tested when attempting to determine the public address of a device and decrypt encrypted messages received from a device with a

30 resolvable private address. By using a partial indicator of the device identity, the size of the pool of the relevant IRKs may be reduced to a degree that a cloud server may more efficiently determine the appropriate key and decrypt any relevant encrypted messages,

while maintaining a degree of security in connection with the public address and/or other identity of a given device. Some example implementations involve the use of one or more of four types of partial indicators by the server to reduce the key pool size: (1) an explicit end-node group context identifier partial indicator; (2) a forwarding gateway identity partial indicator; (3) a forwarding gateway provided end-node identity partial indicator; and (4) a time correlation partial indicator.

Partial Indicator 1 - Explicit End-Node Group Context Identifier

[0062] As noted herein, one of the types of partial indicators that may be used by a server to reduce the relevant key pool size is an explicit end-node group context identifier. In some example implementations, an explicit group context identifier partial indicator may be provided when a relevant sensor and/or other end-node, in its messages, indicates a subgroup to which the device belongs. By identifying a particular subgroup, the use of such a partial indicator may enable the reduction of the key pool size from the full size of all known devices (which may be referred to herein as n) to a fraction of that determined by the subgroup size, referenced herein as m . As such, if the size of subgroup is m , the relevant pool size of IRKs to search for and/or test is reduced in accordance with the ratio m/n . It will be appreciated that in some example situations where m is relatively large with respect to n , the server will still need to search and/or otherwise test a relatively large pool. However, and particularly in system environments where n is very large, the use of an explicit end-node group context identifier as a partial indication of the identity of a given device will typically result in a significant reduction in the relevant pool size. For example, a subgroup of a million nodes within a 100 million sensor system results in key pool of 1% of the whole key set).

[0063] The sensor may indicate its group context in an advertisement and/or other message through a variety of approaches. For example, the group context may be indicated in a specially formed source address. In some example implementations of such as approach, the address format presented in Figure 3 may be augmented and/or otherwise modified to allow for the inclusion of the group context indication. In another example approach, the group context may be indicated in a payload section of an advertisement or other message. It will be appreciated that, in some example implementations adopting such an approach, the group context indication may be provided without implicating or

requiring changes in an address standard and/or other standards that may be applicable to a Bluetooth LE environment. In another example approach, the group context may be indicated in a URL that the sensor and/or other end-node provides to a gateway when requesting forwarding of a message to the cloud server.

- 5 **[0064]** In another example approach arising in the context of systems involving IPv6, the group context identifier could be incorporated into the relevant IPv6 source address. In another example approach, the group context may be indirectly indicated in the relevant cloud server port used for data upload. For example, in systems involving IPv6 protocols, a packet may be sent to a server via a specific address and port combination. In
- 10 such situations, the server's port may be considered as a group indicator (such that devices of group 1 would send data to port 60000, for example, devices of group 2 would send data to port 60001, for example, and the like). It will be appreciated that alternative approaches may also be taken, such as in examples where security protocols block certain ports associated with a server and/or otherwise restrict the ports to which data may be directed.
- 15 **[0065]** It will be appreciated that, in many example implementations, the group context value only has relevance to and/or otherwise makes sense to the relevant cloud server, and nonetheless allows the cloud server to reduce the pool of keys to be tested in connection with a given message and/or device. In particular, the group context identifier typically does not indicate anything other than set of relevant keys, and typically does not
- 20 indicate anything about a country, gender, device type, or other similar information regarding the identity of the device. In some example implementations, the group context identifier may be constructed and/or otherwise assigned such that a group includes enough devices to prevent and/or deter an attacker from conducting meaningful tracking of a particular device based on any group context identifier that the attacker may become able
- 25 to view. In some example situations, a group size on the order of 100,000 or 1,000,000 devices per context may be effective in this regard. In some example implementations, the partial indicator itself may also be encrypted. For example, a secret key may be shared between the server and the node to allow for separate encryption of the partial indicator. In some example implementations, the random address associated with a device may be used
- 30 as an initialization vector for the encryption, and/or the payload may contain a separate random number which may be used for the purposes of partial indicator encryption. In some example implementations, the group context identifier may be composed of a hash

value and random number, which the cloud server can utilize to determine the actual group the device belongs to. In some such example implementations, the server calculates hash values of all the relevant group identifiers and the received random value, and checks if the hash matches. If the hash matches, the server may be considered to have found the group the device belongs to.

Partial Indicator 2 - Forwarding Gateway Identity:

[0066] Some example implementations involve the use of a forwarding gateway identity as a partial indicator of an identity of a relevant sensor and/or other end node. For example, when a server detects a packet with a new privacy source address being forwarded by a gateway, it is often the case that a previously and/or recently heard device has just changed its address to a new privacy enabled source address. For example, some network environments are constructed with rules that typically require a sensor and/or other end-node or device to change and/or refresh its address every 15 minutes, for example. It will be appreciated that other time periods and/or other rules may be imposed with respect to the changing and/or refreshing of an address. In some such situations, the identity of the forwarding gateway associated with an incoming message may allow a server to identify a reduced pool of potentially relevant IRKs. In some such example implementations, a cloud server may reduce the pool of potentially relevant IRKs by testing keys that have recently and successfully been used for decrypting data packets forwarded by the same gateway that forwarded the newly received packet and/or other message. In some such example implementations, and in other example implementations, the server may also test keys that have recently and successfully been used for decrypting data packets forwarded by geographically nearby gateways. Such an approach may be advantageous in situations where a device may have simply moved and is now associated with a different but nearby gateway. In some such example implementations, and in other example implementations, the server may test keys that have recently and successfully been used for decrypting data packets forwarded by a previous gateway which may be associated with a device. Such an approach may be advantageous in situations where a sensor and/or other end-node may have run out of power and/or otherwise experienced a disruption in operation, and has since reconnected with the system. In some example implementations, the cloud server may determine the forwarding gateway identity from a

security certificate the forwarding gateway presents to the cloud server, access credentials the forwarding gateway presents to the cloud server, from the forwarding gateway's source Internet Protocol address (which may be a gateway's IPv4 and/or IPv6 source address, for example) or from the IPv6 prefix portion of an end-node's IPv6 source address. For example, an IPv6 address of an Internet-of-Things (IoT) may be composed of a 64-bit prefix and a 64-bit interface identifier. In some example implementations involving such an IPv6 address, the interface identifier may contain a privacy address, and the 64-bit prefix may identify the subnet the device is in, and thus effectively also identifies the gateway that is serving the end node. As such, the relevant IPv6 prefix may be used as forwarding gateway identity information.

