HU000035780T2

(19) **HU**

(11) Lajstromszám: **E 035 780**

(13) **T2**

MAGYARORSZÁG
Szellemi Tulajdon Nemzeti Hivatala

EURÓPAI SZABADALOM
SZÖVEGÉNEK FORDÍTÁSA

(21) Magyar ügyszám: **E 14 183535**
(22) A bejelentés napja: **2012. 09. 12.**

(96) Az európai bejelentés bejelentési száma:
EP 20120183535
(97) Az európai bejelentés közzétételi adatai:
EP 2827630 A1 **2015. 01. 21.**
(97) Az európai szabadalom megadásának meghirdetési adatai:
EP 2827630 B1 **2017. 07. 05.**

(51) Int. Cl.:

H04W 12/06	*(2006.01)*
H04L 9/32	*(2006.01)*
H04L 29/06	*(2006.01)*
H04W 84/02	*(2006.01)*
H04W 36/14	*(2006.01)*
H04L 9/08	*(2006.01)*
H04W 12/04	*(2006.01)*

(30) Elsőbbségi adatok:

201161533627 P	**2011. 09. 12.**	**US**
201161535234 P	**2011. 09. 15.**	**US**
201261583052 P	**2012. 01. 04.**	**US**
201261606794 P	**2012. 03. 05.**	**US**
201261611553 P	**2012. 03. 15.**	**US**
201261645987 P	**2012. 05. 11.**	**US**
201213610730	**2012. 09. 11.**	**US**

(72) Feltaláló(k):
Cherian, George, San Diego, 92121-1714 (US)
Hawkes, Philip Michael, San Diego, CA 92121-1714 (US)
Abraham, Santosh Paul, San Diego, CA 92121-1714 (US)
Sampath, Hemanth, San Diego, CA 92121 (US)

(73) Jogosult(ak):
Qualcomm Incorporated, San Diego, CA 92121-1714 (US)

(74) Képviselő:
Danubia Szabadalmi és Jogi Iroda Kft., Budapest

(54) **Rendszerek és eljárások link felépítés és autentikáció végrehajtására**

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 827 630 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
05.07.2017 Bulletin 2017/27

(21) Application number: **14183535.5**

(22) Date of filing: **12.09.2012**

(51) Int Cl.:
H04W 12/06 *(2009.01)* ***H04W 12/04*** *(2009.01)*
H04L 9/08 *(2006.01)* ***H04W 36/14*** *(2009.01)*
H04L 9/32 *(2006.01)* ***H04L 29/06*** *(2006.01)*
H04W 84/02 *(2009.01)*

(54) **SYSTEMS AND METHODS OF PERFORMING LINK SETUP AND AUTHENTICATION**

SYSTEME UND VERFAHREN ZUR DURCHFÜHRUNG VON VERKNÜPFUNGSEINRICHTUNG UND -AUTHENTIFIZIERUNG

SYSTÈMES ET PROCÉDÉS PERMETTANT D'EFFECTUER UNE AUTHENTIFICATION ET UN ÉTABLISSEMENT DE LIAISON

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **12.09.2011 US 201161533627 P**
15.09.2011 US 201161535234 P
04.01.2012 US 201261583052 P
05.03.2012 US 201261606794 P
15.03.2012 US 201261611553 P
11.05.2012 US 201261645987 P
11.09.2012 US 201213610730

(43) Date of publication of application:
21.01.2015 Bulletin 2015/04

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
12780324.5 / 2 756 700

(73) Proprietor: **Qualcomm Incorporated**
San Diego, CA 92121-1714 (US)

(72) Inventors:
- **Cherian, George**
  San Diego, 92121-1714 (US)
- **Hawkes, Philip Michael**
  San Diego, CA 92121-1714 (US)
- **Abraham, Santosh Paul**
  San Diego, CA 92121-1714 (US)
- **Sampath, Hemanth**
  San Diego, CA 92121 (US)

(74) Representative: **Wegner, Hans**
Bardehle Pagenberg Partnerschaft mbB
Patentanwälte, Rechtsanwälte
Prinzregentenplatz 7
81675 München (DE)

(56) References cited:
US-A1- 2011 154 039

- **HITOSHI MORIOKA (ROOT): "TGai Authentication Protocol Proposal ; 11-11-0976-02-00ai-tgai-authentication-protocol-proposal", IEEE DRAFT; 11-11-0976-02-00AI-TGAI-AUTHENTICATION-PROTOCOL-PROPOSAL, IEEE-SA MENTOR, PISCATAWAY, NJ USA, vol. 802.11ai, no. 2, 21 July 2011 (2011-07-21), pages 1-24, XP017674098,**
- **GEORGE CHERIAN (QUALCOMM INC): "Fast Re-authentication ; 11-11-1160-00-00ai-fast-re-authentication" ,IEEE DRAFT; 11-11-1160-00-00AI-FAST-RE-AUTHENTICATION, IEEE-SA MENTOR, PISCATAWAY, NJ USA, vol. 802.11ai, 5 September 2011 (2011-09-05), pages 1-8, XP017673791,**

EP 2 827 630 B1

Description

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority from commonly owned U.S. Provisional Patent Application No. 61/533,627 (Qualcomm docket number 113346P1) filed September 12, 2011, U.S. Provisional Patent Application No. 61/535,234 (Qualcomm docket number 113346P2) filed September 15, 2011, U.S. Provisional Patent Application No. 61/583,052 (Qualcomm docket number 113346P3) filed January 4, 2012, U.S. Provisional Patent Application No. 61/606,794 (Qualcomm docket number 121585P1) filed March 5, 2012, and U.S. Provisional Patent Application No. 61/645,987 (Qualcomm docket number 121585P2) filed May 11, 2012, and U.S. Provisional Patent Application No. 61/611,553 (Qualcomm docket number 121602P1) filed March 15, 2012. Moreover, the contents of the non-provisional application with the Qualcomm docket number 113346 titled: WIRELESS COMMUNICATION USING CONCURRENT REAUTHENTICATION AND CONNECTION SETUP, filed on September 11, 2012, and the non-provisional application with Qualcomm docket number 121602, titled: SYSTEMS AND METHODS FOR ENCODING EXCHANGES WITH A SET OF SHARED EPHEMERAL KEY DATA, filed on September 11, 2012, are relevant.

BACKGROUND

Field

[0002] The following relates generally to wireless communication and more specifically to link setup and authentication processes in wireless communication.

Description of Related Art

[0003] Advances in technology have resulted in smaller and more powerful computing devices. For example, there currently exist a variety of portable personal computing devices, including wireless computing devices, such as portable wireless telephones, personal digital assistants (PDAs), and paging devices that are small, lightweight, and easily carried by users. More specifically, portable wireless telephones, such as cellular telephones and internet protocol (IP) telephones, can communicate voice and data packets over wireless networks. Further, many such wireless telephones include other types of devices that are incorporated therein. For example, a wireless telephone can also include a digital still camera, a digital video camera, a digital recorder, and an audio file player. Also, such wireless telephones can process executable instructions, including software applications, such as a web browser application, that can be used to access the Internet. As such, these wireless telephones can include significant computing capabilities.

[0004] Wireless communication networks enable communication devices to transmit and/or receive information while on the move. These wireless communication networks may be communicatively coupled to other public or private networks to enable the transfer of information to and from the mobile access terminal. Such communication networks typically include a plurality of access points (AP) which provide wireless communication links to access terminals (e.g., mobile communication devices, mobile phones, wireless user terminals). The access points may be stationary (e.g., fixed to the ground) or mobile (e.g., mounted on vehicles, satellites, etc.) and positioned to provide wide area of coverage as the access terminal moves within the coverage area.

[0005] Portable devices may be configured to communicate data via these wireless networks. For example, many devices are configured to operate according to an Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification that enables wireless exchange of data via an access point. In some communication systems, when a mobile access terminal attaches to a communication network through an access point, it performs network access authentication. Each time a mobile access terminal connects to a different access point, the authentication process may need to be repeated. However, repeating this authentication process can introduce significant setup delays.

[0006] Many communication devices are configured to perform a link setup both at an initial connection stage and one or more reconnection stages. Current systems assume pre-shared key to AP-IP address assignment after authentication to protect IP address assignments.

[0007] While utilization of multiple messages communicated among two or more message processing points in the system allows link setup, reducing the number of messages communicated while maintaining a required authentication level of the communication is highly desired.

[0008] Furthermore, a mobile communication device may scan for a nearby access point before link setup can be performed. This scanning may be "passive" or "active." In "passive" scanning, the device may listen for access point activity (e.g., a control message). In "active" scanning, the device may broadcast a query and then wait for responses from nearby access points. Thus, "passive" scanning may be time consuming and "active" scanning may consume both time as well as power at the mobile communication device.

[0009] XP017674098 discloses a fast re-authentication, wherein an association request is sent at least partly unprotected. ANonce is included in the association response.

[0010] The present invention is defined by the subject matter of the independent claims. Preferred embodiments are defined by the dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Various features, nature and advantages may become apparent from the detailed description set forth below when taken in conjunction with the drawings in which like reference characters identify correspondingly similar elements throughout.

FIG. 1 is a conceptual diagram illustrating an example of a wireless network.
FIG. 2 is a block diagram illustrating an exemplary user device.
FIG. 3 is a flow diagram illustrating messaging that may be performed in a conventional connection setup.
FIG. 4 is a flow diagram illustrating messaging that may be performed according to one or more aspects of the present disclosure.
FIG. 5 is a flow diagram illustrating messaging that may be performed in performing link setup and authentication.
FIG. 6 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication.
FIG. 7 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication.
FIG. 8 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication.
FIG. 9 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication.
FIG. 10 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication.
FIG. 11 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication.
FIG. 12 is a flow diagram illustrating messaging that may be performed during a re-authentication protocol.
FIG. 13 illustrates a key hierarchy that may be used for a re-authentication protocol.
FIG. 14 is a flow diagram showing an exemplary process to generate and bundle a re-authentication request and a discover request into an association request.
FIG. 15 is a flow diagram showing an exemplary process operational at a base station to receive and extract a re-authentication request and an upper layer message from an association request sent by a station/terminal.
FIG. 16 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication.
FIG. 17 is a flow diagram showing an exemplary process operable at the station of FIG. 16 to perform link setup and authentication.
FIG. 18 is a flow diagram showing an exemplary process operable at the access point of FIG. 16 to perform link setup and authentication.
FIG. 19 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication.
FIG. 20 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication.
FIG. 21 is a flow diagram showing an exemplary process operable at the station of FIGS. 19-20 to perform link setup and authentication.
FIG. 22 is a flow diagram showing an exemplary process operable at the access point of FIGS. 19-20 to perform link setup and authentication.
FIG. 23 is a diagram illustrating messaging that may be performed according to other aspects of link setup and authentication.
FIG. 24 is a flow diagram showing an exemplary process operable at a station to perform link setup and authentication as shown in FIG. 23.
FIG. 25 is a flow diagram showing an exemplary process operable at an access point to perform link setup and authentication as shown in FIG. 23.
FIG. 26 is a diagram illustrating messaging that may be performed according to other aspects of link setup and authentication.
FIG. 27 is a flow diagram showing an exemplary process operable at a station to perform link setup and authentication as shown in FIG. 26.
FIG. 28 is a flow diagram showing an exemplary process operable at an access point to perform link setup and authentication as shown in FIG. 26.

DETAILED DESCRIPTION

[0012] In the following description, reference is made to the accompanying drawings in which is shown, by way of illustration, specific embodiments in which the disclosure may be practiced. The embodiments are intended to describe aspects of the disclosure in sufficient detail to enable those skilled in the art to practice the invention. In the following, the parts of the description and drawings referring to embodiments which are not covered by the claims are not to be understood as embodiments of the invention but as background art or examples useful for understanding the invention. The scope of the present invention is defined only by the appended claims.

[0013] Features and aspects described herein provide devices and methods for a fast setup time during a re-authentication process of a connection setup. For example, the described techniques may enable a mobile device (e.g., station (STA)) to perform link setup with respect to an access point (AP) without first listening for a beacon or soliciting a probe response from the access point. The beacon or probe response may typically include an access point nonce (ANonce) to be used during

link setup. Thus, the described techniques may enable the STA to perform link setup without having previously received the ANonce. In accordance with a "modified 4-way handshake" technique the STA may send an unprotected association request to the AP and may receive the ANonce from the AP in an association response. The received ANonce may then be used for key derivation. In accordance with a "next ANonce" technique the STA may receive, during a first link setup initiated using a first ANonce, a second ANonce for use in a second link setup subsequent to the first link setup.

[0014] The described techniques may also enable the use of a temporary key for upper layer signaling protection. For example, instead of sending an unprotected association request, a STA may receive a first ANonce (e.g., ANonce1) via a beacon or a probe response from an AP and may derive a first key (e.g., a first pairwise transient key (PTK)) based on the first ANonce. The first key may be used to protect the association request sent by the STA to the AP. In response to receiving the association request, the AP may generate a second ANonce (e.g., ANonce2) and may derive a second key (e.g., a second PTK) based on the second ANonce. The AP may transmit an association response to the STA that includes the second ANonce and that is protected using the second key. The STA may derive the second key based on the second ANonce and may use the second key to process the association response and complete link setup. The second key may also be used to protect subsequent messages (e.g., data messages) communicated between the STA and the AP.

[0015] Alternately, instead of receiving an ANonce from the AP via a beacon or probe response, the STA may receive an ANonce-seed in the beacon or probe response. The ANonce-seed may be a cryptographic seed value that is frequently updated by the AP. The STA may generate an ANonce by hashing the ANonce-seed with the media access control (MAC) address of the STA. Thus, unlike an ANonce that is broadcasted to multiple STAs via a beacon message, the ANonce generated at the STA based on the ANonce-seed and the STA's MAC address may be unique to the STA. The generated ANonce may be used by the STA to initiate a link setup with the AP. During the link setup, the AP may generate the ANonce based on the ANonce-seed and the MAC address of the STA, which may be included in link setup messages (e.g., an association request) from the STA. It will be noted that in contrast to other handshaking techniques, this technique may involve the STA generating the ANonce before the AP. Advantageously, the ANonce may be unique to the STA, may be sent "in the clear" (i.e., unencrypted), and may not be predictable by unauthorized devices before transmission by the AP.

[0016] In a particular embodiment, a method includes sending an unprotected association request from a mobile device to an access point. The method also includes receiving an association response from the access point, where the association response includes an ANonce. The method includes generating, at the mobile device, a pairwise transient key (PTK) using the ANonce.

[0017] In another particular embodiment, an apparatus includes a processor and a memory storing instructions executable by the processor to send an unprotected association request to an access point and to receive an association response from the access point, where the association response includes an ANonce. The instructions are also executable by the processor to generate a PTK using the ANonce.

[0018] In another particular embodiment, a method includes, at an access point, receiving an unprotected association request from a mobile device. The method also includes extracting an initiate message from the unprotected association request and sending the initiate message to an authentication server. The method further includes receiving an answer message from the authentication server, where the answer message includes a re-authentication master session key (rMSK). The method includes generating an ANonce and sending an association response to the mobile device, where the association response includes the ANonce.

[0019] In another particular embodiment, an apparatus includes a processor and a memory storing instructions executable by the processor to receive an unprotected association request from a mobile device. The instructions are also executable by the processor to extract an initiate message from the unprotected association request and to send the initiate message to an authentication server. The instructions are further executable by the processor to receive an answer message from the authentication server, where the answer message includes a rMSK. The instructions are executable by the processor to generate an ANonce and to send an association response to the mobile device, where the association response includes the ANonce.

[0020] In another particular embodiment, a method includes initiating, at a mobile device, a first link setup with an access point using a first ANonce. The method also includes receiving, during the first link setup with the access point, a second ANonce for use in a second link setup with the access point subsequent to the first link setup, where the second ANonce is distinct from the first ANonce.

[0021] In another particular embodiment, an apparatus includes a processor and a memory storing instructions executable by the processor to initiate a first link setup with an access point using a first ANonce. The instructions are also executable by the processor to receive, during the first link setup with the access point, a second ANonce for use in a second link setup with the access point subsequent to the first link setup, where the second ANonce is distinct from the first ANonce.

[0022] In another particular embodiment, a method includes sending, from an access point to a mobile device during a first link setup that uses a first ANonce, a second ANonce for use in a second link setup with the mobile device subsequent to the first link setup, where the sec-

ond ANonce is distinct from the first ANonce.

[0023] In another particular embodiment, an apparatus includes a processor and a memory storing instructions executable by the processor to send, to a mobile device during a first link setup that uses a first ANonce, a second ANonce for use in a second link setup with the mobile device subsequent to the first link setup, where the second ANonce is distinct from the first ANonce.

[0024] In another particular embodiment, a method includes receiving, at a mobile device, a first ANonce from an access point. The method also includes generating a first PTK using the first ANonce. The method further includes sending an association request to the access point, where the association request includes a SNonce and is protected using the first PTK. The method includes receiving an association response from the access point, where the association response includes a second ANonce and is protected using a second PTK. The method also includes generating the second PTK using the second ANonce and the SNonce. The method further includes using the second PTK to protect at least one subsequent message to be sent to the access point.

[0025] In another particular embodiment, an apparatus includes a processor and a memory storing instructions executable by the processor to generate, at an access point, an ANonce-seed to be sent to a mobile device. The instructions are also executable by the processor to generate an ANonce based on the ANonce-seed and a MAC address of the mobile device that is received from the mobile device. The instructions are further executable by the processor to perform a link setup with the mobile device based on the generated ANonce.

[0026] In wireless networks such as 802.11 (WiFi) networks, a mobile user may move from one network to another. In some cases the networks may be managed by a same network carrier or entity.

[0027] Some non-limiting examples of such use cases are:

1. Hot-Spot Pass-Through

(A) A user may pass by (several, non-overlapping) publicly accessible WiFi hot-spots (e.g., at coffee shops or other public locations). While having connectivity, the user terminal may upload and download information such as e-mails, social networking messages, etc. Another example is passengers onboard a train that may pass through multiple train stations with WiFi access points.

2. Train

(B) A user may be onboard a train in which a WiFi service is provided to customers via a local Access Point (AP). This AP may use a wireless, 802.11-based backbone to connect to track-side infrastructure. A directional antenna may be used to provide continuous coverage along the tracks

3. Toll / Weight Station Drive By

(C) A vehicle on a highway driving through a toll station or passing by a weight station may be able to connect to an AP at the toll station or weight station. While driving by (or being weighed) information such as billing the customer with tolls or exchange of freight information may be provided.

[0028] Enabling applications for these non-overlapping but related connections may rely upon a standard IP protocol suite and potentially trust in the underlying wireless technology to establish a secure link.

[0029] In some proposed systems for setup of Internet Protocol (IP) connections, after receiving a beacon, there may be 16 roundtrip exchanges (32 messages communicated to and from an access terminal) to establish a secure link for the access terminal.

[0030] In selected embodiments of proposed systems described herein, a fast link setup can be performed wherein the number of messages to setup an IP connection and secure link after receiving the beacon is reduced to 1 roundtrip exchange (2 messages) from the previous 16 roundtrip exchanges (32 messages). An Extensible Authentication Protocol/Re-authentication Protocol (EAP/ERP) may be used as part of the fast link setup.

[0031] FIG. 1 is a conceptual diagram illustrating an example of a wireless network configuration for communicating data between one or more terminals and an access point. The network configuration 100 of FIG. 1 maybe used for communicating data between one or more terminals and an access point. The network configuration 100 includes an access point 102 coupled to a network 104. The access point 102 may be configured to provide wireless communications to various communication devices such as wireless devices (which may also be referred to herein as stations (STAs) and access terminals (ATs) 106, 108, 110). As a non-limiting example, the access point 102 may be a base station. As non-limiting examples, the stations/terminals 106, 108, 110 may be a personal computer (PC), a laptop computer, a tablet computer, a mobile phone, a personal digital assistant (PDA), and/or any device configured for wirelessly sending and/or receiving data, or any combination thereof. The network 104 may include a distributed computer network, such as a transmission control protocol/internet protocol (TCP/IP) network.

[0032] The access point 102 may be configured to provide a variety of wireless communications services, including but not limited to: Wireless Fidelity (WiFi) services, Worldwide Interoperability for Microwave Access (WiMAX) services, and wireless session initiation protocol (SIP) services. The stations/terminals 106, 108, 110 may be configured for wireless communications (includ-

ing, but not limited to communications in compliance with the 802.11, 802.11-2007, and 802.11x family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE)). In addition, the stations/terminals 106, 108, 110 may be configured to send data to and receive data from the access point 102.

[0033] FIG. 2 is a block diagram illustrating an exemplary station/terminal 200. A processor 210 (e.g., a Digital Signal Processor (DSP)) is coupled to a memory 232 for storing information such as data for processing and transmission and instructions 260 for execution on the processor 210. The instructions may be executable by the processor 210 to perform various methods and functions of a station/terminal, as described herein. Moreover, an access point (AP), an authentication server (AS), and a Dynamic Host Configuration Protocol (DHCP) server may similarly include a processor and memory storing instructions executable by the processor to perform various methods and functions of an AP, AS, and DHCP server, respectively, as described herein.

[0034] A display controller 226 may be coupled to the processor 210 and to a display device 228. A coder/decoder (CODEC) 234 can also be coupled to the processor 210. As non-limiting examples of user interface devices, a speaker 236 and a microphone 238 may be coupled to the CODEC 234. A wireless controller 240 may be coupled to the processor 210 and to an antenna 242. In a particular example, the processor 210, the display controller 226, the memory 232, the CODEC 234, and the wireless controller 240 may be included in a system-in-package or system-on-chip device 222. In a particular example, an input device 230 and a power supply 244 may be coupled to the system-on-chip device 222. Moreover, in a particular example, as illustrated, the display device 228, the input device 230, the speaker 236, the microphone 238, the antenna 242, and the power supply 244 may be external to the system-on-chip device 222. However, each of the display device 228, the input device 230, the speaker 236, the microphone 238, the wireless antenna 242, and the power supply 244 can be coupled to a component of the system-on-chip device 222, such as an interface or a controller.

[0035] FIG. 3 is a flow diagram illustrating messaging that may be performed in a conventional connection setup. The messages shown between the station/terminal 302 and the access point 304 may include a probe and authentication request. An Extensible Authentication Protocol (EAP) Over Local Area Network (LAN) (EAPOL) process may start and include an identification phase, a Protected EAP (PEAP) phase, and an EAP-Microsoft Challenge Handshake authentication Protocol (EAP-MSCHAPv2). Upon EAP success, an EAPOL key may be established. Thus, at least 16 messages must be communicated to or from the station/terminal 302 to establish the link setup and authentication.

[0036] In particular embodiments of the proposed system described herein, the number of messages to setup an IP connection (after receiving the beacon) is reduced to 2 messages (from 16 messages). Extensible Authentication Protocol Re-authentication Protocol (ERP) may be used as part of the re-authentication as described more fully below with respect to FIGS. 12 and 13 and may include the following optimizations. The station/terminal (STA) 302 may perform full EAP authentication once, and keeps using ERP fast re-authentication for fast initial link setup thereafter.

[0037] A re-authentication Master Session Key (rMSK) is generated by the station/terminal 302 prior to sending an association request without obtaining a challenge from the network. A pairwise transient key (PTK) is generated by the station (STA) 302 from the rMSK and includes a key confirmation key (KCK), a key encryption key (KEK), and a Transient Key (TK).

[0038] The association request is sent by the station 302 and bundles an EAP reauthorization request with a Dynamic Host Configuration Protocol (DHCP)-Discover-with-Rapid-Commit and a SNonce (e.g., SNonce is picked up by the STA 302, i.e., station nonce). The bundled message may be included as one or more information elements (IEs). The EAP reauthorization request is authenticated by the authentication server (Auth Server) 308 using a re-authentication integrity key (rIK). The DHCP-Discover-with-Rapid-Commit and SNonce are protected using the re-authentication Master Session Key (rMSK) or pairwise transient key (PTK) derived from the rMSK. The DHCP-Discover-with-Rapid-Commit may be encrypted and MIC'd (Message Integrity Code) or not encrypted but MIC'd. While some of the examples herein may utilize a discover request (e.g., Discover-with-Rapid-Commit) to illustrate an efficient re-authentication concept, it should be understood that any message used at an upper layer (of a protocol stack) to assign IP address may be used instead.

[0039] If the DHCP Message is encrypted, the access point 304 may hold the DHCP-Discover-with-Rapid-Commit & SNonce messages until the EAP-re-authentication request is validated by the authentication server 308. To validate the message, access point (AP) 304 waits until it receives an rMSK from the Authentication server 308 and derives the pairwise transient key (PTK). Based on the rMSK obtained from authentication server 308, the access point 304 derives the PTK which is used for MIC (Message Integrity Code) as well as to decrypt the message.

[0040] If the DHCP Message is not encrypted, the access point 304 may forward the DHCP-Discover-with-Rapid-Commit to a DHCP-Server with the expectation that majority of the cases the message came from a correct device (but retain the SNonce messages until the EAP re-authentication request is validated by the authentication server 308). Even though the DHCP-Discover-with-Rapid-Commit may be sent to the DHCP-Server, the access point 304 will hold a DHCP-Acknowledge until it verifies the DHCP Discover message based on the rMSK obtained from the authentication server 308 and the access point 304 derives the PTK.

[0041] The access point (AP) 304 then sends the DHCP-Acknowledge + a GTK/IGTK protected with the PTK. In other words, the DHCP-Acknowledge is encrypted and message integrity is protected.

[0042] A non-limiting aspect may include the one or more of the following steps in a process for link setup and authentication.

