US 20090271626A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2009/0271626 A1**

(43) **Pub. Date: Oct. 29, 2009**

WANG

(54) **METHODS AND DEVICES FOR ESTABLISHING SECURITY ASSOCIATIONS IN COMMUNICATIONS SYSTEMS**

(75) Inventor: **Jui-Tang WANG**, Hsinchu (TW)

Correspondence Address:
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413 (US)

(73) Assignee: **Industrial Technology Research Institute**

(21) Appl. No.: **12/203,652**

(22) Filed: **Sep. 3, 2008**

Related U.S. Application Data

(60) Provisional application No. 60/969,773, filed on Sep. 4, 2007, provisional application No. 60/981,767, filed on Oct. 22, 2007, provisional application No. 60/985,538, filed on Nov. 5, 2007.

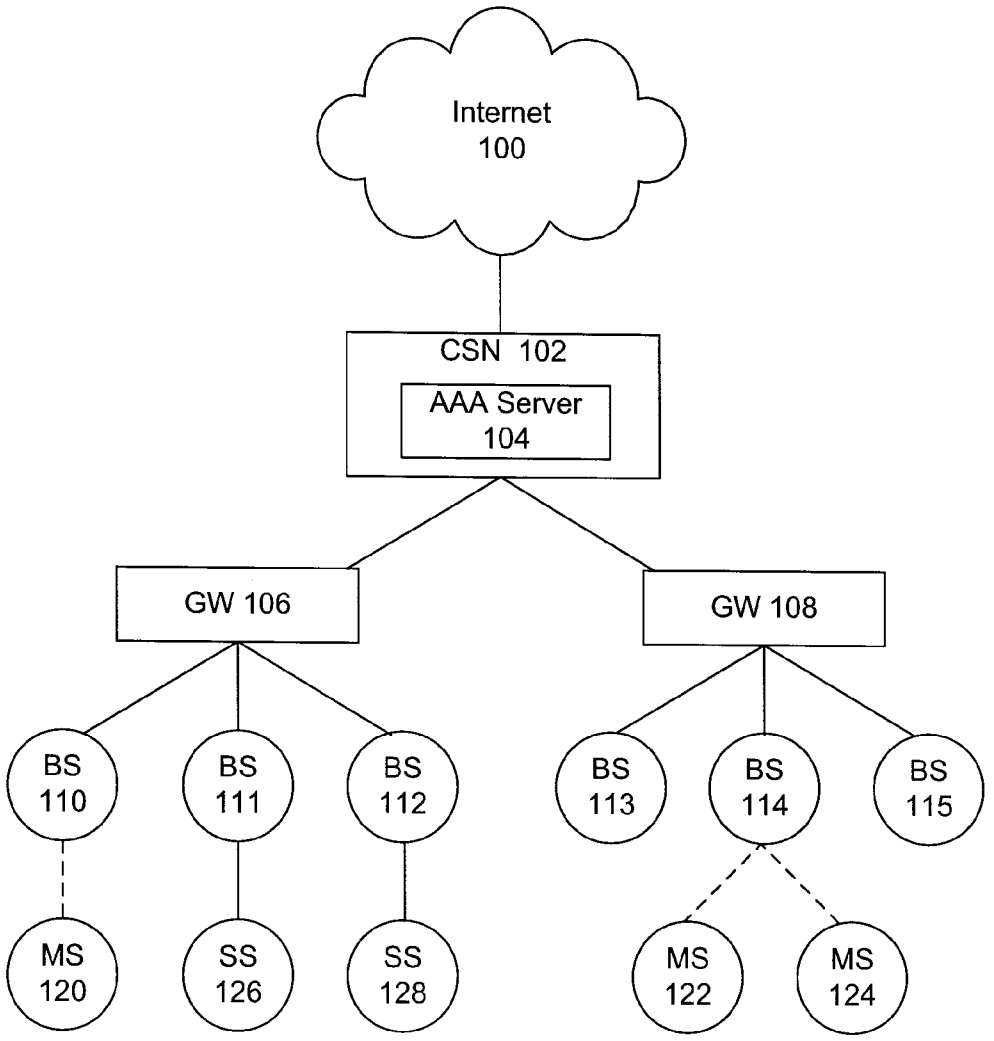
Publication Classification

(51) **Int. Cl.**
H04L 9/32 (2006.01)
H04K 1/00 (2006.01)

(52) **U.S. Cl.** **713/170**; 380/272

(57) **ABSTRACT**

A method of providing secure communications between a base station, a relay station, and a mobile station in a communication network includes authenticating the mobile station over the communication network; generating, by the base station, security material, wherein the security material comprises at least one of a traffic encryption key (TEK) and a message authentication code key (MACK); transmitting, by the base station, the security material to the mobile station; and transmitting, by the base station, the security material to the relay station.



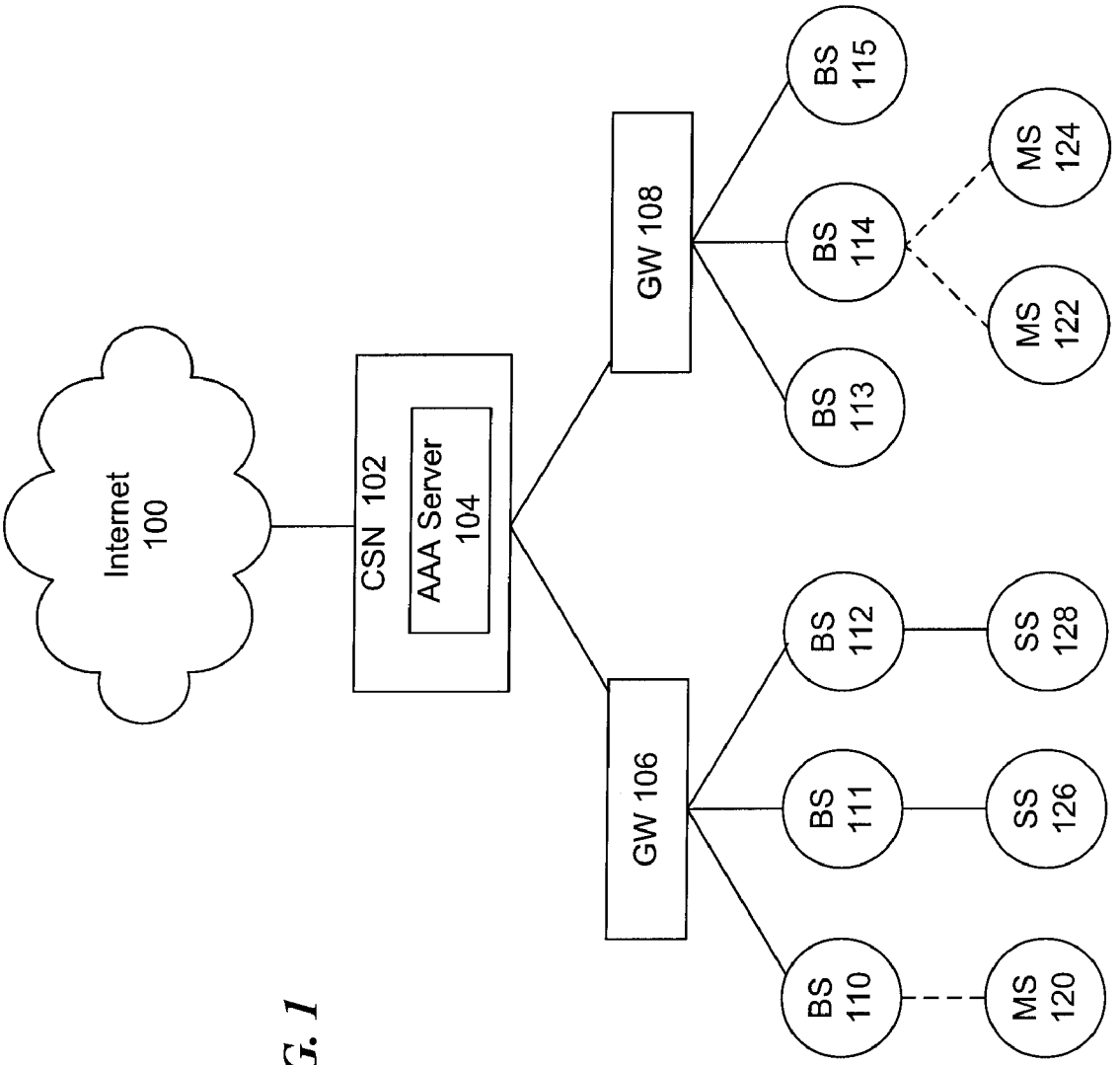

Internet
100
CSN 102
AAA Server
104
GW 106
GW 108
BS
110
BS
111
BS
112
BS
113
BS
114
BS
115
MS
120
SS
126
SS
128
MS
122
MS
124