Partial Indicator 3 - Forwarding gateway provided end-node identity:

[0067] As noted herein, one of the types of partial indicators that may be used by a server to reduce the relevant key pool size is a forwarding gateway-provided end-node identity. It will be appreciated that some protocols that are applicable to sensors and/or other end-nodes impose requirements on the timing and/or other conditions under which a sensor and/or other end-node may change and/or refresh its address. For example, under typical Bluetooth specifications, the privacy source address of a sensor and/or other end-node should be periodically changed (such as every 15 minutes, for example). Such rules and/or other requirements are designed at least in part to make unauthorized device tracking difficult.

[0068] Some example implementations of embodiments of the invention described and/or otherwise disclosed herein recognize that if a particular device is periodically sending messages (for example, every five seconds or some other interval), the forwarding gateway may expect when a device would likely send a subsequent advertisement and/or other message. As such, if an advertisement and/or other message arrives from unknown source address (referenced herein as "DEF", for the purposes of clarity, for example) at the exact moment the gateway was expecting to receive an advertisement and/or other message from a device that had previously been identified as having another address (referenced herein as "ABC", for the purposes of clarity, for example) the gateway may indicate to the cloud server that the message received from "DEF" was received at a particular time at which the gateway expected to receive a message from "ABC" and that the message may

therefore be from the sensor and/or other end-node “ABC”. Upon receipt of such information from the gateway, the cloud server may prioritize the testing of an IRK that was successfully used with ABC to determine if the new, unknown device is actually a previously identified device that previously used the privacy address ABC but has since
5 changed addresses. If so, the key that was used for ABC will decrypt data from DEF.

[0069] In some example implementations, the forwarding gateway may be able to take other approaches to determining if a device using a new address is in fact an old device that has simply changed and/or refreshed its address. For example, the gateway may utilize a geographic and/or other physical positioning system (such as GPS,
10 triangulation protocols, and/or other location determining protocols, for example) to determine a physical position of sender. Upon determining the physical location of a sender, the gateway may determine if the new device is located at or near the location at which a previous device was located, thus increasing the likelihood that the “new” address may be the result of an address change event. In some example implementations, the
15 positioning gateway may use a directional antenna (such as those used in connection with a High Accuracy Indoor Positioning (HAIP) system, for example), and/or a received signal strength indicator (RSSI). In some such example implementations, and in other example implementations, a distributed gateway may use triangulation to estimate the device position and thus detect a device changing its address based on location. In some example
20 implementations, a gateway may also use information associated with other detected devices, as not all the devices typically change their addresses at the same time. As such, detecting the continued presence of other devices may provide some information on which device’s address has changed.

25 *Partial Indicator 4 - Time Correlation:*

[0070] As noted herein, one of the types of partial indicators that may be used by a server to reduce the relevant key pool size is a time correlation indication. While the gateway can estimate very accurate moments in time when an end-node is expected to send advertisements (as discussed herein with respect to partial indicator 3 above), it is also
30 possible for a server to conduct time correlation procedures. For example, if a server is expecting a certain number of devices to send messages to the cloud server at a given time and/or over the course of a given time interval (such as may be measured on the order of one or more seconds, minutes, hours, or days, or any other time interval or unit of any size,

for example), the server may identify and prioritize the testing of keys that have been previously determined for devices that are expected to report at a given time and/or in the course of a given time interval. In some example implementations that use such a partial indicator, upon receipt of a message from a device with an unknown key, the server may first identify the devices that were expected to send a message at or near the time at which the message was received and test the keys associated with those devices.

[0071] Some example implementations of embodiments of the invention described and/or otherwise disclosed herein contemplate the use of one or more of the partial indicators described herein to reduce the pool of potentially relevant IRKs to be tested against an incoming message. Some such example implementations arise in the context of a system environment similar to those shown in Figures 1 and 4, where numerous sensors may interact with gateways to pass messages to a cloud server and/or other similar network entity. In some such example implementations, a sensor may send a Bluetooth LE advertisement and/or other message to the cloud server with a URL that indicates the device group context (such as in accordance with partial indicator 1) in the URL, which may take the form of: *http://iotp.server.nokia.com/?ctx=123*, where the portion of the URL “*?ctx=123*” reflects the indication of the group context. In some such example implementations, the forwarding gateway (which may include, for example, a forwarding gateway responsible for performing power on self tests (POSTs)) amends the URL with an explicit device partial indicator (such as in accordance with partial indicator 3 above) such that the URL may be expressed as:

http://iotp.server.nokia.com/?ctx=123&gwhint=ab:cd:ef:01:02:03, where the expression “*?ctx=123&gwhint=ab:cd:ef:01:02:03*” reflects both the context information and partial indicator of a device identity.

[0072] Upon receipt of such a URL, the cloud server can further utilize a partial indicator such as one discussed in connection with partial indicator 2 above, to determine which keys have been used with the forwarding gateway and its nearby gateways recently. Likewise, the cloud server may also use a time correlation indication similar to that discussed in connection with partial indicator 4 to determine from which pool of devices inbound communications are expected at a time when the relevant message was received.