[0043] First, a user may obtain a station/terminal 302 and perform a full EAP authentication as part of an initial setup with a specific network (e.g., a specific WiFi network). As a non-limiting example, perhaps the full EAP authentication may be maintained for a specific authentication period, such as, for example, one year.

[0044] Second, during the authentication period, the user passes by (several, non-overlapping) publicly accessible WiFi hot-spots (e.g. at coffee shops and other public places). In other words, this step may be performed multiple times and with multiple access points 304 that are part of the setup network during the authentication period. The station/terminal 302 will perform a Fast Initial Link Setup (FILS) with the network using ERP. Bundling of the ERP with the DHCP-Rapid-Discovery using the association request message will reduce the signaling for the association request to one roundtrip as explained more fully below. During the authentication period, the user's station/terminal 302 may continue to perform ERP for Fast Initial Link Setup (FILS) when connecting with the network.

[0045] Third, as expiration of the authentication period approaches, the user may be warned to perform a "full attachment" to the network again, within a given period of time (for example, 2 weeks). During this period, the user will continue to be able to use fast-authentication based on earlier full-EAP authentication until it expires, or a full attachment is performed. The full attachment notification may originate from the network or may be configured locally on the station/terminal 302.

[0046] Fourth, if the user doesn't perform full attachment, after one year, the network will fail ERP, and will initiate full EAP authentication for another year as outlined in step 1.

[0047] FIGS. 4-11 illustrate various different scenarios for performing the two message link setup and authentication.

[0048] FIG. 4 is a flow diagram illustrating a first example of performing efficient link setup and authentication for a client station. At steps 0a and 0b, while communicatively coupled to a first access point AP1 304A, the station/terminal (STA) 302 may perform full EAP authentication. Upon moving (step 1) closer to a second access point AP2 304B, and detecting its beacon (step 2), the station/terminal 302 may seek to re-authenticate itself via the second access point AP2 304B. In this process, the access point 304B transmits a beacon/probe which includes a capability indicator for Fast Initial Link Setup (FILS). The capability indicator may indicate the ability to handle an association request with the bundled ERP and DHCP-Rapid-Discovery. In step 3, the station/terminal 302 generates a re-authentication master session keys (rMSK) (see FIG. 13) using ERP before sending the association request, where:

rMSK = KDF (K, S);
K = rRK; and
S = rMSK label | "\0" | SEQ | length.

[0049] The station/terminal 302 packs the one or more messages as information elements (IEs) (or parameters/payload) of an association request (Step 3). For example, such association request may include: 1) EAP re-authentication initiate (Message Integrity using rIK); 2) DHCP Discover with Rapid Commit (Encrypted & Message integrity using KCK/KEK); and/or 3) EAPOL-Key (SNonce, ANonce) (Message integrity using KCK). The EAPOL-Key may be configured as an entire frame or subset. The ANonce (i.e., access point nonce) may be selected by the station/terminal 302 and sent to the access point AP2 304B. The access point (AP2) 304B can ensure that the station/terminal 302 is using an ANonce sent in the past several seconds/milliseconds (e.g., a recent ANonce obtained from the beacon for the AP2), for example. The access point AP2 304B holds the DHCP & EAPOL-Key message until it receives a root Master Session Key (rMSK) from the authentication server 308. The access point AP2 304B generates a PTK from the rMSK. The access point AP2 304B performs a Message Integrity Code (MIC) exchange for the DHCP & EAPOL Key messages and decrypts the DHCP. The access point AP2 304B uses the rMSK to derive KCK/KEK to protect a DHCP-acknowledge and an EAPOL Key message before sending to the station/terminal 302.

[0050] In various examples, the ANonce may be sent by the AP2 304B either using the beacon to allow stations that use passive scanning, or in a Probe Response message when active scanning is used. When the ANonce is sent by the AP2 304B using the beacon, the ANonce may be changed in every beacon, or a multiple of beacons. The station 302 may include the ANonce picked by the station 302 in the Association Request message sent from the station 302 to AP2 304B.

[0051] FIG. 5 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. This process may be referred to as Option 1a. The processes performed in FIG. 5 are similar to those performed in FIG. 4 (Option 1) except that the rMSK is used (instead of the KCK/KEK of the PTK) to authenticate the DHCP-Discover and EAPOL-Key messages encapsulated in the association request message.

[0052] FIG. 6 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. This process may be referred to as Option 1b. The processes performed in FIG. 6 are similar to those performed in FIG. 4 (Option 1) except for the following possible differences. In step 2 shown on FIG. 6, the access point 304 may advertise a capability

that the DHCP-request can be encrypted. In step 4 shown on FIG. 6, the station/terminal 302 may decide if the DHCP message should be encrypted or not. Several factors may be taken into consideration by the station/terminal 302, such as, for example, if the DHCP-discover request contains any private information, etc. If the station/terminal decides to encrypt the DHCP-discover request, then the access point 304 may hold the message (as shown in FIGS. 4 and 5).

[0053] If the station/terminal decides not to encrypt the DHCP-discover request, following steps may be performed. In step 4 shown on FIG. 6, the DHCP-Discover request information element (IE) or parameter is only Message-Integrity protected. Based on step 4, the access point 304 sends the DHCP-Discover-With-Rapid-Commit (step 6) without waiting for a response for an EAP re-authenticate-initiate request (step 9). This process causes the IP address assignment to take place in parallel with the EAP re-authentication procedure. In step 7a shown on FIG. 6, the access point holds the DHCP-acknowledge that came from the DHCP server until step 10b, where the DHCP-Discover is validated. If the message integrity fails, then the access point 304 initiates a procedure to delete the IP address assigned using the DHCP-acknowledge.

[0054] FIG. 7 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. This process may be referred to as Option 2. The processes performed in FIG. 7 are similar to those performed in FIG. 4 (Option 1) except for the following possible differences. Instead of authenticating the DHCP message and the EAPOL-Key message independently, the combined payload that includes the EAP re-authentication, the DHCP-Discover and the EAPOL-Key may be authenticated using KCK/KEK. The access point 304 extracts the EAP re-authentication-initiate message and forwards it to the authentication server 308 without validating the entire message, which was authenticated using KCK/KEK. The access point 304 authenticates the entire message after it receives the rMSK from the authentication server 308.

[0055] FIG. 8 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. This process may be referred to as Option 2a. The processes performed in FIG. 8 are similar to those performed in FIG. 5 (Option 1a) except for the following possible differences. Instead of authenticating the DHCP message and the EAPOL-Key message independently, the combined payload that includes the EAP re-authentication, the DHCP-Discover and the EAPOL-Key may be authenticated using the rMSK. The access point 304 extracts the EAP re-authentication-initiate message and forwards it to the authentication server 308 without validating the entire message, which was authenticated using rMSK. The access point 304 authenticates the entire message after it receives the rMSK from the authentication server 308. The DHCP discover message (step 9) may be sent before step 5. In this case, the IP address assigned is ignored if the authentication is not successful.

[0056] FIG. 9 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. This process may be referred to as Option 2b. The processes performed in FIG. 9 are similar to those performed in FIG. 4 except for the following possible differences. In step 2, the access point may advertise the capability that the DHCP-request can be encrypted. In step 4, the station/terminal 302 decides if the DHCP message should be encrypted or not. Several factors may be taken into consideration by the station/terminal 302, such as, for example, if the DHCP-discover request contains any private information etc. If the station/terminal 302 decides to encrypt the DHCP-discover request, then the access point 304 will hold the message as described above in option 2 and option 2a. If the station/terminal 302 decides not to encrypt the DHCP-discover request, then the following steps may be performed. In step 4, the DHCP-discover message IE is only message-integrity protected. Based on step 4, the access point 304 sends the DHCP-Discover-With-Rapid-Commit (step 6) without waiting for response for the EAP Re-authentication-Initiate-Request (step 9). This process causes the IP address assignment to take place in parallel with the EAP re-authentication procedure. In step 7a, the access point 304 holds the DHCP-acknowledge that came from the DHCP server until step 10b, where the DHCP-discover is validated. If the message integrity fails, then the access point 304 initiates a procedure to delete the IP address assigned using the DHCP-acknowledge message.

[0057] FIG. 10 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. This process may be referred to as Option 3. The processes performed in FIG. 10 are similar to those performed in FIGS. 4 and 5 (Options 1 and 1a) except for the following possible differences. The ANonce may be sent in the association response along with an "Install PTK, GTK, IGTK" message. Steps 9 and 11 in FIG. 10 may be performed in parallel with steps 5-7 as described in option 1b and option 2b.

[0058] An option 4 may also be derived from options 1 and 2 except for the following possible differences. Instead of a single message at step 4 (i.e., the association request), the association request may be split as message 1 (M1), which encapsulates the DHCP-discover message and message 2 (M2), which encapsulates the EAP re-authentication-initiate message and the SNonce. The access point 304 will not act on the DHCP-discover message until it receives the EAPOL-Key. The two messages (M1 & M2) may be separated by a SIFS period. This option 4 may have an advantage that the EAPOL structure can be re-used.

[0059] FIG. 11 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. This process may be referred to as Option 5. The processes performed in FIG. 11 are

similar to those performed in FIG. 4 (Option 1) except for the following possible differences. The access point 304 transmits the Beacon/Probe response, which includes the Fast Initial Link Setup (FILS) capability indicator for concurrent ERP and/or IP address assignment. In this scenario, the lease timer of the IP address assigned by the access point 304 is not expired. The station/terminal 302 uses the IP address assigned by a first access point 304A in a DHCP request sent to a second access point 304 to confirm if it can continue to use that IP address. If the IP address has expired, then the DHCP server 306 sends a DHCP-NAK.

[0060] FIG. 12 is a flow diagram illustrating messaging that may be performed during a re-authentication protocol. The first time the station/terminal 302 attaches to a network, it performs a full EAP exchange with the authentication server 308. As a result, a master session key (MSK) is distributed to the EAP authenticator. The master session key (MSK) is then used by the authenticator and the station/terminal 302 to establish transient session keys (TSKs) as needed. At the time of the initial EAP exchange, the station/terminal 302 and the authentication server 308 also derive an EMSK, which is used to derive a re-authentication Root Key (rRK). More specifically, a re-authentication Root Key (rRK) may be derived from the extended MSK (EMSK) or from a Domain-Specific Root Key (DSRK), which itself is derived from the EMSK. The re-authentication Root Key (rRK) may be only available to the station/terminal 302 and the authentication server 308 and is generally not distributed to any other entity. Further, a re-authentication Integrity Key (rIK) may be derived from the re-authentication Root Key (rRK). The station/terminal 302 and the authentication server 308 may use the re-authentication integrity key (rIK) to provide proof of possession while performing an ERP exchange. The re-authentication integrity key (rIK) is also generally not handed out to any other entity and is generally only available to the station/terminal 302 and the authentication server 308.

[0061] Two new EAP codes, EAP-Initiate and EAP-Finish, are defined for the purpose of EAP re-authentication. When the station/terminal 302 requests and ERP it performs the ERP exchange shown in the bottom box of FIG. 12.

[0062] FIG. 13 illustrates a key hierarchy that may be used for a re-authentication protocol. The master session key (MSK) may be derived from a root key and a pairwise master key (PMK) may be derived from the master session key (MSK). The extended MSK (EMSK) may be derived from the root key. For the ERP exchange, various additional keys may be derived from the extended MSK (EMSK). DSRK1-DSRKn may be derived. Each of the Domain-Specific Root Key (DSRK) keys may include the rRK. From the re-authentication root key (rRK), the re-authentication integrity key (rIK) and re-authentication master session keys (rMSK1 ... rMSKn) may be derived. Each of the rMSKs may include a pairwise master key (PMK). A pairwise transient key (PTK) (which may include a key confirmation key (KCK), a key encryption key (KEK), and a transient key (TK)) may be derived from the PMK.

[0063] FIG. 14 is a flow diagram showing an exemplary process 1400 operational at a station/terminal to generate and bundle a re-authentication request and an upper layer message (e.g., discover request) into an association request. Operation block 1402 indicates that a beacon including a random number or nonce (e.g., ANonce) is received from the access point. At operation block 1404, the terminal generates a re-authentication request with an extensible authentication protocol from an encryption key using the random number or nonce. At operation block 1406, the terminal generates an upper layer message. For example, such upper layer message may be a discover request, a dynamic host configuration protocol (DHCP) discover-with-rapid-commit request, and/or internet protocol (IP) address assignment message.

[0064] Operation block 1408 indicates that in some aspects the terminal may generate a re-authentication master session key (rMSK) responsive to results of a previous authentication process. Operation block 1410 indicates that in some aspects the terminal may generate a Pairwise Transient Key (PTK) from the rMSK, the random number (ANonce), and/or a locally generated random number (SNonce).

[0065] Operation block 1412 indicates that in some aspects the terminal may encrypt the upper layer message with the rMSK. Operation block 1414 indicates that in some aspects the terminal may encrypt the upper layer message with the PTK or a combination of the KCK and KEK. In other aspects, the upper layer message may be unencrypted.

[0066] Operation block 1416 indicates that in some aspects the terminal may generate the association request as a first message encapsulating a DHCP-discover message, a second message encapsulating an EAPOL-re-authentication-initiate message.

[0067] Operation block 1418 indicates that the terminal bundles the upper layer message and the re-authentication request as an association request. Operation block 1420 indicates that in some aspects the terminal may transmit the first message and the second message separately.

[0068] FIG. 15 is a flow diagram showing an exemplary process 1500 operational at a base station to receive and extract a re-authentication request and an upper layer message from an association request sent by a station/terminal. Operation block 1502 indicates that in some aspects the access point may generate a random number and transmit a beacon including the random number.

[0069] Operation block 1504 indicates that the access point receives from a terminal an association request including an upper layer message (e.g., discover request) and a re-authentication request bundled together. Operation block 1506 indicates that the access point extracts

the upper layer message from the association request and forwards it to a configuration server. Operation block 1508 indicates that the access point extracts the re-authentication request from the association request and forwards it to an authentication server.

[0070] Operation block 1510 indicates that in some aspects the access point may receive an encryption key from the authentication server. Operation block 1512 indicates that in some aspects the access point may generate a PTK from the encryption key, the random number, and a received random number received from the terminal. Operation block 1514 indicates that in some aspects the access point may verify the upper layer message with a combination of the KCK and KEK within the PTK, which includes an Extensible Authentication Protocol Over LAN (EAPOL) key Confirmation Key (KCK) and the EAPOL Key Encryption Key (KEK).

[0071] It will be noted that particular embodiments described with reference to FIGS. 4-15 may involve a 4-way handshake for fast initial link setup. Generally, the 4-way handshake may include: 1) The AP sending an ANonce to the STA, 2) the STA sending a SNonce to the AP, 3) the AP sending a PTK to the STA, and 4) the STA confirming completion of the handshake.

[0072] Thus, the first part of the 4-way handshake may involve an STA listening for a beacon or soliciting a probe response from an access point prior to initiating link setup with the access point. For example, the beacon or probe response may include the ANonce that will be used by the STA for encryption and/or message integrity purposes. However, listening for a beacon may consume time, and soliciting a probe response may consume time and power. Thus, time and power at the STA may be conserved by enabling the STA to perform link setup without first listening for a beacon or soliciting a probe response from the access point.

[0073] FIG. 16 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. In particular, FIG. 16 illustrates a modified 4-way handshake that enables link setup without first listening for a beacon or soliciting a probe response from an access point.

[0074] Selected messages and operations illustrated in FIG. 16 may correspond to messages and operations illustrated in FIGS. 4-11, with the following modifications. The STA 302 may generate an rMSK and a SNonce, at step 2, and send an unprotected association request to the AP 304, at step 3. The unprotected association request may include the SNonce. In contrast to the embodiment of FIG. 4, the STA 302 may perform these operations prior to receiving the ANonce and deriving the PTK. Because the STA 302 sends the association request before receiving the ANonce and deriving the PTK, the AP 304 may extract and forward the EAP re-authentication initiate portion of the association request to the AS 308, as indicated at step 4, without performing ANonce verification as described in FIG. 4. Instead, the AP 304 may rely on the AS 308 transmitting an answer message with a derived rMSK (step 7) as authentication for the STA 302.

[0075] After receiving the rMSK, the AP 304 may generate the ANonce, at step 9, and derive the PTK based on the ANonce, the rMSK, and the SNonce, at step 10a. Thus, the PTK may be derived at the AP 304 prior to being derived at the STA 302. The AP 304 may send an association response including the ANonce to the STA 302, at step 12, where the association response is protected using the KCK and KEK of the PTK. After receiving the association response from the AP 304, the STA 302 may generate the PTK using the rMSK, the SNonce, and the ANonce in the association response, at step 12a.

[0076] The association response sent from the AP 304 (which includes the ANonce), is integrity-protected using the ANonce. Information elements other than the ANonce in the association response may also be encrypted. Thus, the AP 304 may "pre-protect" (i.e., pre-encrypt/pre-integrity-protect) the association response using a PTK generated at the AP 304 using the SNonce obtained from the STA 302 in the association request, a rMSK obtained from the AS 308, and the locally generated ANonce that has not yet been transmitted to the STA 302. Upon receiving the association response, the STA 302 extracts the ANonce from the association response, generates the PTK, and verifies the integrity protection of the message. Thus, the STA 302 "post-validates" the message based on a key obtained from the message. Such pre-protection and post-validation may enable faster link setup than conventional handshake schemes that first confirm keys and then protect data using the keys.

[0077] The embodiment of FIG. 16 may thus enable the STA 302 to perform a modified 4-way handshake for link setup without first listening for a beacon or soliciting a probe response. This may reduce link setup time and conserve power at the STA 302. It should be noted that because the STA 302 does not wait for a beacon/probe response, the STA 302 may use an alternative addressing mechanism for the unprotected association request. For example, when the AP 304 is "known" to the STA 302, the STA 302 may have previously stored a basic service set identifier (BSSID) of the AP 304 in a memory of the STA 302. To initiate link setup, the STA 302 may retrieve the stored BSSID and may send the unprotected association request to the AP 304 based on the BSSID. Situations in which the AP 304 may be "known" to the STA 302 include when the AP 304 has previously been visited by the STA 302 (e.g., a "home" AP or an "office" AP), and when the STA 302 has not moved recently (e.g., as determined by a cellular and/or global positioning system (GPS) capability of the STA 302). Thus, in a particular embodiment, the STA 302 may send the association request responsive to location information determined at the STA 302 (e.g., when the STA 302 "knows" that the target AP 304 is in the vicinity of the STA 302).

[0078] FIG. 17 is a flow diagram showing an exemplary process 1700 operable at the STA 302 of FIG. 16 to perform link setup and authentication. At 1702, a mobile de-

vice (e.g., the STA 302) may retrieve a BSSID of an access point previously visited by the mobile device. Proceeding to 1704, the mobile device may generate a rMSK and a SNonce. Advancing to 1706, the mobile device may send an unprotected association request to the access point based on the BSSID. For example, referring to FIG. 16, the STA 302 may send the unprotected association request to the AP 304 at step 3.

[0079] Continuing to 1708, the mobile device may receive an association response from the access point, where the association response includes an ANonce. At 1710, the mobile device may generate a PTK using the rMSK, the SNonce, and the ANonce in the received association response. For example, referring to FIG. 16, the STA 302 may receive the association response from the AP 304 at step 12 and may derive the PTK at step 12a.

[0080] FIG. 18 is a flow diagram showing an inventive process 1800 operable at the AP 304 of FIG. 16 to perform link setup and authentication. At 1802, an access point receives an unprotected association request from a mobile device, where the unprotected association request includes a SNonce. Proceeding to 1804, the access point extracts an initiate message from the unprotected association request. Continuing to 1806, the access point sends the initiate message to an authentication server and receives an answer message from the authentication server, where the answer message includes a rMSK. For example, referring to FIG. 16, the AP 304 may receive the unprotected association request from the STA 302 at step 3 and may receive the rMSK from the AS 308 at step 8.

[0081] Advancing to 1808, the access point may generate an ANonce. The access point also generates a PTK using the rMSK, the ANonce, and the SNonce, at 1810. Continuing to 1812, the access point sends an association response to the mobile device, where the association response includes the ANonce and is protected using the PTK. For example, referring to FIG. 16, the AP 304 may generate the ANonce at step 9, derive the PTK at step 10a, and send the association response to the STA 302 at step 12.

[0082] FIG. 19 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. In particular, FIG. 19 illustrates providing, during a first link setup a "next" ANonce that can be used during a second link setup subsequent to the first link setup.

[0083] Selected messages and operations illustrated in FIG. 16 may correspond to messages and operations illustrated in FIGS. 4-11, with the following modifications. The STA 302 may initiate a first link setup 1902 with the AP 304 using a first ANonce (e.g., ANonce[x]). In a particular embodiment, the first ANonce may have previously been sent by the AP 304 and received by the STA 302 via a beacon or probe response (e.g., as shown at step 2a), retrieved from a memory of the STA 302 (e.g., as shown at step 2b), or any combination thereof.

[0084] During the first link setup 1902, the STA 302 may transmit an association request to the AP 304 using the first ANonce (e.g., ANonce[x]). The AP 304 may provide a second ANonce (e.g., ANonce[x+1]) to the STA 302 during the first link setup 1902. The second ANonce may be for use in a subsequent second link setup 1904 with the AP 304. For example, the second ANonce may be provided in an association response (e.g., as shown at step 4a), in an EAPOL message (e.g., as shown at step 4b), or any combination thereof.

[0085] When the STA 302 initiates the second link setup 1904 with the AP 304, the STA 302 may use the second ANonce (e.g., ANonce[x+1]) instead of waiting for a beacon or soliciting a probe response. In a particular embodiment, the second ANonce (e.g., ANonce[x+1] may have a validity lifetime that is set by the AP 304, and the STA 302 may determine that the second ANonce is valid, at step 5a, prior to initiating the second link setup 1904. If the second ANonce is determined to be invalid, the STA 302 may proceed as described with reference to FIG. 20.

[0086] Upon determining that the second ANonce (e.g., ANonce[x+1]) is valid, the STA may initiate the second link setup 1904 using the second ANonce. During the second link setup 1904, the STA 302 may send a second association request using the second ANonce, as shown at step 6. The STA 302 may also receive a third ANonce (e.g., ANonce[x+2]), to be used in a subsequent third link setup with the AP 304, as shown at step 7a or 7b.

[0087] FIG. 20 is a flow diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. The messages and operations illustrated in FIG. 20 may correspond to those shown in FIG. 19 with the following modifications.

[0088] At step 5a, the STA 302 may determine that the second ANonce (e.g., ANonce[x+1]) is invalid (e.g., due to expiration of a validity time period). Thus, instead of being able to use the second ANonce during the second link setup 1904, the STA 302 may wait for or solicit a new ANonce (e.g., ANonce[y]) via a beacon or probe response, as shown at step 5b. The new ANonce may then be used to initiate the second link setup 1904. During the second link setup 1904, the STA 302 may receive from the AP 304 another ANonce (e.g., ANonce[y+1]) for use in a subsequent third link setup.

[0089] Thus, the embodiments described in FIGS. 19-20 may provide a "next ANonce" to mobile devices, so that a subsequent link setup may be performed faster and may consume less power. In addition, it should be noted that for ease of illustration, the embodiments of FIGS. 19-20 may not include all messaging involved in link setup. For example, messaging related to DHCP operations and messaging between the AP 304 and the AS 308 is not shown.

[0090] FIG. 21 is a flow diagram showing an exemplary process 2100 operable at the STA 302 of FIGS. 19-20 to perform link setup and authentication. At 2102, a mobile device may initiate a first link setup with an access

point using a first ANonce. The first ANonce may be retrieved from a memory and/or received from the access point via a beacon or a probe response. Advancing to 2104, the mobile device may receive, during the first link setup with the access point, a second ANonce for use in a subsequent second link setup with the access point. The second ANonce may be received in an association response and/or an EAPOL message. For example, referring to FIGS. 19-20, the STA 302 may initiate the first link setup 1902 using the first ANonce (e.g., ANonce[x]) and may receive the second ANonce (e.g., ANonce[x+1]) during the first link setup 1902.

[0091] Continuing to 2106, the mobile device may determine whether the second ANonce is valid. For example, the mobile device may make such a determination prior to initiating the second link setup. To illustrate, the mobile device may use a timer that is sent along with the second ANonce or a pre-configured timer to determine if the second ANonce is valid. When the second ANonce is determined to be valid, the mobile device may initiate the second link setup using the second ANonce, at 2108. For example, referring to FIG. 19, the STA 302 may initiate the second link setup 1904 using the second ANonce (e.g., ANonce[x+1]).

[0092] When the second ANonce is determined to be invalid, the mobile device may receive a new ANonce from the access point, at 2110. The new ANonce may be received in a beacon or a probe response. Proceeding to 2112, the mobile device may initiate a link setup with the access point using the new ANonce. For example, referring to FIG. 20, the mobile device may use the new ANonce (e.g., ANonce[y]) for the link setup.

[0093] FIG. 22 is a flow diagram showing an exemplary process 2200 operable at the AP 304 of FIGS. 19-20 to perform link setup and authentication. At 2202, an access point may send a first ANonce to a mobile device. The first ANonce may be sent prior to initiation of a first link setup that uses the first ANonce. Advancing to 2204, the access point may send to the mobile device, during the first link setup, a second ANonce for use in a subsequent second link setup with the mobile device. For example, referring to FIGS. 19-20, during the first link setup 1902 that uses the first ANonce (e.g., ANonce[x]), the AP 304 may send to the STA 302 the second ANonce (e.g., ANonce[x+1]) for use in the subsequent second link setup 1904.