FIG. 1

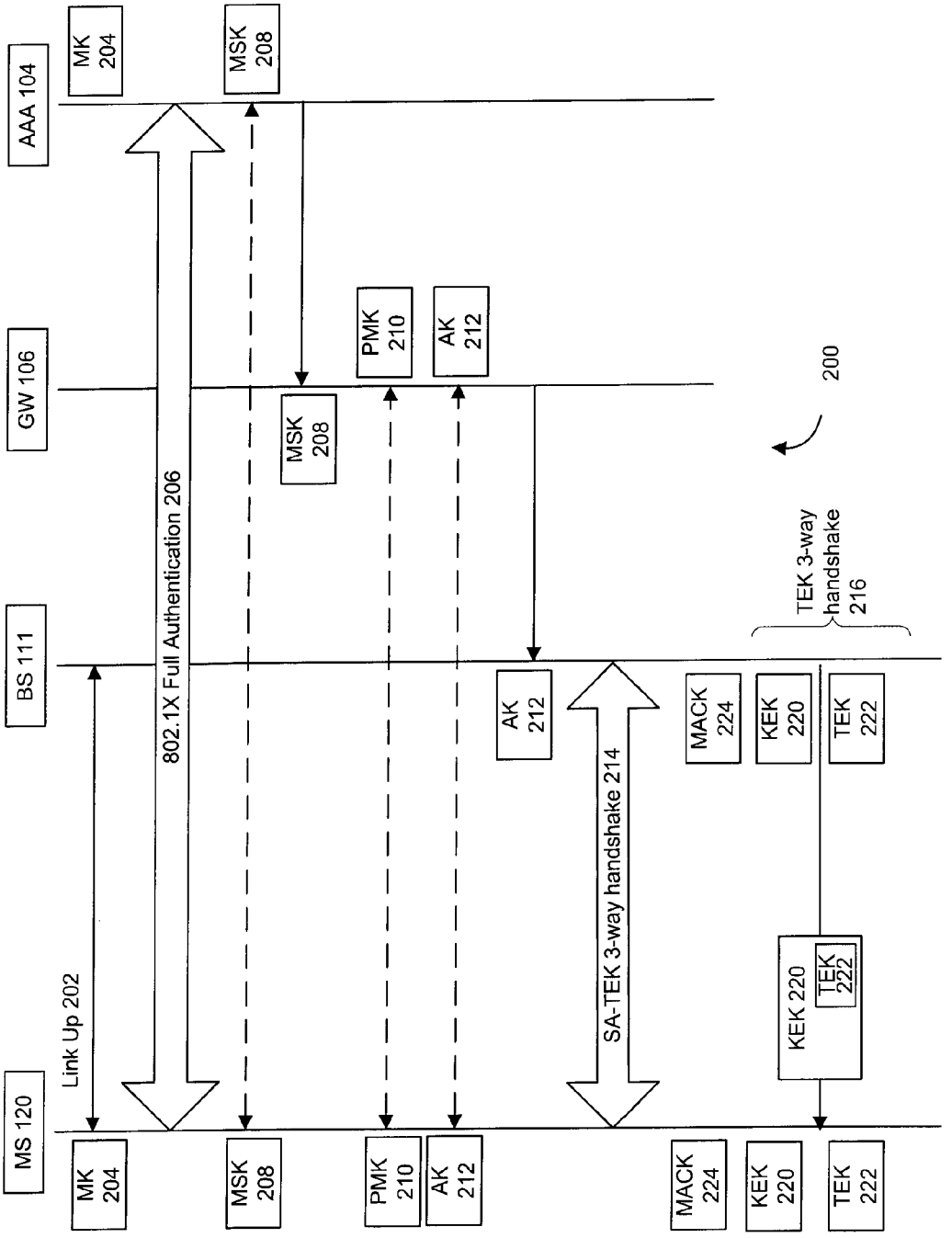

AAA 104
GW 106
BS 111
MS 120
MK 204
MSK 208
PMK 210
AK 212
MACK 224
KEK 220
TEK 222
802.1X Full Authentication 206
Link Up 202
SA-TEK 3-way handshake 214
TEK 3-way handshake 216
200

FIG. 2

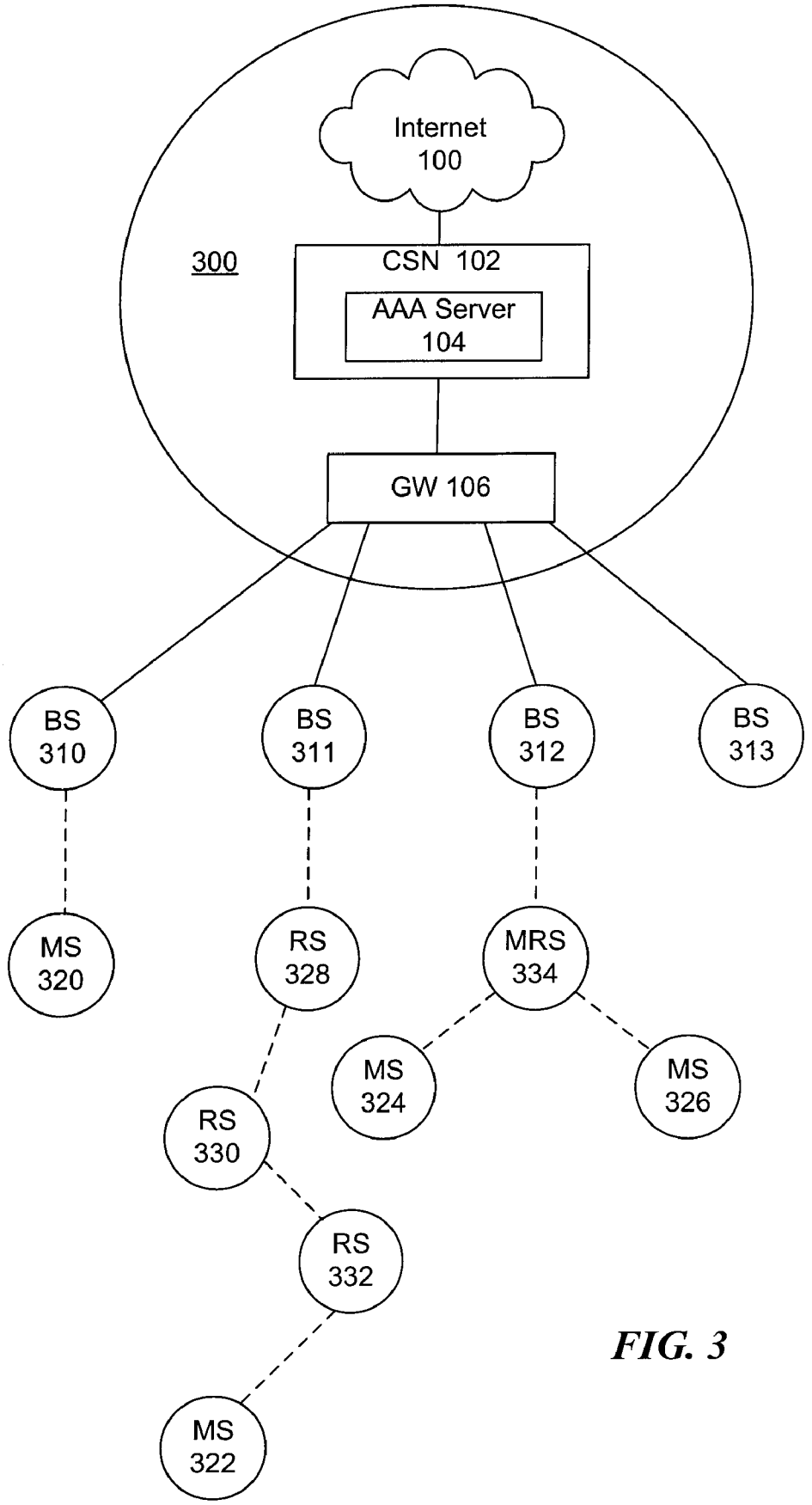

Internet
100
300
CSN 102
AAA Server
104
GW 106
BS
310
BS
311
BS
312
BS
313
MS
320
RS
328
MRS
334
MS
324
MS
326
RS
330
RS
332
MS
322

FIG. 3

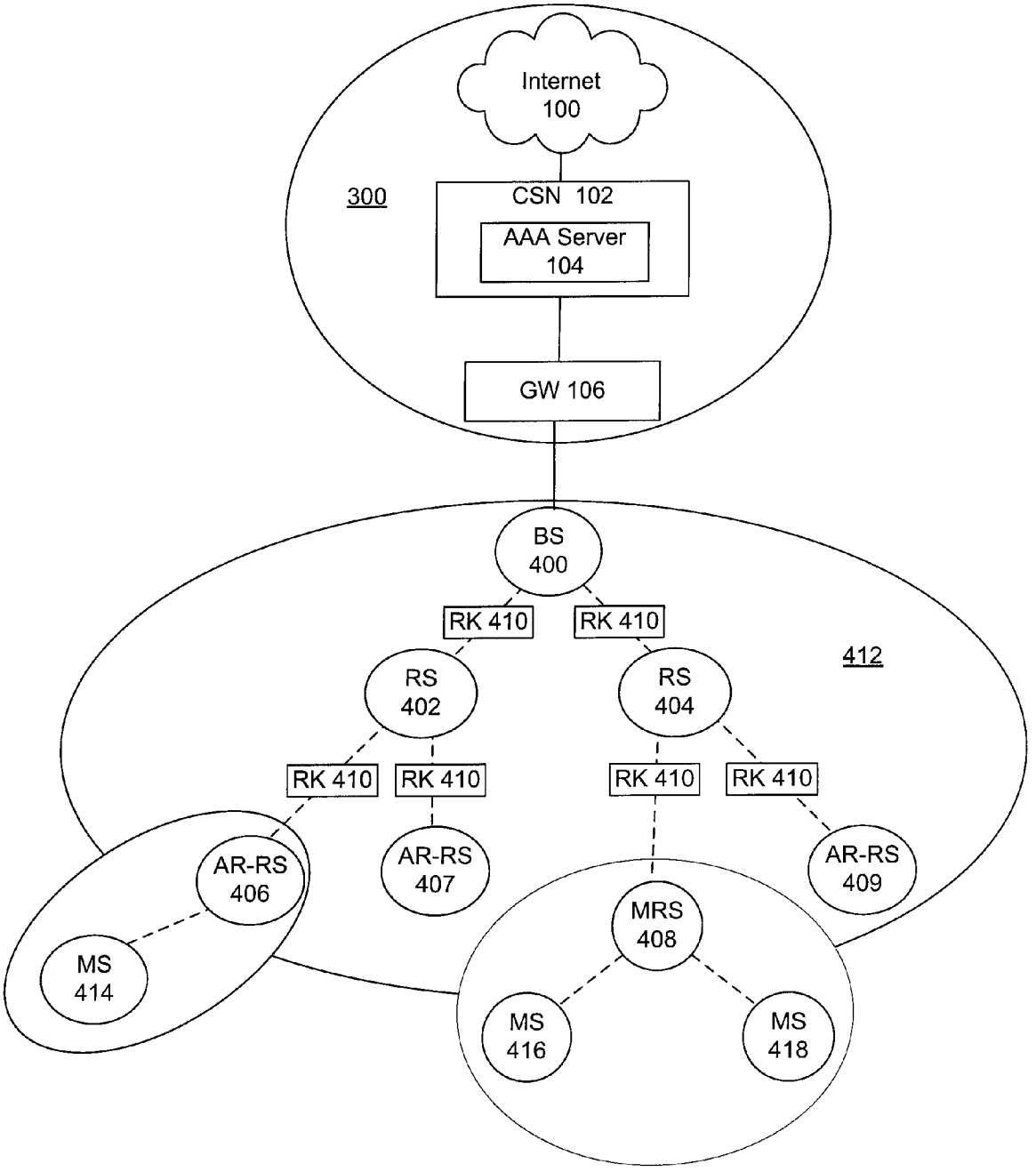

Internet
100
300
CSN 102
AAA Server
104
GW 106
BS
400
RK 410
RK 410
412
RS
402
RS
404
RK 410
RK 410
RK 410
RK 410
AR-RS
406
AR-RS
407
AR-RS
409
MRS
408
MS
414
MS
416
MS
418