[0073] In some example implementations, after developing a pool of candidate addresses through the use of the partial indicators, the server can prioritize the keys. For

example, the server may start by testing to determine whether the same key that worked previously for device ab:cd:ef:01:02:03 (which may be identified as set out above with respect to partial indicator 3, for example) works with the message received by the cloud server. If that key does not work, then the server may test keys used previously for data forwarded by the same gateway or nearby gateways (such as in accordance with partial indicator 2, for example). In the event that those keys failed to be the correct key, then server may try keys from all devices that are expected to communicate at the time message was received (such as may be determined in connection with partial indicator 4, for example) and that are also part of the identified group (such as may be identified in connection with partial identifier 1, for example). In the event that all such keys from the reduced, prioritized pool of keys fail, the server may then test all keys indicated by the group context id (such as may be identified in connection with partial identifier 1, for example).

[0074] Referring now to Figure 5, the operations performed by the apparatus 200 of Figure 2 in accordance with an example embodiment of the present invention are depicted as an example process flow 500. In this regard, the apparatus includes means, such as the processor 202, the memory 204, the user interface 206, the communication interface 208 or the like, for receiving, at a server, a message transmitted by an end-node, wherein the message comprises an encrypted payload and wherein the end-node is configured with a privacy-enabled address; receiving, at the server a partial indication of the identity of the end-node; determining, based at least in part on the partial indication of the identity of the end-node, a plurality of identity resolving keys to be tested against the message; and identifying a correct identity resolving key from amongst the plurality of identity resolving keys.

[0075] The apparatus includes means, such as the processor 202, the memory 204, the user interface 206, the communication interface 208 or the like, for receiving, at a server, a message transmitted by an end-node, wherein the message comprises an encrypted payload and wherein the end-node is configured with a privacy-enabled address. With reference to Figure 5, process flow 500 may commence at block 502, which includes receiving an encrypted message from an end-node. As discussed throughout this disclosure, many example implementation of embodiments of the invention are directed to reducing the load imposed on a server when determining the key(s) that will allow the

server to identify the source of a message and decrypt the encrypted payload of the message. In some example implementations of process flow 500 in general, and block 502 in particular, the message is a Bluetooth Low Energy advertisement message. In some such example implementations, and in other example implementations, the end-node
5 associated with the message may be a sensor and/or other device and may be configured such that a resolvable private address is associated with the message.

[0076] The apparatus also includes means, such as the processor 202, the memory 204, the user interface 206, the communication interface 208 or the like, for receiving, at the server a partial indication of the identity of the end-node. With reference to Figure 5,
10 process flow 500 may continue to block 504, which includes receiving a partial indication of the identity of the end-node. As noted herein, some example implementations of embodiments of the invention contemplate the use of one or more partial indications or “hints” to assist the server in reducing the pool of potentially relevant IRK keys to test against an incoming message and/or resolvable private address. In many example
15 implementations, the partial indication may be received from the end-node, a relevant gateway, and/or determined by the server. However, any approach to receiving a partial indication of an identity of an end-node may be used in connection with example implementations of block 504.

[0077] The partial indication of the identity of the end-node may take any of a
20 number of forms, including but not limited to those discussed in examples contained herein. For example, the partial indication of the identity of the end-node may be associated with an end-node group context identifier. Any of the example implementations and approaches to the provision and use of such a partial indication, including but not limited to those discussed in connection with partial indication 1 presented herein may be
25 used in example implementations of block 504. In another example, the partial indication of the identity of the end-node is associated with a forwarding gateway identity. Any of the example implementations and approaches to the provision and use of such a partial indication, including but not limited to those discussed in connection with partial indication 2 presented herein may be used in example implementations of block 504. In
30 another example, the partial indication of the identity of the end-node is associated with a forwarding gateway end-node identity. Any of the example implementations and approaches to the provision and use of such a partial indication, including but not limited

to those discussed in connection with partial indication 3 presented herein may be used in example implementations of block 504. In yet another example, the partial indication of the identity of the end-node is associated with a time at which a message is expected to be received. Any of the example implementations and approaches to the provision and use of such a partial indication, including but not limited to those discussed in connection with partial indication 4 presented herein may be used in example implementations of block 504.

[0078] The apparatus also includes means, such as the processor 202, the memory 204, the user interface 206, the communication interface 208 or the like, for determining, based at least in part on the partial indication of the identity of the end-node, a plurality of identity resolving keys to be tested against the message. With reference to Figure 5, process flow 500 may proceed to block 506, which includes determining the pool of identity resolving keys or IRKs. As discussed herein, particularly with respect to Figures 3 and 4, along with the discussion of the partial indicators 1-4, many example implementations of example embodiments of the invention are aimed at allowing a server operating in a network environment that contains very large numbers of end-nodes (such as sensors that maybe communicating in a unidirectional manner with a gateway, for example) to efficiently reduce and/or prioritize the number of potential IRKs to be tested to determine the identity of a relevant end-node and decrypt the encrypted payload of a message received from such end-node. Any of the approaches to using one or more partial indications of an end-node identity disclosed and/or otherwise contemplated herein may be used in connection with example implementations of block 506, including but not limited to the use of partial indications to identify candidate end-nodes and/or IRKs that should be prioritized for testing.

[0079] The apparatus also includes means, such as the processor 202, the memory 204, the user interface 206, the communication interface 208 or the like, for identifying a correct identity resolving key from amongst the plurality of identity resolving keys. With reference to Figure 5, process flow 500 may proceed to block 508, which includes identifying the correct identity resolving key. Any of the approaches described and/or otherwise contemplated herein with respect to the testing and/or other identification of an IRK may be used in connection with example implementations of block 508. For example, a hash value and a localhash value may be calculated and compared using the functions

described herein with respect to Figure 3. In some such example implementations, and in other example implementations, each key from within the determined pool or plurality of keys is tested to determine whether it is the correct key. Upon identification of the correct key, the testing process may be terminated, thus further reducing the computational and/or other resource load on the server.

