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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 October 2021 (21.10.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/211315 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04W 12/03* (2021.01)
H04W 12/02 (2009.01)

(21) International Application Number:
PCT/US2021/025743

(22) International Filing Date:
05 April 2021 (05.04.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/010,370 15 April 2020 (15.04.2020) US

(71) Applicant: **GOOGLE LLC** [US/US]; 1600 Amphitheatre Parkway, Mountain View, California 94043 (US).

(72) Inventors: **YUNG, Marcel M.M.**; 1600 Amphitheatre Parkway, Mountain View, California 94043 (US). **LAZAROV, David**; 1600 Amphitheatre Parkway, Mountain View, California 94043 (US).

(74) Agent: **JOHNSON, Matthew**; 291 E. Shore Drive, Suite 200, Eagle, Idaho 83616 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

(54) Title: END-TO-END ENCRYPTED LOCATION-FINDING

(57) Abstract: This document describes methods, devices, systems, and means to ensure end-to-end encryption of location information that is forwarded through a potentially untrustworthy cloud service that serves to forward the location information from a sighting device to an owner of a sighted device. The end-to-end encryption of location information preserves the privacy of location information that is provided by sighter devices that are not associated with the owner as the location information traverses network nodes from the sighter to the owner.

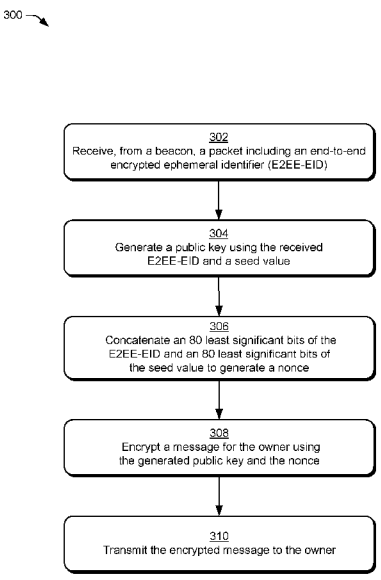


Fig. 3

WO 2021/211315 A1

[Continued on next page]

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

END-TO-END ENCRYPTED LOCATION-FINDING

BACKGROUND

[0001] Beacon systems using ephemeral identifiers are designed to give developers control over which clients can make use of their beacon signals. Ephemeral identifiers and keys shared between a beacon and the beacon's owner enable resolver services to determine the owner of a beacon when a sighter sends the ephemeral identifier to the resolver service. The communication between the sighter of the beacon and the resolver as well as the communication between the resolver and the owner are secured; however, any communication between the beacon and/or the sighter and the owner is not secure and is visible to the resolver.

SUMMARY

[0002] This summary is provided to introduce simplified concepts of end-to-end encrypted location-finding. The simplified concepts are further described below in the Detailed Description. This summary is not intended to identify essential features of the claimed subject matter, nor is it intended for use in determining the scope of the claimed subject matter.

[0003] In aspects, methods, devices, systems, and means for end-to-end encrypted location-finding in a wireless network are described in which a sighter receives, from a beacon, a packet including an end-to-end encrypted ephemeral identifier (E2EE-EID). The sighter generates a public key using the received E2EE-EID and a seed value. The sighter concatenates an 80 least significant bits of the E2EE-EID and an 80 least significant bits of the seed value to generate a nonce. The sighter encrypts a message for the owner using the generated public key and the nonce, and the sighter transmits the encrypted message to the owner.

[0004] In aspects, methods, devices, systems, and means for end-to-end encrypted location-finding in a wireless network are described in which a beacon determines an identity key that is shared between the beacon and an owner. The beacon generates an end-to-end encrypted

ephemeral identifier (E2EE-EID) using the identity key and a time value. The beacon generates a beacon packet including the E2EE-EID and transmits the beacon packet, the transmitted beacon packet being usable by a sighter receiving the beacon packet to transmit a secure message to the owner.

[0005] In aspects, methods, devices, systems, and means for end-to-end encrypted location-finding in a wireless network are described in which an owner retrieves a message from a resolver, the message including an end-to-end encrypted ephemeral identifier (E2EE-EID). The owner generates a public key using the received E2EE-EID and a seed value. The owner concatenates an 80 least significant bits of the E2EE-EID and an 80 least significant bits of the seed value to generate a nonce, and the owner decrypts the received message using the generated public key and the nonce.

[0006] While features and concepts of the described systems and methods for end-to-end encrypted location-finding can be implemented in any number of different environments, systems, devices, and/or various configurations, embodiments of end-to-end encrypted location-finding are described in the context of the following example devices, systems, and configurations.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Embodiments of end-to-end encrypted location-finding are described with reference to the following drawings. The same numbers are used throughout the drawings to reference like features and components:

FIG. 1 illustrates an example environment in which various embodiments of end-to-end encrypted location-finding can be implemented.

FIG. 2 illustrates example data and control transactions between devices in accordance with aspects of end-to-end encrypted location-finding.

FIG. 3 illustrates an example method of end-to-end encrypted location-finding in accordance with embodiments of the techniques described herein.

FIG. 4 illustrates an example method of end-to-end encrypted location-finding in accordance with embodiments of the techniques described herein.

FIG. 5 illustrates an example method of end-to-end encrypted location-finding in accordance with embodiments of the techniques described herein.

FIG. 6 illustrates an example network device that can be implemented in a network environment in accordance with one or more embodiments of the techniques described herein.

FIG. 7 illustrates an example beacon device that can be implemented in a network environment in accordance with one or more embodiments of the techniques described herein.

DETAILED DESCRIPTION

[0008] This document describes methods, devices, systems, and means to ensure end-to-end encryption of location information that is forwarded through a potentially untrustworthy cloud service that serves to forward the location information from a sighting device to an owner of a sighted device. The end-to-end encryption of location information preserves the privacy of location information that is provided by sighter devices that are not associated with the owner as the location information traverses network nodes from the sighter to the owner.

[0009] Many electronic devices advertise short-range wireless signals while they operate, devices such as earbuds, smart watches, smartphones, cameras, tracking tags, or the like. Using suitable wireless technologies and protocols, the advertised wireless signals enable receivers, such as smartphones, network-connected speakers, home automation hubs, security hubs, or the like, to identify these electronic devices. If a receiver is aware of its location (*e.g.*, geographic location) the receiver can upload a location at which an advertised signal was received from an electronic device together with an identity of the electronic device. For example, the receiver can upload the location at which the electronic device was sighted to a service (*e.g.*, a cloud-based service) to allow an owner of the electronic device to query for the location of the electronic device in the event the owner misplaces the electronic device.

[0010] However, the privacy of the reported location information of the electronic device and the device's identity must be considered, in order to protect against bad actors potentially obtaining and exploiting this information. Having the electronic device broadcast an unchanging identifier in an advertisement transmission could enable anyone to track the electronic device, including potentially using the information to track a person (such as the person who owns the electronic device) carrying the electronic device or any object to which the electronic device may be affixed.

[0011] Protocols like Eddystone-EID and FastPair introduced techniques to protect the privacy of the identity of the electronic device by having the electronic device advertise a message that included a rotating identifier based on a predetermined mechanism to allow the owner (and only the owner) to identify the electronic device. However, additional protections can be added to these approaches to keep the reported location of the electronic device private to all but the owner.

[0012] For example, low-power wireless beacons, such as Bluetooth Low Energy (Bluetooth LE, BLE) beacons, transmit information in a beacon packet (*e.g.*, an advertising channel protocol data unit (PDU)). A beacon may transmit broadcast information that is directly identifiable, such as unencrypted data, or broadcast an identifier that changes every few minutes, such as an ephemeral identifier (ephemeral ID, EID). The ephemeral identifier can be resolved to useful information by an owner that shares an identity key (the Ephemeral Identity Key, or EIK) with the individual beacon. Although the following discussion frequently refers to BLE, BLE is an example wireless technology that is discussed for simplicity, but the ephemeral identifiers discussed herein may also be applied to another wireless technology (*e.g.*, Ultra Wideband (UWB), Wireless Local Area Network (WLAN), Near Field Communication (NFC), a personal area network (PAN), IEEE 802.15.4, ZigBee, Thread, or the like) in a similar manner.

Example Environment

[0013] FIG. 1 illustrates an example environment 100 in which various embodiments of end-to-end encrypted location-finding can be implemented. The environment 100 includes a beacon 110, a sighter 120, a resolver 130, and an owner 140. The beacon 110 is a device, such as a BLE beacon, a headset, or the like that periodically broadcasts (*e.g.*, transmits) beacon packets, as shown at 102. The sighter (or observer) 120 is a device, such as a smartphone, that can receive the beacon packets and forward the received packets to a resolver service, as shown at 104. For example, the sighter 120 forwards the received packets to a resolver service 130 via the Internet 150. In this example, the Internet 150 represents any combination of wired and/or wireless, local and/or wide area networks that interconnect the sighter 120, the resolver 130, and/or the owner 140. The resolver 130, such as a cloud-based resolver service (resolution service) compares received EIDs against hash values of shared keys and associated owners to determine the correct owner and forward the received packet to the correct owner 140, as shown at 106. Alternatively or additionally, the owner 140 can query the resolver 130 for packets or messages received from sighters 120 for any beacons 110 associated with the owner 140. The owner 140 is a device or service, such as a smartphone, computer, or cloud-based service, associated with the beacon 110. The owner 140 may own one or more beacons 110 and store the shared keys for each of those beacons 110.