FIG. 4

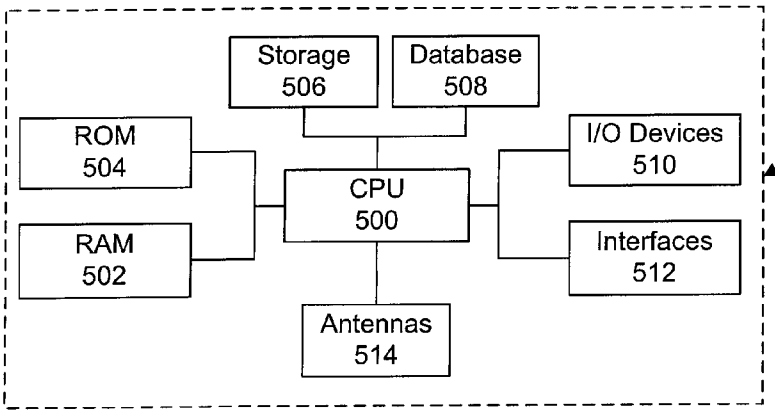


FIG. 5A

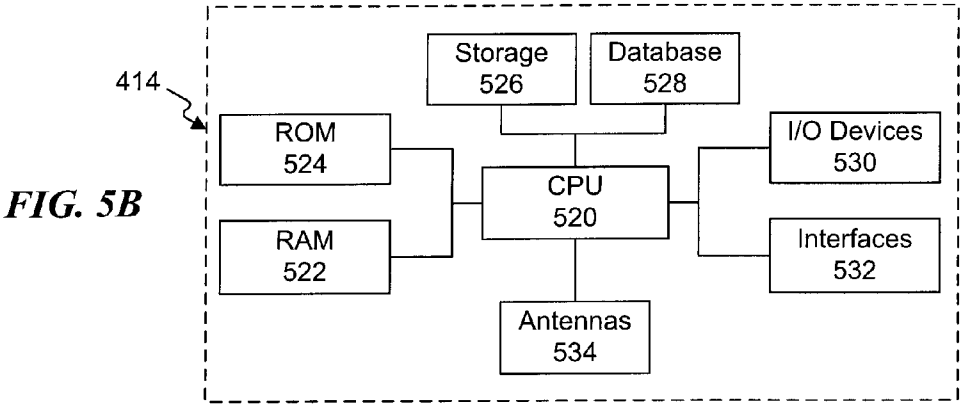


FIG. 5B

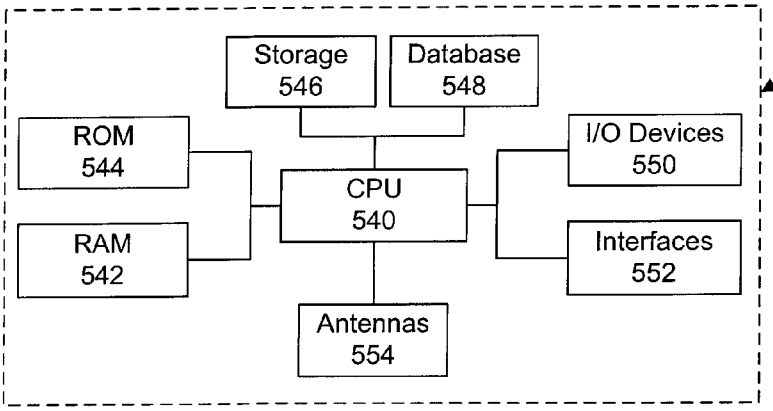


FIG. 5C

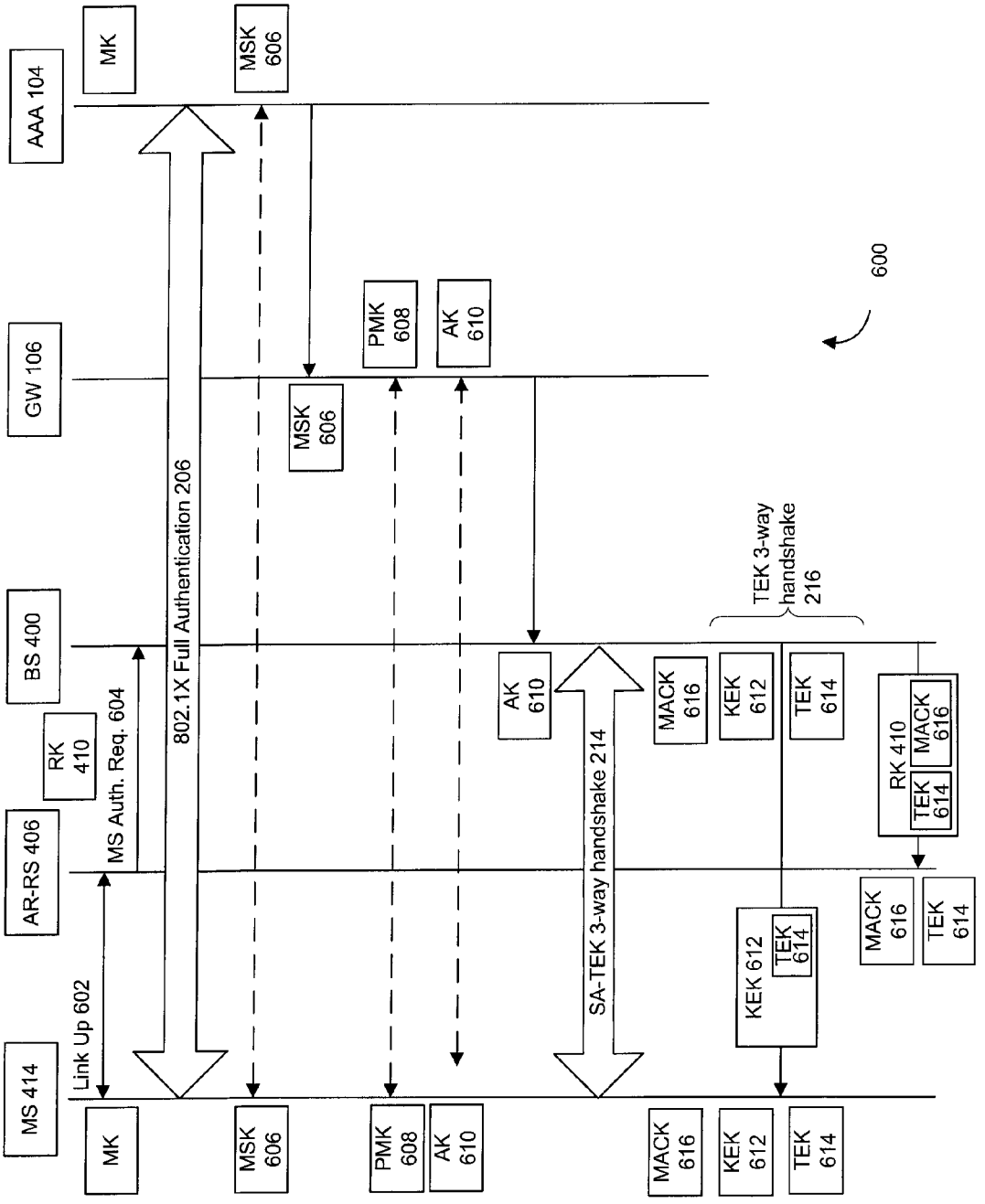

AAA 104
GW 106
BS 400
AR-RS 406
MS 414
MK
MSK 606
PMK 608
AK 610
RK 410
MACK 616
KEK 612
TEK 614
802.1X Full Authentication 206
MS Auth. Req. 604
Link Up 602
SA-TEK 3-way handshake 214
TEK 3-way handshake 216
600

