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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 September 2012 (07.09.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/118445 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04W 12/04* (2009.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/SG2012/000062

(22) International Filing Date:
1 March 2012 (01.03.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201101532-8 3 March 2011 (03.03.2011) SG
201106745-1 19 September 2011 (19.09.2011) SG
201108175-9 4 November 2011 (04.11.2011) SG

(71) Applicant *(for all designated States except US)*: **AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 1 Fusionopolis Way, #20-10 Connexis, Singapore 138632 (SG).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **YEOW, Wai Leong** [SG/SG]; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way #21-01, Connexis South Tower, Singapore 138632 (SG). **TEO, Chee Ming Joseph** [SG/SG]; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way #21-01, Connexis South Tower, Singapore 138632 (SG). **PATHMASUNTHARAM, Jaya Shankar s/o** [SG/SG]; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way #21-01, Connexis South Tower, Singapore 138632 (SG). **HOANG, Anh Tuan** [VN/SG]; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way #21-01, Connexis South Tower, Singapore 138632 (SG).

(74) Agent: **VIERING, JENTSCHURA & PARTNER LLP**; P.O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (SG).

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

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

[Continued on next page]

(54) Title: KEY MANAGEMENT SCHEME FOR SECURE COMMUNICATION IN A CELLULAR MOBILE COMMUNICATION SYSTEM

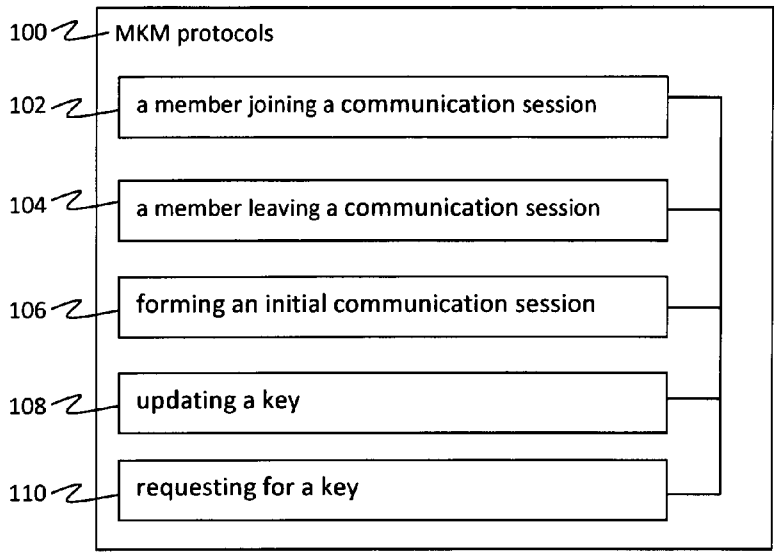

Figure 1

(57) Abstract: The present invention is directed to a base station of a cellular mobile communication system, the cellular mobile communication system comprising a communication network for providing a communication session for a plurality of communication terminals of the communication network, the base station comprising a determiner configured to determine whether there is a change of the participants of the communication session; a key provider configured to provide a key to be used for secure communication in the communication session after the change of participants; and a transceiver configured to send to the communication terminals participating in the communication session after the change of the participants a message comprising the key. A method of performing secure communication is also disclosed.

WO 2012/118445 A1

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

Published:

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

Key Management Scheme for Secure Communication in a Cellular Mobile Communication System

Cross-Reference To Related Application

[0001] This application makes reference to and claims the benefit of priority of the applications for "Methods For Multicast Key Management For IEEE 802.16n HR-Network" filed on March 3, 2011, "Mechanisms to Support Higher Reliability and Secure Communications in IEEE 802.16 Networks" filed on September 19, 2011, and "Mechanisms To Support HR-MS Forwarding To Network, Secure Communication, And Local Forwarding In IEEE 802.16 Networks" filed on November 4, 2011, all with the Intellectual Property Office of Singapore, and there duly assigned application numbers 201101532-8, 201106745-1, and 201108175-9, respectively.

Technical Field

[0002] Various embodiments generally relate to the field of key management schemes or protocols in cellular mobile communication systems, in particular, Multicast Key Management (MKM) protocols in networks using IEEE 802.16 communication standards.

Background

[0003] The IEEE 802.16n System Requirements Document (SRD) specifies a requirement for High Reliability (HR) network. One requirement is for the support of multicast communications for mobile stations (HR-MSs) so as to enable functions and applications such as Push-to-Talk (PTT) and Group communications, etc. The multicast communications can take place with or without Base Station (HR-BS) in order to provide high reliability.