[0014] End-to-end encrypted location-finding can be used with any suitable devices configured for communication as illustrated in FIG. 1. The owner 140 can be any owner computing system. The beacon 110 can be any device associated with the owner computing system. A communication from the device to the owner computing system is anonymized (by hiding the identities of both the device and owner computing system) and involving a routing system (*e.g.*, the resolver 130) to resolve the anonymity into an identification of the owner computing system and device and connecting the device to the owner computing system. The sighter 120 can be any sighter system that is an intermediary device that receives a beacon packet from the device and

sends sighting information about the sighting of the device to its owner computing system in spite of the anonymity. The sighting information is kept secure from the resolver (and any other network nodes) except the owner computing system.

[0015] The beacon 110 is a device that periodically transmits (broadcasts) a beacon packet (*e.g.*, a BLE advertisement packet) that includes an ephemeral identifier (EID) that is generated from a shared key (EIK), which is shared between the beacon 110 and the owner 140, and the time at which the EID is generated by the beacon 110. The beacon 110 calculates a new EID at a rotation rate known to the beacon 110 and its owner 140. The beacon 110 may have limited computational and power resources and broadcasts the beacon packets over a limited range. The sighter 120 can receive beacon packets from the beacon 110 and has access to a longer-range network (*e.g.*, a Wide Area Network, WAN). The sighter 120 can connect to cloud-based services, such as the resolver 130, over the longer-range network. This enables the sighter 120 to forward received beacon packets to a cloud-based resolver 130. The resolver 130 can be a device (server) or a collection of devices that form a cloud-based service. The resolver 130 stores a set of owners 140 and associated EIDs for those owners. The resolver 130 compares a received EID from a beacon packet to its stored set of EIDs to determine the associated owner 140 for the received beacon packet. Once an owner 140 is identified for a received beacon packet, the resolver 130 can forward the beacon packet to the correct owner 140 of that packet.

[0016] At initialization of a beacon 110, the beacon 110 and the owner 140 use an elliptic curve Diffie-Hellman key agreement protocol to exchange a key (EIK) that is shared between the beacon 110 and the owner 140, as shown at 108. The shared EIK enables the resolver 130 to resolve, based on time, the identity of the beacon 110 from the EID and to direct a message from the beacon 110 and/or the sighter 120 to the owner 140. The communication between the sighter 120 and the resolver 130 as well as the communication between the resolver 130 and the owner 140 are secured using Transport Layer Security (TLS). However, any communication between the beacon 110 and/or the sighter 120 and the owner 140 is visible to the resolver 130. Adding a secure

(encrypted) end-to-end communication channel from the sighter 120 to the owner 140 provides secrecy for messages from the beacon 110 and/or sighter 120 to the owner 140 using the resolver 130 as a routing element that cannot access the encrypted payload of a message between the sighter 120 and the owner 140.

End-to-End Encrypted Location-Finding

[0017] In aspects, when the beacon 110 is paired with the owner 140, the beacon 110 and the owner 140 (*e.g.*, by using an application on a smartphone) initiate a common state and agree upon a shared, 256-bit symmetric identity key (the EIK) as described above. The beacon 110 and the owner 140 also determine a frequency (*e.g.*, a rotation period) for rotating the value of the end-to-end encrypted ephemeral identifier (E2EE-EID) that the beacon 110 includes in the broadcast packets transmitted by the beacon 110. The beacon 110 includes an internal clock. For example, the beacon 110 can maintain an internal clock that is incremented at one second intervals. From these parameters (the rotation period, the identity key, and the current time from the clock), the beacon 110 and the owner 140 (or any device possessing these three parameters) can define a pseudorandom number generator, the output of which is predictable to whoever is in possession of these parameters.

[0018] The end-to-end encrypted location-finding protocol uses this pseudorandom number generator mechanism. A random number is generated by using 256-bit Advanced Encryption Standard (AES) Electronic Codebook (ECB) (AES-ECB-256) to encrypt the data structure illustrated in Table 1:

Byte offset	**Field**	**Description**
0 - 10	Padding	Value = 0xFF
11	K	Rotation period exponent
12-15	TS[0]...TS[3]	Beacon time counter, in 32-bit big-endian format. The K lowest bits are cleared.

16 - 26	Padding	Value = 0x00
27	K	Rotation period exponent
28 - 31	TS[0]...TS[3]	Beacon time counter, in 32-bit big-endian format. The K lowest bits are cleared.

Table 1.

[0019] The result of the AES-ECB-256 of the data structure is a 256-bit number denoted as r. For the following calculations, the elliptic curve domain parameters (F_p, n, and G) of SECP160R1 (as defined in SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 20, 2000) are used for elliptic curve cryptographic (ECC) operations herein.

[0020] r' is projected to the finite field, F_p, by calculating:

$$r = r' mod\ n \quad (1)$$

[0021] R, is calculated by:

$$R = r * G \quad (2)$$

which is a point on the curve representing the public key being used. The beacon advertises R_x, which is the x coordinate of R, as its E2EE ephemeral identifier. Note that R_x is 20 bytes long to fit in a standard BLE advertisement channel PDU.

[0022] An E2EE-EID frame is encoded in the advertisement channel PDU as a Service Data block associated with the Eddystone service Universally Unique Identifier (UUID). The E2EE-EID frame layout is illustrated in Table 2:

Byte offset	**Field**	**Description**
0	Frame Type	Value = 0x40
1	E2EE-EID[0]	20-byte Ephemeral Identifier that can be used to derive an encryption key.
2	E2EE-EID[1]	
...	...	
20	E2EE-EID[19]	

Table 2.

End-to-End Encrypted Location-Finding Encryption

[0023] To encrypt a message, *m*, (*e.g.*, the message is the reported location where the sighter 120 received an advertisement packet from the beacon 110) the sighter 120, having received R_x from the beacon 110, generates a random number, *s*, in F_p, as described above.

[0024] The sighter 120 computes a seed, *S*, from the random number and the ECC base point, *G*:

$$S = s * G \tag{3}$$

[0025] The sighter 120 computes the point, *R*, on the curve representing the public key from the received R_x:

$$R = (R_x, R_y) \tag{4}$$

by the substitution in the curve equation and picking an arbitrary R_y value out of the possible results.

[0026] The sighter 120 computes a public key, *k*:

$$k = HKDFSAH256((s * R)_x) \tag{5}$$

where $(s * R)_x$ is the *x* coordinate of the curve multiplication result.

[0027] UR_x and LR_x are the upper (most significant) and lower (least significant) 80-bits of R_x, respectively (in big-endian format). Similarly, US_x and LS_x are the upper and lower 80-bits of S, respectively (in big-endian format).

[0028] The sighter 120 computes a nonce where:

$$nonce = LR_x \,||\, LS_x \tag{6}$$

[0029] The sighter 120 computes (*m'*, *tag*), where:

$$(m', tag) = AESEAX256ENC\ (k, nonce, m) \tag{7}$$

[0030] The sighter 120 sends a message to the owner 140 that includes UR_x, S_x, m', and *tag* in the message. The message may be forwarded via an untrusted node, such as the resolver 130.

End-to-End Encrypted Location-Finding Decryption

[0031] The owner device 140, which is in possession of the identity key and the rotation period exponent, receives the message from the sighter 120 and decrypts the message. The owner 140 having received UR_x, obtains the beacon time counter value on which UR_x is based and computes the anticipated value of r as defined above.

[0032] The owner 140 computes:

$$R = r * G \tag{8}$$

and verifies a match to the value of UR_x provided in the message received from the sighter 120.

[0033] The owner 140 computes the seed, S:

$$S = (S_x, S_y) \tag{9}$$

by substitution in the curve equation and picking an arbitrary S_y value out of the possible results.

[0034] The owner 140 computes the public key, k:

$$k = HKDFSHA256((r * S)_x) \tag{10}$$

where $(r * S)_x$ is the x coordinate of the curve multiplication result.