[0094] FIG. 23 is a diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. In particular, FIG. 23 illustrates use of a "temporary" key (e.g., PTK) for upper layer signaling protection during link setup. Since upper layer signaling messages have built-in security protection (between the STA 302 and the authentication server 308), the upper layer signaling messages may be protected using a "weaker" ANonce (e.g., an ANonce that has lower security properties), which may enable a faster signaling procedure for association. A "stronger" ANonce is derived in parallel to the upper layer signaling and is used for further data transfer, as described herein.

[0095] Selected messages and operations illustrated in FIG. 23 may correspond to message and operations illustrated in FIGS. 4-11, with the following modifications. The AP 304 may send a first ANonce (e.g., ANonce1) to the STA 302, as shown at step 2. The STA 302 may derive a first PTK (e.g., PTK1) based on ANonce1 and the SNonce of the STA 302, as shown at step 3a. At step 4, the STA 302 may send an association request to the AP 304. The association request may include the SNonce and may be protected using PTK1. To illustrate, the association request may be protected using a first key confirmation key (KCK1) derived from PTK1.

[0096] At step 8a, the AP 304 may derive PTK1 based on ANonce1 and the SNonce included in the association request. At step 12, the AP may generate a second ANonce (e.g., ANonce2) and may derive a second PTK (e.g., PTK2) based on ANonce2 and the SNonce. At step 13, the AP 304 may send an association response to the STA 302, where the association response includes ANonce2 and is protected using PTK2. To illustrate, the association response may be protected using a KCK and a key encryption key (KEK) derived based on PTK2. The STA 302 may generate PTK2, at step 14, based on the SNonce and ANonce2 to complete link setup. PTK2 may be used by the STA 302 and the AP 304 to protect subsequent messages (e.g., data messages) communicated between the STA 302 and the AP 304.

[0097] Thus, unlike the message flow illustrated in FIG. 16, which involves transmission of an unprotected association request, the message flow of FIG. 23 protects the association request using a "temporary" PTK1. It will be noted that although PTK1 is generated using an ANonce that can be known to multiple STAs (e.g., ANonce1 may be broadcasted to multiple STAs via a beacon), only one message (the association request) is protected using the "temporary" key PTK1. Subsequent messages, including the association response and data messages between the STA 302 and the AP 304, are protected using a different key PTK2. The message flow of FIG. 23 may thus be preferable in situations where the AP is not "known" or "trusted," such as in public access areas.

[0098] FIG. 24 is a flow diagram showing an exemplary process 2400 operable at a station, such as the STA 302 that communicates and processes messages as illustrated by FIG. 23, to perform link setup and authentication. At 2402, a mobile device (e.g., the STA 302) may receive a first ANonce (e.g., ANonce1) from an access point (e.g., the AP 304). Advancing to 2404, the mobile device may generate a first PTK (e.g., PTK1) using the first ANonce. Continuing to 2406, the mobile device may send an association request to the access point. The association request may include a SNonce and may be protected using the first PTK.

[0099] At 2408, the mobile device may receive an association response from the access point. The association response may include a second ANonce (e.g., ANonce2) and may be protected using a second PTK

(e.g., PTK2). Advancing to 2410, the mobile device may generate the second PTK using the second ANonce and the SNonce. Continuing to 2412, the mobile device may use the second PTK to protect one or more subsequent messages to be sent to the access point.

[0100] FIG. 25 is a flow diagram showing an exemplary process 2500 operable at an access point, such as the AP 304 that communicates and processes messages as illustrated by FIG. 23, to perform link setup and authentication. At 2502, an access point (e.g., the AP 304) may send a first ANonce (e.g., ANonce1) to a mobile device (e.g., the STA 302). For example, the first ANonce may be sent via a unicast probe response or a broadcast beacon. Advancing to 2504, the access point may receive an association request from the mobile device. The association request may include a SNonce and may be protected using a first PTK (e.g., PTK1). At 2506, the access point may generate the first PTK based on the first ANonce and the SNonce.

[0101] Continuing to 2508, the access point may generate a second ANonce (e.g., ANonce2) and a second PTK (e.g., PTK2) based on the second ANonce and the SNonce. At 2510, the access point may send an association response to the mobile device. The association response may include the second ANonce and may be protected using the second PTK.

[0102] FIG. 26 is a diagram illustrating messaging that may be performed according to other aspects of link setup and authentication. In particular, FIG. 26 illustrates use of an ANonce-seed to generate an ANonce.

[0103] Selected messages and operations illustrated in FIG. 26 may correspond to messages and operations illustrated in FIGS. 4-11, with the following modifications. The AP 304 may send an ANonce-seed to the STA 302 in a beacon or probe response, as shown at step 2. In a particular embodiment, the ANonce-seed is a 64-bit cryptographic seed value that is frequently updated by the AP 304. In a particular embodiment, the ANonce-seed is broadcast to a plurality of STAs (e.g., in a beacon). The STA 302 may use the ANonce-seed to generate a device specific ANonce, as shown at step 3. In a particular embodiment, the ANonce is generated be performing a function (e.g., a hashing function) on the ANonce-seed and a value unique to and/or descriptive of the STA 302 (e.g., a MAC address of the STA 302 or some other value associated with the STA 302). It will be appreciated that unlike an ANonce broadcasted to multiple STAs, the ANonce generated in step 3 may be unique to the STA 302. The STA 302 may perform a link setup with the AP 304 based on the generated ANonce.

[0104] At step 8a, the AP 304 may derive the ANonce based on the ANonce-seed and the MAC address of the STA 302. For example, the MAC address of the STA 302 may be retrieved by the AP 304 from the association response sent in step 4. The AP 304 may perform and complete the link setup with the STA 302 after generating the ANonce.

[0105] It will be noted that unlike other handshaking techniques, the embodiment of FIG. 26 involves the STA 302 generating the ANonce before the AP 304. However, to preserve backward compatibility, the ANonce generated in accordance with the ANonce-seed techniques of FIG. 26 may share similar properties to ANonces in handshaking techniques. For example, the ANonce may be unique to the STA 302, the ANonce and/or ANonce-seed may be sent "in the clear" (e.g., using a beacon or probe response message as shown at step 2 or an EAPOL-Key message as shown at step 4), and the ANonce may not be predictable by unauthorized devices before transmission by the AP 304.

[0106] FIG. 27 is a flow diagram showing an exemplary process 2700 operable at a station, such as the STA 302 that communicates and processes messages as illustrated by FIG. 26, to perform link setup and authentication. At 2702, a mobile device (e.g., the STA 302) may receive an ANonce-seed from an access point (e.g., the AP 304). Advancing to 2704, the mobile device may generate an ANonce based on the ANonce-seed and a MAC address of the mobile device. Continuing to 2706, the mobile device may perform a link setup with the access point based on the generated ANonce.

[0107] FIG. 28 is a flow diagram showing an exemplary process 2800 operable at an access point, such as the AP 304 that communicates and processes messages as illustrated by FIG. 26, to perform link setup and authentication. At 2802, an access point (e.g., the AP 304) may send an ANonce-seed to a mobile device (e.g., the STA 302). Advancing to 2804, the access point may receive a MAC address of the mobile device. For example, the MAC address may be included in a message from the mobile device, such as an association request. Continuing to 2806, the access point may generate an ANonce based on the ANonce-seed and the MAC address of the mobile device. At 2808, the access point may verify the authenticity of the mobile device by comparing the ANonce reported by the mobile device to the ANonce computed by the access point. If the mobile device passes the verification, then the access point may perform a link setup with the mobile device based on the generated ANonce.

[0108] It should be noted that although various embodiments and options may be described herein as alternatives, different characteristics from different embodiments and options may be combined to perform link setup an authentication.

[0109] Various techniques described herein may be applied to pull-based and push-based data scenarios. For example, the modified 4-way handshake described with reference to FIGS. 16-18 and the "next" ANonce technique described with reference to FIGS. 19-22 may be applied to pull-based and push-based data scenarios. One or more applications executed by a mobile device, such as e-mail and social networking applications, may periodically check for data updates. The modified 4-way handshake or "next" ANonce technique may enable such data update pulls to occur faster and with reduced battery

consumption at the mobile device. As another example, application(s) at the mobile device may be configured to receive pushed data updates (e.g., from servers). An initial portion of a data update may be received over a cellular connection. However, the remainder of the data update may be received faster (e.g., over WiFi) and/or with reduced battery consumption because the initial portion of the data update triggers a fast initial link setup using the modified 4-way handshake or "next" ANonce technique as described herein. The temporary PTK technique described with reference to FIGS. 23-25 and the ANonce-seed technique described with reference to FIGS. 26-28 may also be used in such pull-based and push-based data scenarios.

[0110] In conjunction with the described embodiments, a first apparatus may include means for sending an unprotected association request from a mobile device to an access point. For example, the means for sending may include one or more components of the STAs 106-110, the wireless controller 240, the antenna 242, one or more components of the STA 302, one or more other devices configured to send an unprotected association request, or any combination thereof. The first apparatus may also include means for receiving an association response from the access point, where the association response includes an ANonce. For example, the means for receiving may include one or more components of the STAs 106-110, the wireless controller 240, the antenna 242, one or more components of the STA 302, one or more other devices configured to receive an association response, or any combination thereof. The first apparatus may further include means for generating, at the mobile device, a PTK using the ANonce. For example, the means for generating may include one or more components of the STAs 106-110, the processor 210, one or more components of the STA 302, one or more other devices configured to generate a PTK, or any combination thereof.

[0111] A second apparatus may include means for receiving an unprotected association request at an access point from a mobile device. For example, the means for receiving the unprotected association request may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to receive an unprotected association request (e.g., a wireless controller and/or antenna of an AP), or any combination thereof. The second apparatus may also include means for extracting an initiate message from the unprotected association request. For example, the means for extracting may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to extract an initiate message (e.g., a processor of an AP), or any combination thereof. The second apparatus may further include means for sending the initiate message to an AS. For example, the means for sending the initiate message may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to send an initiate message (e.g., a wireless controller and/or antenna of an AP), or any combination thereof.

[0112] The second apparatus may include means for receiving an answer message from the AS, where the answer message includes a rMSK. For example, the means for receiving the answer message may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to receive an answer message (e.g., a wireless controller and/or antenna of an AP), or any combination thereof. The second apparatus may also include means for generating an ANonce. For example, the means for generating may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to generate an ANonce (e.g., a processor of an AP), or any combination thereof. The second apparatus may further include means for sending an association response from the access point to the mobile device, where the association response includes the ANonce. For example, the means for sending the association response may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to send an association response (e.g., a wireless controller and/or antenna of an AP), or any combination thereof.

[0113] A third apparatus may include means for means for initiating, at a mobile device, a first link setup with an access point using a first ANonce. For example, the means for initiating may include one or more components of the STAs 106-110, the processor 210, one or more components of the STA 302, one or more other devices configured to initiate a link setup, or any combination thereof. The third apparatus may also include means for receiving, during the first link setup with the access point, a second ANonce for use in a second link setup with the access point subsequent to the first link setup. For example, the means for receiving may include one or more components of the STAs 106-110, the wireless controller 240, the antenna 242, one or more components of the STA 302, one or more other devices configured to receive an ANonce, or any combination thereof.

[0114] A fourth apparatus may include means for sending, from an access point to a mobile device during a first link setup that uses a first ANonce, a second ANonce for use in a second link setup with the mobile device subsequent to the first link setup. For example, the means for sending the second ANonce may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to send an ANonce (e.g., a wireless controller and/or antenna of an AP), or any combination thereof. The fourth apparatus may also include means for sending the first ANonce to the mobile device via a beacon or a probe response prior to initiation of the first link setup, where the second ANonce is distinct from the first ANonce. For example, the means for sending the first ANonce may include one

or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to send an ANonce (e.g., a wireless controller and/or antenna of an AP), or any combination thereof.

[0115] A fifth apparatus may include means for receiving, at a mobile device, a first ANonce from an access point. For example, the means for receiving may include one or more components of the STAs 106-110, the wireless controller 240, the antenna 242, one or more components of the STA 302, one or more other devices configured to receive an ANonce, or any combination thereof. The apparatus may also include means for generating a first PTK using the first ANonce. For example, the means for generating may include one or more components of the STAs 106-110, the processor 210, one or more components of the STA 302, one or more other devices configured to generate a PTK, or any combination thereof. The first ANonce may be considered a "weak" ANonce, for example due to being broadcast to multiple STAs in a beacon or due to being predictable in value. However, the use of such a "weak" ANonce may be acceptable because of implicit security embedded in upper layer signaling messages. Moreover, a second, "stronger" ANonce may be derived and used for further data transfer, as described herein.

[0116] The apparatus may further include means for sending an association request to the access point, where the association request includes a SNonce and is protected using the first PTK. For example, the means for sending may include one or more components of the STAs 106-110, the wireless controller 240, the antenna 242, one or more components of the STA 302, one or more other devices configured to send an association request, or any combination thereof.

[0117] The apparatus may include means for receiving, at the mobile device, an association response from the access point, where the association response includes a second ANonce and is protected using a second PTK. For example, the means for receiving may include one or more components of the STAs 106-110, the wireless controller 240, the antenna 242, one or more components of the STA 302, one or more other devices configured to receive an association response, or any combination thereof. The second ANonce may be considered a "strong" ANonce.

[0118] The apparatus may also include means for generating, at the mobile device, the second PTK using the second ANonce and the SNonce. For example, the means for generating may include one or more components of the STAs 106-110, the processor 210, one or more components of the STA 302, one or more other devices configured to generate a PTK, or any combination thereof. The apparatus may further include means for using the second PTK to protect at least one subsequent message to be sent from the mobile device to the access point. For example, the means for using may include one or more components of the STAs 106-110, the processor 210, one or more components of the STA 302, one or more other devices configured to protect a message, or any combination thereof.

[0119] A sixth apparatus may include means for sending, from an access point, a first ANonce to a mobile device. For example, the means for sending may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to send an ANonce, or any combination thereof. The apparatus may also include means for receiving an association request from the mobile device, where the association request includes a SNonce and is protected using a first PTK. For example, the means for receiving may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to receive an association request, or any combination thereof.

[0120] The apparatus may further include means for generating, at the access point, the first PTK based on the first ANonce and the SNonce. For example, the means for generating may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to generate a PTK, or any combination thereof. The apparatus may include means for generating a second ANonce. For example, the means for generating a second ANonce may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to generate an ANonce, or any combination thereof. The apparatus may also include means for generating a second PTK based on the second ANonce and the SNonce. For example, the means for generating may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to generate a PTK, or any combination thereof.

[0121] The apparatus may further include means for sending an association response to the mobile device, where the association response includes the second ANonce and is protected using the second PTK. For example, the means for sending may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to send an association response, or any combination thereof.

[0122] A seventh apparatus may include means for receiving, at a mobile device, an ANonce-seed from an access point. The ANonce-seed may be broadcasted to a plurality of devices (e.g., via a beacon). For example, the means for receiving an ANonce-seed may include one or more components of the STAs 106-110, the wireless controller 240, the antenna 242, one or more components of the STA 302, one or more other devices configured to receive an ANonce-seed, or any combination thereof. The apparatus may also include means for generating, at the mobile device, an ANonce based on the ANonce-seed and a MAC address of the mobile device. For example, the means for generating may include one or more components of the STAs 106-110, the processor 210, one or more components of the STA 302, one or

more other devices configured to generate an ANonce, or any combination thereof.

[0123] The apparatus may further include means for performing a link setup with the access point based on the generated ANonce. For example, the means for performing may include one or more components of the STAs 106-110, the processor 210, one or more components of the STA 302, one or more other devices configured to perform a link setup, or any combination thereof.

[0124] An eighth apparatus may include means for sending, from an access point, an ANonce-seed to a mobile device. For example, the means for sending may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to send an ANonce-seed, or any combination thereof.

[0125] The apparatus may also include means for receiving a MAC address of the mobile device. For example, the means for receiving may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to receive a MAC address, or any combination thereof. The apparatus may further include means for generating an ANonce based on the ANonce-seed and the MAC address of the mobile device. For example, the means for generating may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to generate an ANonce, or any combination thereof.

[0126] The apparatus may include means for performing a link setup with the mobile device based on the generated ANonce. For example, the means for performing may include one or more components of the AP 102, one or more components of the AP 304, one or more other devices configured to perform a link setup, or any combination thereof.

[0127] The previous description of the disclosed embodiments is provided to enable a person skilled in the art to make or use the disclosed embodiments. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the principles defined herein may be applied to other embodiments without departing from the scope of the disclosure. Thus, the present disclosure is not intended to be limited to the embodiments disclosed herein but is to be accorded the widest scope possible consistent with the principles and novel features as defined by the following claims.

[0128] Elements described herein may include multiple instances of the same element. These elements may be generically indicated by a numerical designator (e.g. 110) and specifically indicated by the numerical indicator followed by an alphabetic designator (e.g., 110A) or a numeric indicator preceded by a "dash" (e.g., 110-1). For ease of following the description, for the most part element number indicators begin with the number of the drawing on which the elements are introduced or most fully described.

[0129] It should be understood that any reference to an element herein using a designation such as "first," "second," and so forth does not limit the quantity or order of those elements, unless such limitation is explicitly stated. Rather, these designations may be used herein as a convenient method of distinguishing between two or more elements or instances of an element. Thus, a reference to first and second elements does not mean that only two elements may be employed there or that the first element must precede the second element in some manner. In addition, unless stated otherwise, a set of elements may comprise one or more elements.

[0130] Specific implementations shown and described are only examples and should not be construed as the only way to implement the present disclosure unless specified otherwise herein. It is readily apparent to one of ordinary skill in the art that the various examples in the present disclosure may be practiced by numerous other partitioning systems.

[0131] Those of ordinary skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout this description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof. Some drawings may illustrate signals as a single signal for clarity of presentation and description. It will be understood by a person of ordinary skill in the art that the signal may represent a bus of signals, wherein the bus may have a variety of bit widths and the present disclosure may be implemented on any number of data signals, including a single data signal.

[0132] In the description, elements, circuits, and functions may be shown in block diagram form in order not to obscure the present disclosure in unnecessary detail. Conversely, specific implementations shown and described are exemplary only and should not be construed as the only way to implement the present disclosure unless specified otherwise herein. Additionally, block definitions and partitioning of logic between various blocks is exemplary of a specific implementation. It is readily apparent to one of ordinary skill in the art that the present disclosure may be practiced by numerous other partitioning systems. For the most part, details concerning timing considerations and the like have been omitted where such details are not necessary to obtain a complete understanding of the present disclosure and are within the abilities of persons of ordinary skill in the relevant art.

[0133] One or more of the components, acts, features and/or functions described herein and illustrated in the drawings may be rearranged and/or combined into a single component, act, feature, or function or embodied in several components, acts, features, or functions. Additional elements, components, acts, and/or functions may also be added without departing from the invention. The algorithms described herein may also be efficiently implemented in software and/or embedded in hardware.

[0134] Also, it is noted that the embodiments may be described as a process that is depicted as a flowchart, a flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination corresponds to a return of the function to the calling function or the main function.

[0135] Moreover, a storage medium may represent one or more devices for storing data, including read-only memory (ROM), random access memory (RAM), magnetic disk storage mediums, optical storage mediums, flash memory devices and/or other machine-readable mediums and, processor-readable mediums, and/or computer-readable mediums for storing information. The terms "machine-readable medium," "computer-readable medium," and/or "processor-readable medium" may include, but are not limited to non-transitory mediums such as portable or fixed storage devices, optical storage devices, and various other mediums capable of storing, containing or carrying instruction(s) and/or data. Thus, the various methods described herein may be fully or partially implemented by instructions and/or data that may be stored in a "machine-readable medium," "computer-readable medium," and/or "processor-readable medium" and executed by one or more processors, machines and/or devices.

[0136] Furthermore, embodiments may be implemented by hardware, software, firmware, middleware, microcode, or any combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine-readable medium such as a storage medium or other storage(s). A processor may perform the necessary tasks. A code segment may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, a software package, a class, or any combination of instructions, data structures, or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, or memory contents. Information, arguments, parameters, data, etc. may be passed, forwarded, or transmitted via any suitable means including memory sharing, message passing, token passing, network transmission, etc.

[0137] The various illustrative logical blocks, modules, circuits, elements, and/or components described in connection with the examples disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic component, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing components, e.g., a combination of a DSP and a microprocessor, a number of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration. A general-purpose processor, configured for executing embodiments described herein, is considered a special purpose processor for carrying out such embodiments. Similarly, a general-purpose computer is considered a special purpose computer when configured for carrying out embodiments described herein.

[0138] The methods or algorithms described in connection with the examples disclosed herein may be embodied directly in hardware, in a software module executable by a processor, or in a combination of both, in the form of processing unit, programming instructions, or other directions, and may be contained in a single device or distributed across multiple devices. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. A storage medium may be coupled to the processor such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor.

[0139] For example, STA functionality may be implemented using instructions stored on a processor-readable medium. A particular medium may store instructions executable to cause a processor to generate an unprotected association request to be sent by a mobile device to an access point. The instructions may also be executable to cause the processor to generate a PTK using an ANonce retrieved from an association response from the access point. Another particular medium may store instructions executable by a processor to initiate, at a mobile device, a first link setup with an access point using a first ANonce. The instructions may also be executable to cause the processor to receive, during the first link setup with the access point, a second ANonce for use in a second link setup with the access point subsequent to the first link setup.

[0140] As another example, AP functionality may be implemented using instructions stored on a processor-readable medium. For example, a particular medium may store instructions executable to cause a processor to extract an initiate message from an unprotected association request received from a mobile device. The instructions may also be executable to cause the processor to extract a rMSK from an answer message received from an authentication server responsive to the initiate message. The instructions may further be executable to cause the

processor to generate an ANonce and to generate an association response to be sent to the mobile device, where the association response includes the ANonce. Another particular medium may store instructions executable by a processor to send, from an access point to a mobile device during a first link setup that uses a first ANonce, a second ANonce for use in a second link setup with the mobile device subsequent to the first link setup.

[0141] Those of skill in the art would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware, software, or a combination thereof depends upon the particular application and design selections imposed on the overall system.

Claims

1. A method operable at an access point (304) comprising:

   receiving (1802) an unprotected association request from a mobile device (302), the association request including a station nonce, SNonce;
   extracting (1804) an initiate message from the unprotected association request;
   sending (1806) the initiate message to an authentication server (308);
   receiving an answer message from the authentication server (308), wherein the answer message includes a re-authentication master session key, rMSK;
   generating (1808) an access point nonce, ANonce;
   generating (1810) a pairwise transient key, PTK, using the rMSK, the ANonce, and the SNonce; and
   sending (1812) an association response to the mobile device (302),
   wherein the association response includes the ANonce,
   and the association response is protected using the PTK.

2. The method of claim 1, wherein the unprotected association request is sent based on a basic service set identifier, BSSID, of the access point (304).

3. The method of claim 1, further comprising sending a dynamic host configuration protocol ,DHCP, discover message to a DHCP server.

4. The method of claim 3, further comprising receiving a DHCP acknowledge message from the DHCP server in response to the DHCP discover message, wherein the DHCP discover message indicates an internet protocol, IP, address.

5. The method of claim 1, wherein the association response is integrity-protected, and wherein information elements other than the ANonce are encrypted.

6. The method of claim 1, wherein the access point (304) relies on the authentication server (308) transmitting an answer message with a derived rMSK as authentication for the mobile device (302).

7. The method of claim 1, wherein the PTK is derived at the access point (304) prior to being derived at the mobile device (302).

8. A computer-program, when being run on a computer, comprising instructions for performing a method according to any of the claims 1 to 7.

9. An apparatus (304) comprising:

   means for receiving an unprotected association request at an access point (304) from a mobile device (302), the association request including a station nonce, SNonce;
   means for extracting an initiate message from the unprotected association request;
   means for sending the initiate message to an authentication server (308);
   means for receiving an answer message from the authentication server (308), wherein the answer message includes a re-authentication master session key, rMSK;
   means for generating an access point nonce, ANonce;
   means for generating a pairwise transient key, PTK, using the rMSK, the ANonce, and the SNonce; and
   means for sending an association response from the access point (304) to the mobile device (302), wherein the association response includes the ANonce, and the association response is protected using the PTK.

10. The apparatus (304) of claim 9, wherein the unprotected association request is sent based on a basic service set identifier, BSSID, of the access point (304).

11. The apparatus (304) of claim 9, further comprising means for sending a dynamic host configuration protocol, DHCP, discover message to a DHCP server.

12. The apparatus (304) of claim 11, further comprising

means for receiving a DHCP acknowledge message from the DHCP server in response to the DHCP discover message, wherein the DHCP discover message indicates an internet protocol, IP, address.

13. The apparatus (304) of claim 9, wherein the association response is integrity-protected, and wherein information elements other than the ANonce are encrypted.

14. The apparatus (304) of claim 9, wherein the access point (304) relies on the authentication server (308) transmitting an answer message with a derived rMSK as authentication for the mobile device (302).

15. The apparatus (304) of claim 9, wherein the PTK is derived at the access point (304) prior to being derived at the mobile device (302).

Patentansprüche

1. Verfahren durchführbar auf einem Zugriffspunkt (304), aufweisend:

Empfangen (1802) einer ungeschützten Assoziierungsanfrage von einem Mobilgerät (302), die Assoziierungsanfrage aufweisend ein station nonce, SNonce;
Extrahieren (1804) einer Initiierungsnachricht von der ungeschützten Assoziierungsanfrage;
Senden (1806) der Initiierungsnachricht an einen Authentifizierungsserver (308);
Empfangen einer Antwortnachricht von dem Authentifizierungsserver (308), wobei die Antwortnachricht einen Reauthentifizierungs-Master-Session-Key, rMSK, aufweist;
Erzeugen (1808) eines Zugriffspunkt nonce, ANonce;
Erzeugen (1810) eines Pairwise Transient Key, PTK, unter Verwendung des rMSK, des ANonce und des SNonce; und
Senden (1812) einer Assoziierungsantwort an das Mobilgerät (302), wobei die Assoziierungsantwort das ANonce aufweist und die Assoziierungsantwort geschützt wird unter Verwendung des PTK.