[0004] To ensure secure multicast communications such that an attacker is not able to masquerade as a multicast member or eavesdrop in the multicast communications, multicast key management (MKM) protocols have to be designed for the 802.16n networks.

[0005] Although multicast is already supported in existing IEEE 802.16 standards and a Multicast and Broadcast Rekeying Algorithm (MBRA) has already been proposed, however, it was pointed out in existing literature that MBRA is not scalable and also does not provide backward and forward secrecy. Without backward secrecy, a new joining member is able to decrypt previous secure multicast communications sent before it joined. Without forward secrecy, a leaving member is still able to decrypt future secure multicast communications after leaving the multicast group. Further, the necessary use of both Group Key Encryption Key (GKEK) and Group Traffic Encryption Key (GTEK) in existing IEEE 802.16 standards increases key storage space.

[0006] Thus, there is a need to provide a key management scheme for secure communication, in particular, in a cellular mobile communication system of the IEEE 802.16n standard, seeking to address at least the above problems.

Summary of the Invention

[0007] In a first aspect, the present invention relates to a base station of a cellular mobile communication system, the cellular mobile communication system comprising a communication network for providing a communication session for a plurality of communication terminals of the communication network, the base station comprising a determiner configured to determine whether there is a change of the participants of the communication session; a key provider configured to provide a key to be used for secure communication in the communication session after the change of participants; and a transceiver configured to send to the communication terminals participating in the communication session after the change of the participants a message comprising the key.

[0008] According to a second aspect, the present invention relates to a method of performing secure communication among communication terminals in a cellular mobile

communication system, the cellular mobile communication system comprising a communication network for providing a communication session for a plurality of communication terminals of the communication network, the method comprising determining whether there is a change of the participants of the communication session; providing a key to be used for secure communication in the communication session after the change of participants; and sending to the communication terminals participating in the communication session after the change of the participants a message comprising the key.

Brief Description of the Drawings

[0009] In the drawings, like reference characters generally refer to the same parts throughout the different views. The drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention. In the following description, various embodiments of the invention are described with reference to the following drawings, in which:

[0010] Figure 1 shows an exemplary overview of the multicast key management (MKM) protocols/schemes, in accordance to various embodiments;

[0011] Figure 2 shows a schematic block diagram of a base station of a cellular mobile communication system, in accordance to various embodiments;

[0012] Figure 3 shows an example of a multicast scenario depicting communication terminals leaving a session in IEEE 802.16n HR network, in accordance to various embodiments;

[0013] Figure 4 shows a flow diagram of the scenario of Figure 3, in accordance to various embodiments;

[0014] Figure 5 shows a flow chart of the scenario of Figure 3, in accordance to various embodiments;

[0015] Figure 6 shows a non-limiting illustrative example of a multicast scenario when new nodes joins the multicast group in IEEE 802.16n HR network, in accordance to various embodiments;

[0016] Figure 7 shows a flow diagram of the scenario of Figure 6, in accordance to various embodiments;

[0017] Figure 8 shows a flow chart of the scenario of Figure 6 using the PKI-based approach, in accordance to various embodiments;

[0018] Figure 9 shows a flow chart of the scenario of Figure 6 using the pre-shared key-based approach, in accordance to various embodiments;

[0019] Figure 10 shows a flow diagram for MulticastKey-Request, in accordance to various embodiments;

[0020] Figure 11 shows a non-limiting illustrative example of a multicast scenario initial group (or communication session) formation in IEEE 802.16n HR network, in accordance to various embodiments;

[0021] Figure 12 shows a flow diagram of the scenario of Figure 11, in accordance to various embodiments;

[0022] Figure 13 shows a flow chart of the scenario of Figure 11 using the PKI-based approach, in accordance to various embodiments;

[0023] Figure 14 shows a flow chart of the scenario of Figure 11 using the pre-shared key-based approach, in accordance to various embodiments;

[0024] Figure 15 shows an example of Multicast Key Update / Rekey procedure (unicast), in accordance to various embodiments;

[0025] Figure 16 shows an example of Multicast Key Update / Rekey procedure (multicast), in accordance to various embodiments;

[0026] Figure 17 shows an example of MAK update, in accordance to various embodiments;

[0027] Figure 18 shows an example of MAK group update, in accordance to various embodiments;

[0028] Figure 19 shows a block diagram of an overall view of key management procedure, in accordance to various embodiments;

[0029] Figure 20 shows a schematic block diagram of a method of performing secure communication among communication terminals in a cellular mobile communication system, in accordance to various embodiments;

[0030] Figure 21 shows a flow diagram of an exemplary Join Event, in accordance to one embodiment; and

[0031] Figure 22 shows a flow diagram of an exemplary Leave Event, in accordance to one embodiment.