[0035] The owner 140 computes the nonce:

$$nonce = LR_x \,||\, LS_x \tag{11}$$

[0036] The owner 140 computes the decrypted value of the message, m:

$$m = AESEAX256DEC\ (k, nonce, m', tag) \tag{12}$$

Location-Finding System

[0037] When a user procures a beacon device that supports end-to-end encrypted location-finding (*e.g.*, a standalone beacon device, a device including a beacon, a Bluetooth device that supports beacon transmissions in addition to supporting other Bluetooth profiles, or the like), the user provisions the beacon device to configure end-to-end encrypted location-finding. For example, the user initiates provisioning using an application on a user device (*e.g.*, a smartphone or a computing device) by setting the identity key and rotation period as described above. The

identity key is shared between the beacon device (the beacon 110) and the user device (the owner 140) but kept secret from other devices in the system, such as the sighter 120 and the resolver 130. While the resolver 130 (*e.g.*, a cloud-based resolver service) does not know the identity key, the resolver 130 is made aware of the existence of the beacon 110 and the associated owner 140. For example, the provisioning application provides the associated identities of the beacon 110 and the owner 140 to the resolver 130 that in turn stores those identities in any suitable manner for later use to resolve the identity of the owner 140 for messages received from the sighter 120. The beacon 110 is any device capable of storing the identity key, maintaining clock time, generating an E2EE-EID, and transmitting a beacon packet that includes the E2EE-EID. For example, the beacon 110 may be a fix-mounted beacon, an asset tag affixable to a moveable object, a personal tag carried by a person, wireless earbuds, a smart-watch, a camera, a mobile phone, a mobile computing device, or the like.

[0038] The owner device 140 periodically precalculates (*e.g.*, on a daily basis) the anticipated ephemeral identifiers for that period (*e.g.*, for the next 24 hours), as described above. The owner device 140 then truncates the precalculated ephemeral identifiers. For example, the owner device 140 truncates the precalculated ephemeral identifier to any suitable length, such as keeping the number of least significant bits that is equal to one-half of the length of the public key. In another example, the owner device 140 truncates the precalculated ephemeral identifier to keep the 80 least significant bits of the precalculated ephemeral identifier. The owner device 140 then uploads the truncated, precalculated ephemeral identifiers to the resolver 130. The resolver 130 associates the truncated, precalculated ephemeral identifiers with the previously stored associated identities of the beacon 110 and the owner 140 for later use in resolving ownership of messages received from one or more sighters 120.

[0039] The sighter 120 is any device capable of receiving and decoding a beacon packet to recover the identifier of a beacon 110, generating and encrypting a message (as described above), and communicating the message to the resolver 130. For example, the sighter device 120 includes

a smartphone, a wireless local area network (WLAN) access point, a home automation hub, a security hub, an HVAC hub, an energy management hub, a smart-speaker, a thermostat, a hazard detector (*e.g.*, for smoke and/or carbon monoxide), a network-connected camera, a lighting unit, a lighting controller, an entryway interface device, an occupancy sensor, a home-automation border router, a handheld (*e.g.*, mobile) tag scanner, a fix-mounted tag scanner, or any other types of wireless network devices such as connected appliances and/or controlled systems, such as refrigerators, stoves and ovens, washers, dryers, air conditioners, pool heaters, irrigation systems, security systems, and so forth, as well as other electronic and computing devices, such as televisions, entertainment systems, computers, intercom systems, garage-door openers, ceiling fans, control panels, or the like.

[0040] The resolver 130 uses the partial identifier, UR_x, included as part of the message payload sent by the sighter 120, to determine that the sighting reported in the message is a sighting of a particular beacon 110. The resolver 130 associates the reported sighting with the particular beacon 110 and stores the received message and the association of the message to the particular beacon 110. Although the resolver 130 can resolve the beacon 110 associated with a received message, the resolver 130 is not capable of decrypting the message contents to determine the location of the beacon sighting. The resolver 130 may be any device (*e.g.*, a computer server) or a collection of devices that form a cloud-based service.

[0041] Since the resolver 130 has no knowledge of the identity key, the resolver 130 cannot predict future EIDs, and without periodic updates of the truncated, precalculated ephemeral identifiers from the owner 140, the resolver 130 cannot track the beacon 110. The resolver 130 cannot spoof fake locations as the entire public key is not available to the resolver 130 and the resolver 130 cannot be used for a man-in-the-middle attack as the resolver 130 lacks access to the identity key.

[0042] The owner 140 of the beacon device 110 can then query the resolver 130 for the last known location of the beacon 110. The resolver 130 then forwards the encrypted location to the

owner 140. Alternatively or additionally, the resolver 130 can forward messages as they are received or periodically in batches to the owner 140. Given the timestamp in the message, the owner 140 can deduce the anticipated private key of the beacon 110 at the time and perform the decryption algorithm, as described above.

[0043] FIG. 2 illustrates data and control transactions between devices in accordance with aspects of end-to-end encrypted location-finding. Although not illustrated for the sake of illustration clarity, various acknowledgements for messages illustrated in FIG. 2 may be implemented to ensure reliable operations of end-to-end encrypted location-finding.

[0044] At 205, and as described above, the beacon 110 is paired with the owner 140 during provisioning of the beacon 110. The pairing includes sharing keys for end-to-end encrypted location-finding. At 210, the beacon generates the E2EE-EID based on the current time.

[0045] At 215, the beacon 110 generates a beacon packet. The beacon 110 includes the E2EE-EID and in the beacon packet. Note that based on a predetermined rotation rate for the E2EE-EIDs, the beacon 110 repeats the operations of 210 and 215 for each successive cycle of the rotation (not illustrated in FIG. 2). At 220, beacon 110 transmits the beacon packet. The beacon 110 may transmit the beacon packet one or more times during each cycle of the rotation.

[0046] At 225, after receiving a beacon packet from the beacon 110, the sighter 120 generates a message to send to the owner 140. Optionally, the sighter 120 may include additional data in the message, such as the sighter's location when the beacon packet was received. At 230, the sighter sends the message to the resolver 130.

[0047] At 235, the resolver 130 resolves, based on time, the identity of the beacon 110 from the E2EE-EID and compares the identity to a set of owners 140 and associated E2EE-EIDs for those owners. If the resolver identifies the owner 140 for the received message, the resolver forwards, at 240, the message to the owner 140. At 245, the owner decrypts the received message.

Example Methods

[0048] Example methods 300-500 are described with reference to respective FIGs. 3-5 in accordance with one or more embodiments of end-to-end encrypted location-finding. The order in which the method blocks are described are not intended to be construed as a limitation, and any number of the described method blocks can be skipped or combined in any order to implement a method or an alternate method. Generally, any of the components, modules, methods, and operations described herein can be implemented using software, firmware, hardware (*e.g.*, fixed logic circuitry), manual processing, or any combination thereof. Some operations of the example methods may be described in the general context of executable instructions stored on computer-readable storage memory (media) that is local and/or remote to a computer processing system, and implementations can include software applications, programs, functions, and the like. Alternatively or in addition, any of the functionality described herein can be performed, at least in part, by one or more hardware logic components, such as, and without limitation, Field-programmable Gate Arrays (FPGAs), Application-specific Integrated Circuits (ASICs), Application-specific Standard Products (ASSPs), System-on-a-chip systems (SoCs), Complex Programmable Logic Devices (CPLDs), and the like.

[0049] FIG. 3 illustrates example method(s) 300 of end-to-end encrypted location-finding as generally related to securely communicating a message from a sighter to an owner. At block 302, a sighter (*e.g.*, the sighter 120) receives, from a beacon (*e.g.*, the beacon 110), a packet including an end-to-end encrypted ephemeral identifier (E2EE-EID).

[0050] At block 304, the sighter generates a public key (*e.g.*, the public key, k) using the received E2EE-EID and a seed value. At block 306, the sighter concatenates an 80 least significant bits of the E2EE-EID and an 80 least significant bits of the seed value to generate a nonce.

[0051] At block 308, the sighter encrypts a message for the owner using the generated public key and the nonce. At block 310, the sighter transmits the encrypted message to the owner. For example, the sighter forwards the message via a resolver 130 to the owner 140.

[0052] FIG. 4 illustrates example method(s) 400 of end-to-end encrypted location-finding as generally related to generating an ephemeral identifier by a beacon for securely communicating a message to an owner. At block 402, a beacon (*e.g.*, the beacon 110) determines an identity key that is shared between the beacon and the owner. At block 404, the beacon generates an end-to-end encrypted ephemeral identifier (E2EE-EID) using the identity key and a time value.

[0053] At block 406, the beacon generates a beacon packet including the E2EE-EID. At block 408, the beacon transmits the beacon packet, the beacon packet being usable by a sighter (*e.g.*, the sighter 120) to transmit a secure message to the owner.

[0054] FIG. 5 illustrates example method(s) 500 of end-to-end encrypted location-finding as generally related to securely receiving a message from a sighter by an owner. At block 502, an owner (*e.g.*, the owner 140) retrieves a message from a resolver (*e.g.*, the resolver 130), the message including an end-to-end encrypted ephemeral identifier (E2EE-EID). At block 504, the owner generates a public key using the received E2EE-EID and a seed value.

[0055] At block 506, the owner concatenates an 80 least significant bits of the E2EE-EID and an 80 least significant bits of the seed value to generate a nonce. At block 508, the owner decrypts the received message using the generated public key and the nonce.