2. Verfahren nach Anspruch 1, wobei die ungeschützte Assoziierungsanfrage gesendet wird basierend auf einem Basis Service Set Identifier, BSSID, des Zugriffspunktes (304).

3. Verfahren nach Anspruch 1, weiter aufweisend Senden einer Dynamic Host Configuration Protocol, DHCP, Discover Message an einen DHCP Server.

4. Verfahren nach Anspruch 3, weiter aufweisend Empfangen einer DHCP acknowledge message von dem DHCP Server in Antwort auf die DHCP Discover Message, wobei die DHCP Discover Message eine Internet Protocol-, IP, Adresse angibt.

5. Verfahren nach Anspruch 1, wobei die Assoziierungsantwort integritätsgeschützt ist und wobei die Informationselemente außer dem ANonce verschlüsselt sind.

6. Verfahren nach Anspruch 1, wobei der Zugriffspunkt (304) darauf angewiesen ist, dass der Authentifizierungsserver (308) eine Antwortnachricht überträgt mit einem abgeleiteten rMSK als Authentifizierung für das Mobilgerät (302).

7. Verfahren nach Anspruch 1, wobei der PTK bei dem Zugriffspunkt (304) abgeleitet wird, bevor er bei dem Mobilgerät (302) abgeleitet wird.

8. Computerprogramm, das, wenn es auf einem Computer ausgeführt wird, Instruktionen aufweist zum Durchführen eines Verfahrens nach einen beliebigen der Ansprüche 1-7.

9. Vorrichtung (304) aufweisend:

Mittel zum Empfangen einer ungeschützten Assoziierungsanfrage auf einem Zugriffspunkt (304) von einem Mobilgerät (302), die Assoziierungsanfrage beinhaltend ein station nonce, SNonce;
Mittel zum Extrahieren einer Initiierungsnachricht von der ungeschützten Assoziierungsanfrage;
Mittel zum Senden der Initiierungsnachricht an einen Authentifizierungsserver (308);
Mittel zum Empfangen einer Antwortnachricht von dem Authentifizierungsserver (308), wobei die Antwortnachricht einen Reauthentifizierungs-Master-Session-Key, rMSK, aufweist;
Mittel zum Erzeugen eines Zugriffspunkt-Nonce, ANonce;
Mittel zum Erzeugen eines Pairwise Transient Key, PTK, unter Verwendung des rMSK, des ANonce und des SNonce; und
Mittel zum Senden einer Assoziierungsantwort von dem Zugriffspunkt (304) an das Mobilgerät (302), wobei die Assoziierungsantwort das ANonce aufweist und die Assoziierungsantwort unter Verwendung des PTK geschützt wird.

10. Vorrichtung (304) nach Anspruch 9, wobei die ungeschützte Assoziierungsanfrage gesendet wird, basierend auf einem Basis Service Set Identifier, BSSID, des Zugriffspunktes (304).

11. Vorrichtung (304) nach Anspruch 9, weiterhin auf-

weisend Mittel zum Senden einer Dynamic Host Configuration Protocol, DHCP, Discover Message an einen DHCP Server.

12. Vorrichtung (304) nach Anspruch 11, weiterhin aufweisend Mittel zum Empfangen einer DHCP acknowledge message von dem DHCP Server in Antwort auf die DHCP Discover Message, wobei die DHCP Discover Message eine Internet Protocol-, IP, Adresse angibt.

13. Vorrichtung (304) nach Anspruch 9, wobei die Assoziierungsantwort integritätsgeschützt ist und wobei Informationselemente außer dem ANonce verschlüsselt sind.

14. Vorrichtung (304) nach Anspruch 9, wobei der Zugriffspunkt (304) darauf angewiesen ist, dass der Authentifizierungsserver (308) eine Antwortnachricht mit einem abgeleiteten rMSK überträgt, als Authentifizierung für das Mobilgerät (302).

15. Vorrichtung (304) nach Anspruch 9, wobei der PTK bei dem Zugriffspunkt (304) abgeleitet wird, bevor er bei dem Mobilgerät (302) abgeleitet wird.

Revendications

1. Procédé opérationnel au niveau d'un point d'accès (304) comprenant :

la réception (1802) d'une demande d'association non protégée en provenance d'un dispositif mobile (302), la demande d'association comportant un nonce de station, SNonce ;
l'extraction (1804) d'un message de lancement de la demande d'association non protégée ;
l'envoi (1806) du message de lancement à un serveur d'authentification (308) ;
la réception d'un message de réponse en provenance du serveur d'authentification (308), dans lequel le message de réponse comporte une clé maîtresse de session de réauthentification, rMSK ;
la génération (1808) d'un nonce de point d'accès, ANonce ; la génération (1810) d'une clé transitoire par paire, PTK, à l'aide de la rMSK, de l'ANonce et du SNonce ; et
l'envoi (1812) d'une réponse d'association au dispositif mobile (302),
dans lequel la réponse d'association comporte l'ANonce, et la réponse d'association est protégée à l'aide de la PTK.

2. Procédé selon la revendication 1, dans lequel la demande d'association non protégée est envoyée sur la base d'un identifiant d'ensemble de services de base, BSSID, du point d'accès (304).

3. Procédé selon la revendication 1, comprenant en outre l'envoi d'un message de découverte de protocole de configuration dynamique de l'hôte, DHCP, à un serveur DHCP.

4. Procédé selon la revendication 3, comprenant en outre la réception d'un message d'accusé de réception DHCP en provenance du serveur DHCP en réponse au message de découverte DHCP, dans lequel le message de découverte DHCP indique une adresse de protocole Internet, IP.

5. Procédé selon la revendication 1, dans lequel la réponse d'association est protégée en termes d'intégrité, et dans lequel des éléments d'informations autres que l'ANonce sont chiffrés.

6. Procédé selon la revendication 1, dans lequel le point d'accès (304) s'appuie sur la transmission par le serveur d'authentification (308) d'un message de réponse avec une rMSK dérivée en tant qu'authentification pour le dispositif mobile (302).

7. Procédé selon la revendication 1, dans lequel la PTK est dérivée au niveau du point d'accès (304) avant d'être dérivée au niveau du dispositif mobile (302).

8. Programme d'ordinateur, lorsqu'il est exécuté sur un ordinateur, comprenant des instructions pour réaliser un procédé selon l'une quelconque des revendications 1 à 7.

9. Appareil (304) comprenant :

un moyen pour recevoir une demande d'association non protégée au niveau d'un point d'accès (304) en provenance d'un dispositif mobile (302), la demande d'association comportant un nonce de station, SNonce ;
un moyen pour extraire un message de lancement de la demande d'association non protégée ;
un moyen pour envoyer le message de lancement à un serveur d'authentification (308) ;
un moyen pour recevoir un message de réponse en provenance du serveur d'authentification (308), dans lequel le message de réponse comporte une clé maîtresse de session de réauthentification, rMSK ;
un moyen pour générer un nonce de point d'accès, ANonce ; un moyen pour générer une clé transitoire par paire, PTK, à l'aide de la rMSK, de l'ANonce et du SNonce ; et
un moyen pour envoyer une réponse d'association du point d'accès (304) au dispositif mobile (302), dans lequel la réponse d'association

comporte l'ANonce, et la réponse d'association est protégée à l'aide de la PTK.

10. Appareil (304) selon la revendication 9, dans lequel la demande d'association non protégée est envoyée sur la base d'un identifiant d'ensemble de services de base, BSSID, du point d'accès (304).

11. Appareil (304) selon la revendication 9, comprenant en outre un moyen pour envoyer un message de découverte de protocole de configuration dynamique de l'hôte, DHCP, à un serveur DHCP.

12. Appareil (304) selon la revendication 11, comprenant en outre un moyen pour recevoir un message d'accusé de réception DHCP en provenance du serveur DHCP en réponse au message de découverte DHCP, dans lequel le message de découverte DHCP indique une adresse de protocole Internet, IP.

13. Appareil (304) selon la revendication 9, dans lequel la réponse d'association est protégée en termes d'intégrité, et dans lequel des éléments d'informations autres que l'ANonce sont chiffrés.

14. Appareil (304) selon la revendication 9, dans lequel le point d'accès (304) s'appuie sur la transmission par le serveur d'authentification (308) d'un message de réponse avec une rMSK dérivée en tant qu'authentification pour le dispositif mobile (302).

15. Appareil (304) selon la revendication 9, dans lequel la PTK est dérivée au niveau du point d'accès (304) avant d'être dérivée au niveau du dispositif mobile (302).

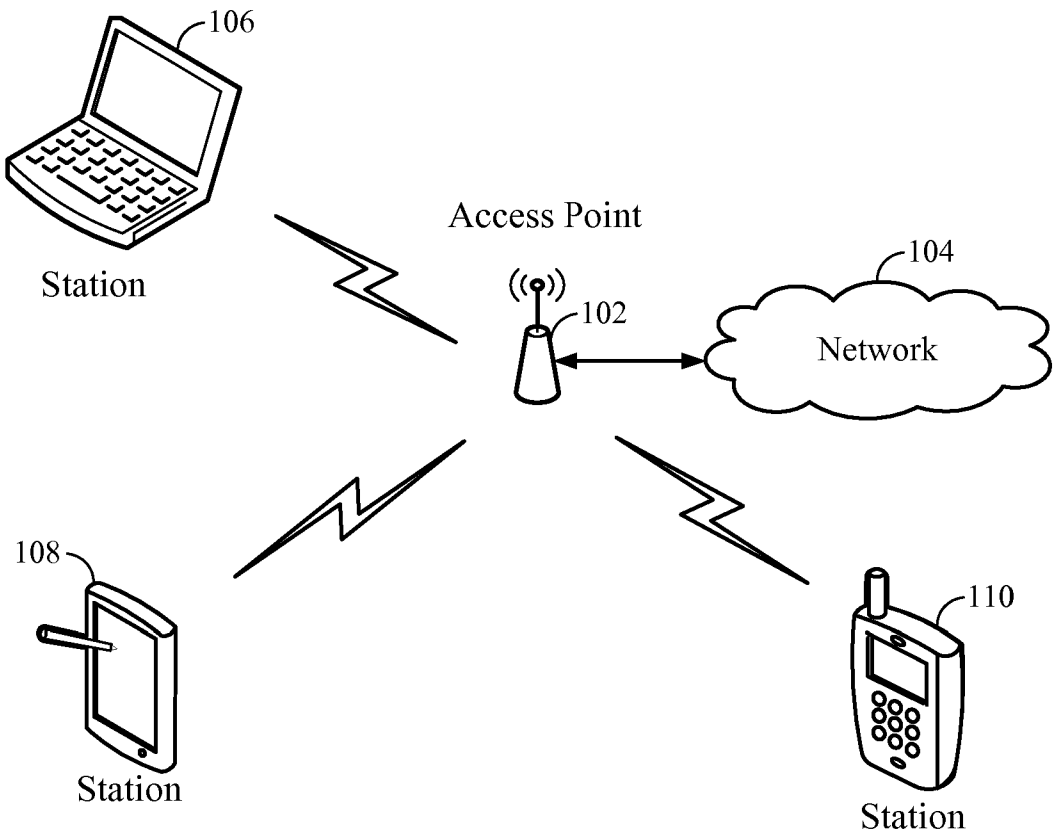
106
Station
Access Point
102
104
Network
108
Station
110
Station

FIG. 1

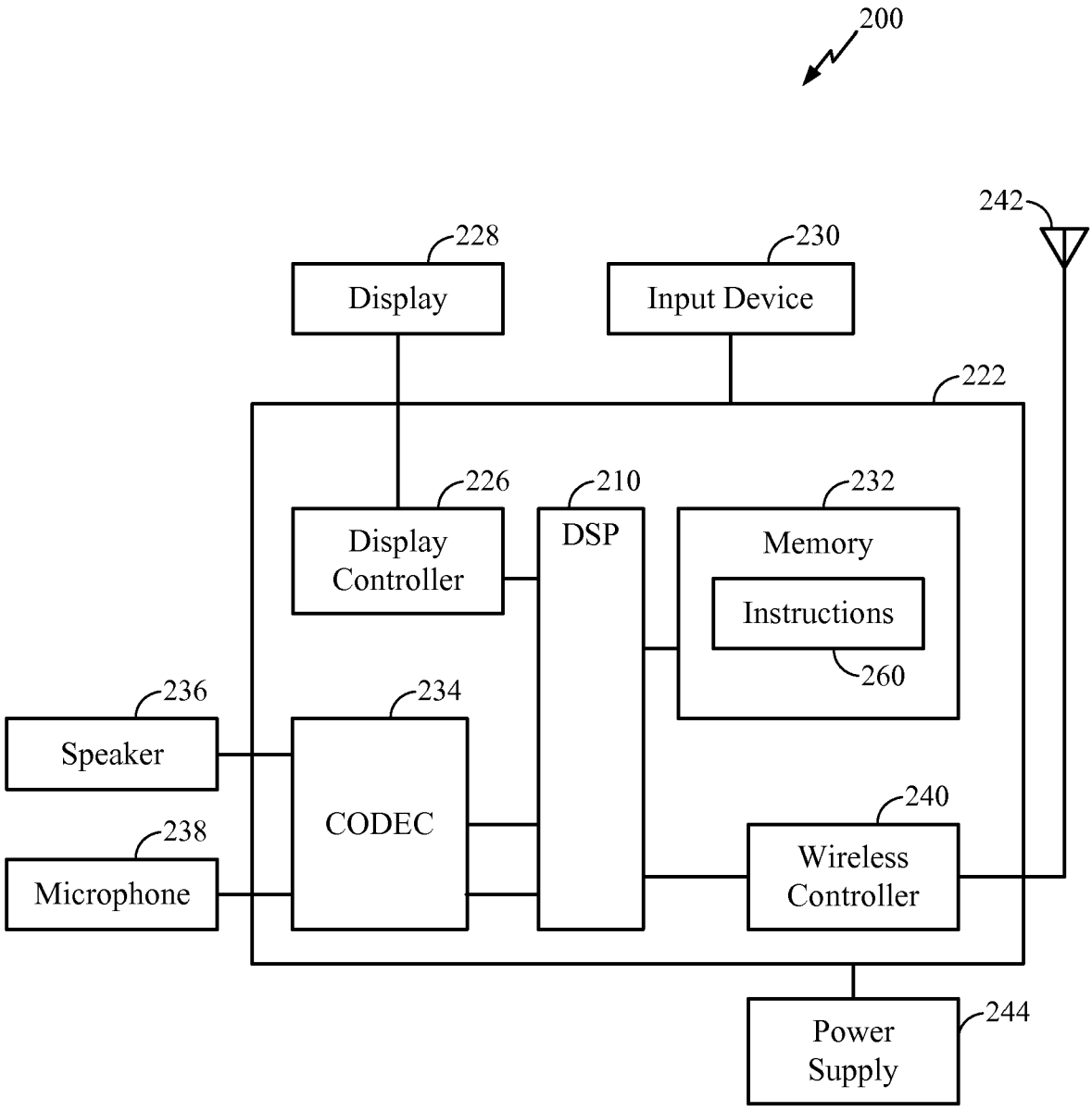
200
242
228
Display
230
Input Device
222
226
Display Controller
210
DSP
232
Memory
Instructions
260
236
Speaker
234
CODEC
238
Microphone
240
Wireless Controller
Power Supply
244

FIG. 2

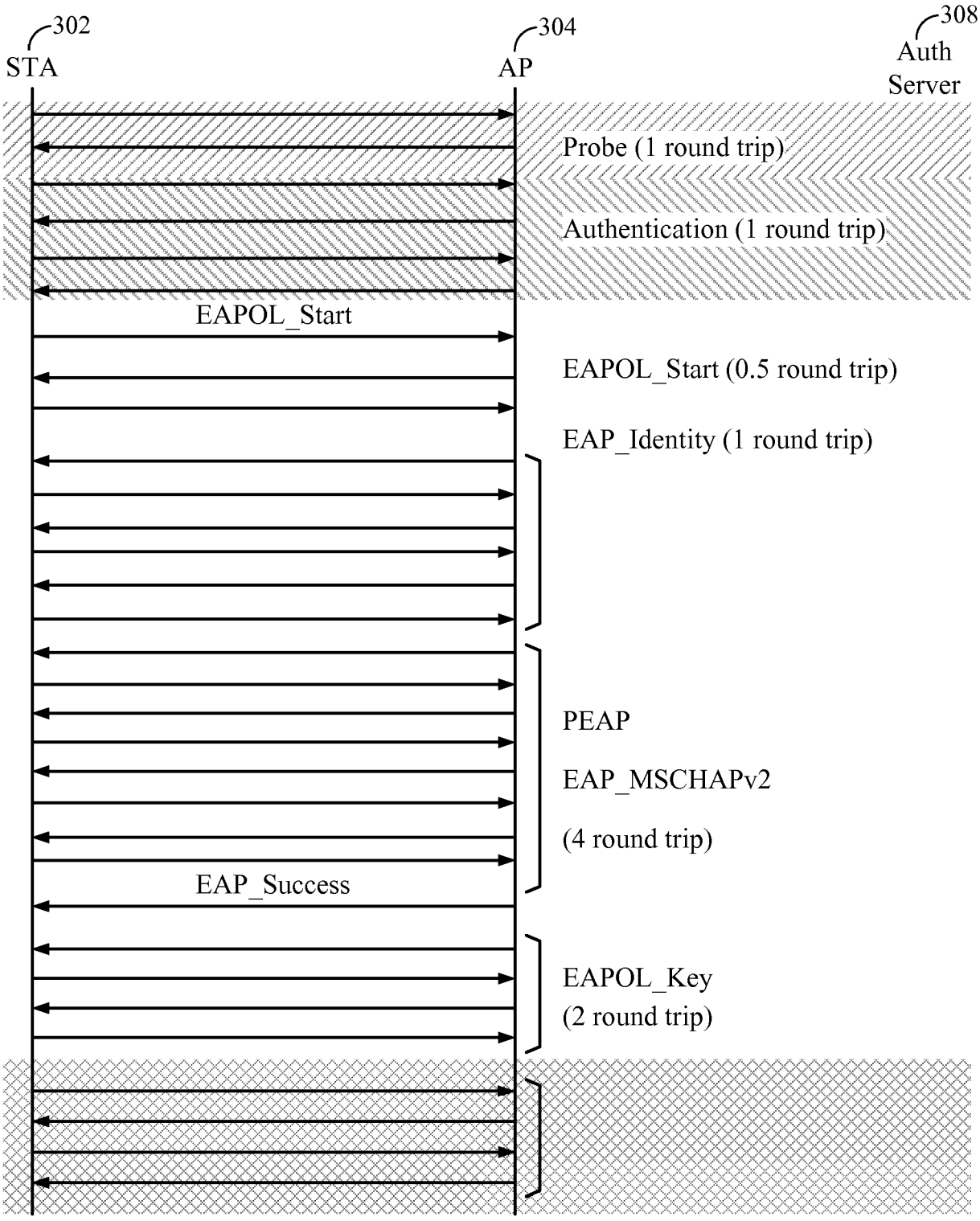
302
STA
304
AP
308
Auth
Server
Probe (1 round trip)
Authentication (1 round trip)
EAPOL_Start
EAPOL_Start (0.5 round trip)
EAP_Identity (1 round trip)
PEAP
EAP_MSCHAPv2
(4 round trip)
EAP_Success
EAPOL_Key
(2 round trip)

FIG. 3

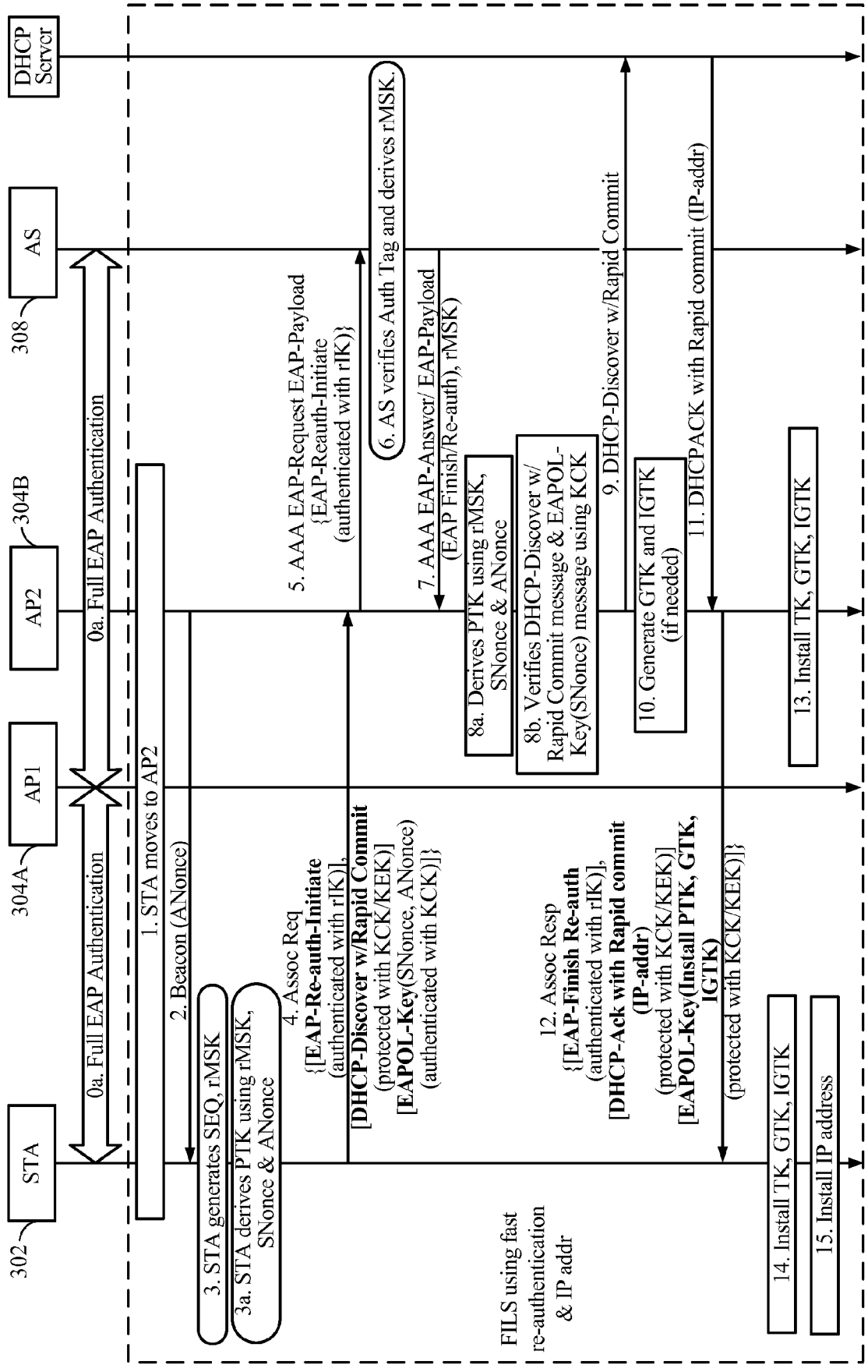

FIG. 4 (Option 1)

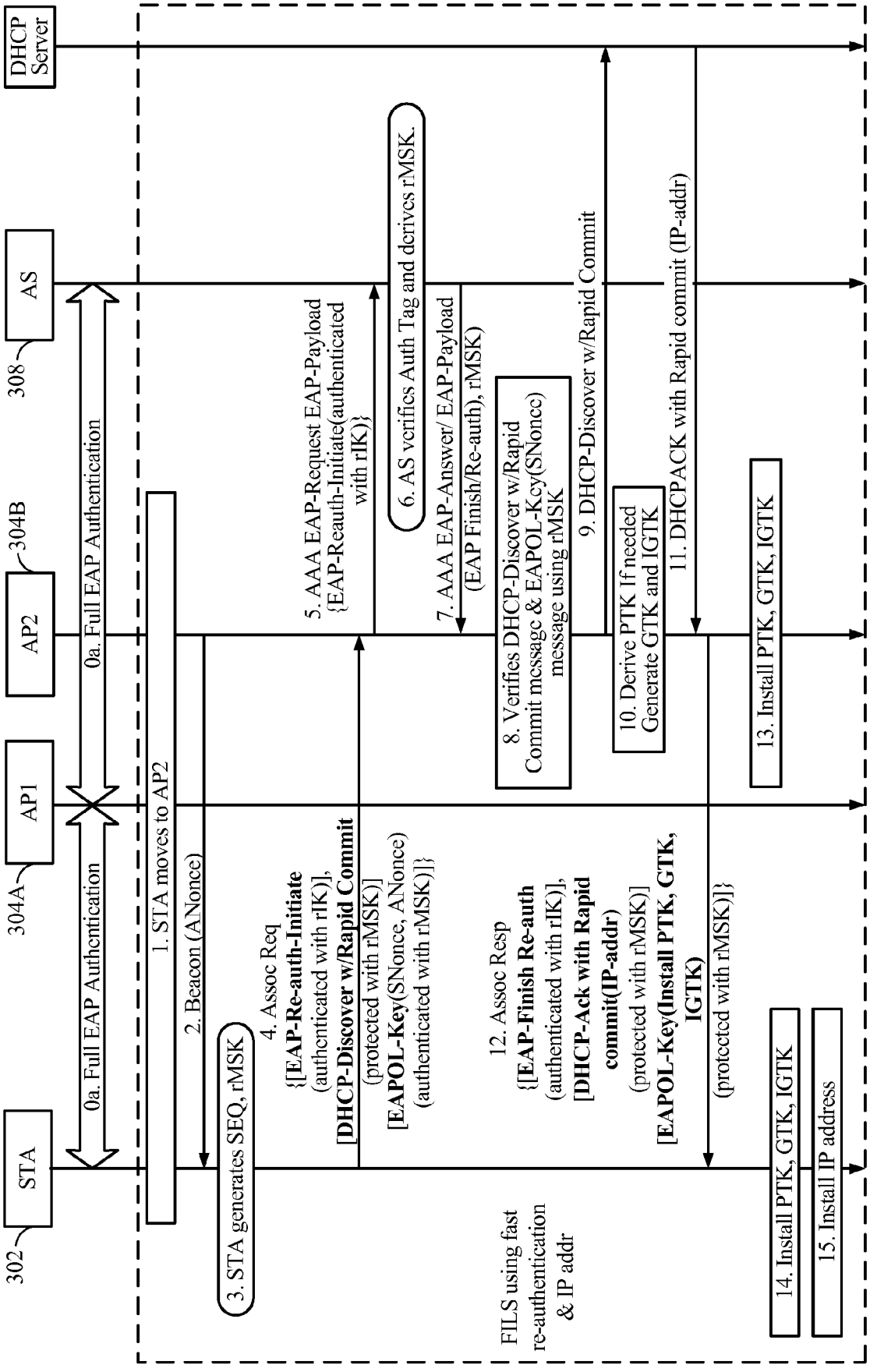

FIG. 5 (Option 1a)