FIG. 6

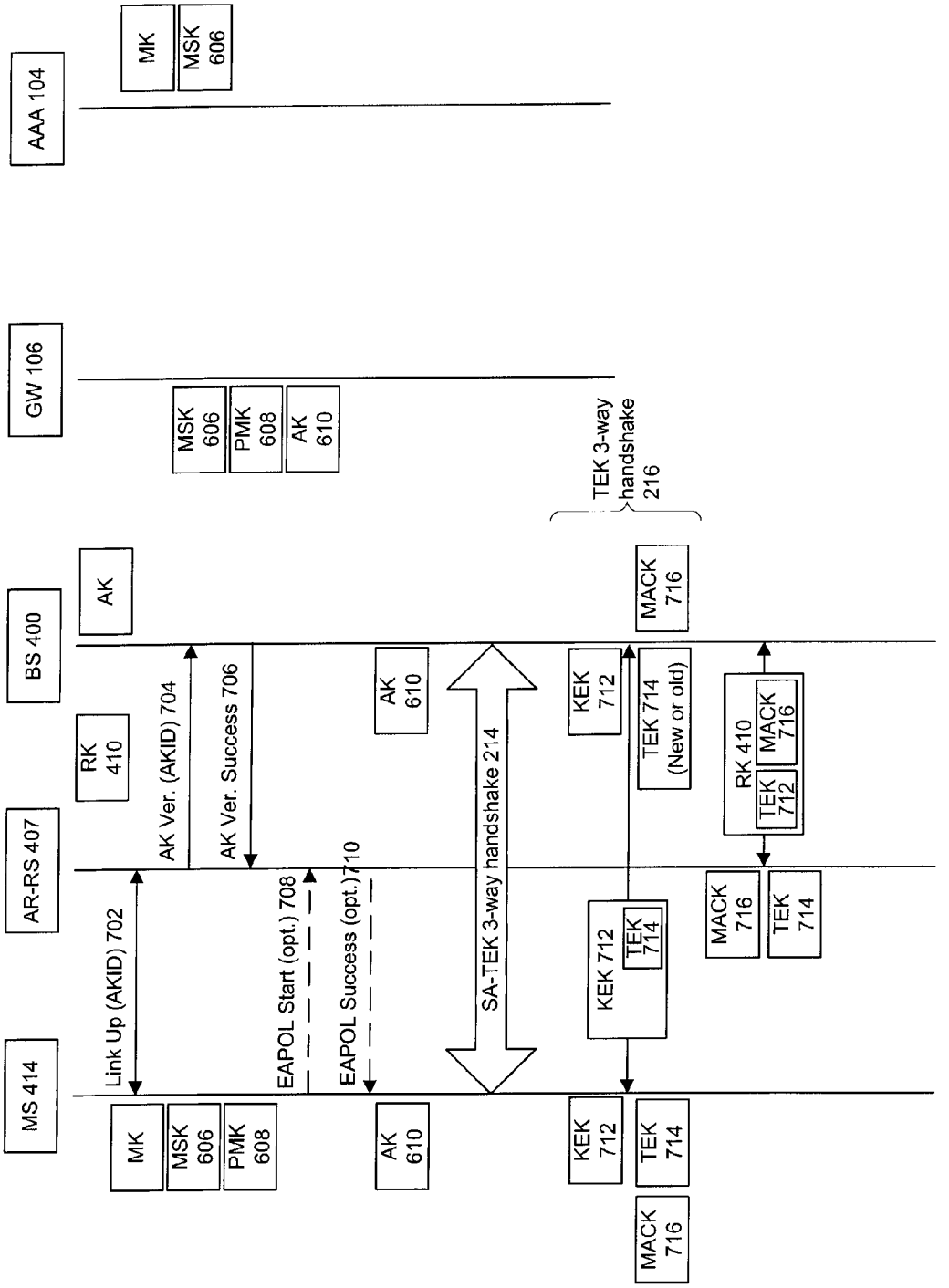

MS 414
AR-RS 407
BS 400
GW 106
AAA 104
Link Up (AKID) 702
AK Ver. (AKID) 704
AK Ver. Success 706
EAPOL Start (opt.) 708
EAPOL Success (opt.) 710
SA-TEK 3-way handshake 214
TEK 3-way handshake 216
RK 410
AK
MK
MSK 606
PMK 608
AK 610
KEK 712
TEK 714
MACK 716
TEK 714 (New or old)
RK 410 TEK 712 MACK 716

FIG. 7

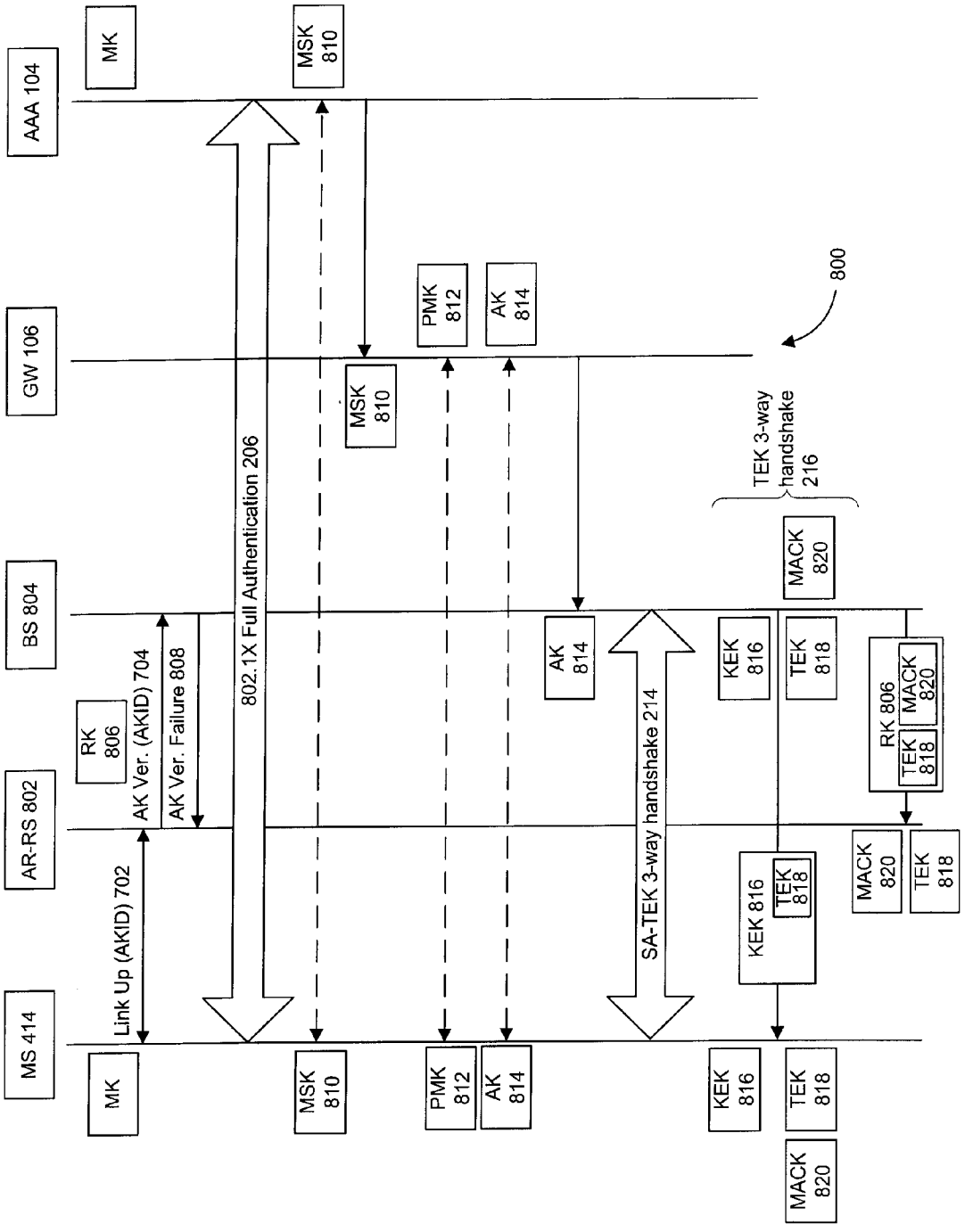

MS 414
AR-RS 802
BS 804
GW 106
AAA 104
800
MK
MSK 810
PMK 812
AK 814
KEK 816
TEK 818
MACK 820
RK 806
Link Up (AKID) 702
AK Ver. (AKID) 704
AK Ver. Failure 808
802.1X Full Authentication 206
SA-TEK 3-way handshake 214
TEK 3-way handshake 216