Example Devices

[0056] FIG. 6 illustrates an example network device 600 that can be implemented as any of the network devices in a network in accordance with one or more embodiments of end-to-end encrypted location-finding as described herein, such as the beacon 110, the sighter 120, the resolver 130, or the owner 140. The network device 600 can be integrated with electronic circuitry, microprocessors, memory, input output (I/O) logic control, communication interfaces and components, as well as other hardware, firmware, and/or software to implement the device in a network.

[0057] In this example, the network device 600 includes a low-power microprocessor 602 and/or a high-power microprocessor 604 (*e.g.*, microcontrollers or digital signal processors) that process executable instructions. The device also includes an input-output (I/O) logic control 606 (*e.g.*, to include electronic circuitry). The microprocessors can include components of an integrated circuit, programmable logic device, a logic device formed using one or more semiconductors, and other implementations in silicon and/or hardware, such as a processor and memory system implemented as a system-on-chip (SoC). Alternatively or in addition, the device can be implemented with any one or combination of software, hardware, firmware, or fixed logic circuitry that may be implemented with processing and control circuits. The low-power microprocessor 602 and the high-power microprocessor 604 can also support one or more different device functionalities of the device. For example, the high-power microprocessor 604 may execute computationally intensive operations, whereas the low-power microprocessor 602 may manage less-complex processes such as detecting a hazard or temperature from one or more sensors 608. The low-power processor 602 may also wake or initialize the high-power processor 604 for computationally intensive processes.

[0058] The one or more sensors 608 may be included and implemented to detect various properties such as acceleration, temperature, humidity, water, supplied power, proximity, external motion, device motion, sound signals, ultrasound signals, light signals, fire, smoke, carbon monoxide, global-positioning-satellite (GPS) signals, radio-frequency (RF), other electromagnetic signals or fields, or the like. As such, the sensors 608 may include any one or a combination of temperature sensors, humidity sensors, hazard-related sensors, other environmental sensors, accelerometers, microphones, optical sensors up to and including cameras (*e.g.*, charged coupled-device or video cameras), active or passive radiation sensors, GPS receivers, and radio frequency identification detectors. In implementations, the network device 600 may include one or more primary sensors, as well as one or more secondary sensors, such as primary sensors that sense data central to the core operation of the device (*e.g.*, sensing a temperature in a thermostat or sensing

smoke in a smoke detector), while the secondary sensors may sense other types of data (*e.g.*, motion, light or sound), which can be used for energy-efficiency objectives or smart-operation objectives.

[0059] The network device 600 includes a memory device controller 610 and a memory device 612, such as any type of a nonvolatile memory and/or other suitable electronic data storage device. The network device 600 can also include various firmware and/or software, such as an operating system 614 that is maintained as computer executable instructions by the memory and executed by a microprocessor. The device software may also include a messaging application 616 that implements embodiments of end-to-end encrypted location-finding. The network device 600 also includes a device interface 618 to interface with another device or peripheral component and includes an integrated data bus 620 that couples the various components of the wireless network device for data communication between the components. The data bus in the wireless network device may also be implemented as any one or a combination of different bus structures and/or bus architectures.

[0060] The device interface 618 may receive input from a user and/or provide information to the user (*e.g.*, as a user interface), and a received input can be used to determine a setting. The device interface 618 may also include mechanical or virtual components that respond to a user input. For example, the user can mechanically move a sliding or rotatable component, or the motion along a touchpad may be detected, and such motions may correspond to a setting adjustment of the device. Physical and virtual movable user-interface components can allow the user to set a setting along a portion of an apparent continuum. The device interface 618 may also receive inputs from any number of peripherals, such as buttons, a keypad, a switch, a microphone, and an imager (*e.g.*, a camera device).

[0061] The network device 600 can include network interfaces 622, such as a wireless network interface for communication with other wireless network devices in a wireless network, and an external network interface for network communication, such as via the Internet. The

network device 600 also includes wireless radio systems 624 for wireless communication with other wireless network devices via the wireless network interface and for multiple, different wireless communications systems. The wireless radio systems 624 may include Wi-Fi, Bluetooth™, BLE, Mobile Broadband, and/or point-to-point IEEE 802.15.4. Each of the different radio systems can include a radio device, antenna, and chipset that is implemented for a particular wireless communications technology. The network device 600 also includes a power source 626, such as a battery and/or to connect the device to line voltage. An AC power source may also be used to charge the battery of the device.

[0062] FIG. 7 illustrates an example beacon device 700 that can be implemented as the beacon device 110 in a network in accordance with one or more embodiments of end-to-end encrypted location-finding as described herein. The beacon device 700 can be integrated with electronic circuitry, microprocessors, memory, input output (I/O) logic control, communication interfaces and components, as well as other hardware, firmware, and/or software to implement the device in a network.

[0063] In this example, the beacon device 700 includes one or more processors 702 (*e.g.*, microcontrollers or digital signal processors) that process executable instructions. The device also includes an input-output (I/O) logic control 704 (*e.g.*, to include electronic circuitry). The processor(s) can include components of an integrated circuit, programmable logic device, a logic device formed using one or more semiconductors, and other implementations in silicon and/or hardware, such as a processor and memory system implemented as a system-on-chip (SoC). Alternatively or in addition, the device can be implemented with any one or combination of software, hardware, firmware, or fixed logic circuitry that may be implemented with processing and control circuits.

[0064] Optionally or additionally, one or more sensors 706 may be included and implemented to detect various properties such as acceleration, temperature, humidity, water, supplied power, proximity, external motion, device motion, sound signals, ultrasound signals, light

signals, fire, smoke, carbon monoxide, global-positioning-satellite (GPS) signals, radio-frequency (RF), other electromagnetic signals or fields, or the like. As such, the sensors 706 may include any one or a combination of temperature sensors, humidity sensors, hazard-related sensors, other environmental sensors, accelerometers, microphones, optical sensors up to and including cameras (*e.g.*, charged coupled-device or video cameras), active or passive radiation sensors, GPS receivers, and radio frequency identification detectors. In implementations, the beacon device 700 may include one or more primary sensors, as well as one or more secondary sensors, such as primary sensors that sense data central to the core operation of the device (*e.g.*, sensing a temperature in a thermostat or sensing smoke in a smoke detector), while the secondary sensors may sense other types of data (*e.g.*, motion, light or sound), which can be used for energy-efficiency objectives or smart-operation objectives.

[0065] The beacon device 700 includes a memory 708, such as any type of a nonvolatile memory and/or other suitable electronic data storage device. The beacon device 700 can also include various firmware and/or software, such as an operating system 710 that is maintained as computer executable instructions by the memory and executed by a processor. The device software may also include a beaconing application 712 that implements embodiments of an end-to-end encrypted location-finding protocol. Optionally or additionally, the beacon device 700 also includes a device interface 714 to interface with another device or peripheral component. The beacon device 700 includes an integrated data bus 716 that couples the various components of the beacon device for data communication between the components. The data bus in the beacon device may also be implemented as any one or a combination of different bus structures and/or bus architectures.

[0066] The device interface 714 may receive input from a user and/or provide information to the user (*e.g.*, as a user interface), and a received input can be used to determine a setting. The device interface 714 may also include mechanical or virtual components that respond to a user input. For example, the user can mechanically move a sliding or rotatable component, or the

motion along a touchpad may be detected, and such motions may correspond to a setting adjustment of the device. Physical and virtual movable user-interface components can allow the user to set a setting along a portion of an apparent continuum. The device interface 714 may also receive inputs from any number of peripherals, such as buttons, a keypad, a switch, a microphone, and an imager (*e.g.*, a camera device).

[0067] The beacon device 700 can include a wireless radio system 718 for wireless communication. The wireless radio system 718 may include Wi-Fi, Bluetooth™, BLE, Mobile Broadband, and/or point-to-point IEEE 802.15.4. The wireless radio system 718 can include a radio device, antenna, and chipset that is implemented for a particular wireless communications technology. The beacon device 700 also includes a power source 720, such as a battery and/or to connect the device to line voltage. An AC power source may also be used to charge the battery of the device.

[0068] In the following text some examples are described:

Example 1: A method of securely communicating a message from a sighter to an owner, the method comprising the sighter:

receiving, from a beacon, a packet including an end-to-end encrypted ephemeral identifier (E2EE-EID);

generating a public key using the received E2EE-EID and a seed value;

concatenating an 80 least significant bits of the E2EE-EID and an 80 least significant bits of the seed value to generate a nonce;

encrypting a message for the owner using the generated public key and the nonce; and

transmitting the encrypted message to the owner.

Example 2: The method of example 1, further comprising the sighter:

generating the message for the owner.

Example 3: The method of example 2, further comprising the sighter:

including a location of the sighter in the message, the location being the location of the sighter when the sighter received the packet from the beacon.

Example 4: The method of any one of the preceding examples, wherein the encrypting the message for the owner comprises the sighter:

encrypting the message using AES-EAX-256 encryption.

Example 5: The method of any one of the preceding examples, wherein the generating a public key using the received E2EE-EID and a seed value comprises the sighter:

computing a point, *R*, on a curve representing the public key.