Detailed Description

[0032] The following detailed description refers to the accompanying drawings that show, by way of illustration, specific details and embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. Other embodiments may be utilized and structural, and logical changes may be made without departing from the scope of the invention. The various embodiments are not necessarily mutually exclusive, as some embodiments can be combined with one or more other embodiments to form new embodiments.

[0033] In order that the invention may be readily understood and put into practical effect, particular embodiments will now be described by way of examples and not limitations, and with reference to the figures.

[0034] Figure 1 shows an exemplary overview of the multicast key management (MKM) protocols/schemes 100 comprising protocols/schemes for a member joining a communication session (or group) 102, and a member leaving a communication sesssion 104, as well as for forming an initial communication session (or group) 106, updating a key 108, and requesting for a key 110. For communication terminals, for example for high-reliability mobile stations (HR-MSs) to perform secure communication using a key, a high-reliability base station (HR-BS) provides the key to the communication terminals. The secure communication among the communication terminals may be performed without involving the HR-BS.

[0035] A protocol may interchangably be referred to as a procedure.

[0036] In a first aspect, a base station of a cellular mobile communication system is provided as shown in Figure 2. In Figure 2, the base station 200 is a base station of the

cellular mobile communication system 202. The cellular mobile communication system 202 comprises a communication network 204 for providing a communication session for a plurality of communication terminals 206 of the communication network 204. The base station 200 comprises a determiner 208 configured to determine whether there is a change of the participants of the communication session; a key provider 210 configured to provide a key to be used for secure communication in the communication session after the change of participants; and a transceiver 212 configured to send to the communication terminals participating in the communication session after the change of the participants a message comprising the key.

[0037] In some embodiments, the determiner 208 and/or the key provider 210 may be external devices or software that are linked to the base station 200 over the communication network 204. In other words, the determiner 208 and/or the key provider 210 may not be part of the base station 200. As used herein, the term "linked" generally refers to having a communication connection, which may be a wireless communication connection, between the the determiner 208 and/or the key provider 210 and the base station 200.

[0038] In the context of various embodiments, the term "base station" (BS or interchangably referred to as HR-BS) refers to a node of a network, which communicates directly with the communication terminal, for example, the MS or HR-MS. It may be apparent that, in a network comprised of a plurality of network nodes including a BS, for example, the base station 200 of Figure 2, various operations performed for communication with an MS may be performed by the BS, or network nodes other than the BS. The term 'BS' may interchangably be referred to as the term 'fixed station', 'Node B', 'eNode B (eNB)', 'access point', 'Advanced Base Station (ABS)', 'MS operating in BS mode', etc.

[0039] In various embodiments, the base station 200 may be an appointed communication terminal. An appointed communication terminal refers to a communication terminal that performs the tasks typically carried out by a base station. The appointed communication terminal may be involved in communicating with other

communication terminals in the capacity of a base station. The appointed communication terminal may be a MS operating in BS mode.

[0040] As used herein, the term "communication terminal" may refer to a machine that assists data transmission, that is sending and/or receiving data information. Accordingly, the communication terminal may also be generally referred to as a node. For example, the communication terminal may be a communication terminal of the plurality of communication terminals 206. A communication terminal may be, for example but not limited to, a station, or a mobile station (MS), or a substation, or a port, or a mobile phone, or a cellular phone.

[0041] In one embodiment, the communication terminal may comprise a MS of the cellular mobile communication system. In other embodiments, the MS may be any of a Personal Digital Assistant (PDA), a cellular phone, a Personal Communication Service (PCS) phone, a Global System for Mobile (GSM) phone, a Wideband Code Division Multiple Access (WCDMA) phone, a Mobile Broadband System (MBS) phone, etc. The term 'MS' may interchangably be referred to as the term 'User Equipment (UE)', 'Subscriber Station (SS')), 'Mobile Subscriber Station (MSS)', 'mobile terminal', 'Advanced Mobile Station (AMS)', etc.