[0080] The apparatus also optionally includes means, such as the processor 202, the memory 204, the user interface 206, the communication interface 208 or the like for caching the correct identity resolving key from amongst the plurality of identity resolving keys for use with a subsequent message received from the end-node. With reference to

Figure 5, process flow 500 may proceed to optional block 510, which includes caching the identified correct IRK. As discussed herein, the aim of many example implementations of embodiments of the invention is to reduce the load placed on a server associated with the identification of the correct key to use with one of a very large group of sensors and/or other end-nodes that are sending messages to the server. As such, in some example implementations of process flow 500, correctly identified IRKs are cached and/or otherwise stored in memory and/or other storage accessible by the server such that when subsequent messages are received from a previously identified end-node, the previously determined correct IRK may be tested first. In many such situations, such as when a particular sensor or other end-node remains stationary or otherwise associated with a particular gateway, the cached IRK will be the appropriate IRK to use.

[0081] It will be appreciated that, in many situations and contexts, example implementations of embodiments of the invention described and/or otherwise disclosed herein may significantly reduce the load placed on a server, particularly with respect to common cases for handling encrypted advertisements and/or other messages from

Bluetooth LE nodes that are changing their privacy addresses. In particular, many example implementations result in a significant reduction in the likelihood that all available keys must be checked to identify the correct key (with the exception of a first connection case). In some situations, the information associated with partial indicator 2 discussed above may be sufficient to reduce the key pool size to a small size, such that more resource consuming search events may be needed only for very mobile devices that frequently change gateways and/or addresses. In contexts that involve a large proportion of devices in a fixed position, (such as at or within a home, for example), the devices may always be connected through

the same gateway, and would therefore remain within a pool size determined in connection with partial indicator 2. It will be appreciated that, in many situations that involve wearable devices, such devices may also remain under the same gateway, especially if the device(s) relies on a smartphone as the gateway and the smartphones remains collocated with and/or otherwise near the wearable (such that the wearable appears stationary and/or near stationary in relation to the smartphone gateway).

[0082] It will be appreciated that example implementations of the invention described and/or otherwise disclosed herein may assist in the implementation of networks involving unidirectional communication involving large numbers of sensors, and may also assist in facilitating the changes of addresses for location tags associated with HAIP systems. It will also be appreciated that at least some example implementations may be performed and/or established while conforming to Bluetooth standards.

[0083] In general, some example implementations of embodiments of the invention effectively trade the addition of a limited number of additional bytes of data to be transmitted over a network interface (such as the additional information associated with providing a group context indicator, extending URL and/or providing another other partial indicator) for a significant reduction in server load, which may be realized through the reduction of the pool of potentially relevant IRKs. In particular, by using partial indicators that allow for the pool to be reduced to focus on keys associated with a limited number of gateways, the key pool size for many common cases may be significantly reduced and thus compounding the resource savings by reducing the server load and attendant costs associated with many of the messages received by a cloud server. While a full pool search will typically be needed in a first connection case, the need for such a full, resource intensive search is, in many example implementations, significantly decreased outside of the context of the first connection of a given device. Such a reduction in full search needs may be particularly noticeable in contexts where a given device remains associated with the same gateway or use a relatively small set of gateways that are geographically close to each other.

[0084] Many example implementations of embodiments of the invention are able to significantly reduce server load while maintaining a degree of security with respect to the identity and/or location of a given device. It will be appreciated, however, that the introduction of group context information may, in some cases, potentially assist an

unauthorized entity seeking to identify a device by significantly decreasing the potential pool size. For example, the group context information may identify a pool of 100,000 devices within a device population of millions of devices. Consequently, in situations where device identity security is paramount, a partial indication incorporating a group context may optionally be omitted (or structured such that the group context still identifies a very large group) such that network attackers and/or other unauthorized entities may be hindered, but that still significantly helps reduce load on the server.

[0085] It will be appreciated that the use of gateway-related partial indications does not help an attacker, as the partial indicators provided by the gateway may be securely transmitted from the gateway to the server, such as through the use of a secure connection, such as TLS, for example. Moreover, since an attacker typically does not have view on the data associated with all gateways (unless an attacker also deploys a large set of listeners), example implementations of the invention need not weaken security on that aspect either. Moreover, as example implementations of the invention may be established without implicating the keying or other security aspects associated with Bluetooth and/or related protocols, the Bluetooth security and device privacy aspects may be unaffected.

[0086] As described above, Figure 5 illustrates a flowchart of an apparatus 200, method, and computer program product according to example embodiments of the invention. It will be understood that each block of the flowchart, and combinations of blocks in the flowchart, may be implemented by various means, such as hardware, firmware, processor, circuitry, and/or other devices associated with execution of software including one or more computer program instructions. For example, one or more of the procedures described above may be embodied by computer program instructions. In this regard, the computer program instructions which embody the procedures described above may be stored by the memory device 204 of an apparatus employing an embodiment of the present invention and executed by the processor 202 of the apparatus. As will be appreciated, any such computer program instructions may be loaded onto a computer or other programmable apparatus (such as hardware, for example) to produce a machine, such that the resulting computer or other programmable apparatus implements the functions specified in the flowchart blocks. These computer program instructions may also be stored in a computer-readable memory that may direct a computer or other programmable apparatus to function in a particular manner, such that the instructions stored in the

computer-readable memory produce an article of manufacture the execution of which implements the function specified in the flowchart blocks. The computer program instructions may also be loaded onto a computer or other programmable apparatus to cause a series of operations to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable apparatus provide operations for implementing the functions specified in the flowchart blocks.