Example 6: The method of any one of the preceding examples, wherein the packet is a Bluetooth advertisement packet, and wherein the Bluetooth advertisement packet is received on a Bluetooth advertising channel.

Example 7: A method of generating an ephemeral identifier by a beacon for securely communicating a message to an owner, the method comprising the beacon:

determining an identity key that is shared between the beacon and the owner;

generating an end-to-end encrypted ephemeral identifier (E2EE-EID) using the identity key and a time value;

generating a beacon packet including the E2EE-EID; and

transmitting the beacon packet, the beacon packet being usable by a sighter to transmit a secure message to the owner.

Example 8: An electronic device comprising:

a wireless transceiver;

a processor; and

instructions that are executable by the processor to configure the electronic device to perform any one of the methods of examples 1 to 7.

Example 9: The electronic device of example 8, wherein the electronic device is a beacon, and wherein the beacon is one of: a fix-mounted beacon, an asset tag affixable to a moveable object, a personal tag carried by a person, wireless earbuds, a smart-watch, a camera, a mobile phone, or a mobile computing device.

Example 10: The electronic device of example 8, wherein the electronic device is a sighter, and wherein the sighter is one of: a smartphone, a wireless local area network (WLAN) access point, a home automation hub, a security hub, an HVAC hub, an energy management hub, a smart-speaker, a thermostat, a hazard detector, a network-connected camera, a lighting unit, a lighting controller, an entryway interface device, an occupancy sensor, a home-automation border router, a handheld tag scanner, or a fix-mounted tag scanner.

Example 11: A method of securely receiving a message from a sighter by an owner, the method comprising the owner:

retrieving the message from a resolver, the message including an end-to-end encrypted ephemeral identifier (E2EE-EID);

generating a public key using the received E2EE-EID and a seed value;

concatenating an 80 least significant bits of the E2EE-EID and an 80 least significant bits of the seed value to generate a nonce; and

decrypting the received message using the generated public key and the nonce.

Example 12: The method of example 11, wherein the message includes a location of the sighter, the location being the location of the sighter when the sighter received a packet from a beacon that generated the E2EE-EID.

Example 13: The method of example 11 or example 12, wherein the decrypting the received message comprises the owner:

decrypting the message using AES-EAX-256 decryption.

Example 14: An electronic device comprising:

a processor; and

instructions that are executable by the processor to configure the electronic device to perform any one of the methods of examples 11 to 13.

Example 15: A computer-readable storage media comprising instructions that, responsive to execution by a processor, cause a method as recited in any one of claims 1 to 7 and claims 11 to 13 to be performed.

[0069] Although embodiments of end-to-end encrypted location-finding have been described in language specific to features and/or methods, the subject of the appended claims is not necessarily limited to the specific features or methods described. Rather, the specific features and methods are disclosed as example implementations of end-to-end encrypted location-finding, and other equivalent features and methods are intended to be within the scope of the appended claims. Further, various different embodiments are described, and it is to be appreciated that each described embodiment can be implemented independently or in connection with one or more other described embodiments.

CLAIMS

1. A method of securely communicating a message from a sighter to an owner, the method comprising the sighter:

receiving, from a beacon, a packet including an end-to-end encrypted ephemeral identifier (E2EE-EID);

generating a public key using the received E2EE-EID and a seed value;

concatenating an 80 least significant bits of the E2EE-EID and an 80 least significant bits of the seed value to generate a nonce;

encrypting a message for the owner using the generated public key and the nonce; and

transmitting the encrypted message to the owner.

2. The method of claim 1, further comprising the sighter:

generating the message for the owner.

3. The method of claim 2, further comprising the sighter:

including a location of the sighter in the message, the location being the location of the sighter when the sighter received the packet from the beacon.

4. The method of any one of the preceding claims, wherein the encrypting the message for the owner comprises the sighter:

encrypting the message using AES-EAX-256 encryption.

5. The method of any one of the preceding claims, wherein the generating a public key using the received E2EE-EID and a seed value comprises the sighter:

computing a point, R, on a curve representing the public key.

6. The method of any one of the preceding claims, wherein the packet is a Bluetooth advertisement packet, and wherein the Bluetooth advertisement packet is received on a Bluetooth advertising channel.

7. A method of generating an ephemeral identifier by a beacon for securely communicating a message to an owner, the method comprising the beacon:

determining an identity key that is shared between the beacon and the owner;

generating an end-to-end encrypted ephemeral identifier (E2EE-EID) using the identity key and a time value;

generating a beacon packet including the E2EE-EID; and

transmitting the beacon packet, the beacon packet being usable by a sighter to transmit a secure message to the owner.

8. An electronic device comprising:

a wireless transceiver;

a processor; and

instructions that are executable by the processor to configure the electronic device to perform any one of methods 1 to 7.

9. The electronic device of claim 8, wherein the electronic device is a beacon, and wherein the beacon is one of: a fix-mounted beacon, an asset tag affixable to a moveable object, a personal tag carried by a person, wireless earbuds, a smart-watch, a camera, a mobile phone, or a mobile computing device.

10. The electronic device of claim 8, wherein the electronic device is a sighter, and wherein the sighter is one of: a smartphone, a wireless local area network (WLAN) access point, a home automation hub, a security hub, an HVAC hub, an energy management hub, a smart-speaker, a thermostat, a hazard detector, a network-connected camera, a lighting unit, a lighting controller, an entryway interface device, an occupancy sensor, a home-automation border router, a handheld tag scanner, or a fix-mounted tag scanner.

11. A method of securely receiving a message from a sighter by an owner, the method comprising the owner:

retrieving the message from a resolver, the message including an end-to-end encrypted ephemeral identifier (E2EE-EID);

generating a public key using the received E2EE-EID and a seed value;

concatenating an 80 least significant bits of the E2EE-EID and an 80 least significant bits of the seed value to generate a nonce; and

decrypting the received message using the generated public key and the nonce.

12. The method of claim 11, wherein the message includes a location of the sighter, the location being the location of the sighter when the sighter received a packet from a beacon that generated the E2EE-EID.

13. The method of claim 11 or claim 12, wherein the decrypting the received message comprises the owner:

decrypting the message using AES-EAX-256 decryption.

14. An electronic device comprising:

a processor; and

instructions that are executable by the processor to configure the electronic device to perform any one of methods 11 to 13.

15. A computer-readable storage media comprising instructions that, responsive to execution by a processor, cause a method as recited in any one of claims 1 to 7 and claims 11 to 13 to be performed.