[0042] The plurality of communication terminals 206 may be referred to as a plurality of stations.

[0043] As used herein, the term "communication system" broadly refers to a system used to communicate information. According to one embodiment, the communication system is a cellular mobile communication system, for example the cellular mobile communication system 202 of Figure 2, comprising transmitting and receiving elements for communicating information.

[0044] In various embodiments, the communication system 202 may work in accordance with a IEEE 802.16 communication standard.

[0045] In the context of various embodiments, the term "communication network" generally refers to a wireless communication network. In various embodiments, the communication network, for example, the communication network 204 of Figure 2, may be a communication network according to a 802.16 communication standard. In one

embodiment, the communication network 204 may be a communication network according to the 802.16n communication standard. The term "communication network" also includes any method or medium for transmitting (or receiving) information from one node to another. A communication network is formed via a communication connection among nodes. A "communication connection" may generally refer to a link to provide information transfer between one node and another node.

[0046] In some embodiments, the terms "communication network" and "communication system" may be interchangably used.

[0047] In the context of various embodiments, the term "determiner" may refer to a computer-related entity, for example, hardware, a combination of hardware and software, software, or software in execution. A determiner, for example the determiner 208 of Figure 2 may be, but is not limited to, a process running on a processor, a processor, an object, an executable, a thread of execution, a program, and a computer that may be operable in the base station 200. As used herein, the term "determine" may refer but is not limited to "compute", "verify", "check", "evaluate", "establish", or "assess". In some examples, the determiner may be part of the base station. In other example, the determiner may be an external device linked to the base station; thereby not consituting part of the base station.

[0048] In the context of various embodiments, the term "communication session" may generally refer to a unit of communication access between two or more communication terminals. The term "communication session" may also more specifically refer to the period from the start to the end of the logical connection for communication executed between two or more communication terminals. A communication session may be provided with a set of transmitting communication terminals and receiving communication terminals, and the data stream(s) flowing from transmitting communication terminals to receiving communication terminals, or, logically the linked sending/receiving of one or more data/control streams between the transmitting communication terminals and receiving communication terminals. A multimedia conference may be an example of a communication session. A communication session may also be referred but not limited to as a "group", "grouping", or "assembly".

[0049] In various embodiments, the communication session may be a multicast session, that is, a communication session for a plurality of communication terminals, for example, more than two communication terminals.

[0050] In the context of various embodiments, the term "key" refers to a code that may be required for secure communication and may typically be shared among communication terminals in the session or the fresh session. Example of a key may be a multicast master key, a multicast authentication key, an encryption key, a traffic encryption key, a multicast (or group) traffic encryption key (MTEK or GTEK), or a multicast access code key. Existing 802.16 networks use an exclusive key KEK to securely transport GTEK or MTEK. In contrast, various embodiments of the present invention generally involve the use of unicast key shared between a base station and a mobile station and as a result render the exclusive key KEK redundant; thereby generally improving efficiency.

[0051] In various embodiments, the key for secure communication in the communication session after the change of participants may be a multicast traffic encryption key for secure communication in the communication session after the change of participants.

[0052] As used herein, the term "secure communication" refers to communication that is encrypted using a key for example, a public or private key. A public key is a key known to all communication terminals in the communication system 202 and a pre-shared key is key known to a group of communication terminals in the communication system 202, for example, communication terminals in a particular communication session. A private key is a key known only to a particular communication terminal in the communication system.

[0053] To "provide" a key interchangably refers to generate a key, obtain a key, retrieve a key from a key storage space, compute a key or derive a key.

[0054] In the context of various embodiments, the term "transceiver" refers to a combination transmitter/receiver. For example, a transceiver may be the transmitter and receiver combined into a single package. In general, a transceiver comprises both transmitting and receiving capabilities and functions.

[0055] The term "send" may refer but is not limited to transmit. In this context, the transceiver 212 means a node configured to send voice or data service.

[0056] As used herein, the term "message" refers to a signal or a communication signal. In the context of various embodiments, a message may be a short information sent from one entity (node), for example, the base station 200 of Figure 2, to at least another one entity (node), for example, a communication terminal of the plurality of communication terminals 206. A message may be a packet or a cluster.

[0057] For example, a message may comprise precisely formatted data that is sent and received by nodes and may represent a request, report, or an event. The message may be comprised in or encoded in or indicated in another message or information.