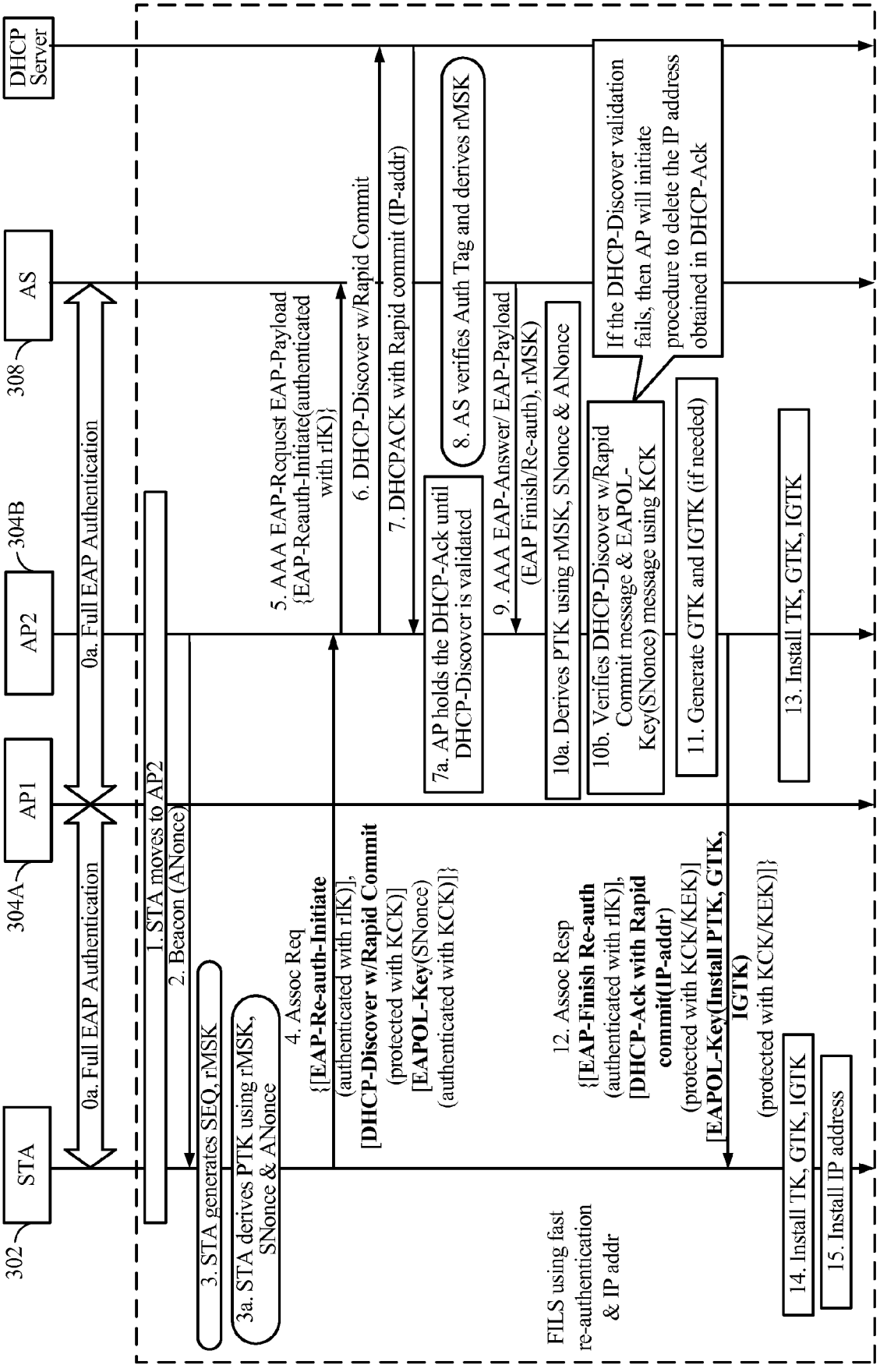

FIG. 6 (Option 1b)

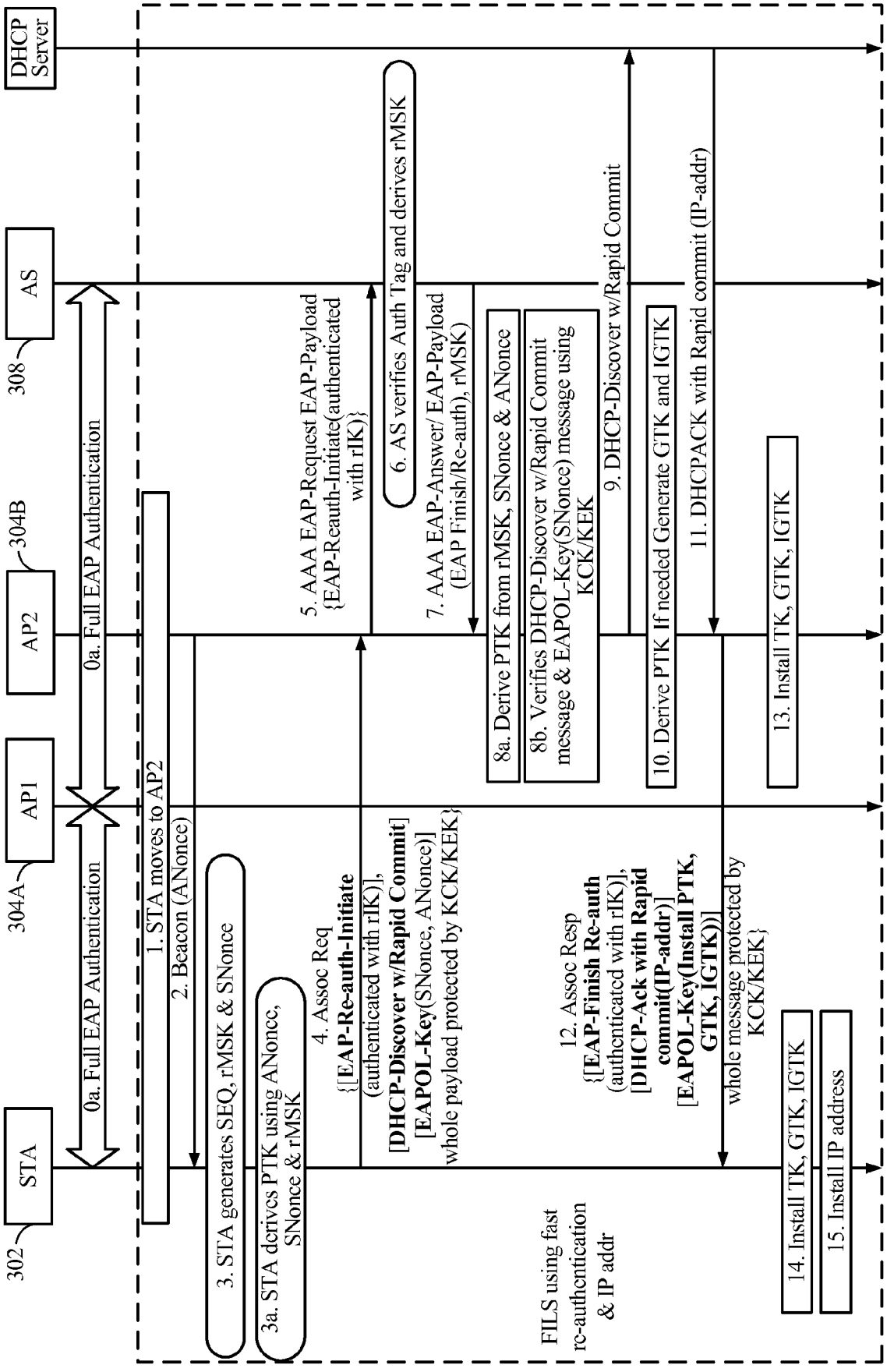

FIG. 7 (Option 2)

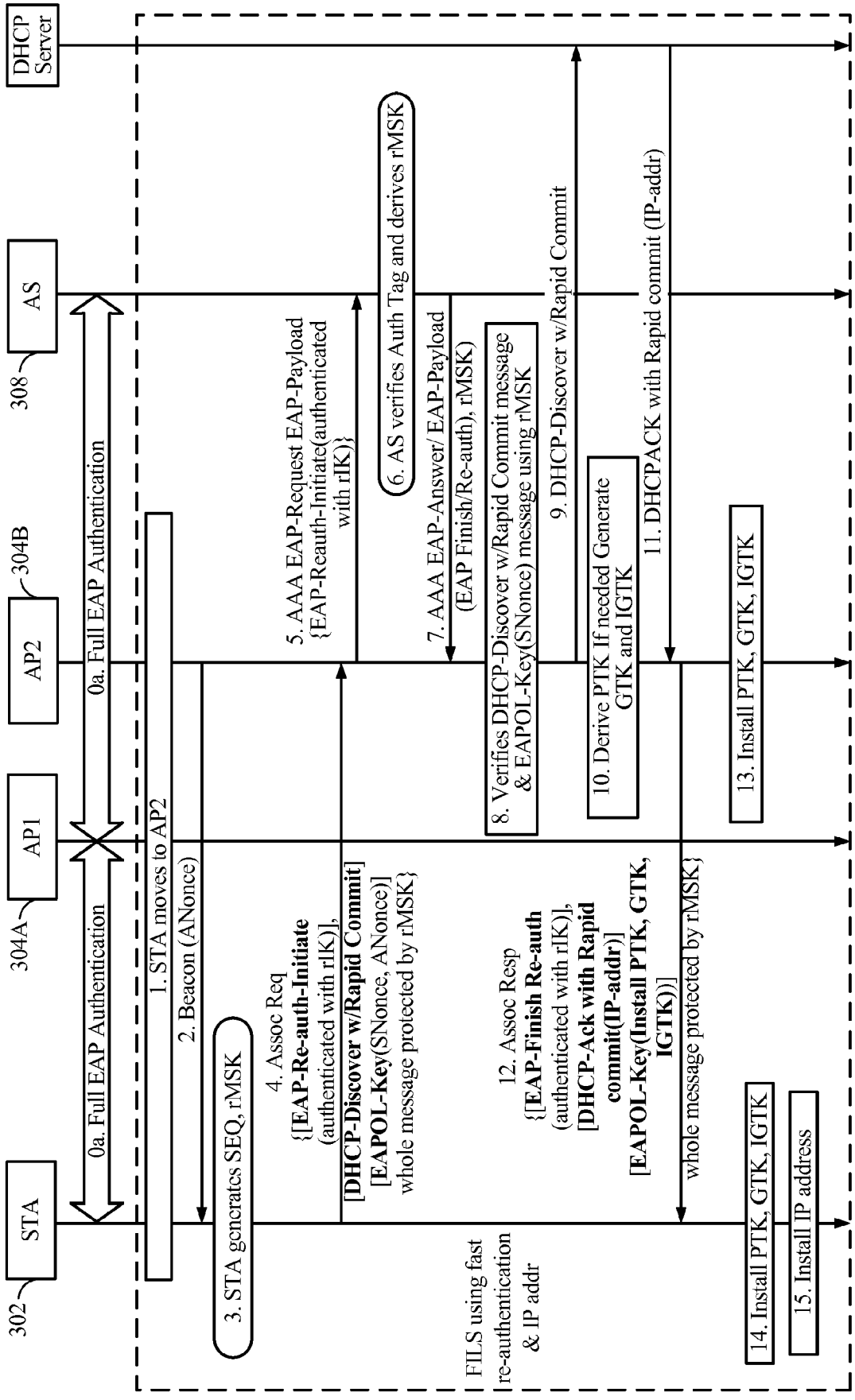

FIG. 8 (Option 2a)

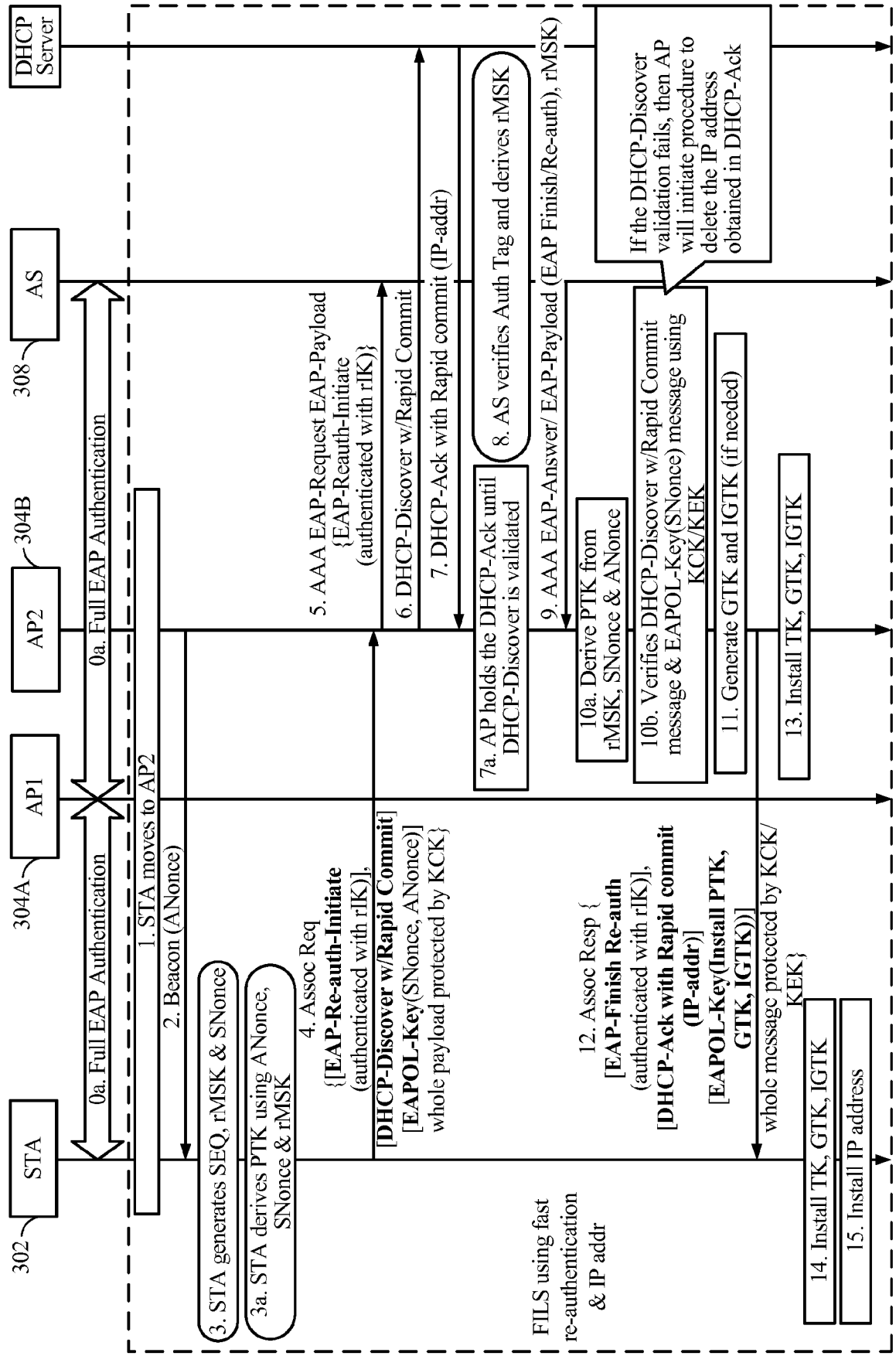

FIG. 9 (Option 2b)

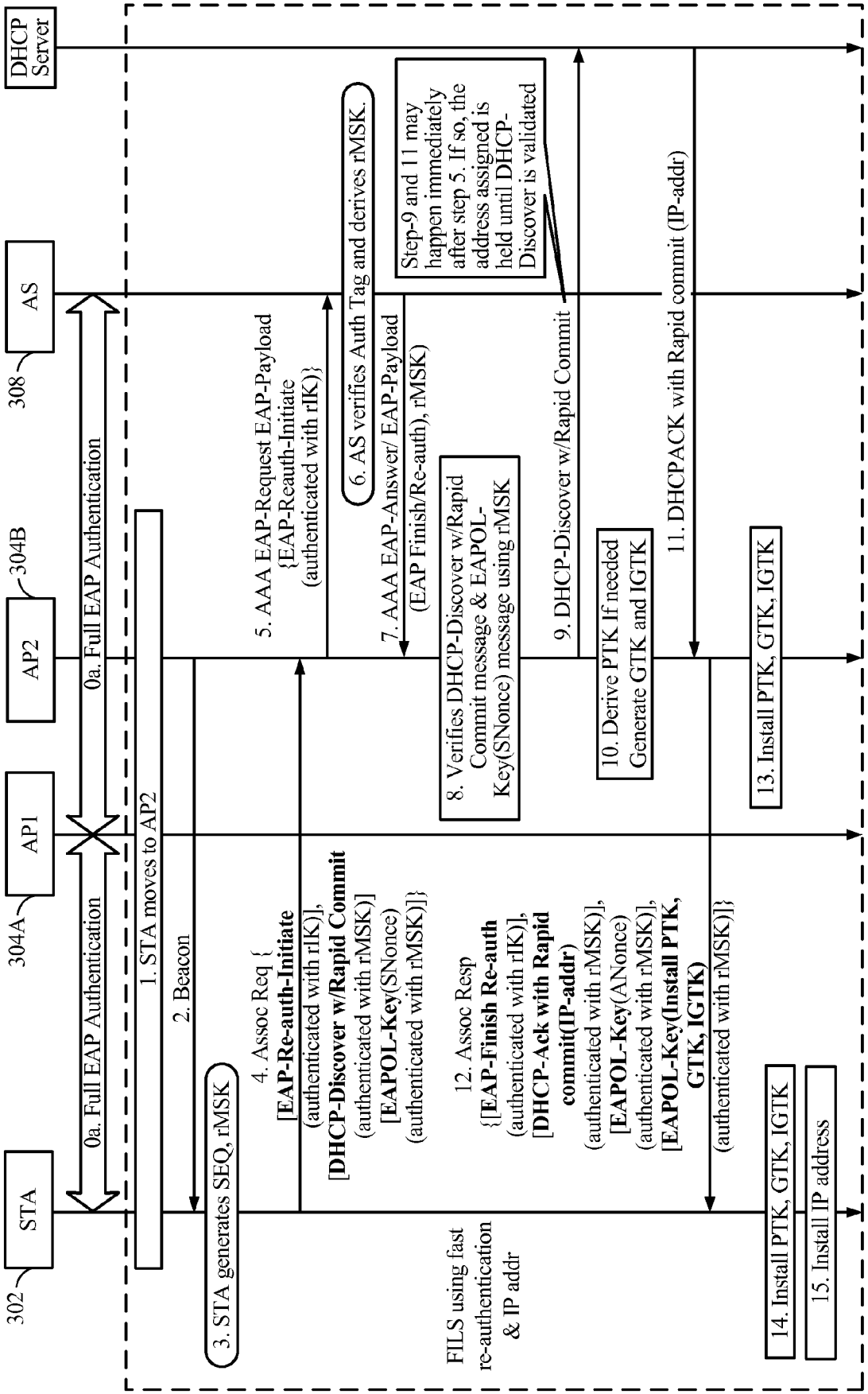

FIG. 10 (Option 3)

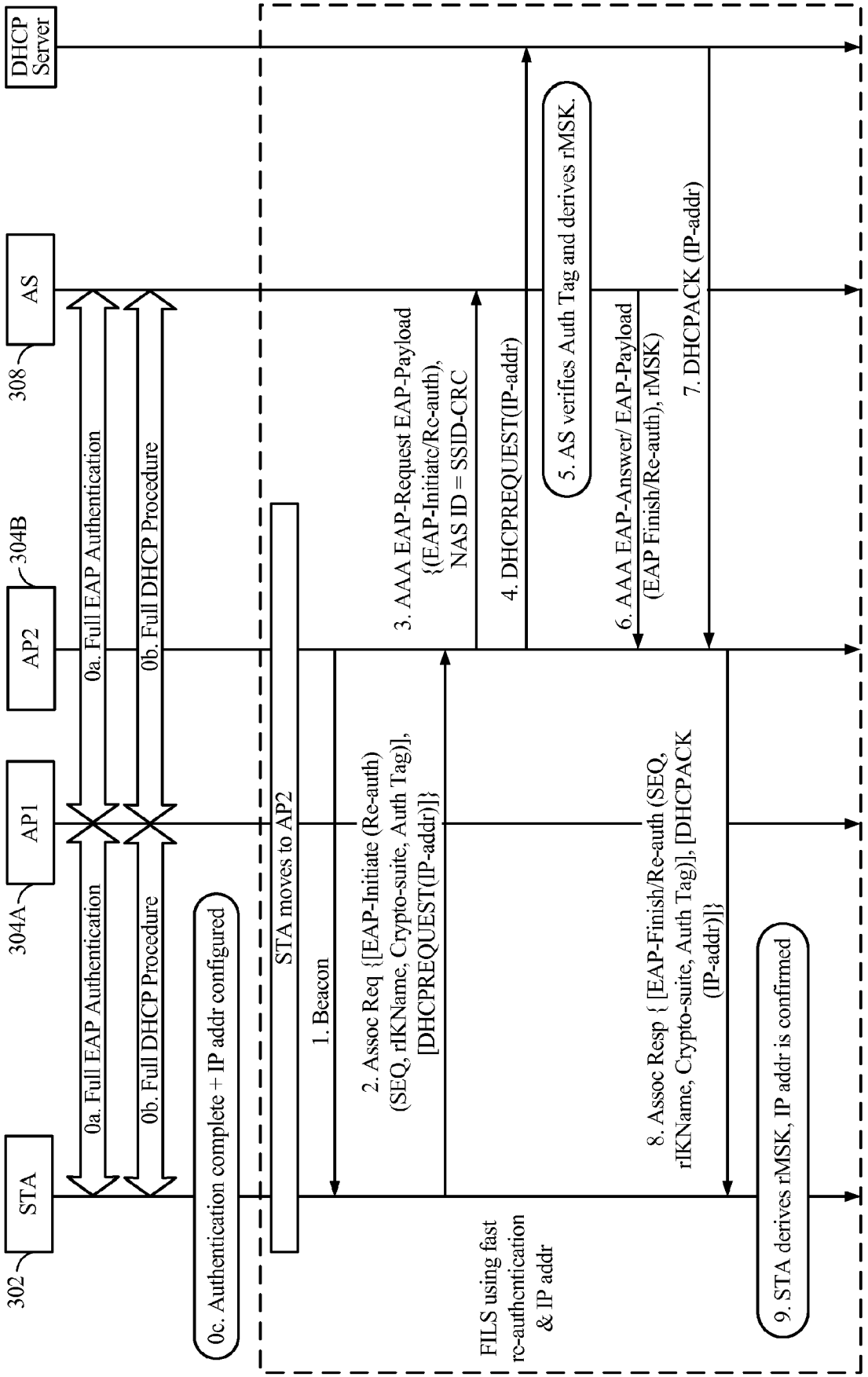

FIG. 11 (Option 5)