FIG. 8

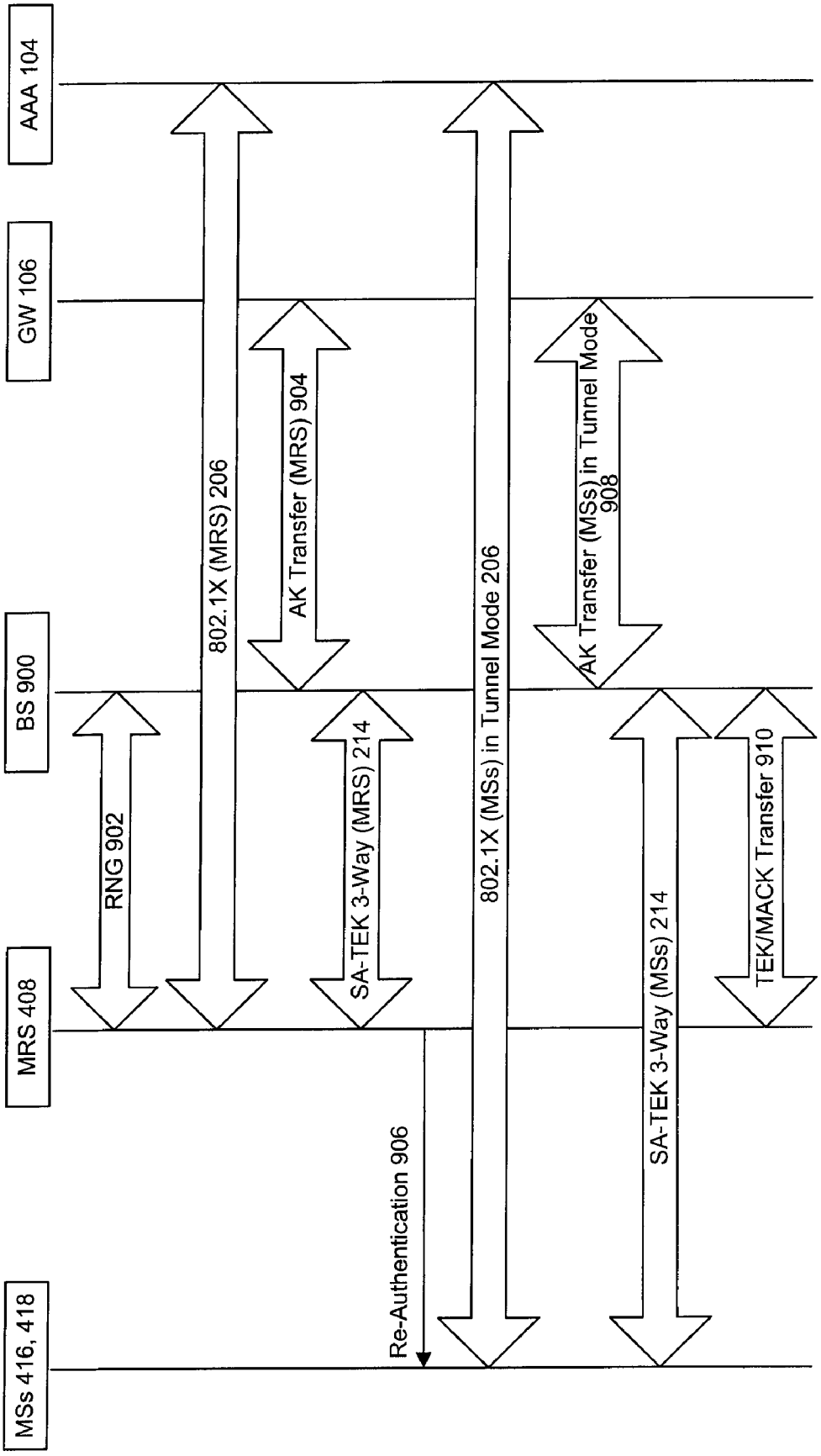

AAA 104
GW 106
BS 900
MRS 408
MSs 416, 418
802.1X (MRS) 206
AK Transfer (MRS) 904
AK Transfer (MSs) in Tunnel Mode 908
RNG 902
SA-TEK 3-Way (MRS) 214
802.1X (MSs) in Tunnel Mode 206
SA-TEK 3-Way (MSs) 214
TEK/MACK Transfer 910
Re-Authentication 906

FIG. 9

METHODS AND DEVICES FOR ESTABLISHING SECURITY ASSOCIATIONS IN COMMUNICATIONS SYSTEMS

PRIORITY

[0001] This application claims the benefit of priority of U.S. Provisional Application No. 60/969,773, filed Sep. 4, 2007; U.S. Provisional Application No. 60/981,767, filed Oct. 22, 2007; and U.S. Provisional Application No. 60/985,538, filed Nov. 5, 2007, all of which are incorporated by reference herein in their entirety for any purpose.

TECHNICAL FIELD

[0002] The present disclosure relates to the field of communications and, more particularly, to systems and methods for establishing security associations in a communication system.

BACKGROUND

[0003] Conventional wireless network environments connect mobile electronic devices to a service provider. More specifically, WiMAX (Worldwide Interoperability for Microwave Access) network environments connect a client device, through intermediate connections, to, for example, the Internet. WiMAX is a wireless networking technology that provides communication to wireless devices over significant distances. Authentication and reauthentication delays, however, can slow communication with the client device and decrease the efficiency of a WiMAX environment.

[0004] FIG. **1** is a block diagram of an exemplary prior art wireless communication system for use in an IEEE 802.16d/802.16e WiMAX wireless communication system. Access to Internet **100** is provided to at least one connectivity service network (CSN) **102**, using at least one authentication, authorization, and accounting (AAA) server **104**. CSN **102** is connected to gateways (GWs) **106** and **108**. Gateways **106** and **108** are each a type of communication network authenticator and typically connected to several base stations (BSs) **110**-**115**, the number of such BSs depending on network demands in a given area, though a gateway may instead be connected to only a single base station. Only two gateways **106** and **108** are shown, but it is possible to have greater or fewer gateways depending on the number of required base stations.

[0005] In FIG. **1**, six base stations are shown as an exemplary WiMAX environment, but greater or fewer base stations may be provided depending on the number of available gateways and the network demands in the WiMAX environment. Base stations, such as base station **110** and base station **114**, communicate with one or more client devices. Client devices include mobile stations (MSs), such as mobile stations **120**, **122** and **124**, to which the base stations provide wireless network service, and subscriber stations (SSs), such as subscriber stations **126** and **128**, to which base stations provide wired or wireless network service. The network needs of several client devices may be satisfied by a single base station, and a single base station may satisfy the network needs of both mobile stations and subscriber stations.

[0006] In the conventional WiMAX environment, such as that shown in FIG. **1**, each time mobile station **120** is initially served by a gateway, e.g., gateway **106**, via an associated base station, e.g., base station **110**, it is necessary to authenticate mobile station **120**. Following such authentication, so long as mobile station **120** moves in areas that enable continued service via the original authenticating gateway, no further gateway authentication is required. However, if mobile station **120** moves to an area served by a different gateway, e.g., gateway **108**, mobile station **120** is handed over to the different gateway, so that it is necessary for that different gateway to reauthenticate mobile station **120** as part of the handoff processing before service may be provided. After a client device has been authenticated or reauthenticated, security associations, or the sharing of security information between two network entities such as mobile station **120** and base station **110**, are established to ensure that communications between the two entities are secure.

[0007] Authentication protocol standards have been created to standardize advance authentication techniques. These standardized protocols may include, for example, IEEE 802.1X authentication, extensible authentication protocol (EAP) method for global system for mobile communications (GSM) subscriber identity (EAP-SIM) and extensible authentication protocol method for universal mobile telecommunications systems (UMTS) authentication and key agreement (EAP-AKA) and/or a combination of the extensible authentication protocol (EAP) and the remote authentication dial in user service (RADIUS) protocol. In addition, standardized handshake protocols, such as security association signaling protocols, e.g., security association and traffic encryption key (SA-TEK) 3-way handshakes, and traffic encryption key (TEK) 3-way handshakes may be used to establish security associations over a communication link.

[0008] In IEEE 802.16d/802.16e WiMAX wireless communication systems, these standardized techniques are performed between a base station and a mobile station. Each standardized authentication technique requires multiple transmissions, which consume authentication time and processing overhead.

[0009] FIG. **2** is a signaling diagram of exemplary prior art authentication and authorization in an IEEE 802.16d and 802.16e WiMAX wireless communication system. An initialization process **200** is used to ensure that a mobile station requesting network service is authorized to access the network and to provide a security association between mobile stations and base stations to allow secure message transmission. For example, initialization process **200** may be used to provide a security association between mobile station **120** just after it moved into the range of base station **111** after previously being within the range of base station **110**.

[0010] In the first step of initialization process **200**, mobile station **120** is wirelessly connected to base station **111** through the link up process **202** which includes, for example, a ranging request and a ranging response. Mobile station **120** must then go through a multi-step process of authentication such as IEEE 802.1X full authentication **206** with AAA server **104** through gateway **106**. Then AAA server **104** computes a master session key (MSK) **208** for mobile station **120** and transfers MSK **208** to gateway **106**, which stores MSK **208** in its cache. The product of authentication through, for example, the EAP method or other authentication method is the transfer of MSK **208**, which is known to AAA server **104**, gateway **106**, and mobile station **120**. Gateway **106** will generate a pairwise master key (PMK) **210** and an authentication key (AK) **212** for mobile station **120**, and transfer AK **212** to base station **111**.

[0011] Mobile station **120** may also independently hold and store MSK **208** in its memory and may generate AK **212**. Then base station **111** may perform the SA-TEK 3-way hand-

shake procedure **214** to confirm that the AK held by mobile station **120** is the same AK **212** held by base station **111**. Using AK **212**, commonly held by base station **111** and mobile station **120**, base station **111** and mobile station **120** may both respectively calculate a common message authentication code key (MACK) **224** and a common key encryption key (KEK) **220**. MACK **224** may identify an authenticated message generated by mobile station **120** and base station **111**. KEK **220** may protect transmission of traffic encryption keys from base station **120** to mobile station **111**. Base station **110** and mobile station **120** may perform SA-TEK 3 way handshake procedure **214** using MACK **224** to authenticate each other. When SA-TEK 3-way handshake procedure **214** has been successfully completed, the base station **110** may generate a traffic encryption key (TEK) **222** and then carry out a TEK 3-way handshake procedure **216** with KEK **220** to establish security association with the mobile station **120**. TEK **222** is typically randomly generated by the base station **111** and is used to encrypt data transmitted between mobile station **120** and base station **111** after mobile station **120** has been authenticated and authorized to access the network. SA-TEK 3-way handshake **214** and TEK 3-way handshake **216** are well-known in the art and will not be discussed further.

[0012] In initialization process **200** for use in IEEE 802.16d and 802.16e WiMAX wireless communication systems as shown in FIG. **2**, base station **111** controls whether data transmission occurs over the channel between base station **111** and mobile station **120** because base station **111** and mobile station **120** both hold the same TEK **222**, KEK **220**, and AK **212**, from which MACK **224** can be derived. After mobile station **120** has established a security association with base station **111**, or, in other words, after mobile station **120** has been granted permission to communicate over the network, encrypted data transmission occurs between mobile station **120** and base station **111** using TEK **222**.

[0013] Referring again to FIG. **1**, in operation, the strength of the signal and transmission quality may decrease as the network signal travels from gateway **106** or gateway **108** to base stations **110-115** to client devices **120**, **122**, **124**, **126**, and **128**. Additionally, the signal and transmission quality decrease as a mobile station travels further from its serving base station. Signal quality and coverage may also be affected by factors such as physical structures, signal interferences, weather and transmission conditions and formats. Therefore, coverage gaps or holes may exist and users in those areas may have limited or no network access.

[0014] One solution to avoid or reduce coverage gaps is to provide more base stations, but this solution can be costly. Alternatively, a network may avoid or reduce coverage gaps and/or extend its network coverage by using relay stations (RSs), such as those implementing the concept of multi-hop relaying (MR) as set forth in IEEE 802.16j. Base stations communicate with these relay stations, which boost and relay signals to and from mobile stations and base stations, but otherwise are not involved in authentication and/or establishing security associations.