[0058] The message may comprise a message body, which is a section of a message that contains the contents of the message, and which may be of a predetermined structure. The message may also comprise a message header, which is an information structure in a message that precedes and identifies the information that follows within the message, and describes specifics about the message such as the properties of the message. The message may also refer to a data element encapsulated in a package of flags.

[0059] In various embodiments, a message has a MaxResends and Message Timeout. For example, when a node (e.g. HR-MS, HR-BS etc), say A does not receive the relevant message for the other node B within the Message Timeout time, then the node A will resend its message. If the MaxResends number is reached for that message, then it will initiate another round of authentication or drop the direct communications.

[0060] In various embodiments, the message may be encrypted using an authentication key or an encryption key.

[0061] As used herein, an "authentication key" refers to a key for the purpose of enabling the base station, for example, the base station 200 of Figure 2, to confirm the identity of the communication terminal, for example, any of the plurality of communication terminals 206 of Figure 2, when information is exchanged between the communication terminal and the base station. For example, an authentication key may refer but is not limited to a public authentication key, or a private authentication key, a multicast authentication key, a pre-shared authentication key, a message authentication code

(MAC) key, or a multicast cipher-based message authentication code (MCMAC) key, or a unicast message authentication key.

[0062] The term "encryption" in a broad context may include decryption. Accordingly, the term "encryption key" encompasses a key necessary to encrypt and/or decrypt data. Of course, in some contexts, the term "encryption" does not encompass decryption. For example, an encryption key may refer but is not limited to a multicast (or group) traffic encryption key, or a public encryption key, or a private encryption key, or a pre-shared encryption key, or a unicast encryption key.

[0063] In the context of various embodiments, the term "change of participants" refers to a difference between the participants in a first communication session and the participants in a second communication session. The first communication session and second communication session may be consecutive communication sessions. The term "participants" refers to communication terminals, for example, the plurality of communication terminals 206 of Figure 2.

[0064] In various embodiments, the change of the participants of the communication session may comprise at least one of the plurality of communication terminals 206 in the communication session leaving the communication session, or a communication terminal not in the communication session joining the communication session with the plurality of communication terminals 206.

[0065] As used herein, the term "leaving" refers to the at least one of the plurality of communication terminals 206, initially communicating in a communication session no longer forms part of this communication session and no longer communicates with other communication terminals still in this communication session. For example, the communication terminal leaving the session may be the member leaving a communication session 104 of Figure 1.

[0066] The term "joining" refers to a communication terminal, initially not part of a communication session becomes a part of the communication session and can therefore communicate with other communication terminals, for example, the plurality of communication terminals 206, in the communication session. For example, the

communication terminal joining the communication session may be the member joining a communication session 102 of Figure 1.

[0067] "Leaving" and "joining" are non-permanent states of a communication terminal, that is, a leaving communication terminal may eventually re-join the communication session or a joining communication terminal may eventually leave the communication session. Such states may recurring states.

[0068] "Joining" or "leaving" a communication session refers to a communication session after the change of participants, for example, being formed with the relevant communication terminals. The term "after" refers to a subsquent state of the communication session. In contrast, the term "before" used with reference to a "communication session before the change of participants" means a previous or current/existing state of the communication session.

[0069] For example, in "joining", the communication session after the change of participants may be a common communication session provided for the combination of the joining communication terminal and the communication terminals in the communication session before the change of participants.

[0070] In another example, in "leaving", the communication session after the change of participants may be a common communication session provided for the remaining communication terminals in the communication session before the change of participants with the except of the leaving communication terminal.

[0071] In various embodiments, a base station, for example, the base station 200 of Figure 2, may receive information or a request that involves a MKM protocol, for example, the (MKM) protocols/schemes 100 of Figure 1. Based on the protocol, the base station may send a message comprising a key to communication terminals in a communication session. More specifically, in accordance with the protocols, the base station checks and determines whether there is a change of the participants of a communication session. A change of participants may occur when a communication terminal joins a communication session or when a communication terminal in a communication session leaves the communication session. When joining a communication session, the joining communication terminal is provided with a key to be

used for secure communication with other communication terminals in the communication session. When leaving a communication session, the leaving communication terminal is not provided with a key which is used for secure communication among the remaining communication terminals in the communication session. The protocols in accordance to various embodiments allow for backward secrecy and forward secrecy.