[0087] Accordingly, blocks of the flowchart support combinations of means for performing the specified functions and combinations of operations for performing the specified functions. It will also be understood that one or more blocks of the flowchart, and combinations of blocks in the flowchart, can be implemented by special purpose hardware-based computer systems which perform the specified functions, or combinations of special purpose hardware and computer instructions.

[0088] In some embodiments, certain ones of the operations above may be modified or further amplified. Furthermore, in some embodiments, additional optional operations may be included. Modifications, additions, or amplifications to the operations above may be performed in any order and in any combination.

[0089] Many modifications and other embodiments of the inventions set forth herein will come to mind to one skilled in the art to which these inventions pertain having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the inventions are not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Moreover, although the foregoing descriptions and the associated drawings describe example embodiments in the context of certain example combinations of elements and/or functions, it should be appreciated that different combinations of elements and/or functions may be provided by alternative embodiments without departing from the scope of the appended claims. In this regard, for example, different combinations of elements and/or functions than those explicitly described above are also contemplated as may be set forth in some of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

THAT WHICH IS CLAIMED:

1. A method comprising:

receiving, at a server, a message transmitted by an end-node, wherein the message comprises an encrypted payload and wherein the end-node is configured with a privacy-enabled address;

receiving, at the server a partial indication of the identity of the end-node;

determining, based at least in part on the partial indication of the identity of the end-node, a plurality of identity resolving keys to be tested against the message; and

identifying a correct identity resolving key from amongst the plurality of identity resolving keys.

2. The method of claim 1, wherein the message is a Bluetooth Low Energy advertisement message.

3. The method of claim 1, wherein the message is an Internet Protocol message.

4. The method of at least one of claims 1-3, wherein the partial indication of the identity of the end-node is associated with an end-node group context identifier.

5. The method of at least one of claims 1-4, wherein the partial indication of the identity of the end-node is associated with a forwarding gateway identity.

6. The method of at least one of claims 1-5, wherein the partial indication of the identity of the end-node is associated with a forwarding gateway end-node identity.

7. The method of at least one of claims 1-6, wherein the partial indication of the identity of the end-node is associated with a time at which a message is expected to be received.

8. The method of at least one of claims 1-7, further comprising caching the correct identity resolving key from amongst the plurality of identity resolving keys for use with a subsequent message received from the end-node.

9. An apparatus comprising at least one processor and at least one memory storing computer program code, the at least one memory and the computer program code configured to, with the processor, cause the apparatus to at least:

5 receive, at a server, a message transmitted by an end-node, wherein the message comprises an encrypted payload and wherein the end-node is configured with a privacy-enabled address;

receive, at the server a partial indication of the identity of the end-node;

10 determine, based at least in part on the partial indication of the identity of the end-node, a plurality of identity resolving keys to be tested against the message; and
identify a correct identity resolving key from amongst the plurality of identity resolving keys.

10. The apparatus of claim 9, wherein the message is a Bluetooth Low Energy
15 advertisement message.

11. The apparatus of claim 9, wherein the message is an Internet Protocol message.

12. The apparatus of at least one of claims 9-11, wherein the partial indication of the
20 identity of the end-node is associated with an end-node group context identifier.

13. The apparatus of at least one of claims 9-12, wherein the partial indication of the identity of the end-node is associated with a forwarding gateway identity.

25 14. The apparatus of at least one of claims 9-13, wherein the partial indication of the identity of the end-node is associated with a forwarding gateway end-node identity.

15. The apparatus of at least one of claims 9-14, wherein the partial indication of the identity of the end-node is associated with a time at which a message is expected to be
30 received.

16. The apparatus of at least one of claims 9-15, wherein the at least one memory and the computer program code are further configured to, with the processor, cause the

apparatus to at least cache the correct identity resolving key from amongst the plurality of identity resolving keys for use with a subsequent message received from the end-node.

17. A computer program product comprising at least one non-transitory computer-readable storage medium having computer-executable program code instruction stored therein, the computer-executable program code instructions comprising program code instructions configured to:

receive, at a server, a message transmitted by an end-node, wherein the message comprises an encrypted payload and wherein the end-node is configured with a privacy-enabled address;

receive, at the server a partial indication of the identity of the end-node;

determine, based at least in part on the partial indication of the identity of the end-node, a plurality of identity resolving keys to be tested against the message; and

identify a correct identity resolving key from amongst the plurality of identity resolving keys.

18. The computer program product of claim 17, wherein the message is a Bluetooth Low Energy advertisement message.

19. The computer program product of claim 17, wherein the message is an Internet Protocol message.

20. The computer program product of at least one of claims 17-19, wherein the partial indication of the identity of the end-node is associated with an end-node group context identifier.

21. The computer program product of at least one of claims 17-20, wherein the partial indication of the identity of the end-node is associated with a forwarding gateway identity.

22. The computer program product of at least one of claims 17-21, wherein the partial indication of the identity of the end-node is associated with a forwarding gateway end-node identity.

23. The computer program product of at least one of claims 17-22, wherein the partial indication of the identity of the end-node is associated with a time at which a message is expected to be received.
- 5 24. The computer program product of at least one of claims 17-23, the computer-executable program code instructions further comprising program code instructions configured to cache the correct identity resolving key from amongst the plurality of identity resolving keys for use with a subsequent message received from the end-node.
- 10 25. An apparatus comprising means for performing a method according to at least one of claims 1-8.