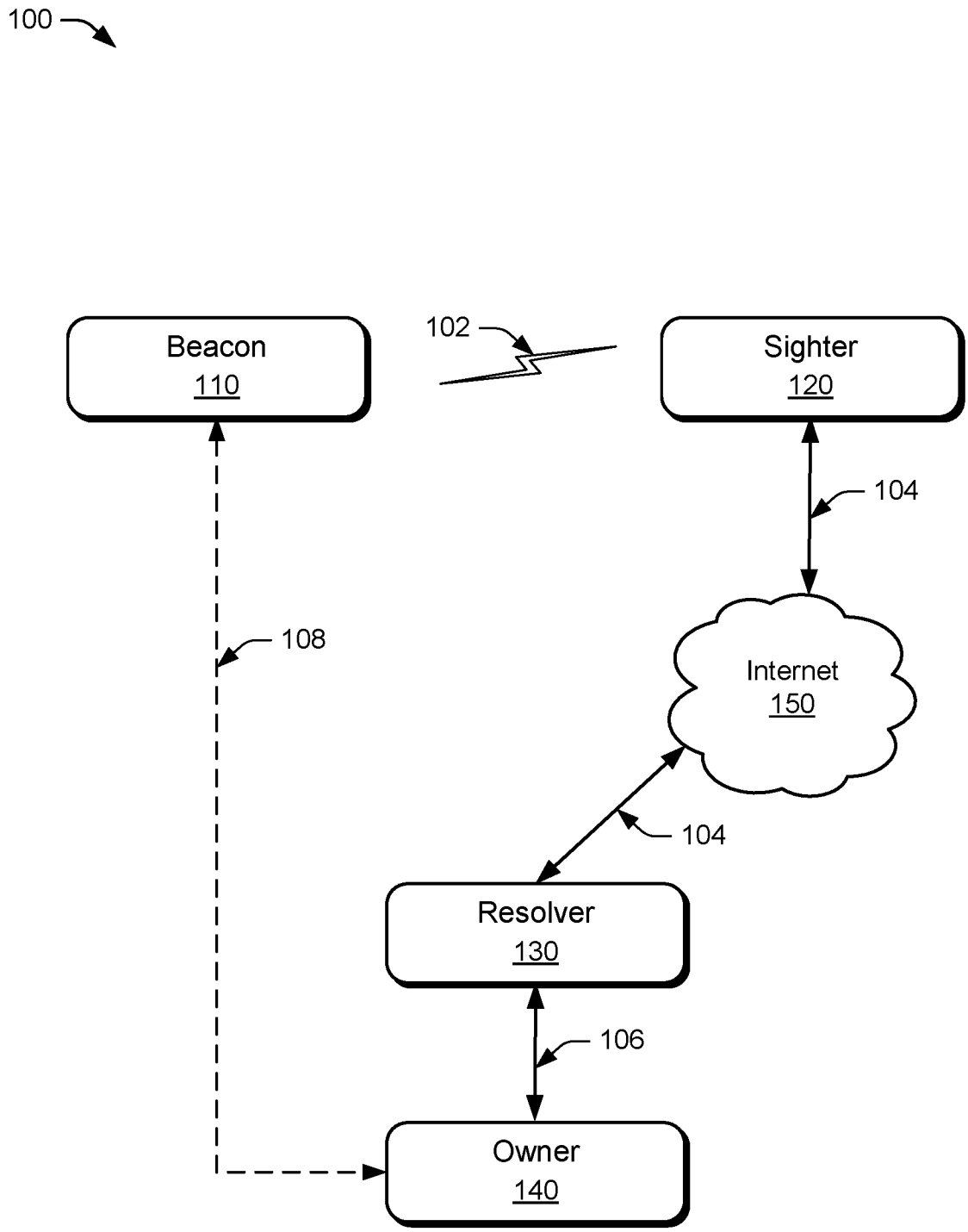

100
Beacon
110
102
Sighter
120
104
108
Internet
150
104
Resolver
130
106
Owner
140

Fig. 1

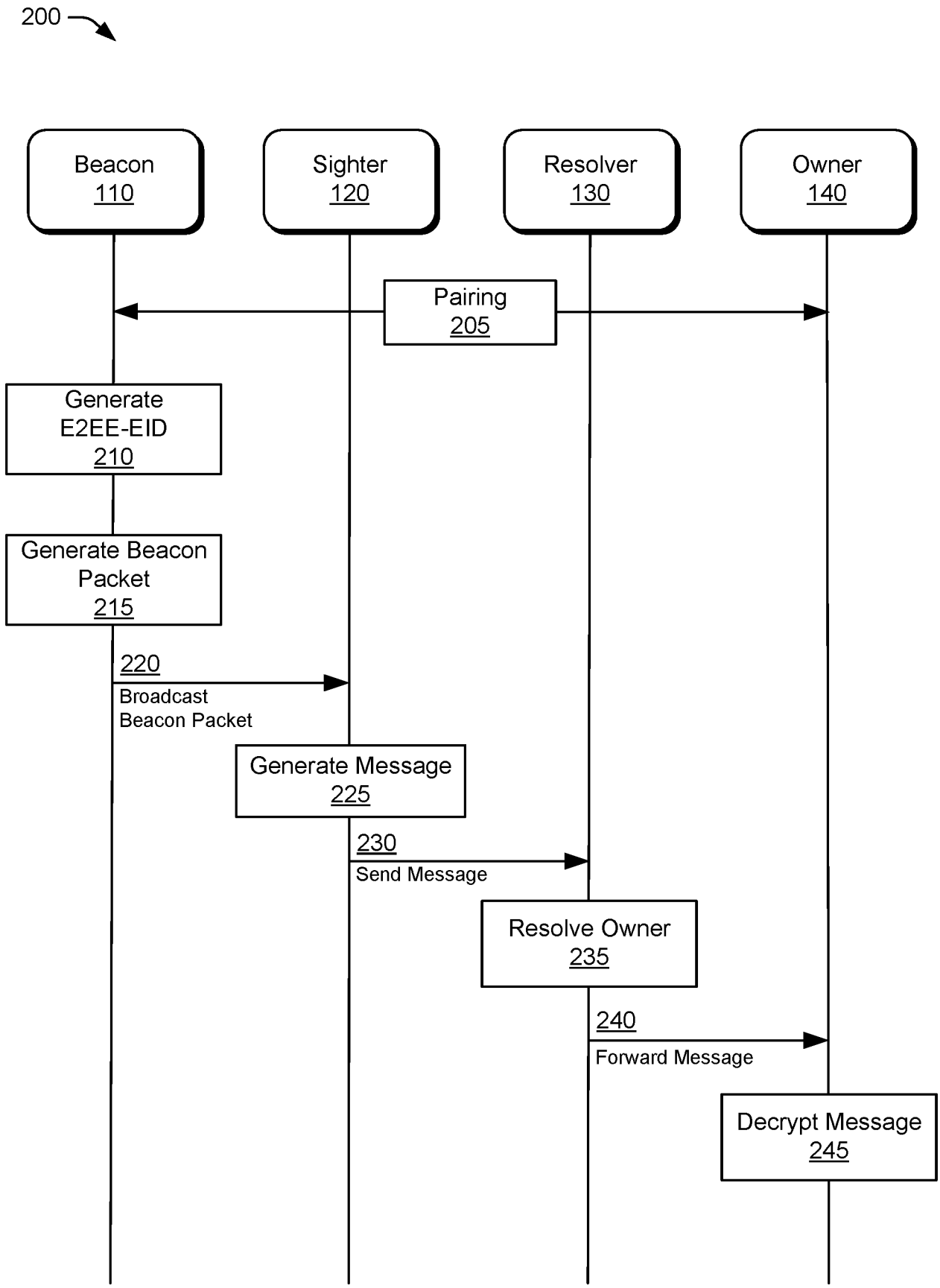

200
Beacon
110
Sighter
120
Resolver
130
Owner
140
Pairing
205
Generate
E2EE-EID
210
Generate Beacon
Packet
215
220
Broadcast
Beacon Packet
Generate Message
225
230
Send Message
Resolve Owner
235
240
Forward Message
Decrypt Message
245

Fig. 2

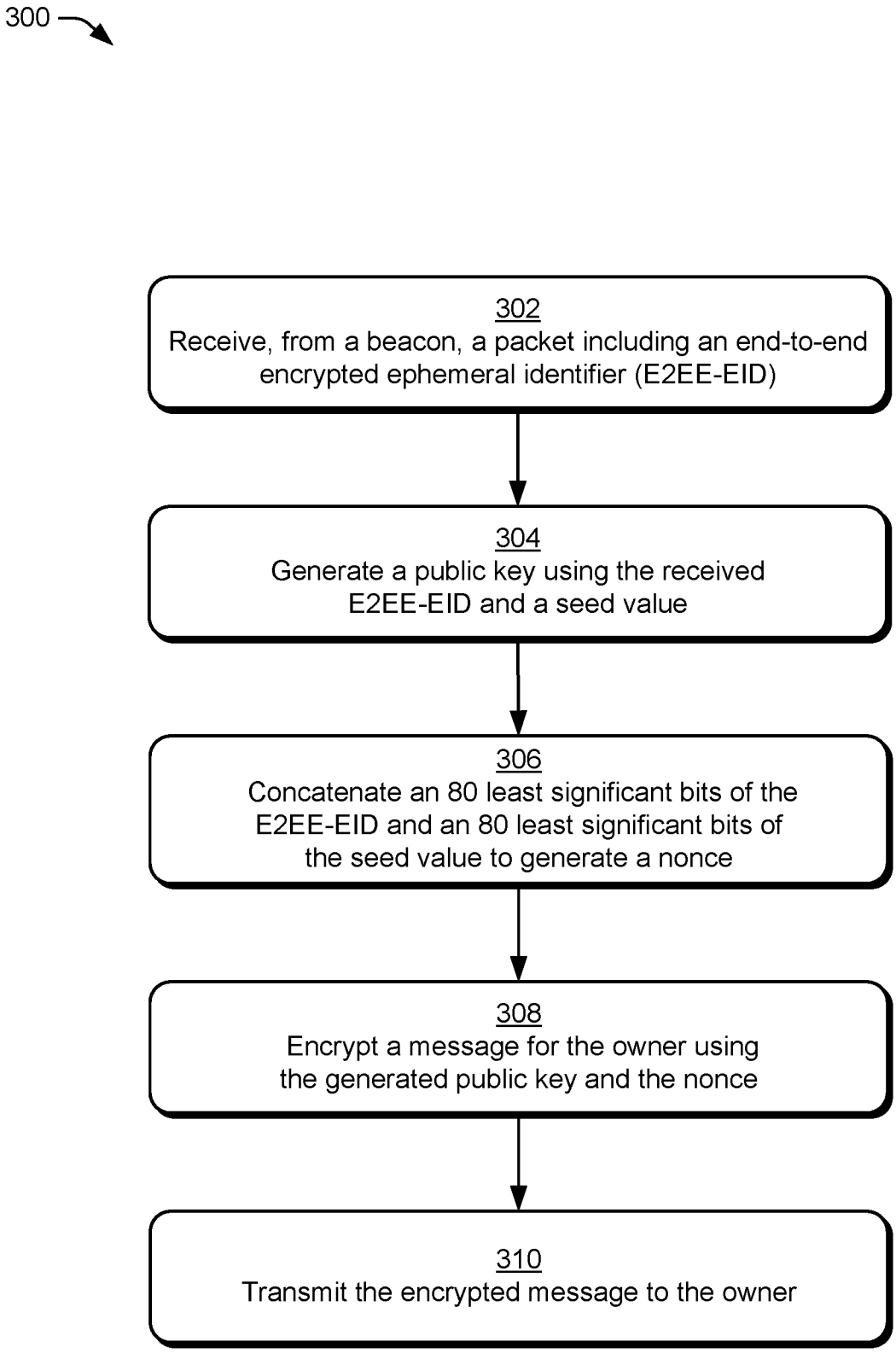

300
302
Receive, from a beacon, a packet including an end-to-end encrypted ephemeral identifier (E2EE-EID)
304
Generate a public key using the received E2EE-EID and a seed value
306
Concatenate an 80 least significant bits of the E2EE-EID and an 80 least significant bits of the seed value to generate a nonce
308
Encrypt a message for the owner using the generated public key and the nonce
310
Transmit the encrypted message to the owner