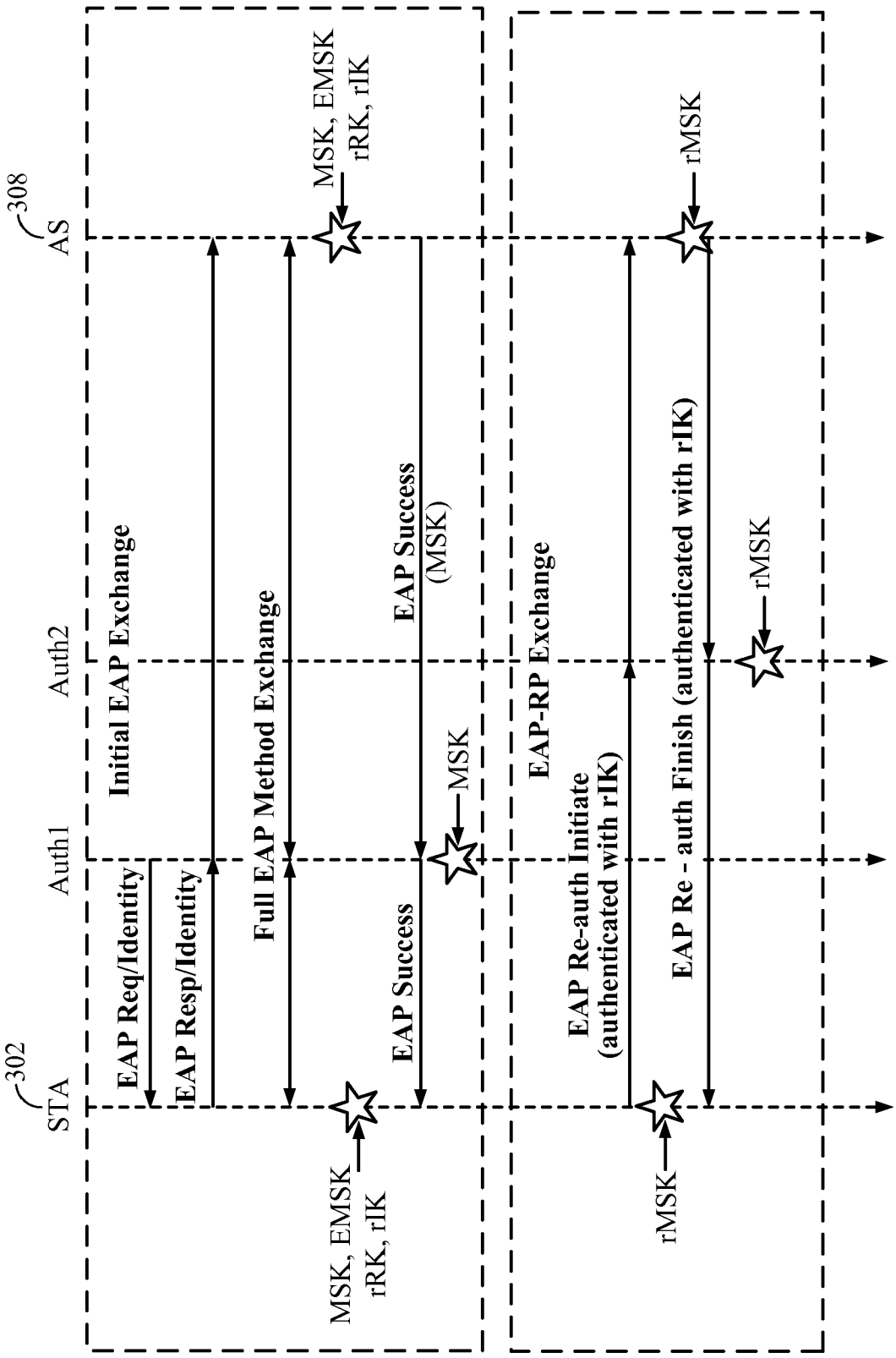
STA
302
Auth1
Auth2
AS
308
Initial EAP Exchange
EAP Req/Identity
EAP Resp/Identity
Full EAP Method Exchange
MSK, EMSK
rRK, rIK
EAP Success
EAP Success
(MSK)
MSK
MSK, EMSK
rRK, rIK
EAP-RP Exchange
EAP Re-auth Initiate
(authenticated with rIK)
EAP Re - auth Finish (authenticated with rIK)
rMSK
rMSK
rMSK

FIG. 12

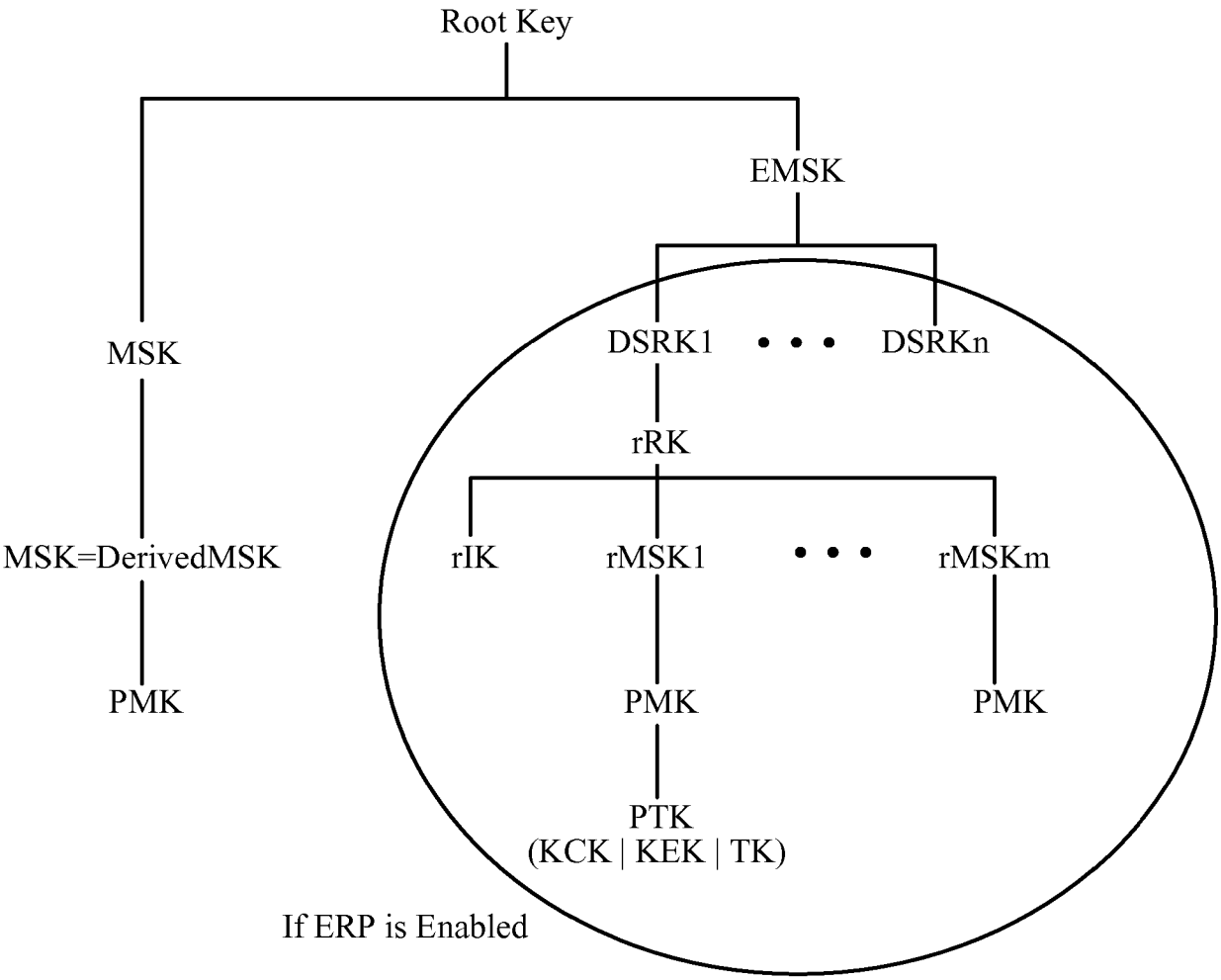
Root Key
EMSK
MSK
DSRK1
DSRKn
rRK
MSK=DerivedMSK
rIK
rMSK1
rMSKm
PMK
PMK
PMK
PTK
(KCK | KEK | TK)
If ERP is Enabled

FIG. 13

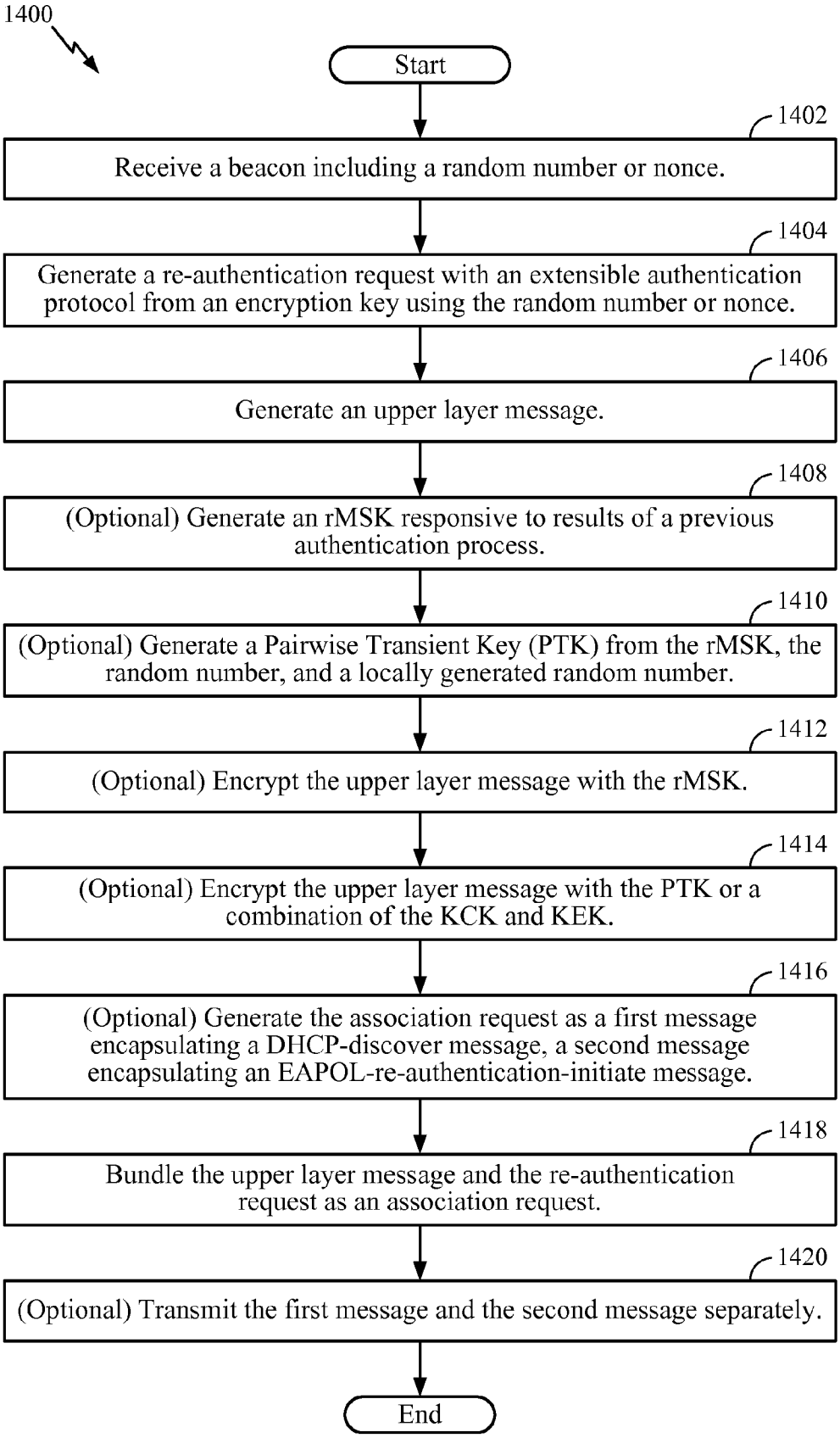
1400
Start
1402
Receive a beacon including a random number or nonce.
1404
Generate a re-authentication request with an extensible authentication protocol from an encryption key using the random number or nonce.
1406
Generate an upper layer message.
1408
(Optional) Generate an rMSK responsive to results of a previous authentication process.
1410
(Optional) Generate a Pairwise Transient Key (PTK) from the rMSK, the random number, and a locally generated random number.
1412
(Optional) Encrypt the upper layer message with the rMSK.
1414
(Optional) Encrypt the upper layer message with the PTK or a combination of the KCK and KEK.
1416
(Optional) Generate the association request as a first message encapsulating a DHCP-discover message, a second message encapsulating an EAPOL-re-authentication-initiate message.
1418
Bundle the upper layer message and the re-authentication request as an association request.
1420
(Optional) Transmit the first message and the second message separately.
End

FIG. 14

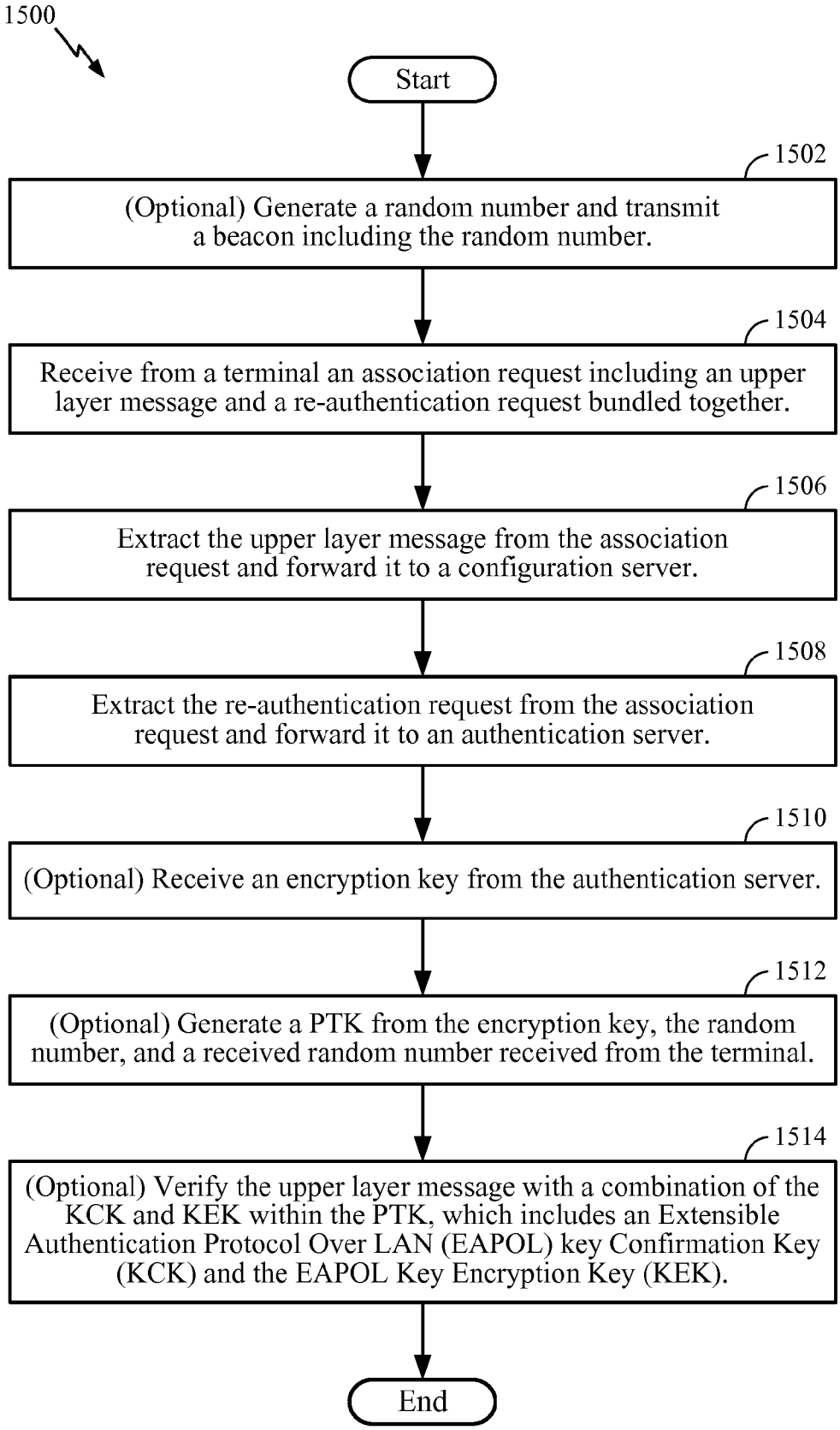
1500
Start
1502
(Optional) Generate a random number and transmit a beacon including the random number.
1504
Receive from a terminal an association request including an upper layer message and a re-authentication request bundled together.
1506
Extract the upper layer message from the association request and forward it to a configuration server.
1508
Extract the re-authentication request from the association request and forward it to an authentication server.
1510
(Optional) Receive an encryption key from the authentication server.
1512
(Optional) Generate a PTK from the encryption key, the random number, and a received random number received from the terminal.
1514
(Optional) Verify the upper layer message with a combination of the KCK and KEK within the PTK, which includes an Extensible Authentication Protocol Over LAN (EAPOL) key Confirmation Key (KCK) and the EAPOL Key Encryption Key (KEK).
End

FIG. 15

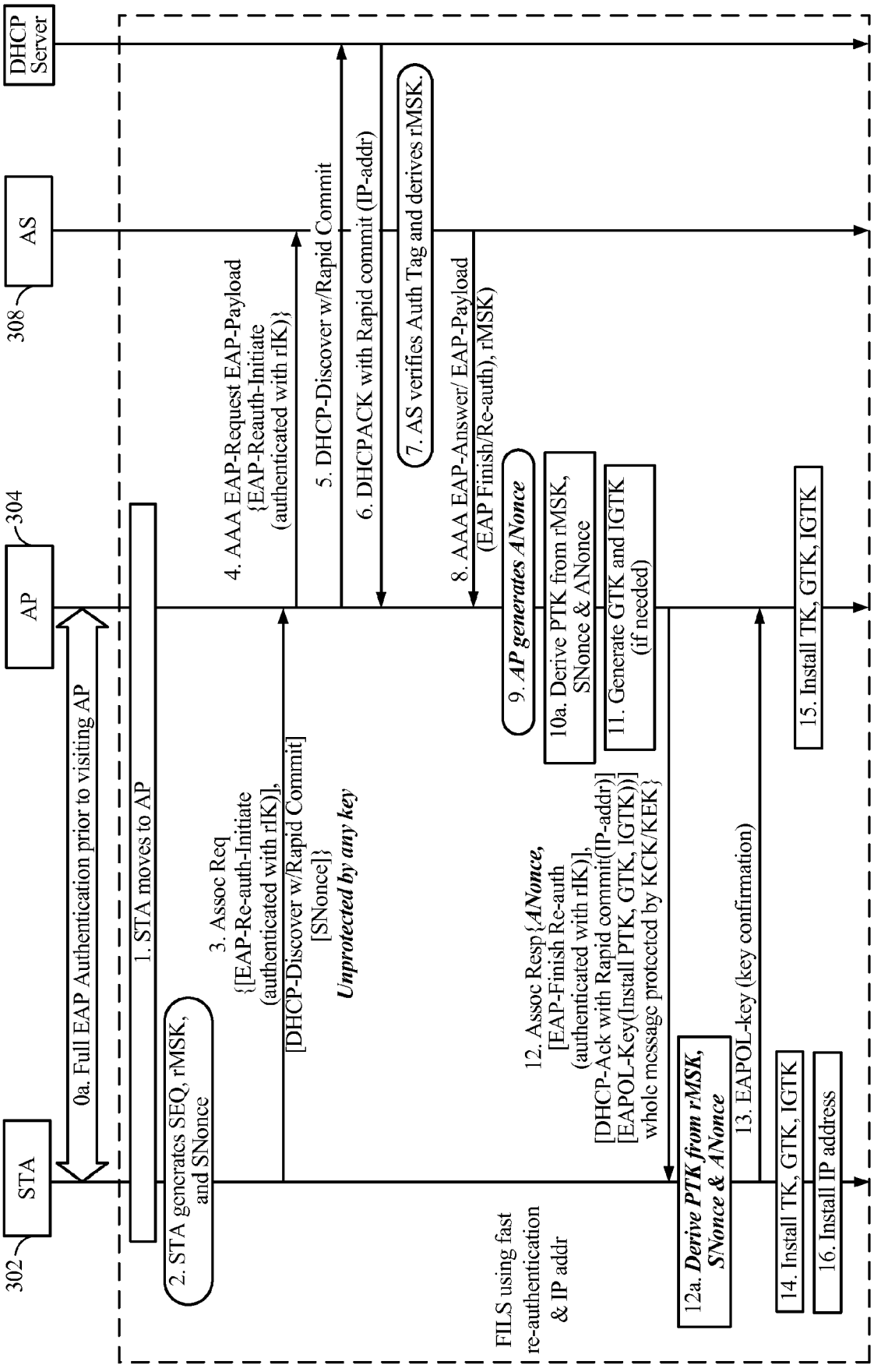
STA
AP
AS
DHCP Server
302
304
308
0a. Full EAP Authentication prior to visiting AP
1. STA moves to AP
2. STA generates SEQ, rMSK, and SNonce
3. Assoc Req {[EAP-Re-auth-Initiate (authenticated with rIK)], [DHCP-Discover w/Rapid Commit] [SNonce]} Unprotected by any key
4. AAA EAP-Request EAP-Payload {EAP-Reauth-Initiate (authenticated with rIK)}
5. DHCP-Discover w/Rapid Commit
6. DHCPACK with Rapid commit (IP-addr)
7. AS verifies Auth Tag and derives rMSK.
8. AAA EAP-Answer/ EAP-Payload (EAP Finish/Re-auth), rMSK)
9. AP generates ANonce
10a. Derive PTK from rMSK, SNonce & ANonce
11. Generate GTK and IGTK (if needed)
12. Assoc Resp {ANonce, [EAP-Finish Re-auth (authenticated with rIK)], [DHCP-Ack with Rapid commit(IP-addr)] [EAPOL-Key(Install PTK, GTK, IGTK))] whole message protected by KCK/KEK}
12a. Derive PTK from rMSK, SNonce & ANonce
13. EAPOL-key (key confirmation)
14. Install TK, GTK, IGTK
15. Install TK, GTK, IGTK
16. Install IP address
FILS using fast re-authentication & IP addr

FIG. 16

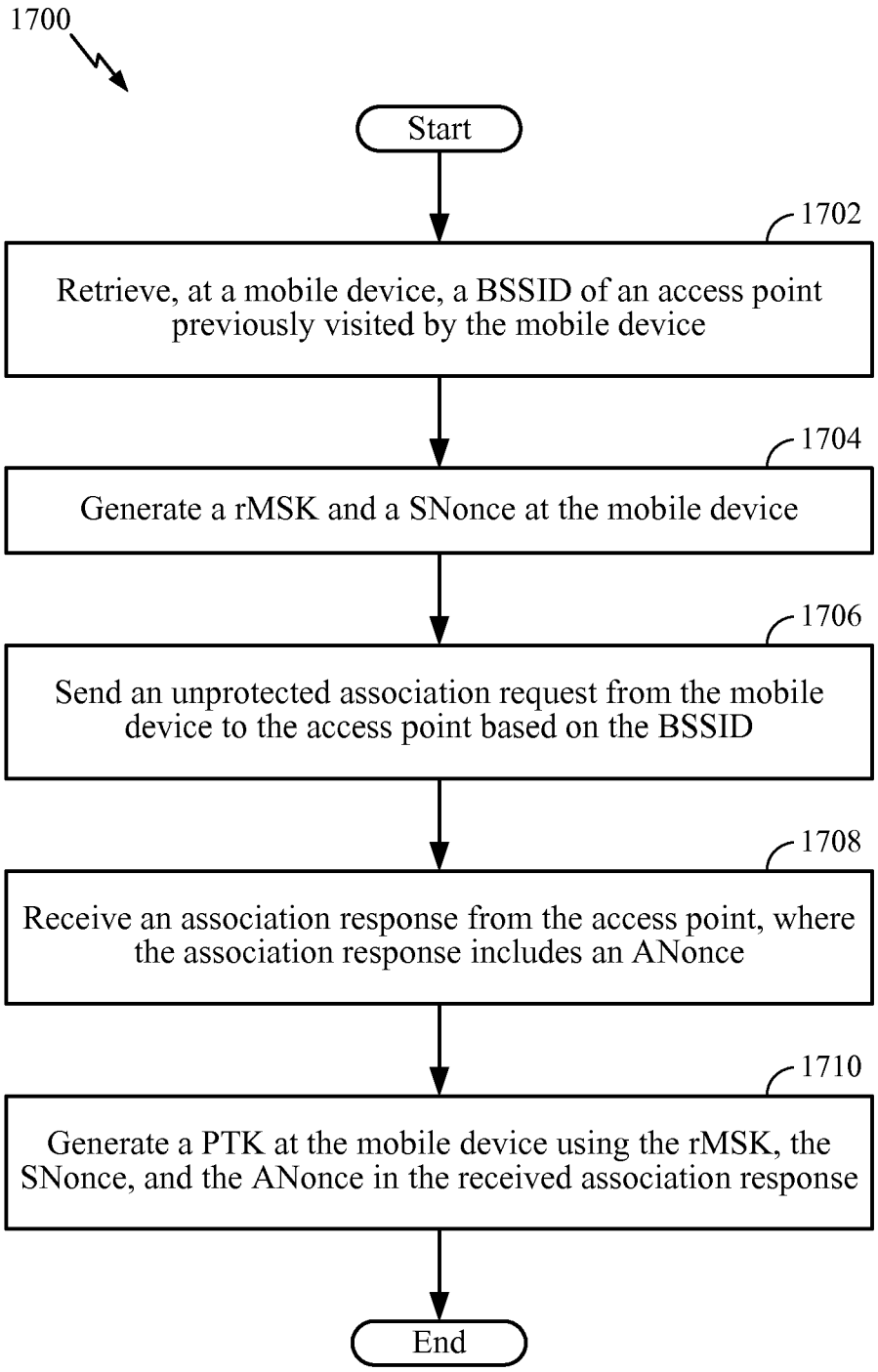
1700
Start
1702
Retrieve, at a mobile device, a BSSID of an access point previously visited by the mobile device
1704
Generate a rMSK and a SNonce at the mobile device
1706
Send an unprotected association request from the mobile device to the access point based on the BSSID
1708
Receive an association response from the access point, where the association response includes an ANonce
1710
Generate a PTK at the mobile device using the rMSK, the SNonce, and the ANonce in the received association response
End