[0015] FIG. **3** is a block diagram of an exemplary prior art wireless communication system for use in an IEEE 802.16j WiMAX wireless communication system with MR architecture. Similar to the IEEE 802.16d and 802.16e WiMAX wireless communication systems, access to Internet **100** is provided through at least one AAA server, such as AAA server **104**, and via at least one gateway, such as gateway **106**. For convenience, Internet **100**, CSN **102**, AAA server **104** and gateway **106** are referred to as core network **300**. Network **300**, and specifically, gateway **106**, typically communicates with base stations **310-313** over a wired connection.

[0016] Four base stations **310-313** are shown in FIG. **3**, but greater or fewer base stations may be provided. Base stations, such as base station **310**, may communicate directly with one or more mobile stations, such as mobile station **320**, via wireless transmission. Base stations, such as base station **311** and base station **312**, may communicate indirectly with one or more mobile stations, such as mobile stations **322**, **324**, and **326**. Base stations typically communicate with one or more relay stations, such as relay stations **328**, **330**, and **332**, via wireless transmission, but they may also communicate over wired connections. Relay stations **328**, **330**, and **332** boost and relay the signal to/from mobile station **322** via wireless transmission. As shown, relay stations **328**, **330**, and **332** are fixed relay stations. However, base stations may also communicate with mobile relay stations (MRSs), such as mobile relay station **334**. A mobile relay station could reside, for example, on a train, plane or automobile and provide its passengers having mobile stations with mobile network access to various base stations and/or relay stations as the mobile relay station travels. As shown in FIG. **3**, mobile relay station **334** provides wireless service to mobile stations **324** and **326**, but the network needs of only one mobile station, or several mobile stations, may be satisfied by a single mobile relay station. Although not shown, base stations, such as base stations **310-313**, may also communicate with one or more subscriber station. The network needs of several client devices, therefore, may be satisfied by a single base station either directly or through one or more relay stations. Moreover, relay stations **328**, **330**, and **332** may provide wireless service to additional relay stations, additional mobile relay stations, and/or additional mobile stations.

[0017] In some applications, the use of relay stations may increase the need for station-to-station (base/relay) handoffs and may require increased processing overhead for such handoffs due to the limited coverage areas of each relay station (including mobile relay stations). In addition, when secure communications are involved, the handoff process from one base/relay station to another base/relay station may require additional overhead and reduce efficiency, bandwidth, or quality of the communication connection.

[0018] The disclosed embodiments are directed to overcoming one or more of the problems set forth above.

SUMMARY OF THE INVENTION

[0019] In one aspect, the present disclosure is directed to a method of providing secure communications between a base station, a relay station, and a mobile station in a communication network. The method authenticates the mobile station over the communication network, and generates, by the base station, security material, wherein the security material comprises at least one of a traffic encryption key (TEK) and a message authentication code key (MACK). The method also transmits, by the base station, the security material to the mobile station. In addition, the method transmits, by the base station, the security material to the relay station.

[0020] In another aspect, the present disclosure is directed to a base station for providing secure communications in a communication network. The base station includes at least one memory to store data and instructions, and at least one processor configured to access the memory. The at least one

processor is configured to, when executing the instructions, authenticate a mobile station over the communication network, and generate security material, wherein the security material comprises at least one of a traffic encryption key (TEK) and a message authentication code key (MACK). The at least one processor is further configured to cause transmission of the security material to the mobile station, and cause transmission of the security material to a relay station.

[0021] In another aspect, the present disclosure is directed to a relay station for providing secure communications in a communication network. The relay station includes at least one memory to store data and instructions, and at least one processor configured to access the memory. The at least one processor is configured to, when executing the instructions, cause transmission of a mobile station verification request to a base station in response to a ranging request from at least one mobile station and perform secure data transmission with the at least one mobile station using security material received from the base station, wherein the security material comprises at least one of a traffic encryption key (TEK) and a message authentication code key (MACK).

[0022] In yet another aspect, the present disclosure is directed to a system for providing secure communications. They system includes a base station configured to provide access to a communication network, authenticate at least one mobile station over the network, generate security material and transmit the security material. The system also includes a relay station in communication with the base station for receiving the security material and for providing secure data transmissions to the at least one mobile station using the security material. The security material includes at least one of a traffic encryption key (TEK) and a message authentication code key (MACK).

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] FIG. **1** is a block diagram of an exemplary prior art wireless communication system for use in an IEEE 802.16d/802.16e WiMAX wireless communication system.

[0024] FIG. **2** is a signaling diagram of exemplary prior art authentication and authorization in an IEEE 802.16d and 802.16e WiMAX wireless communication system.

[0025] FIG. **3** is a block diagram of an exemplary prior art wireless communication system for use in an IEEE 802.16j wireless communication system with multi-hop relaying architecture.

[0026] FIG. **4** is a block diagram of an exemplary wireless communication system for use in an IEEE 802.16j wireless communication system in which selected relay stations serve as authenticator relay-relay stations.

[0027] FIG. **5***a* is a block diagram illustrating an exemplary construction of a base station.

[0028] FIG. **5***b* is a block diagram illustrating an exemplary construction of a mobile station.

[0029] FIG. **5***c* is a block diagram illustrating an exemplary construction of a relay station or mobile relay station.

[0030] FIG. **6** is a signaling diagram of exemplary authentication and authorization in an 802.16j wireless communication system in which relay stations serve as authenticator relay-relay stations.

[0031] FIG. **7** is a signaling diagram of an exemplary handoff from a current authenticator relay-relay station to a target authenticator relay-relay station where both authenticator relay-relay stations communicate with the same base station.

[0032] FIG. **8** is a signaling diagram of an exemplary handoff from an authenticator relay-relay station connected to a current base station to a target connected to a different, target base station.

[0033] FIG. **9** is a signaling diagram of an exemplary mobile relay station handoff between a current base station and a target base station.

DETAILED DESCRIPTION

[0034] Embodiments of the disclosure can provide such security associations in IEEE 802.16j WiMAX wireless communication systems or other wireless communication networking systems that employ relay stations. By providing a relay station with the ability to establish a secure connection with mobile stations and provide mobile stations with access to network **300**, processing overhead can be significantly reduced. Specifically, by providing a relay station with traffic encryption key and/or a message authentication key corresponding to a mobile station seeking access to the network **300**, the relay station can establish a security association with the mobile station and perform mobile station authentication and authorization.

[0035] FIG. **4** is a block diagram of an exemplary wireless communication system for use in an IEEE 802.16j WiMAX wireless communication system in which selected relay stations serve as authenticator relay-relay stations (AR-RSs). In FIG. **4**, a base station **400** is connected over a wire to network **300** and communicates wirelessly with one or more relay stations **402** and **404**, which boost and relay the received signal to AR-RSs **406-409**. As shown in FIG. **4**, AR-RS (MRS) **408** is a mobile relay station. A security zone key, also called a relay key (RK) **410** is distributed by base station **400** to relay stations **402** and **404**, and AR-RSs **406-409** after relay stations **402** and **404**, and AR-RSs **406-409** are authenticated during their initialization to network **300** and is used to provide data and signal protection for the communication channels between relay stations and/or between relay stations and base stations in an IEEE 802.16j network. Relay stations **402** and **404** and/or base station **400** may perform data and signal encryption, decryption and message authentication using relay key **410**. The area of network coverage provided by base station **400**, relay stations **402** and **404**, and AR-RSs **406-409** that share relay key **410** is called a secure relay zone (SRZ) **412**. FIG. **4** illustrates a single mobile station **414** served by AR-RS **406** and two mobile stations **416** and **418** are served by AR-RS (MRS) **408**, but the network needs of several mobile stations may be provided by a single AR-RS. In addition, although only AR-RS **408** is shown as a mobile relay station, additional AR-RSs within SRZ **412** may be mobile relay stations.

[0036] Each time mobile station **414** is initially served by base station **400**, it is necessary to establish a security association with network **300**. So long as mobile station **414** moves within SRZ **412**, it may be possible to bypass further security association establishment and authentication. However, if mobile station **414** moves to an area served by a different base station, mobile station **414** is handed over to the different base station, so that it may be necessary for that different base station to establish another security association with mobile station **414**, and, depending upon whether the different base station is connected through gateway **106**, authenticate mobile station **414** as part of the handoff pro-

cessing. Such reauthentication and/or security association establishment introduces delay in providing service to mobile station **414**.

[0037] FIG. **5***a* is a block diagram illustrating an exemplary construction of a base station such as base station **400**. Base station **400** may be any type of communication device configured to transmit and/or receive data and/or communications to and from one or more mobile stations such as mobile station **414**, relay stations such as relay stations **402** and **404**, and/or AR-RSs such as AR-RSs **406**-**409**, in a wireless communication system. As shown in FIG. **5***a*, each base station **400** may include one or more of the following components: at least one central processing unit (CPU) **500** configured to execute computer program instructions to perform various processes and methods, random access memory (RAM) **502** and read only memory (ROM) **504** configured to access and store information and computer program instructions, memory **506** to store data and information, database **508** to store tables, lists, or other data structures, I/O devices **510**, interfaces **512**, antennas **514**, etc. Each of these components is well-known in the art and will not be discussed further.

[0038] FIG. **5***b* is a block diagram illustrating an exemplary construction of a mobile station such as mobile station **414**. As shown in FIG. **5***b*, each mobile station **414** may include one or more of the following components: at least one CPU **520** configured to execute computer program instructions to perform various processes and methods, RAM **522** and ROM **524** configured to access and store information and computer program instructions, memory **526** to store data and information, database **528** to store tables, lists, or other data structures, I/O devices **530**, interfaces **532**, antennas **534**, etc. Each of these components is well-known in the art and will not be discussed further.

[0039] FIG. **5***c* is a block diagram illustrating an exemplary construction of a relay station or mobile relay station such as AR-RS/mobile relay station **406**. As shown in FIG. **5***c*, each relay station/mobile relay station **406** may include one or more of the following components: at least one CPU **540** configured to execute computer program instructions to perform various processes and methods, random access memory RAM **542** and read only memory ROM **544** configured to access and store information and computer program instructions, memory **546** to store data and information, database **548** to store tables, lists, or other data structures, I/O devices **550**, interfaces **552**, antennas **554**, etc. Each of these components is well-known in the art and will not be discussed further.