Fig. 3

400

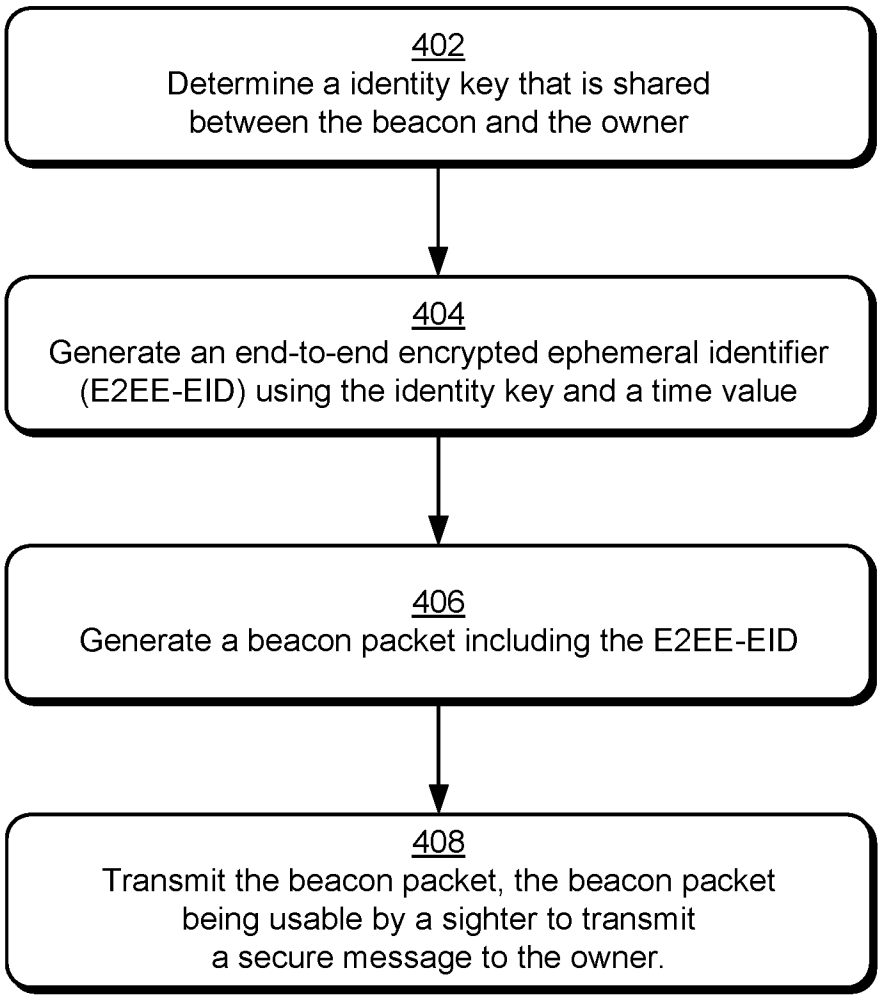

402
Determine a identity key that is shared between the beacon and the owner
404
Generate an end-to-end encrypted ephemeral identifier (E2EE-EID) using the identity key and a time value
406
Generate a beacon packet including the E2EE-EID
408
Transmit the beacon packet, the beacon packet being usable by a sighter to transmit a secure message to the owner.

Fig. 4

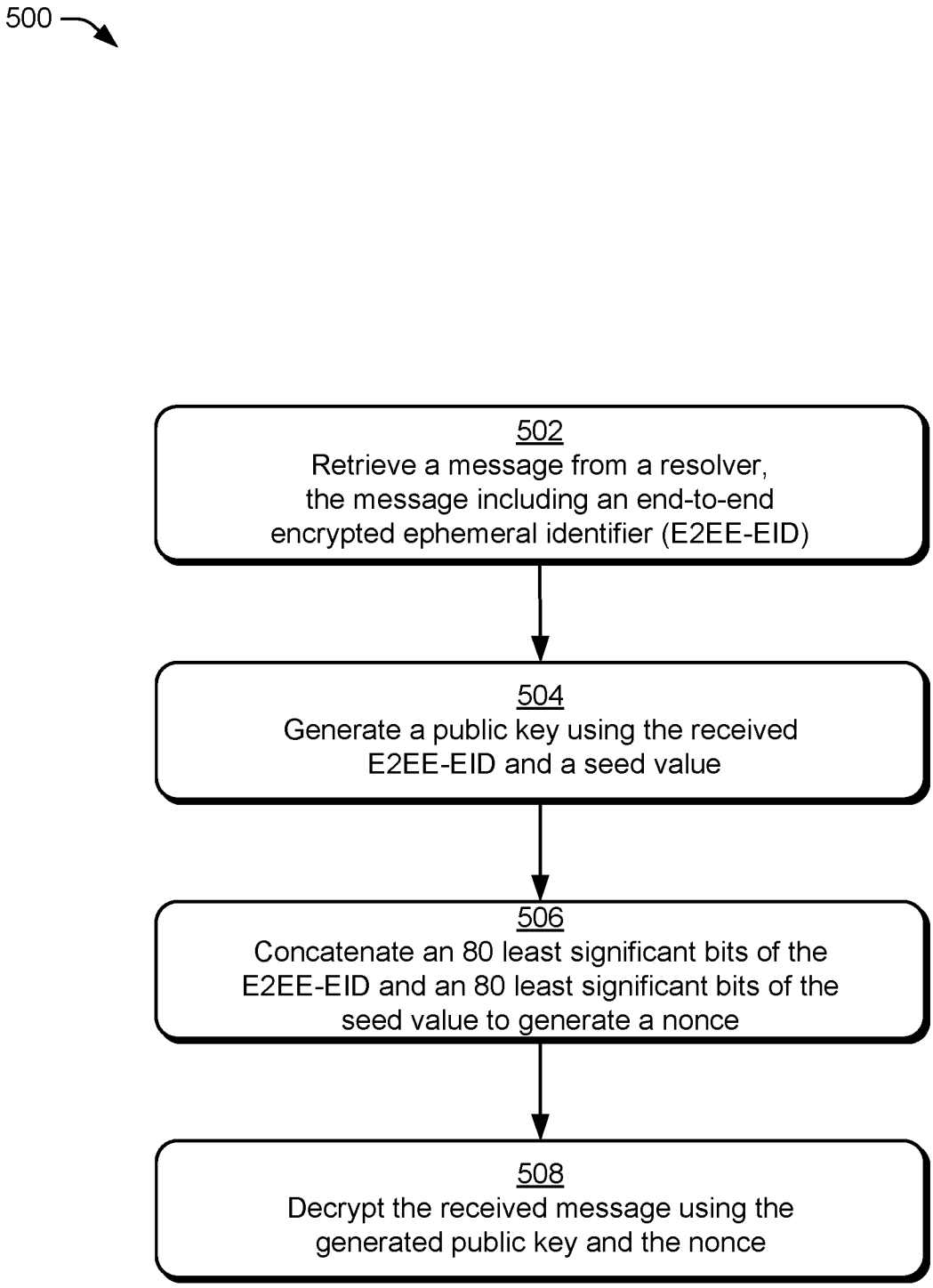

500
502
Retrieve a message from a resolver, the message including an end-to-end encrypted ephemeral identifier (E2EE-EID)
504
Generate a public key using the received E2EE-EID and a seed value
506
Concatenate an 80 least significant bits of the E2EE-EID and an 80 least significant bits of the seed value to generate a nonce
508
Decrypt the received message using the generated public key and the nonce