FIG. 17

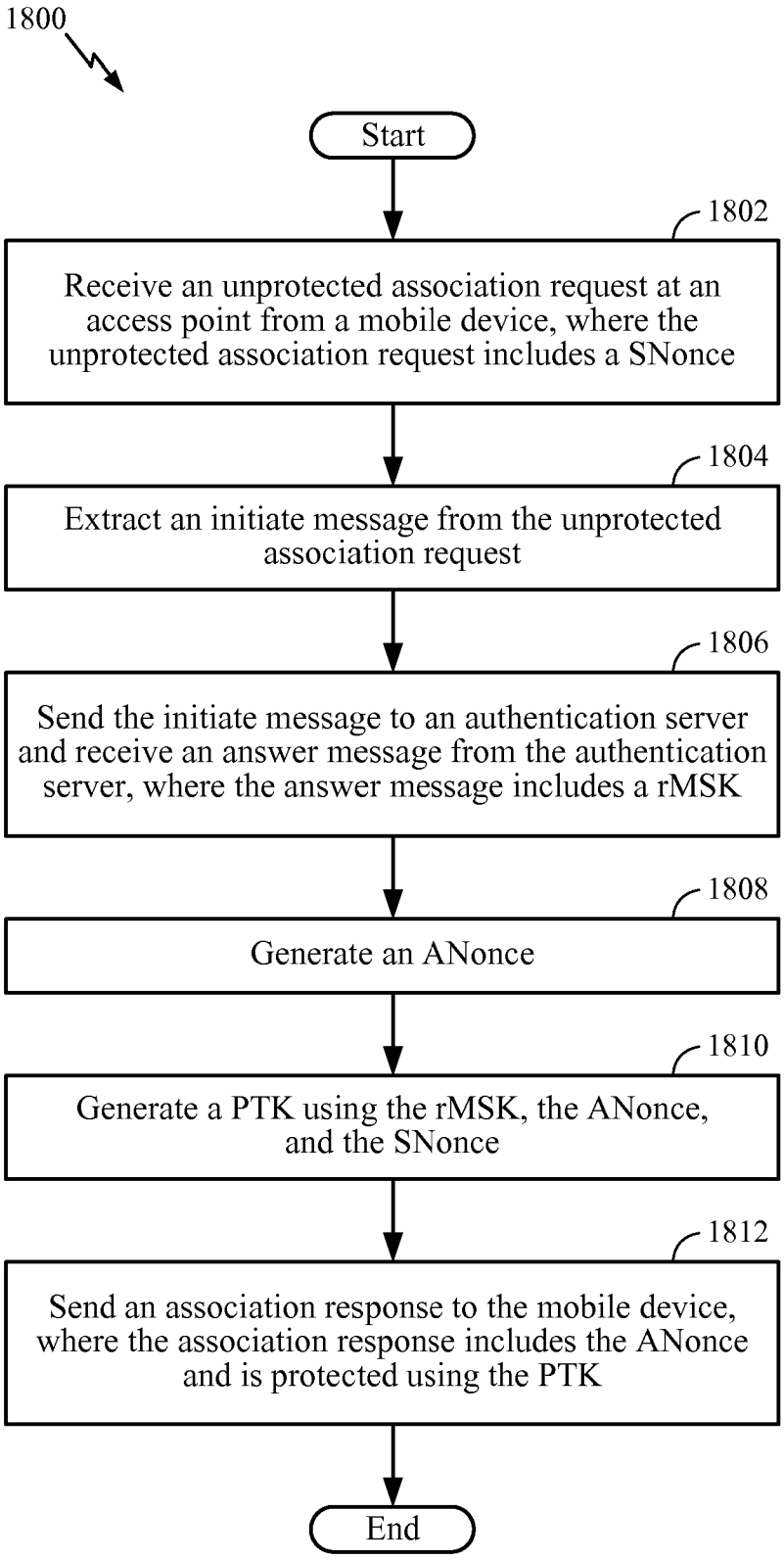
1800
Start
1802
Receive an unprotected association request at an access point from a mobile device, where the unprotected association request includes a SNonce
1804
Extract an initiate message from the unprotected association request
1806
Send the initiate message to an authentication server and receive an answer message from the authentication server, where the answer message includes a rMSK
1808
Generate an ANonce
1810
Generate a PTK using the rMSK, the ANonce, and the SNonce
1812
Send an association response to the mobile device, where the association response includes the ANonce and is protected using the PTK
End

FIG. 18

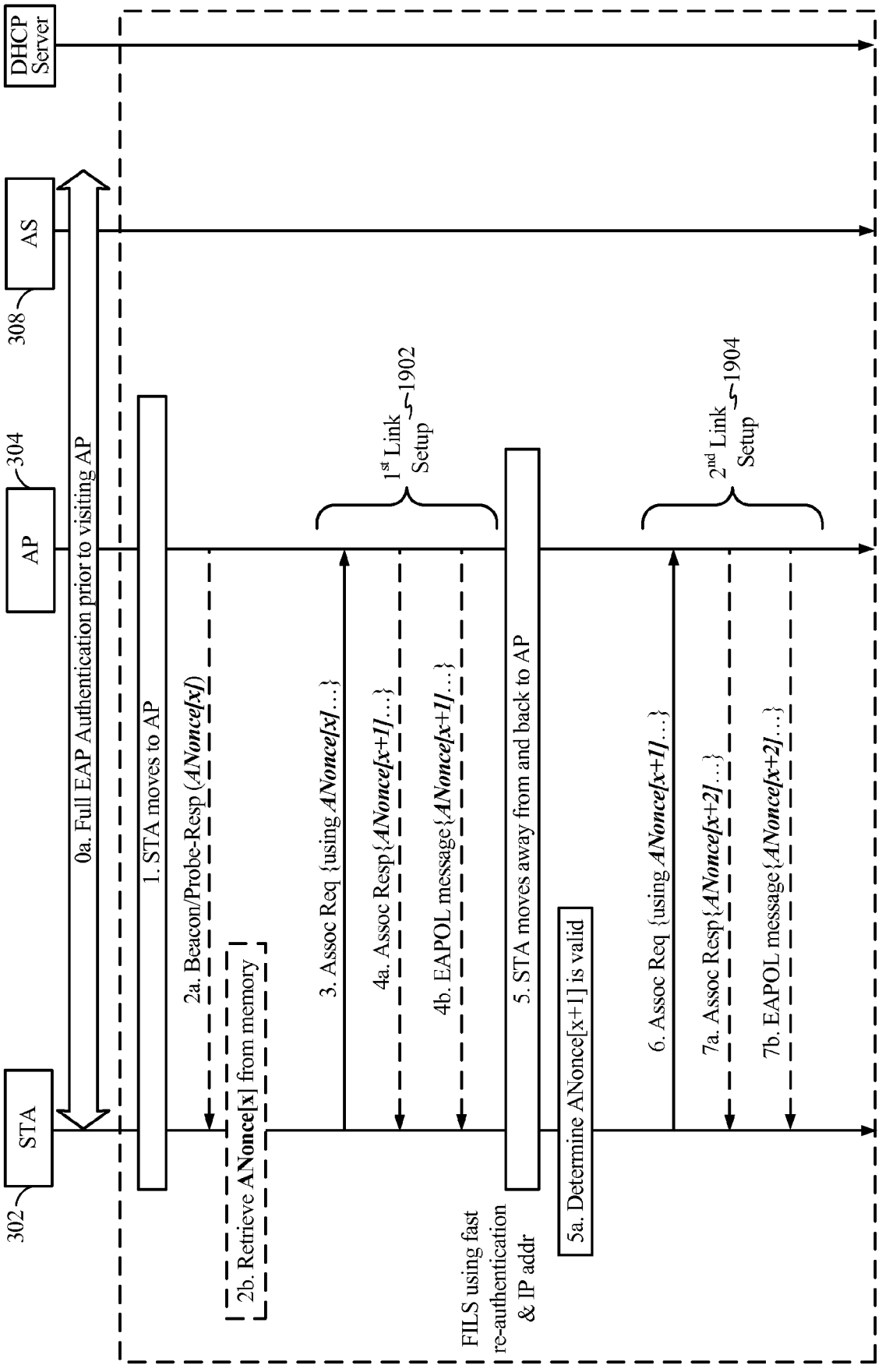
DHCP Server
AS
308
AP
304
STA
302
0a. Full EAP Authentication prior to visiting AP
1. STA moves to AP
2a. Beacon/Probe-Resp (ANonce[x])
2b. Retrieve ANonce[x] from memory
3. Assoc Req {using ANonce[x]...}
4a. Assoc Resp{ANonce[x+1]...}
4b. EAPOL message{ANonce[x+1]...}
1st Link Setup
1902
FILS using fast re-authentication & IP addr
5. STA moves away from and back to AP
5a. Determine ANonce[x+1] is valid
6. Assoc Req {using ANonce[x+1]...}
7a. Assoc Resp{ANonce[x+2]...}
7b. EAPOL message{ANonce[x+2]...}
2nd Link Setup
1904

FIG. 19

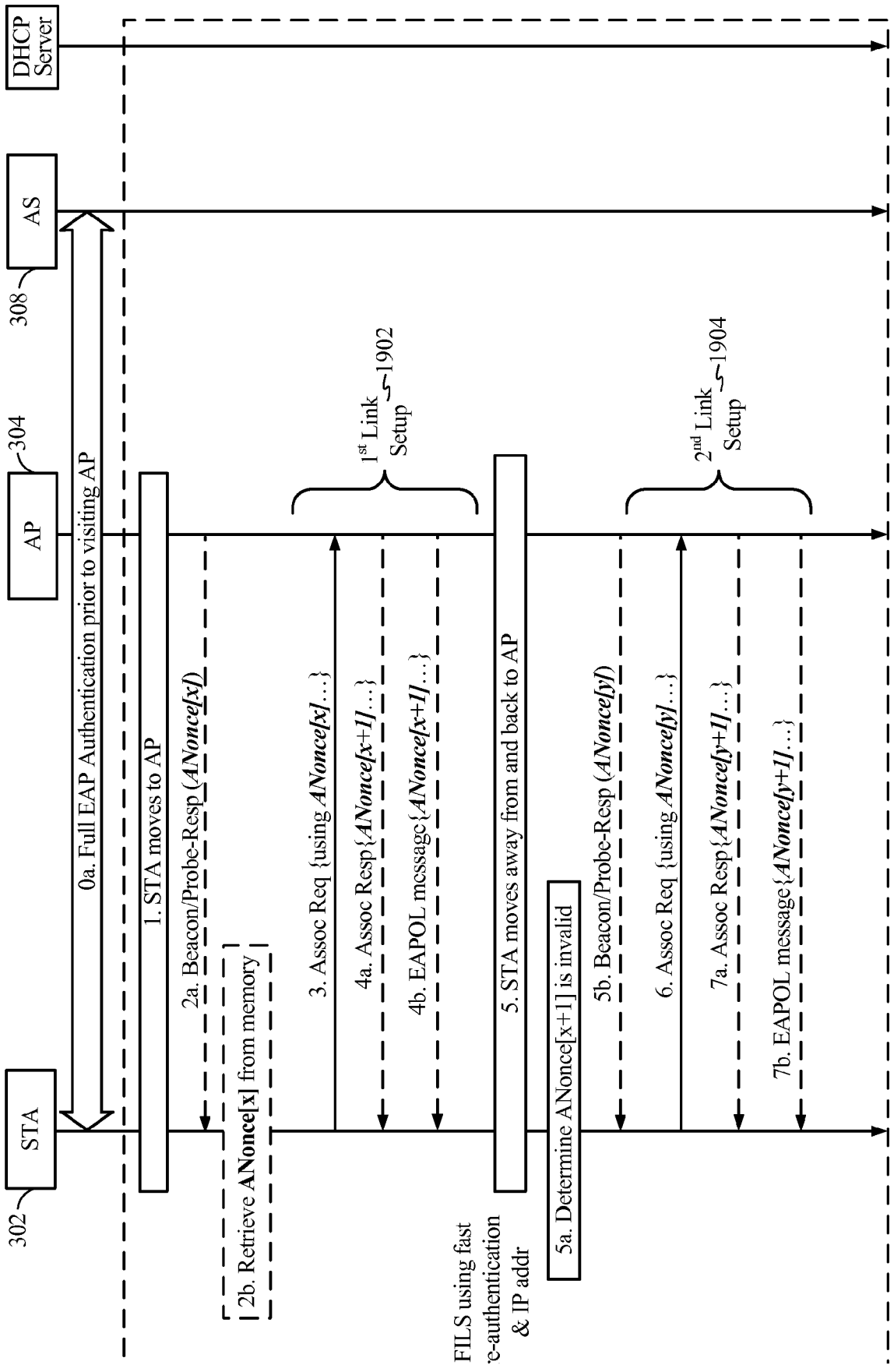
DHCP Server
AS
308
AP
304
STA
302
0a. Full EAP Authentication prior to visiting AP
1. STA moves to AP
2a. Beacon/Probe-Resp (ANonce[x])
2b. Retrieve ANonce[x] from memory
3. Assoc Req {using ANonce[x]...}
4a. Assoc Resp{ANonce[x+1]...}
4b. EAPOL mcssagc{ANonce[x+1]...}
1st Link Setup
1902
FILS using fast re-authentication & IP addr
5. STA moves away from and back to AP
5a. Determine ANonce[x+1] is invalid
5b. Beacon/Probe-Resp (ANonce[y])
6. Assoc Req {using ANonce[y]...}
7a. Assoc Resp{ANonce[y+1]...}
7b. EAPOL message{ANonce[y+1]...}
2nd Link Setup
1904

FIG. 20

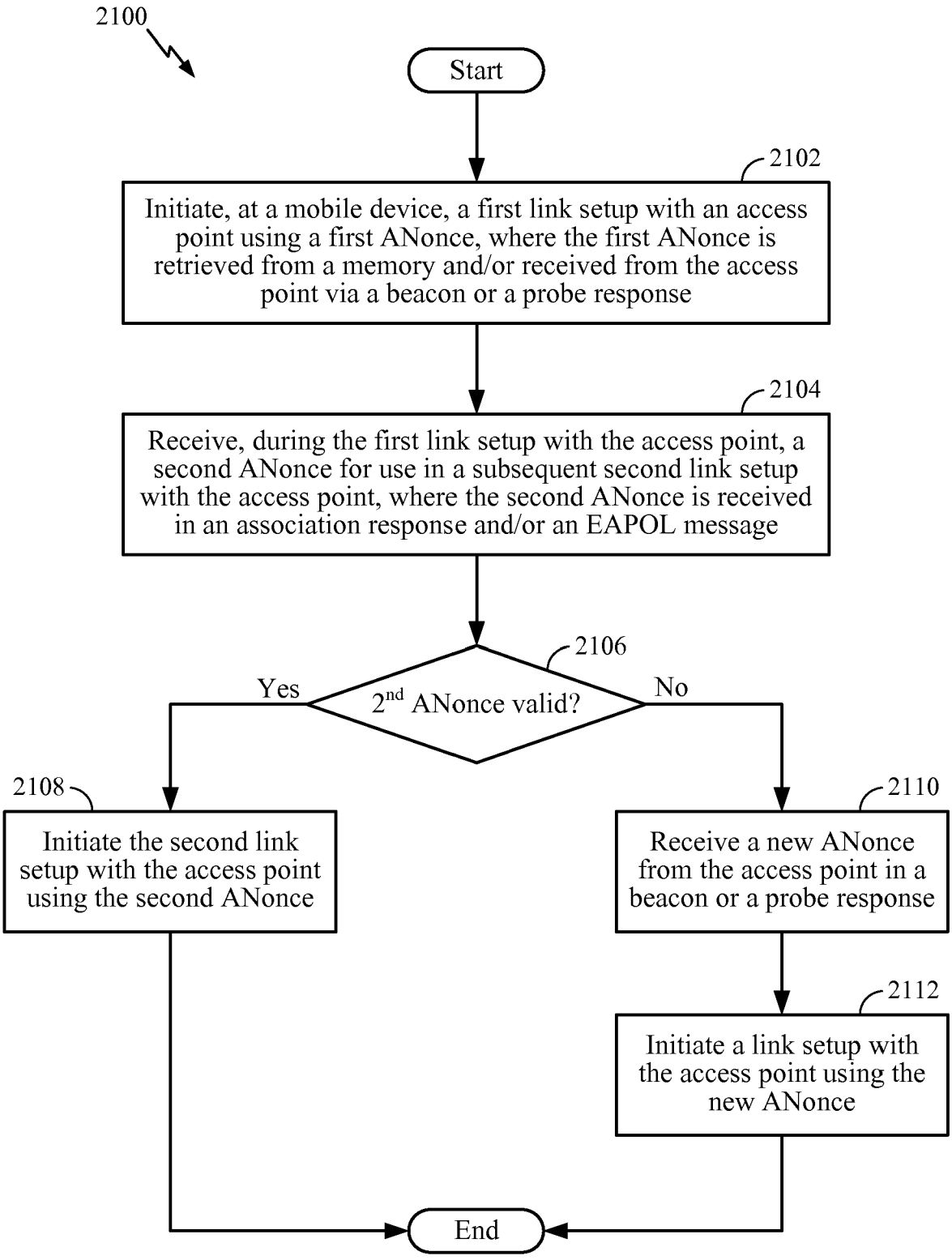
2100
Start
2102
Initiate, at a mobile device, a first link setup with an access point using a first ANonce, where the first ANonce is retrieved from a memory and/or received from the access point via a beacon or a probe response
2104
Receive, during the first link setup with the access point, a second ANonce for use in a subsequent second link setup with the access point, where the second ANonce is received in an association response and/or an EAPOL message
2106
2nd ANonce valid?
Yes
No
2108
Initiate the second link setup with the access point using the second ANonce
2110
Receive a new ANonce from the access point in a beacon or a probe response
2112
Initiate a link setup with the access point using the new ANonce
End

FIG. 21

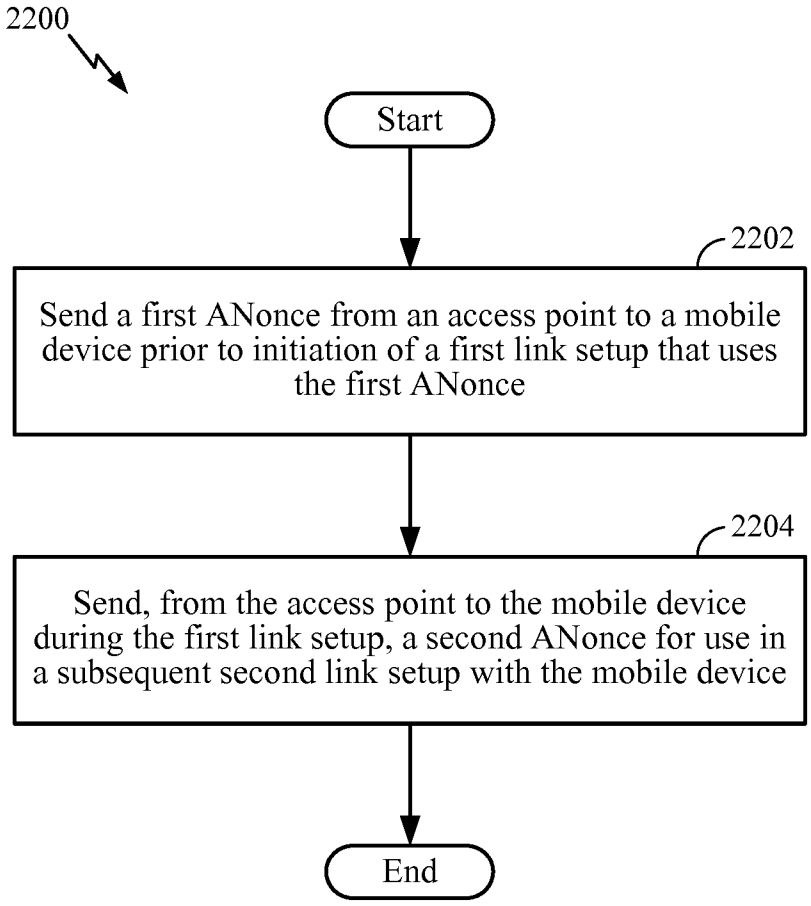
2200
Start
2202
Send a first ANonce from an access point to a mobile device prior to initiation of a first link setup that uses the first ANonce
2204
Send, from the access point to the mobile device during the first link setup, a second ANonce for use in a subsequent second link setup with the mobile device
End

FIG. 22

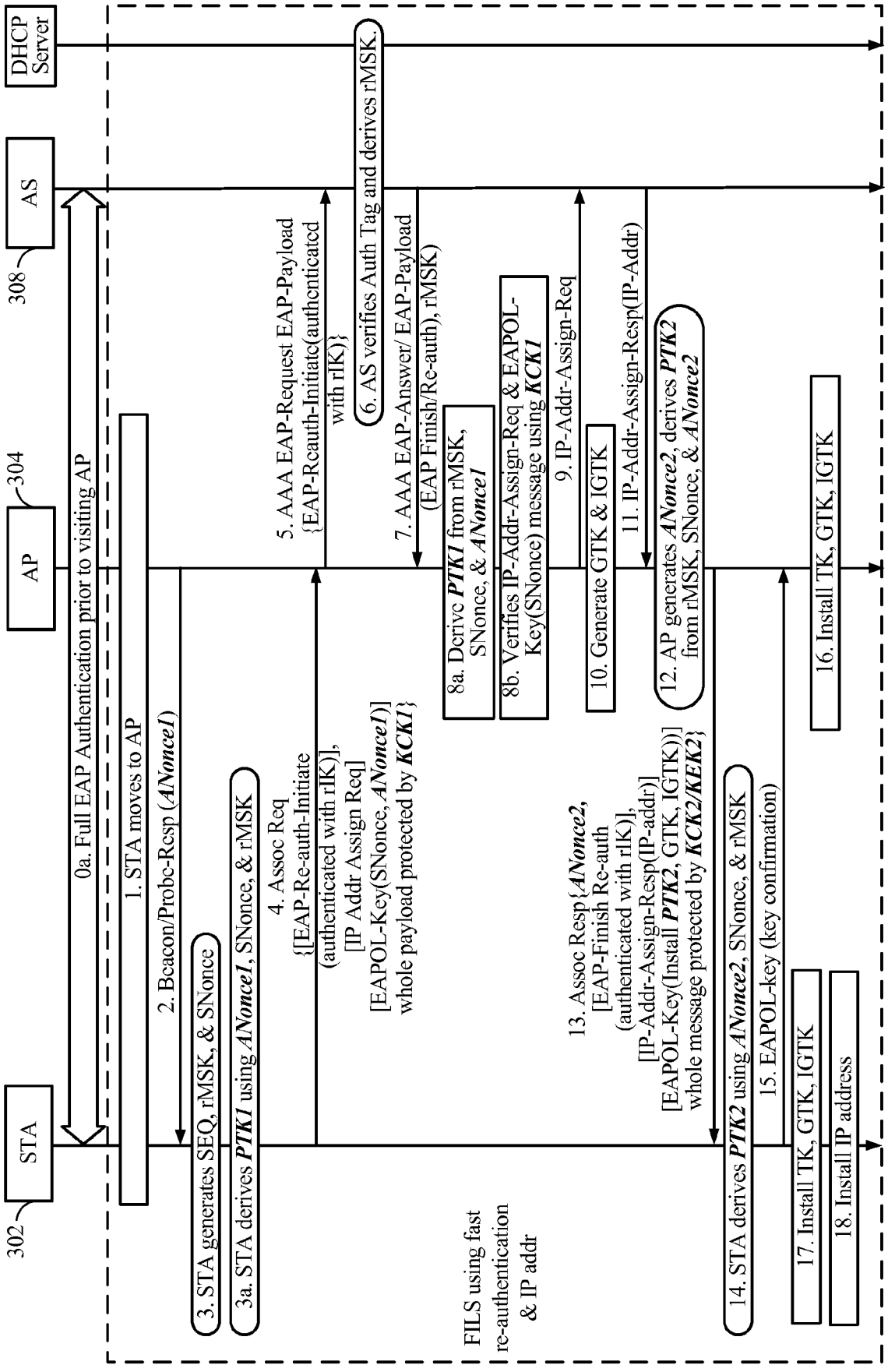
STA
AP
AS
DHCP Server
302
304
308
0a. Full EAP Authentication prior to visiting AP
1. STA moves to AP
2. Bcacon/Probc-Rcsp (ANonce1)
3. STA generates SEQ, rMSK, & SNonce
3a. STA derives PTK1 using ANonce1, SNonce, & rMSK
4. Assoc Req
{[EAP-Re-auth-Initiate
(authenticated with rIK)],
[IP Addr Assign Req]
[EAPOL-Key(SNonce, ANonce1)]
whole payload protected by KCK1}
5. AAA EAP-Request EAP-Payload
{EAP-Rcauth-Initiate(authenticated
with rIK)}
6. AS verifies Auth Tag and derives rMSK
7. AAA EAP-Answer/ EAP-Payload
(EAP Finish/Re-auth), rMSK)
8a. Derive PTK1 from rMSK,
SNonce, & ANonce1
8b. Verifies IP-Addr-Assign-Req & EAPOL-
Key(SNonce) message using KCK1
9. IP-Addr-Assign-Req
10. Generate GTK & IGTK
11. IP-Addr-Assign-Resp(IP-Addr)
12. AP generates ANonce2, derives PTK2
from rMSK, SNonce, & ANonce2
13. Assoc Resp{,ANonce2,
[EAP-Finish Re-auth
(authenticated with rIK)],
[IP-Addr-Assign-Resp(IP-addr)]
[EAPOL-Key(Install PTK2, GTK, IGTK))]
whole message protected by KCK2/KEK2}
14. STA derives PTK2 using ANonce2, SNonce, & rMSK
15. EAPOL-key (key confirmation)
16. Install TK, GTK, IGTK
17. Install TK, GTK, IGTK
18. Install IP address
FILS using fast
re-authentication
& IP addr