[0040] FIG. **6** is a signaling diagram of exemplary authentication and authorization in an IEEE 802.16j WiMAX wireless communication system in which selected relay stations serve as authenticator relay-relay stations. An initialization process **600** is used to ensure that a mobile station requesting network service is authorized to access network **300** and to provide a security association between mobile stations, relay stations and AR-RSs for secure message transmission. For example, process **600** may be used to authenticate and establish a security association with mobile station **414** just after it is turned on, or after it has moved into the coverage area provided by AR-RS **406** from a coverage area provided through a base station connected to gateway **108**.

[0041] At an initial link up **602**, mobile station **414** sends a ranging request to AR-RS **406** indicating the presence of mobile station **414** in the area of coverage for AR-RS **406**. AR-RS **406** responds by sending a ranging response to mobile station **414** to recognize the presence of mobile station **414** in its coverage area. AR-RS **406** sends an Authentication Request **604**, protected by relay key **410**, to base station **400**. Authentication Request **604** informs base station **400** of the identification information of mobile station **414** that is served by AR-RS **406**. Because mobile station **414** has not previously or recently been connected to network **300** through base station **400** and gateway **106**, mobile station **414** authenticates with AAA server **104** using IEEE 802.1X full authentication protocol **206**. AAA server **104** and mobile station **414** will each calculate a master session key (MSK) **606** when IEEE 802.1X full authentication **206** has been successfully completed. Then AAA server **104** transfers MSK **606** to gateway **106**. Upon receiving MSK **606**, gateway **106** calculates PMK **608** using MSK **606** and stores PMK **608** in its cache. Gateway **106** then computes AK **610** from PMK **608**, and sends AK **610** to base station **400**. Upon obtaining AK **610**, base station **400** derives security material, such as KEK **612** and MACK **616** from AK **610**. The MSK **606** is known to the AAA server **104**, the gateway **106**, and a client device such as mobile station **414**. Mobile station **414** therefore independently hold MSK **606** and may derive PMK **608** and AK **610** and also derive the same MACK **616** and KEK **612**. A client device such as mobile station **414** caches PMK **608** in its memory upon successful authentication using, for example, the EAP method. At this point, base station **400** and mobile station **414** perform SA-TEK 3-way handshake procedure **214** with MACK **616** to authenticate each other. When SA-TEK 3-way handshake procedure **214** is successfully completed, base station **400** will generate security material, including traffic encryption key (TEK) **614**, first and then send the security material (e.g. TEK **614**), protected by KEK **612**, to mobile station **414**. In one embodiment, TEK **614** is randomly generated by base station **400** and is used to provide data confidentiality between base station **400** and AR-RS **406**. At the same time, base station **400** also delivers security material, which may include TEK **614** and MACK **616**, protected by relay key **410**, to AR-RS **406**. Relay station **406** may receive MACK **616** to authenticate mobile station **414** directly and receive TEK **614** to encrypt/decrypt encrypted messages transmitted to and/or from mobile station **414**. One or more security keys, such as MK, MSK **606**, PMK **608**, AK **610**, KEK **612**, TEK **614**, MACK **616** may be referred to as security material.

[0042] AR-RS **406** may switch the communication channel between mobile station **414** and AR-RS **406** to an authorized state to provide mobile station **414** with access to network **300**. Moreover, because mobile station **414** and AR-RS **406** have TEK **614**, they may exchange encrypted data transmissions. Specifically, TEK **614** may then be used to encrypt the data transmitted between AR-RS **406** and mobile station **414** after mobile station **414** has been authenticated. If multicast service, where a base station may send messages to multiple client devices simultaneously, is available, BS **400** will also distribute a multicast key, which protects such multicast transmissions, to AR-RS **406** to enable MS **414** to receive transmissions intended for multiple mobile stations.

[0043] FIG. **7** is a signaling diagram of an exemplary handoff from a current AR-RS, for example AR-RS **406**, to a target AR-RS, for example AR-RS **407**, where the current AR-RS and target AR-RS each communicate with the same base station, e.g., base station **400**. In FIG. **7**, a link **702** is created between mobile station **414** and AR-RS **407** when mobile station **414** transmits a ranging request to AR-RS **407** includ-

ing a security material identification such as an authentication key identification (AKID) and AR-RS **407** responds with a ranging response. The AKID identifies the AK currently stored in a memory (e.g., memory **526**, ROM **524**, RAM **522** or database **528**) of mobile station **414** due to mobile station **414**'s prior authentication with AR-RS **406**. AR-RS **407** transmits the AKID to base station **400** in an AK verification signal request **704** to verify that the AK stored in mobile station **414** matches the AK stored in the memory of base station **400** (e.g., memory **506**, ROM **504**, RAM **502** or database **508**). Because AR-RS **406** and AR-RS **407** are within SRZ **412**, they share the same relay key **410**. As such, verification signal request **704** is encrypted using relay key **410** for security purposes. In one exemplary embodiment, because mobile station **414** has previously performed full authentication with base station **400** through AR-RS **406**, the security material in base station **400** and mobile station **414** match (here, both AK **610**). If the AKs match, base station **400** transmits an AK Verification Success message **706** to AR-RS **407**; if the AKs do not match, base station **400** transmits an AK Failure message to AR-RS **407**. In one exemplary embodiment, mobile station **414** may be programmed to transmit out an Extensible Authentication Protocol over Local Area Network (EAPOL)-Start message **708** to trigger IEEE 802.1X full authentication **206**. When AR-RS **407** receives this start message, AR-RS **407** may skip IEEE 802.1X full authentication **206** by sending to mobile station **414** an EAPOL-Success message **710**, thereby indicating that authentication was successful without going through the IEEE 802.1X full authentication protocol **206**.

[0044] At this point, both base station **400** and mobile station **414** may hold the same security material such as AK **610**. Mobile station **414** and base station **400** may each derive MACK **616** from AK **610**. Mobile station **414** and base station **400** may hold previously calculated TEK **614** and/or previously generated KEK **612** and may perform SA-TEK 3-way handshake **214** to authenticate each other directly. Alternatively, as described above in connection with FIG. **6**, base station **400** may generate a new KEK **712** by using AK **610** and may generate a new TEK **714**. Base station **400** encrypts TEK **714** (or TEK **614**) using KEK **712** (or TEK **612**) and transmits encrypted TEK **714** (or TEK **614**) to mobile station **414** for data confidentiality.

[0045] Base station **400** immediately sends security material such as TEK **714** (or **614**) and MACK **616**, protected using relay key **410**, to AR-RS **407**. After AR-RS **407** obtains TEK **714** (or **614**) and MACK **616**, AR-RS **407** may switch the communication channel between mobile station **414** and AR-RS **407** to an authorized state to provide mobile station **414** with access to network **300**. Moreover, because mobile station **414** and AR-RS **407** then each have TEK **714** (or **614**) and MACK **616**, they may send encrypted data transmissions.

[0046] FIG. **8** is a signaling diagram of an exemplary handoff from an AR-RS connected to a current base station, e.g., AR-RS **407** connected to base station **400**, to a target AR-RS **802** connected to a different, target base station **804**. In FIG. **8**, mobile station **414** sends link up message **702** including a security material identification such as AKID to target AR-RS **802**. AKID identifies AK **610** currently stored in the memory of mobile station **414** (e.g., memory **526**, ROM **524**, RAM **522** or database **528**) due to prior authentication with AR-RS **407**. Target AR-RS **802** transmits the AKID to target base station **804** in AK verification signal request **704** to verify that the AK stored in mobile station **414** matches the AK stored in the memory of target base station **804** (e.g., memory **506**, ROM **504**, RAM **502** or database **508**). Target AR-RS **802** is not in communication with the same base station as AR-RS **407**, and as such does not share the same relay key **410**, but rather target AR-RS **802** and target base station **804** share a new relay key **806**. AK verification signal request **704** is therefore encrypted by AR-RS using new relay key **806**. If the AK present at target base station **804** matches the AK within the memory of mobile station **414** (e.g., memory **526**, ROM **524**, RAM **522** or database **528**), target base station **804** will transmit an AK Verification Success message to target AR-RS **806**; if the AKs do not match or either target base station **804** or mobile station **414** do not hold an AK, target base station **804** transmits an AK Verification Failure message **808** to target AR-RS **802**. In the exemplary embodiment shown in FIG. **8**, because mobile station **414** was previously authenticated through base station **400**, either the AK held by mobile station **414**, AK **610**, does not match that held by target base station **804** or target base station **804** does not have any AK corresponding to mobile station **414** so that target base station **804** transmits AK Verification Failure message **808** to mobile station **414**. Upon receipt of AK Verification Failure message **808**, mobile station **414** undergoes IEEE 802.1X full authentication **206** with AAA server **104**, obtains a new MSK **810**, a new PMK **812**, and a new AK **814** from target base station **804**.

[0047] When both target base station **804** and mobile station **414** have new AK **814**, they will derive MACK **820** and KEK **816** from AK **814** and perform SA-TEK 3-way handshake procedure **214** to authenticate each other. When SA-TEK 3-way handshake procedure **214** is successfully completed, the base station **804** may generate a new TEK **818** and transmit new TEK **818** or old TEK **712**, protected by KEK **816** to mobile station **414** for data confidentiality between mobile station **414** and relay station **407**.

[0048] Target base station **804** will also send the TEK **818** and MACK **820**, protected by new relay key **816**, to target AR-RS **802**. After target AR-RS **802** obtains TEK **818** and MACK **820**, it may switch the communication channel between mobile station **414** and target AR-RS **802** to the authorized state to provide mobile station **414** with access to the network **300**. Moreover, because mobile station **414** and target AR-RS **802** then each have TEK **816** and MACK **802**, they may communicate using encrypted data transmissions.