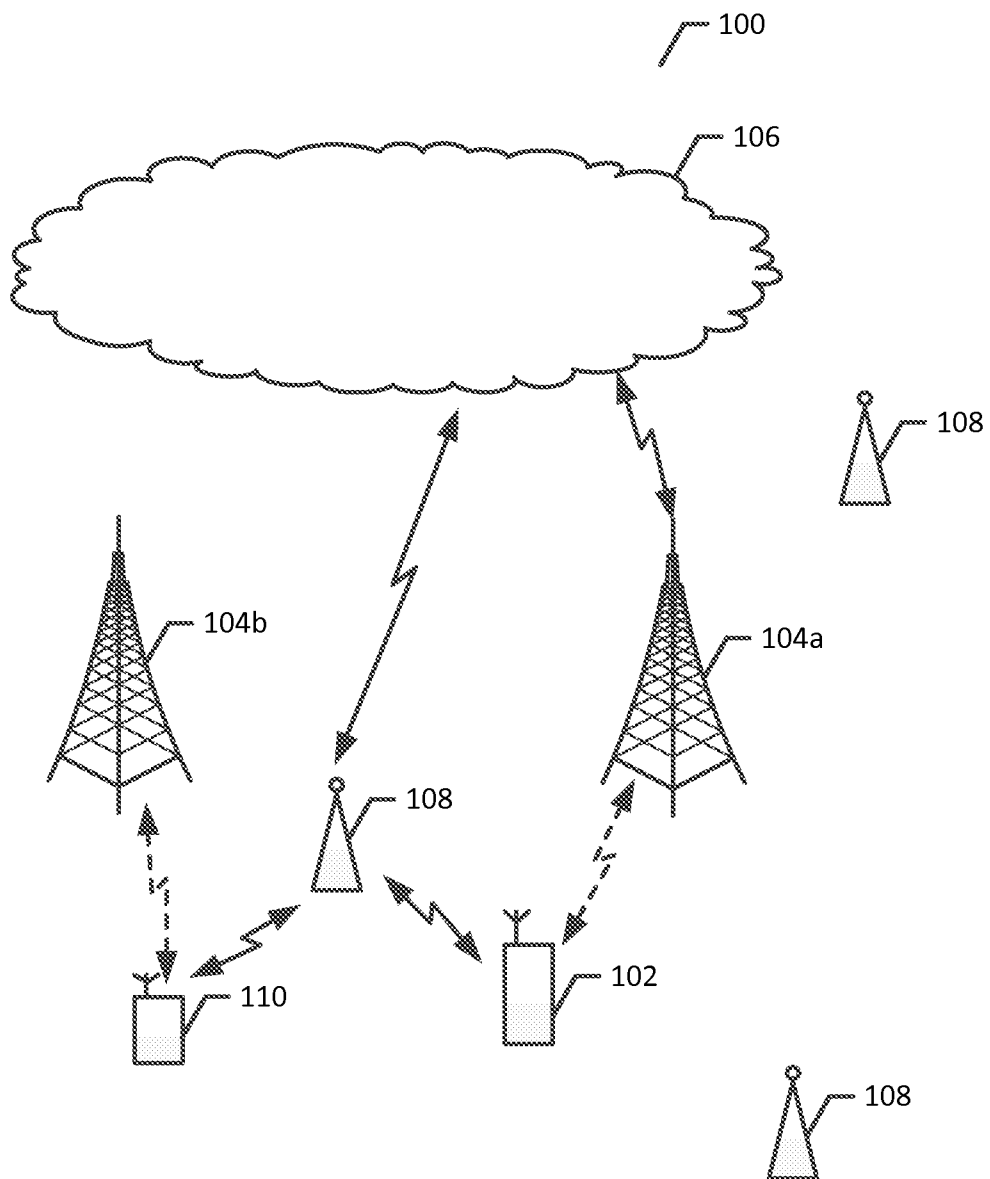


Figure 1

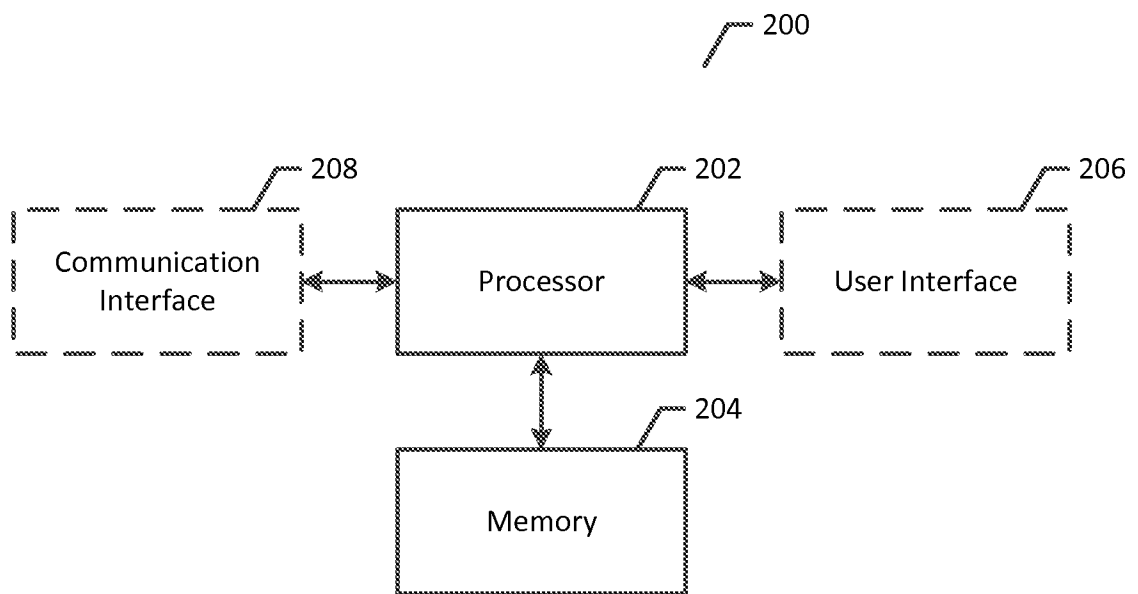


Figure 2

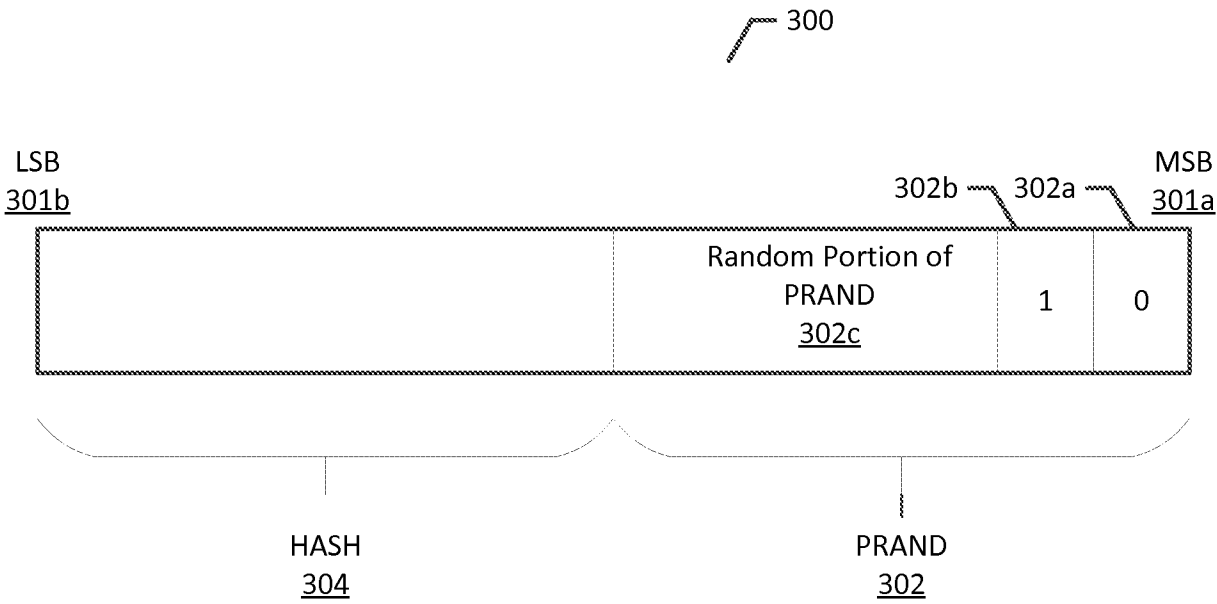


Figure 3

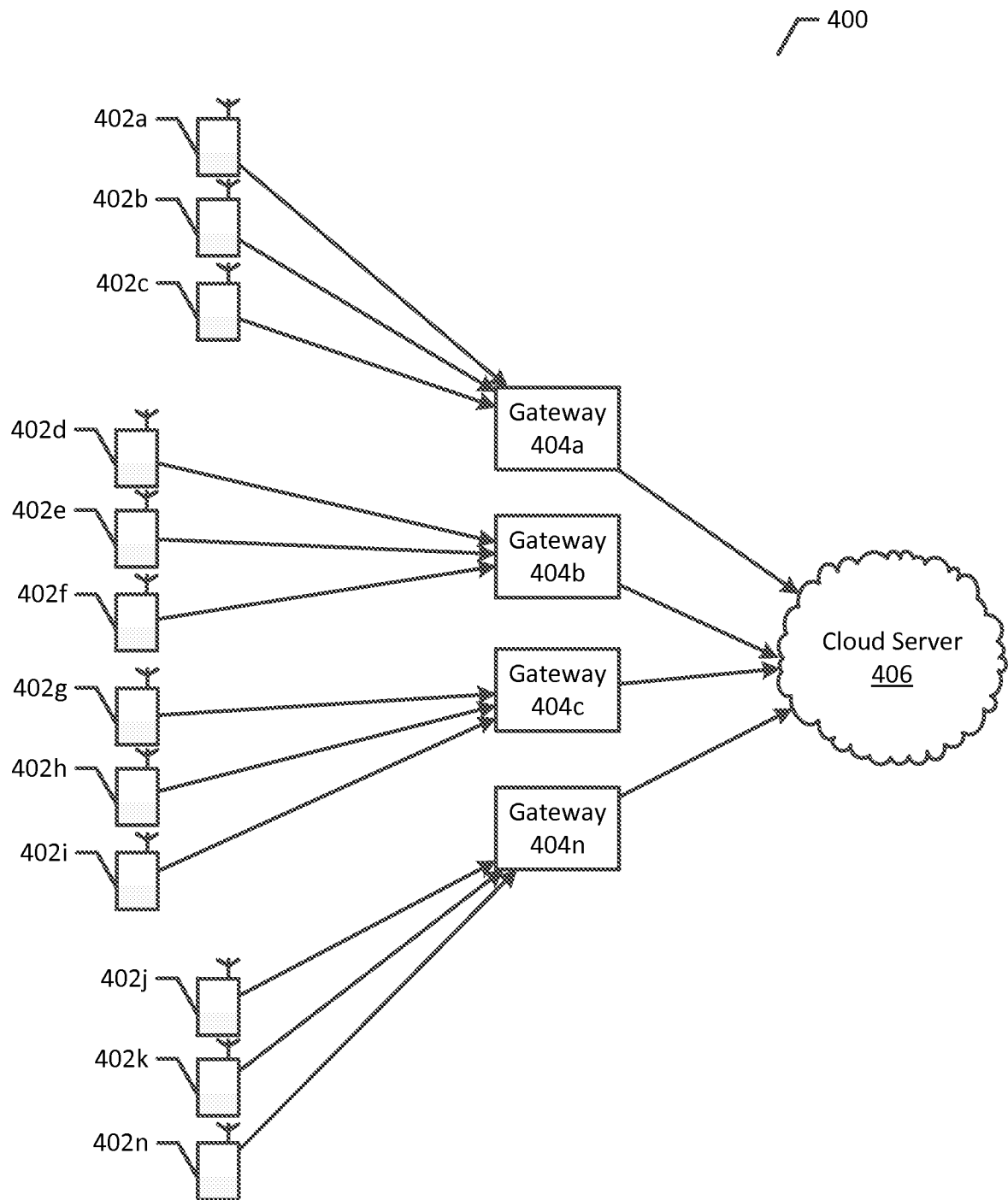


Figure 4

5/5

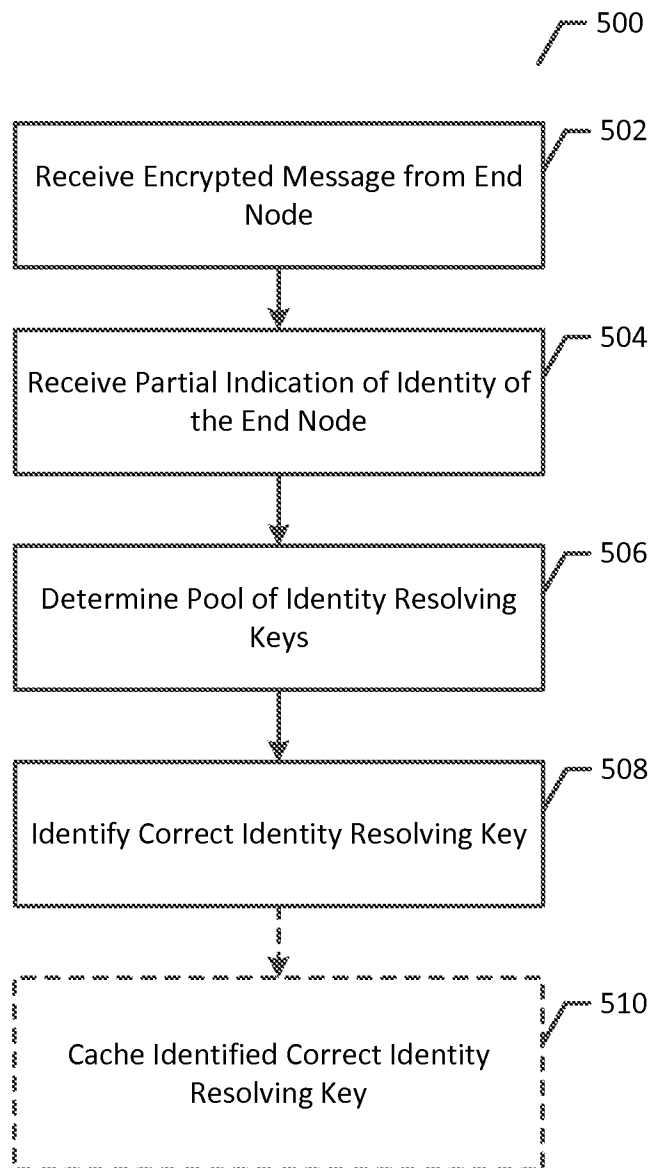


Figure 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2017/050307

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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)

IPC: H04W, H04L

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

FI, SE, NO, DK

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

EPODOC, EPO-Internal full-text databases, WPIAP, XP3GPP, XPAIP, XPESP, XPETSI, XPI3E, XPIEE, XPIETF, XPIOP, XPIPCOM, XPJPEG, XPMISC, XPOAC, XPRD, XPTK, COMPD, INSPEC, NPL, Internet, ESPACENET

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016212194 A1 (PALIN ARTO [FI] et al.) 21 July 2016 (21.07.2016) Abstract, paragraphs [0040], [0057]-[0060], [0065], [0081], [0112], [0116], [0122], [0124]-[0127], [0131], [0144]-[0145], [0169], [0177], [0200]-[0207], [0211]-[0222], [0271], [0278], [0299]-[0301], [0320]-[0321], [0349], [0373], [0428], figures 1A-1B, 2, 2C, 3E-4A, 6A-6B.	1-4, 7-12, 15-20, 23-25
Y	paragraphs [0057]-[0060], [0065], [0116], [0122], [0132], [0195], [0210]-[0222], [0271], [0286], [0300], [0428], claim 1.	5-6, 13-14, 21-22
Y	US 2017041868 A1 (PALIN ARTO [FI] et al.) 09 February 2017 (09.02.2017) Abstract, paragraphs [0156]-[0159], [0165], [0179]-[0196], [0249].	5-6, 13-14, 21-22
A	US 2017013450 A1 (ZIV ALON [IL] et al.) 12 January 2017 (12.01.2017) The whole document.	1-25

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

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search

29 June 2017 (29.06.2017)

Date of mailing of the international search report

03 July 2017 (03.07.2017)

Name and mailing address of the ISA/FI
Finnish Patent and Registration Office
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 29 509 5328

Authorized officer
Harald Kaaja
Telephone No. +358 29 509 5000

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2017/050307

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2017003337 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) [SE]) 05 January 2017 (05.01.2017) The whole document.	1-25
A	EP 2645665 A1 (BROADCOM CORP [US]) 02 October 2013 (02.10.2013) The whole document.	1-25

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2017/050307

CLASSIFICATION OF SUBJECT MATTER

IPC

H04L 29/08 (2006.01)

H04L 9/32 (2006.01)

H04L 29/06 (2006.01)

H04W 4/00 (2009.01)

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2017/050307

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2016212194 A1	21/07/2016	WO 2016114846 A1	21/07/2016
US 2017041868 A1	09/02/2017	CN 106454996 A EP 3128790 A1	22/02/2017 08/02/2017
US 2017013450 A1	12/01/2017	WO 2017007719 A1	12/01/2017
WO 2017003337 A1	05/01/2017	None	
EP 2645665 A1	02/10/2013	CN 103368722 A KR 20130111165 A TW 201340665 A US 2013259230 A1	23/10/2013 10/10/2013 01/10/2013 03/10/2013