FIG. 23

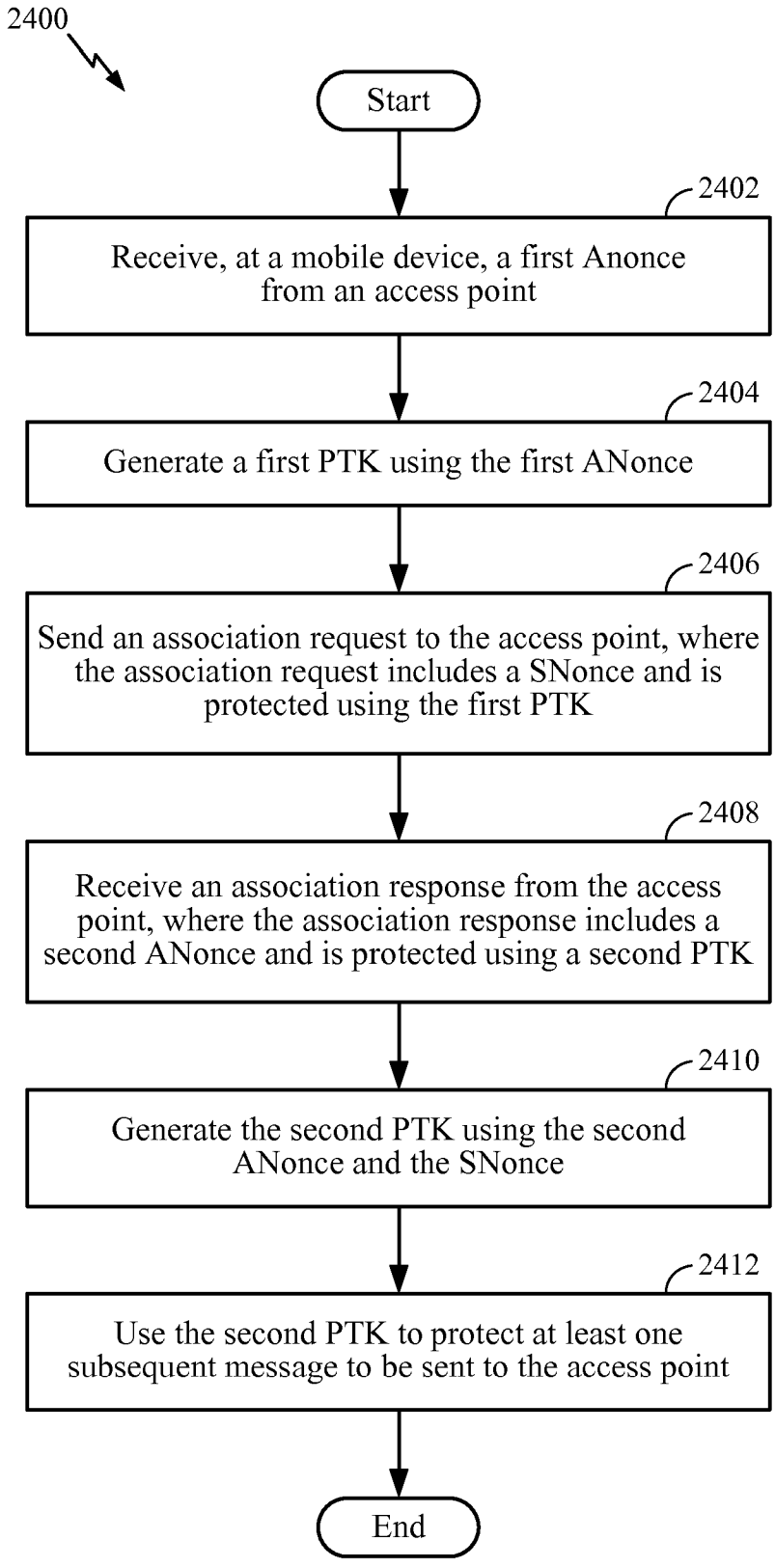
2400
Start
2402
Receive, at a mobile device, a first Anonce from an access point
2404
Generate a first PTK using the first ANonce
2406
Send an association request to the access point, where the association request includes a SNonce and is protected using the first PTK
2408
Receive an association response from the access point, where the association response includes a second ANonce and is protected using a second PTK
2410
Generate the second PTK using the second ANonce and the SNonce
2412
Use the second PTK to protect at least one subsequent message to be sent to the access point
End

FIG. 24

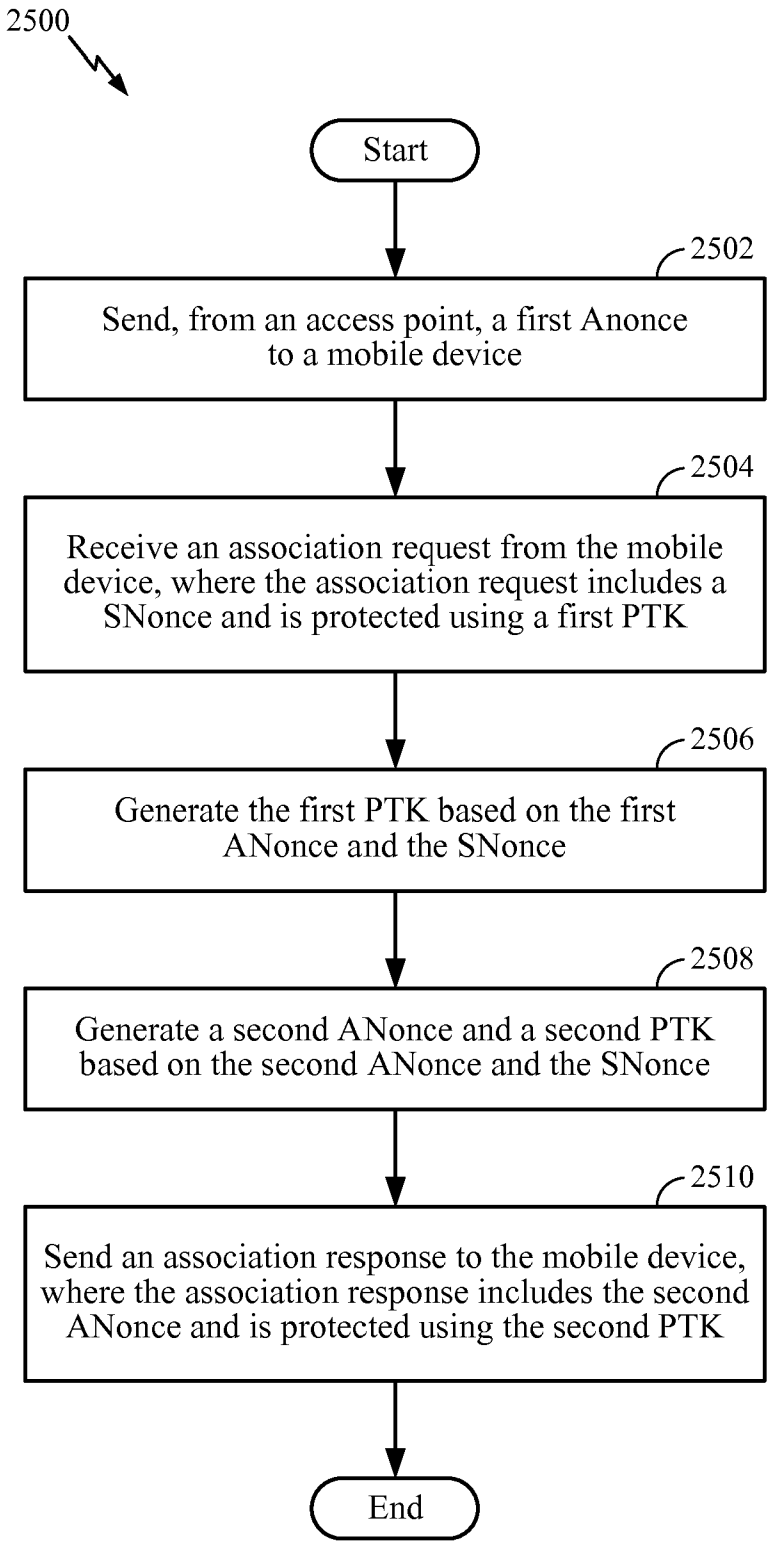
2500
Start
2502
Send, from an access point, a first Anonce to a mobile device
2504
Receive an association request from the mobile device, where the association request includes a SNonce and is protected using a first PTK
2506
Generate the first PTK based on the first ANonce and the SNonce
2508
Generate a second ANonce and a second PTK based on the second ANonce and the SNonce
2510
Send an association response to the mobile device, where the association response includes the second ANonce and is protected using the second PTK
End

FIG. 25

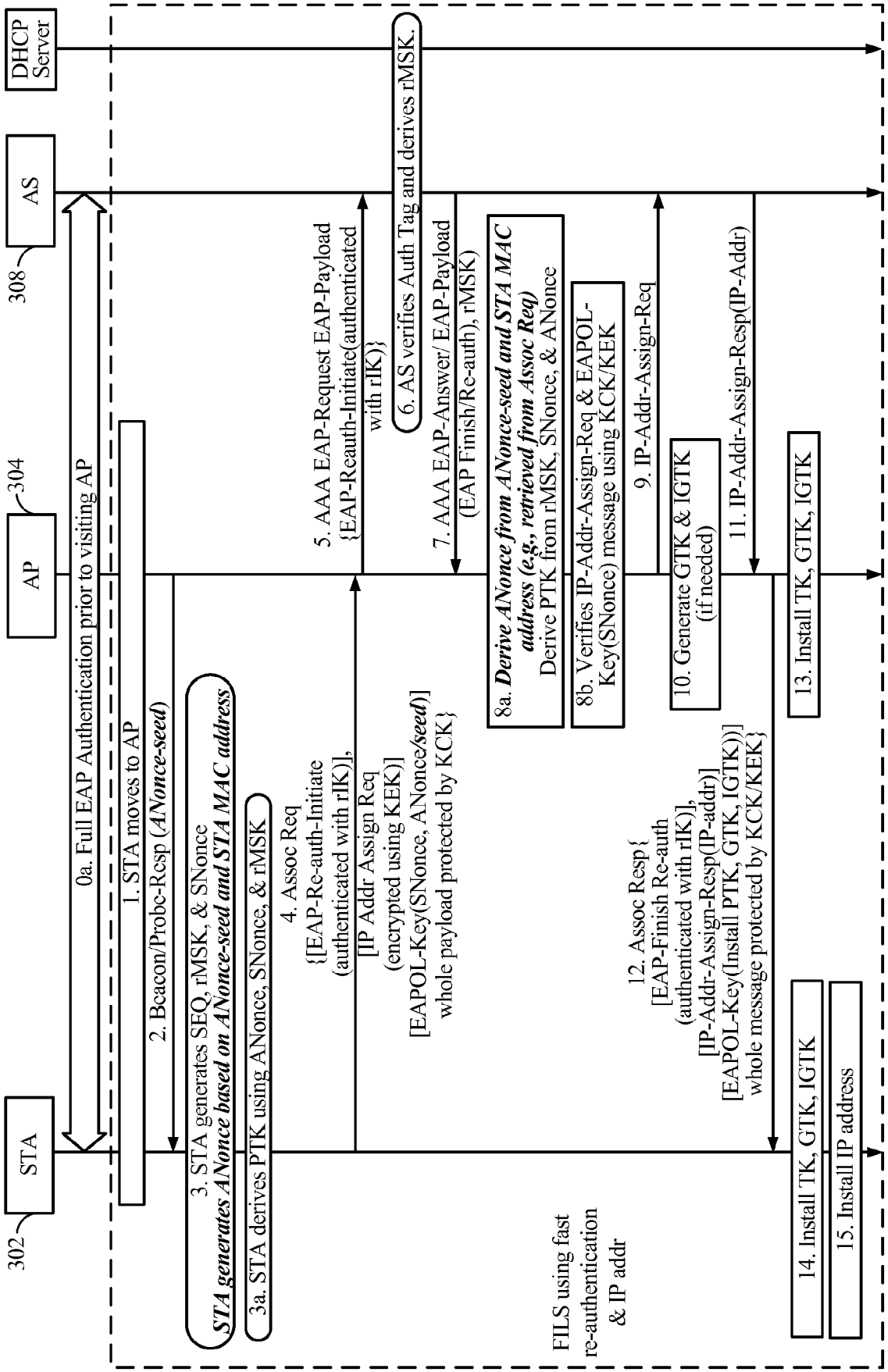
DHCP Server
AS
308
AP
304
STA
302
0a. Full EAP Authentication prior to visiting AP
1. STA moves to AP
2. Bcacon/Probe-Resp (ANonce-seed)
3. STA generates SEQ, rMSK, & SNonce
STA generates ANonce based on ANonce-seed and STA MAC address
3a. STA derives PTK using ANonce, SNonce, & rMSK
4. Assoc Req
{[EAP-Re-auth-Initiate
(authenticated with rIK)],
[IP Addr Assign Req
(encrypted using KEK)]
[EAPOL-Key(SNonce, ANonce/seed)]
whole payload protected by KCK}
5. AAA EAP-Request EAP-Payload
{EAP-Reauth-Initiate(authenticated
with rIK)}
6. AS verifies Auth Tag and derives rMSK.
7. AAA EAP-Answer/ EAP-Payload
(EAP Finish/Re-auth), rMSK)
8a. Derive ANonce from ANonce-seed and STA MAC address (e.g., retrieved from Assoc Req)
Derive PTK from rMSK, SNonce, & ANonce
8b. Verifies IP-Addr-Assign-Req & EAPOL-Key(SNonce) message using KCK/KEK
9. IP-Addr-Assign-Req
10. Generate GTK & IGTK
(if needed)
11. IP-Addr-Assign-Resp(IP-Addr)
12. Assoc Resp{
[EAP-Finish Re-auth
(authenticated with rIK)],
[IP-Addr-Assign-Resp(IP-addr)]
[EAPOL-Key(Install PTK, GTK, IGTK))]
whole message protected by KCK/KEK}
13. Install TK, GTK, IGTK
14. Install TK, GTK, IGTK
15. Install IP address
FILS using fast
re-authentication
& IP addr

FIG. 26

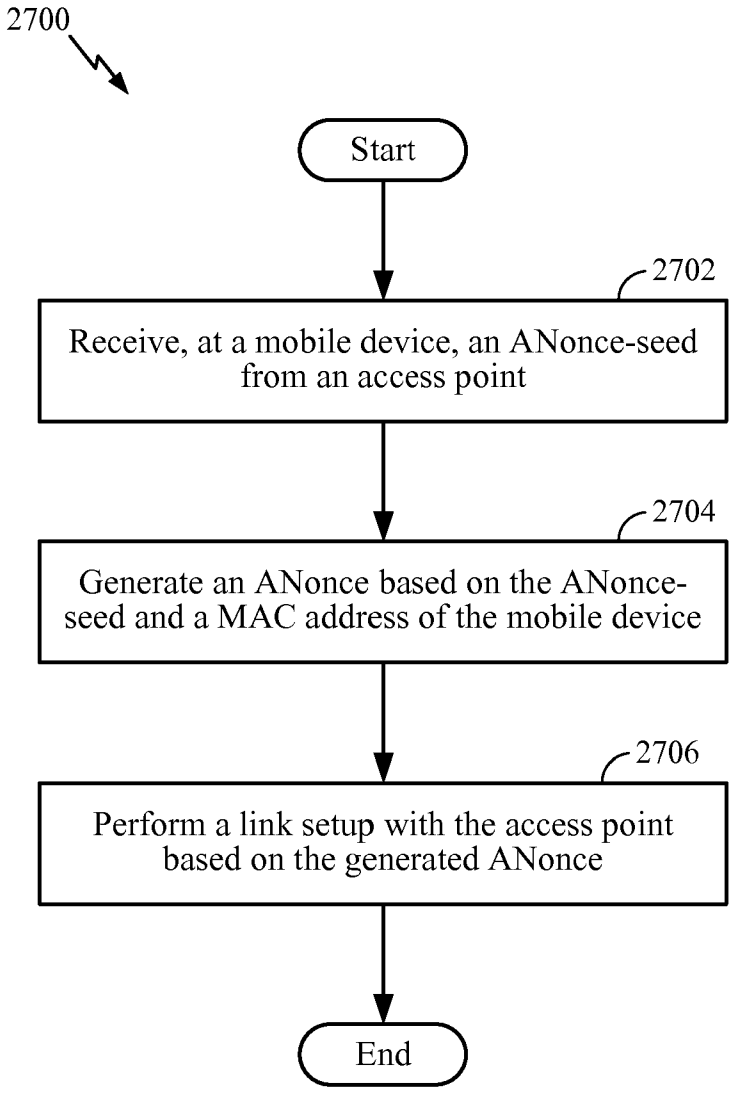
2700
Start
2702
Receive, at a mobile device, an ANonce-seed from an access point
2704
Generate an ANonce based on the ANonce-seed and a MAC address of the mobile device
2706
Perform a link setup with the access point based on the generated ANonce
End

FIG. 27

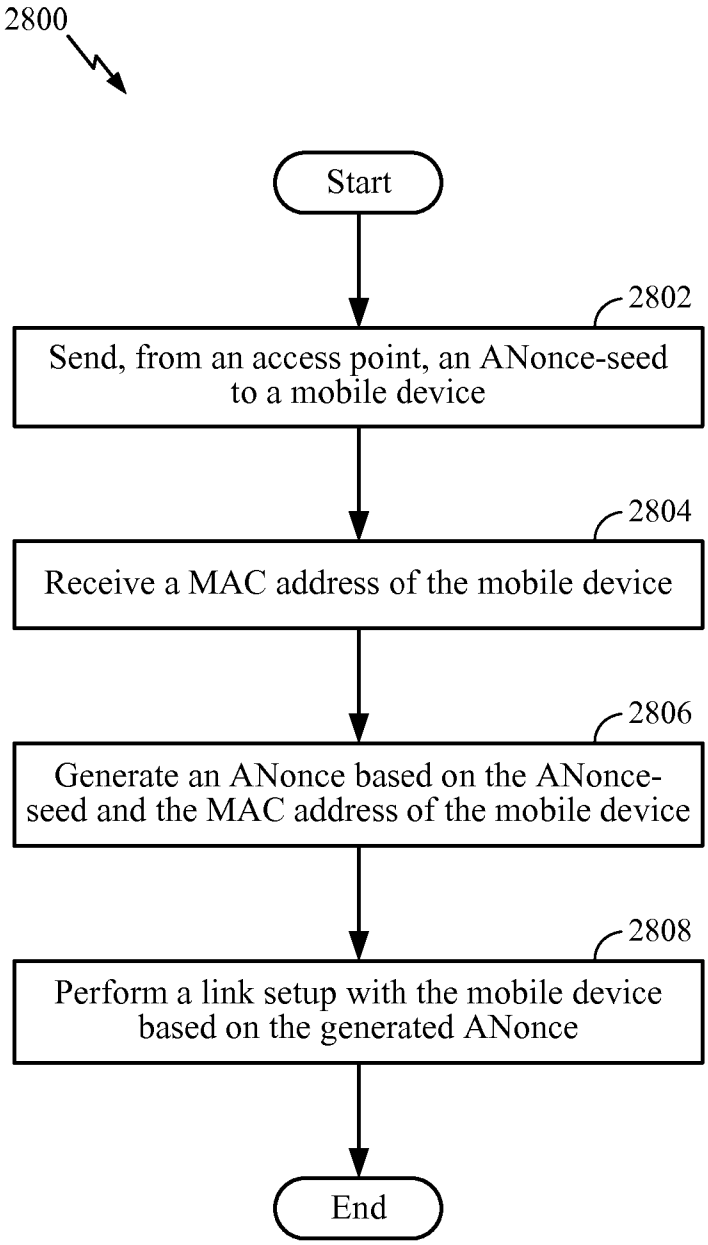
2800
Start
2802
Send, from an access point, an ANonce-seed to a mobile device
2804
Receive a MAC address of the mobile device
2806
Generate an ANonce based on the ANonce-seed and the MAC address of the mobile device
2808
Perform a link setup with the mobile device based on the generated ANonce
End

FIG. 28

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 61533627 A **[0001]**
- US 61535234 A **[0001]**
- US 61583052 A **[0001]**
- US 61606794 A **[0001]**
- US 61645987 A **[0001]**
- US 61611553 A **[0001]**

Rendszerek és eljárások link felépítés és autentikáció végrehajtására

Szabadalmi igénypontok

1. Eljárás, amely egy hozzáférési pontban (304) hatható végre, és tartalmazza:

egy nem védett asszociációs kérelem vételét (1802) egy mobil készüléktől (302), az asszociációs kérelem egy állomás kitűzőt, SNonce, foglal magában;

egy kiindulási üzenet kivonását (1804) a nem védett asszociációs kérelemből;

az inicializálási üzenet küldését (1806) egy autentikációs kiszolgálóhoz (308);

egy válaszüzenet vételét az autentikációs kiszolgálótól (308), ahol a válaszüzenet egy ismételt autentikációs mester ülésszak kulcsot, rMSK, foglal magában;

egy hozzáférési pont kitűző, ANonce, előállítását (1808);

egy párosával tranziens kulcs, PTK, előállítását (1810) az rMSK, az ANonce és a SNonce használatával; és

egy asszociációs válasz küldését (1812) a mobil készülékhez (302),

ahol az asszociációs válasz tartalmazza az ANonce-t, és az asszociációs válasz a PTK használatával védett.

2. Az 1. igénypont szerinti eljárás, ahol a nem védett asszociációs kérelmet egy alap szolgáltatási készlet azonosítója, BSSID, alapján küldjük a hozzáférési pontnak (304).

3. Az 1. igénypont szerinti eljárás, amely tartalmazza továbbá egy dinamikus állomáskonfiguráló protokoll, DHCP, felfedezési üzenet küldését egy DHCP kiszolgálóhoz.

4. A 3. igénypont szerinti eljárás, amely tartalmazza továbbá egy DHCP-t nyugtázó üzenet vételét a DHCP kiszolgálótól válaszképpen a DHCP felfedezési üzenetre, ahol a DHCP felfedezési üzenet egy Internet Protokoll, IP, címet jelez.

5. Az 1. igénypont szerinti eljárás, ahol az asszociációs válasz integritás-védett, és ahol az ANonce-től eltérő információs elemek kódoltak.

6. Az 1. igénypont szerinti eljárás, ahol a hozzáférési pont (304) az autentikációs kiszolgálóra (308) támaszkodik, amely egy válaszüzenetet visz át egy levezetett rMSK-val autentikációként a mobil készülék (302) számára.

7. Az 1. igénypont szerinti eljárás, ahol a PTK-t a hozzáférési pontban (304) vezetjük le, még azelőtt, hogy levezetésre kerülne a mobil készüléken (302).

8. Számítógépi program, amely egy számítógépen futtatva utasításokat tartalmaz az 1-7. igénypontok bármelyike szerinti eljárás végrehajtására.

9. Berendezés (304), amely tartalmaz:

eszközt egy nem védett asszociációs kérelem vételére egy hozzáférési pontban (304) egy mobil készüléktől (302), az asszociációs kérelem egy állomás kitűzőt (SNonce) foglal magában;

eszközt egy iniciálási üzenet kivonására a nem védett asszociációs kérelemből;

eszközt az inicializálási üzenet küldésére egy autentikációs kiszolgálóhoz (308);

eszközt egy válaszüzenet vételére az autentikációs kiszolgálótól (308), ahol a válaszüzenet egy újra autentikációs mester ülésszak kulcsot, rMSK, foglal magában;

eszközt egy hozzáférési pont kitűző, (ANonce) előállítására;

eszközt egy párosával tranziens kulcs, PTK, előállítására, az rMSK , az ANonce és a SNonce használatával; és

eszközt egy asszociációs válasz küldésére a hozzáférési ponttól (304) a mobil készülékhez (302), ahol az asszociációs válasz magában foglalja az ANonce-t, és az asszociációs válasz PTK használatával védett.

10. A 9. igénypont szerinti berendezés (304), ahol a nem védett hozzáférési kérelmet a hozzáférési pont (304) egy alapvető szolgáltatás készlet azonosítója, BSSID, alapján küldik.

11. A 9. igénypont szerinti berendezés (304), amely tartalmaz továbbá eszközt egy dinamikus állomáskonfiguráló protokoll, DHCP, felfedezési üzenet küldésére egy DHCP kiszolgálóhoz.

12. A 11. igénypont szerinti berendezés (304), amely tartalmaz továbbá eszközt egy DHCP nyugtázó üzenet vételére a DHCP kiszolgálótól válaszképpen a DHCP felfedezési üzenetre, vagy a DHCP felfedezési üzenet egy Internet Protokoll, IP, címet jelez.

13. A 9. igénypont szerinti berendezés (304), ahol az asszociációs válasz integritás-védett, és ahol az ANonce-től eltérő információs elemek kódoltak.

14. A 9. igénypont szerinti berendezés (304), ahol a hozzáférési pont (304) az autentikációs kiszolgálóra (308) támaszkodik, amely egy válaszüzenetet visz át egy levezetett rMSK-val, mint autentikációval a mobil készülék számára (302).

15. A 9. igénypont szerinti berendezés (304), ahol a PTK a hozzáférési pontban (304) még az előtt levezetésre kerül, mielőtt az levezetésre kerülne a mobil készüléken (302).