[0049] Although the processes described above for initialization and handoffs apply to mobile relay stations as well, mobile relay stations and the mobile stations accessing the network from within mobile relay stations must also be prepared for a change in base station where the AR-RS (specifically, the mobile relay station) does not change.

[0050] FIG. **9** is a signaling diagram of an exemplary mobile relay station handoff between a current base station and a target base station. In FIG. **9**, mobile relay station AR-RS **408** may associate with a target base station **900** when AR-RS **408** has moved or is about to move into the coverage area for target base station **900**. Mobile stations **416** and **418** are connected to AR-RS **408** and their connection with AR-RS **408** is preferably maintained throughout the transition to target base station **900**. In order to update the AKs of mobile stations **416** and **418**, AR-RS **408** may issue a ranging message **902** prior to sending the mobile stations **416** and **418** to alert mobile stations **416** and **418** of the necessity of updating their security material because AR-RS **408** is within or approaching the coverage area for target base station **900**.

Upon receipt of security material update message **902**, AR-RS **408** undergoes one or more of IEEE 802.1X authentication **206**, SA-TEK 3-way handshake **214**, and TEK 3-way handshake **216** with gateway **106** and AAA **104**. As such, AR-RS **408** must receive an AK and be authenticated in a similar manner to authentication of a mobile station. Gateway **106** may transfer the AK for the mobile relay station at an AK Transfer **904**.

[0051] AR-RS **408** transmits a re-authentication trigger message, or security material update message, **906** to mobile stations **416** and **418**. The re-authentication trigger message **906** may be sent in a multicast transmission to mobile stations **416** and **418**. Upon receipt of the re-authentication trigger message **906**, the mobile stations **416** and **418** perform IEEE 802.1X full authentication **206** with gateway **106** and AAA server **104**. Gateway **106** may calculate a new AK obtained from the existing PMK in the gateway for target base station **900**. Gateway **106** and/or AAA server **104** may transfer all of the security material, such as AKs, for the mobile stations associated with AR-RS **408** to target base station **900** at an AK Transfer **908**, and may do so in a tunnel mode, in which all of the parameters (e.g., AKs) of all mobile stations connecting to AR-RS **408** are transmitted at one time. In tunnel mode, the logical connection between two nodes, e.g., AR-RS **408** and gateway **106** is dedicated, and intermediate nodes do not process the tunnel packets but rather only forward them on. Mobile stations **416** and **418** then undergo SA-TEK 3-way handshake **214** with target base station **900**. Target base station **900** will provide security material such as TEKs and MACKs for each of the mobile stations to AR-RS **408** at a TEK Transfer **910**, and may do so using tunnel mode. In one embodiment, target base station **900** will aggregate security material and send security material for each of the mobile stations to AR-RS **408** at TEK Transfer **910** in a message aggregation mode. In one embodiment, the TEKs and MACKS are received at base station **900** and mobile stations **416** and **418** prior to the inter-base station handoff to avoid a disconnect in service to mobile stations **416** and **418**. AR-RS **408** may then provide secure data transmission to the mobile stations **416** and **418** and may do so without performing an authentication procedure with mobile stations **416** and/or **418**. In addition, AR-RS **408** may update only authentication data within the mobile stations **416** and **418** and, in some embodiments, may not change the traffic encryption key (TEK) held by the mobile stations **416** and/or **418**.

[0052] One of skill in the art will appreciate that although FIG. **9** shows target BS **900** communicating with the network and AAA server **104** via gateway **106**, target base station **900** may also communicate with the network and AAA server **104** via gateway **108**, or another gateway, with the same processing as described in FIG. **9**.

[0053] Systems and methods disclosed herein may be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. Apparatus embodying the invention can be implemented in a computer program product tangibly embodied in a machine-readable storage device for execution by a programmable processor. Method steps consistent with the invention can be performed by a programmable processor executing a program of instructions to perform functions of the invention by operating on the basis of input data, and by generating output data. Embodiments consistent with the invention may be implemented in one or several computer programs that are executable in a programmable system, which includes at least one programmable processor coupled to receive data from, and transmit data to, a storage system, at least one input device, and at least one output device, respectively. Computer programs may be implemented in a high-level or object-oriented programming language, and/or in assembly or machine code. The language or code can be a compiled or interpreted language or code. Processors may include general and special purpose microprocessors. A processor receives instructions and data from memories. Storage devices suitable for tangibly embodying computer program instructions and data include all forms of non-volatile memory, including by way of example semiconductor memory devices, such as EPROM, EEPROM, and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM disks. Any of the foregoing can be supplemented by or incorporated in ASICs (application-specific integrated circuits).

[0054] It will be apparent to those skilled in the art that various modifications and variations can be made in the system and method for establishing security associations in wireless communications systems. For example, one of skill in the art will appreciate that ranging requests and responses are a type of signaling message and that other signaling messages may be used. In addition, one of skill in the art will appreciate that traffic encryption keys are a type of traffic key and that other traffic keys may be used, and that MACKs are a type of verification key and that other verification keys may be used. One of skill in the art will also appreciate that communication between base stations and relay stations can be wireless or wired. It is intended that the standard and examples be considered as exemplary only, with a true scope of the disclosed embodiments being indicated by the following claims and their equivalents.

What is claimed is:

1. A method of providing secure communications between a base station, a relay station, and a mobile station in a communication network, the method comprising:

authenticating the mobile station over the communication network;

generating, by the base station, security material, wherein the security material comprises at least one of a traffic encryption key (TEK) and a message authentication code key (MACK);

transmitting, by the base station, the security material to the mobile station; and

transmitting, by the base station, the security material to the relay station.

2. The method of claim **1**, further comprising transmitting, by the base station, secured communications to the mobile station using the security material.

3. The method of claim **1**, wherein the authenticating includes performing secure authentication.

4. The method of claim **3**, wherein the authenticating includes performing IEEE 802.1X authentication.

5. The method of claim **1**, wherein the authenticating comprises receiving, at the base station, an authentication key (AK) from a communication network authenticator, wherein the security material is generated using the AK, and wherein the security material does not include the AK.

6. The method of claim **1**, wherein the authenticating comprises receiving, at the base station, a security material identification from the mobile station, the security material identification corresponding to an authentication key (AK) stored in the mobile station, transmitting, by the base station, a

verification success message to the mobile station if the base station recognizes the AK, and requiring the mobile station to perform IEEE 802.1X full authentication if the base station does not recognize the AK.

7. The method of claim **1**, further comprising establishing a secure communication path between the base station and the relay station, wherein the base station transmits the at least one security material to the relay station over the secure communication path.

8. The method of claim **1**, wherein communication between the base station and the relay station is wireless.

9. A base station for providing secure communications in a communication network, the base station comprising:

at least one memory to store data and instructions; and

at least one processor configured to access the memory and configured to, when executing the instructions:

authenticate a mobile station over the communication network;

generate security material, wherein the security material comprises at least one of a traffic encryption key (TEK) and a message authentication code key (MACK);

cause transmission of the security material to the mobile station; and

cause transmission of the security material to a relay station.

10. The base station of claim **9**, wherein executing the instruction to authenticate includes performing secure authentication.

11. The base station of claim **10**, wherein executing the instruction to authenticate includes performing IEEE 802.1X authentication.

12. The base station of claim **9**, wherein executing the instruction to authenticate includes receiving, at the base station, an authentication key (AK) from a communication network authenticator, wherein the security material is generated using the AK, and wherein the security material does not include the AK.

13. The base station of claim **9**, wherein executing the instruction to authenticate includes receiving, at the base station, a security material identification from a mobile station, the security material identification corresponding to an authentication key (AK) stored in the mobile station, transmitting, by the base station, a verification success message to the mobile station if the base station recognizes the AK, and requiring the mobile station to perform IEEE 802.1X full authentication if the base station does not recognize the AK.

14. The base station of claim **9**, wherein the at least one processor is further configured to establish a secure communication path between the base station and the relay station, and to transmit the security material to the relay station over the secure communication path.

15. The base station of claim **9**, wherein communication between the base station and the relay station is wireless.

16. A relay station for providing secure communications in a communication network, the relay station comprising:

at least one memory to store data and instructions; and

at least one processor configured to access the memory and configured to, when executing the instructions:

cause transmission of a mobile station verification request to a base station in response to a ranging request from at least one mobile station; and

perform secure data transmission with the at least one mobile station using security material received from the base station, wherein the security material comprises at least one of a traffic encryption key (TEK) and a message authentication code key (MACK).

17. The relay station of claim **16**, wherein the at least one processor is further configured to establish a secure communication path between the base station and the relay station, and wherein the relay station transmits the verification request to the base station over the secure communication path.

18. The relay station of claim **16**, wherein the relay station is a mobile relay station.

19. The relay station of claim **18**, wherein the at least one processor is further configured to cause transmission of a security material update message to the at least one mobile station to alert the at least one mobile station to update its security material.

20. The relay station of claim **19**, wherein the transmission of the security material update message to the at least one mobile station is a multicast transmission.

21. The relay station of claim **16**, wherein communication between the relay station and the base station is wireless.

22. A system for providing secure communications, the system comprising:

a base station configured to provide access to a communication network, authenticate at least one mobile station over the network, generate security material and transmit the security material; and

a relay station in communication with the base station for receiving the security material and for providing secure data transmissions to the at least one mobile station using the security material,

wherein the security material comprises at least one of a traffic encryption key (TEK) and a message authentication code key (MACK).

23. The system of claim **22**, wherein the relay station is a mobile relay station.

24. The system of claim **23**, wherein the base station aggregates the security material and transmits the aggregated security material to the relay station.

25. The system of claim **23**, wherein the relay station provides the secure data transmissions to the at least one mobile station using the security material without performing an authentication procedure with the at least one mobile station.

26. The system of claim **23**, wherein the relay station provides the secure data transmissions to the at least one mobile station using the security material but without changing the traffic encryption key (TEK) held by the at least one mobile station.

27. The system of claim **22**, wherein communication between the base station and the relay station is wireless.

* * * * *