Fig. 5

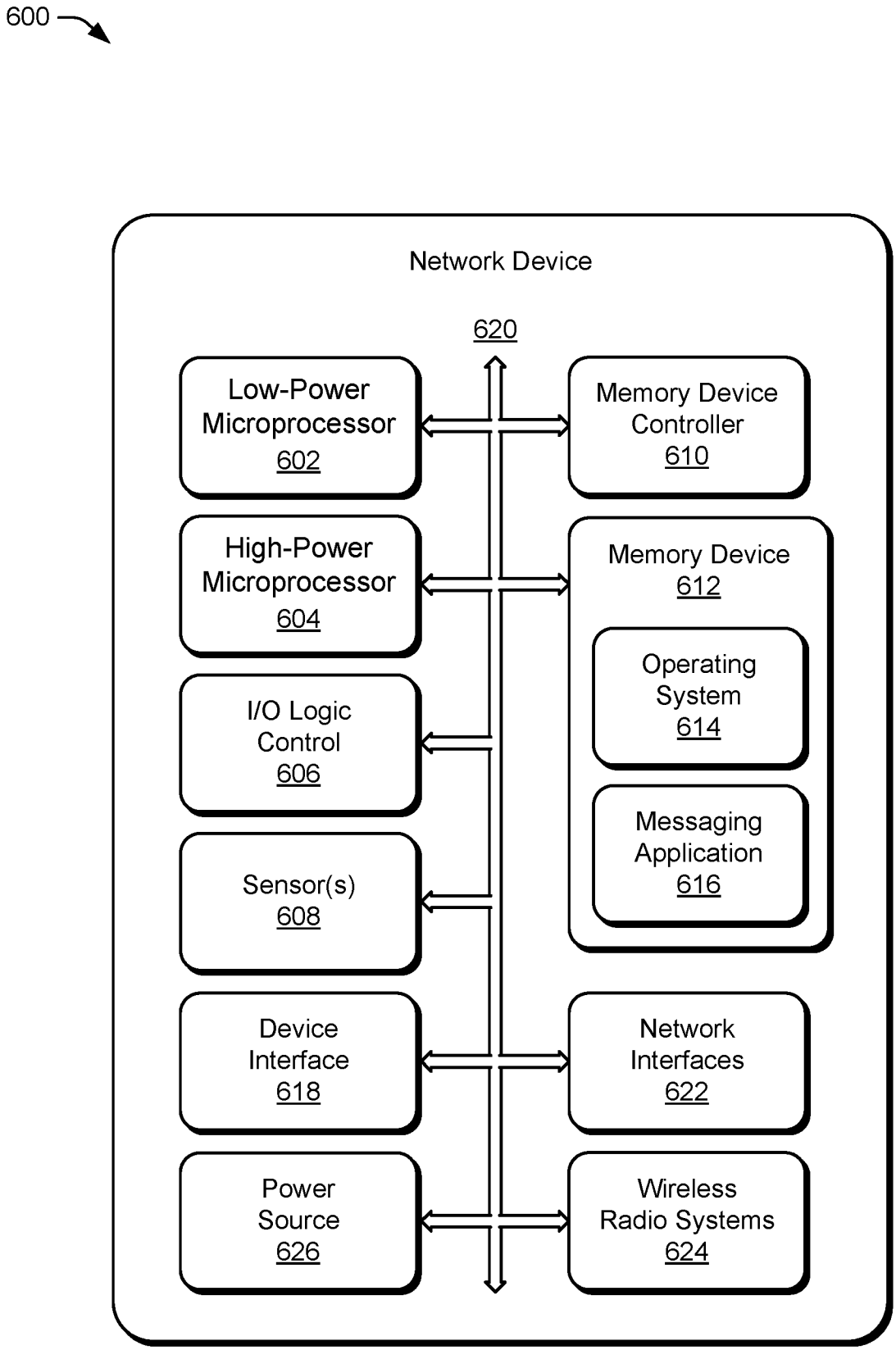
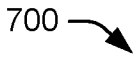

600
Network Device
620
Low-Power Microprocessor 602
High-Power Microprocessor 604
I/O Logic Control 606
Sensor(s) 608
Device Interface 618
Power Source 626
Memory Device Controller 610
Memory Device 612
Operating System 614
Messaging Application 616
Network Interfaces 622
Wireless Radio Systems 624

Fig. 6


700

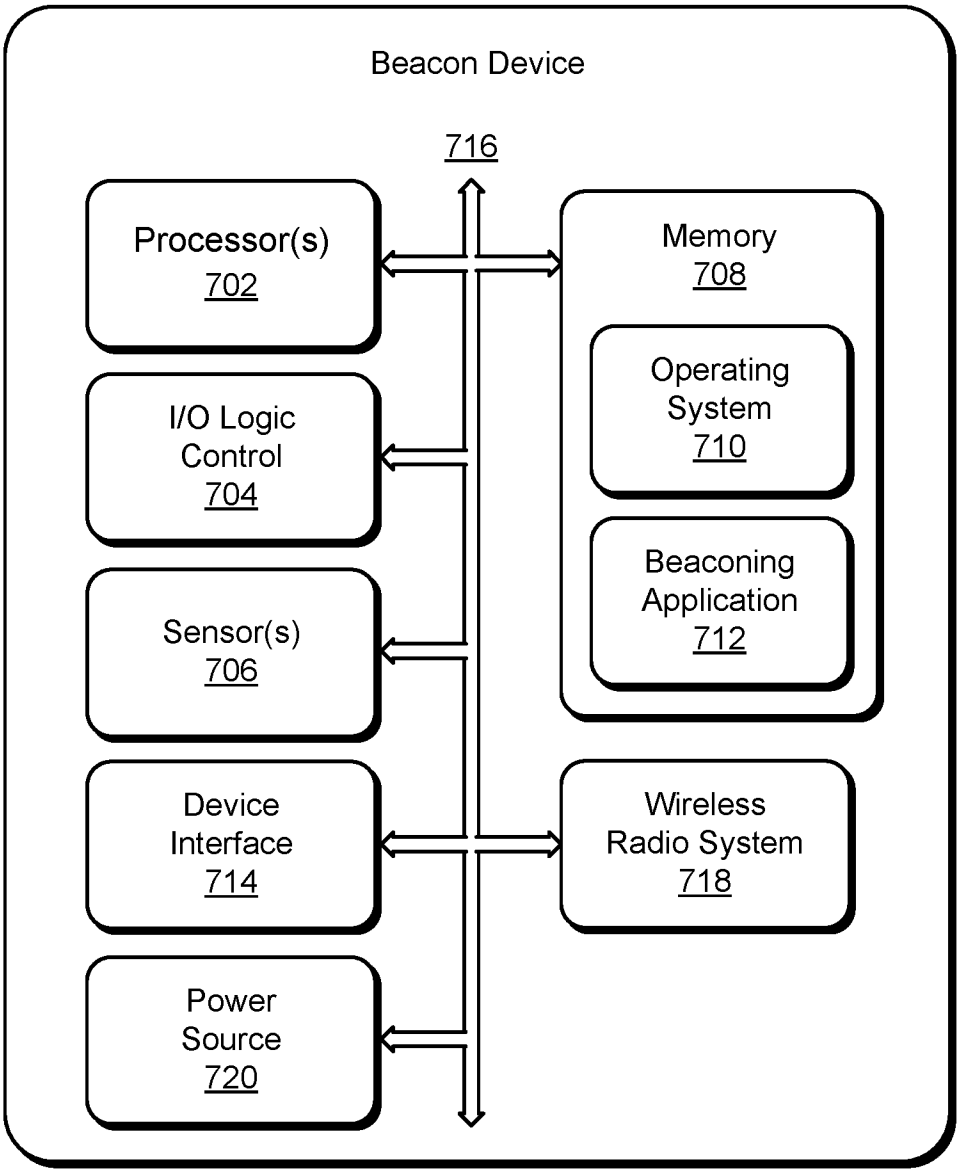

Beacon Device
716
Processor(s)
702
I/O Logic
Control
704
Sensor(s)
706
Device
Interface
714
Power
Source
720
Memory
708
Operating
System
710
Beaconing
Application
712
Wireless
Radio System
718

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2021/025743

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04W12/02 H04W12/03
ADD.

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

B. FIELDS SEARCHED

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

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

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

EPO-Internal, WPI Data, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DAN HARKINS (HPE): "privacy-for-password-identifiers", IEEE DRAFT; 11-20-0543-01-000M-PRIVACY-FOR-PASSWORD-ID ENTIFIERS, IEEE-SA MENTOR, PISCATAWAY, NJ USA , vol. 802.11m, no. 1 1 April 2020 (2020-04-01), pages 1-7, XP068167305, Retrieved from the Internet: URL:https://mentor.ieee.org/802.11/dcn/20/ 11-20-0543-01-000m-privacy-for-password-id entifiers.docx [retrieved on 2020-04-01] paragraph [12.4.3] ----- -/--	1-15

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 July 2021	14/07/2021

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

3

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

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2017/013450 A1 (ZIV ALON [IL] ET AL) 12 January 2017 (2017-01-12) figures 1-8 paragraph [0024] - paragraph [0079] -----	1-15
T	JOPPE W BOS ET AL: "On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography", IACR, INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH, vol. 20090901:153928, 1 September 2009 (2009-09-01), pages 1-19, XP061003560, [retrieved on 2009-09-01] paragraph [0003] -----	

3

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2021/025743

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2017013450 A1	12-01-2017	US 2017013450 A1	12-01-2017
		US 2018007555 A1	04-01-2018