[0072] In various embodiments, the transceiver 212 may be configured to include a nonce into the message.

[0073] In various embodiments, the message comprising the key or its parameters for secure communication in the communication session after the change of participants may be encrypted and/or signed by a pre-shared authentication key when it has been determined that the at least one of the plurality of communication terminals 206 in the communication session is leaving the communication session.

[0074] The pre-shared authentication key is pre-established by some means before the commencement of multicast key management, that is, before the base station starts to determine whether there is a change of the participants of the communication session, to provide a key to be used for secure communication in the communication session after the change of participants; and to send to the communication terminals participating in the communication session after the change of the participants a message comprising the key.

[0075] For example, the at least one of the plurality of communication terminals 206 in the communication session leaving the communication session may be the member leaving a communication session 104 of Figure 1. In this context, the communication session refers to a communication session before the change of participants.

[0076] The terms "parameters" may include MC nonce and/or counter necessary to derive sub-keys. A sub-key is a key that sits within or comprised in another key. A message being further signed by a key or a pre-shared authentication key is to add integrity protection.

[0077] A non-limiting illustrative example of a multicast scenario depicting communication terminals (nodes or HR-MSs) 302 leaving the communication session (or

multicast group) in IEEE 802.16n HR network is shown in Figure 3. The leave scheme/protocol of the public key infrastructure (PKI)-based approach is the same as that of the pre-shared key-based approach. Generally, the PKI-based approach assumes that each node is equipped with Public Key Certificates and Private/public key pair for authentication during multicast key management (MKM). The pre-shared key-based approach assumes that a key has already been pre-established by some means before the commencement of multicast key management.

[0078] The leave protocol may be used to change the multicast key whenever a node leaves the multicast group so as to ensure forward secrecy, i.e. the leaving member is not able to decrypt future secure multicast communications after leaving the multicast group.

[0079] It should be noted that the number of leaving nodes can be more than 1, i.e. $1 \leq l \leq L$ where L is the total number of leaving nodes from the multicast group. A leaving node may interchangably be referred to as a communication terminal leaving the communication session. The flow diagram for this scenario is depicted in Figure 4 and the flow chart for this scenario is shown in Figure 5.

[0080] (Leaving) Step 500: The base station or the appointed mobile station (HR-MSX/BS) 300 generates nonce $N'_{\text{HR-MSX/BS}}$, and new group key *GTEK'*, and computes $\theta'_{\text{HR-MSi}}$ = $MAC(MSKi|GTEK'|N'_{\text{HR-MSX/BS}}|\text{HR-MSX/BSAddr}|\text{HR-MSiAddr}|\text{MulticastGrpID})$ for $1 \leq i \neq L \leq n$, where n is the total number of nodes. The HR-MSX/BS 300 then uses the shared key *MSKi* with the remaining HR-MS*i* for $1 \leq i \neq L \leq n$ 304, 306, 308, 310 to encrypt and obtain $c'_i = \varepsilon_{MSKi}(GTEK', GTEK'\_lifetime, \text{HR-MSX/BSAddr}, N'_{\text{HR-MSX/BS}})$. Finally, HR-MSX/BS sends the following messages 400 to remaining HR-MS*i* for $1 \leq i \neq L \leq n$ 304, 306, 308, 310:

$$\text{HR-MSX/BS} \rightarrow \text{HR-MSi} : \text{Multicast\_Leave\_MSG\_\#1}$$

where Multicast_Leave_MSG_#1 = $\text{MulticastGrpID}|T'_{\text{HR-MSX/BS}}|N'_{\text{HR-MSX/BS}}|\text{HR-MSX/BSAddr}|c'_i|\theta'_{\text{HR-MSi}}$.

[0081] (Leaving) Step 502: Each remaining HR-MS*i* for $1 \leq i \neq L \leq n$ 304, 306, 308, 310 first verifies the received timestamp and nonce for freshness. If the verifications are correct, then each remaining HR-MS*i* 304, 306, 308, 310 uses its shared key *MSKi* to

decrypt c'_i and obtains the new *GTEK'*, and *GTEK'_lifetime*. Next, each remaining HR-MS*i* 304, 306, 308, 310 verifies $\theta'_{\text{HR-MSi}}$. If the verification is correct, then each remaining HR-MS*i* 304, 306, 308, 310 can commence secure multicast.

[0082] Each remaining HR-MS*i* 304, 306, 308, 310 uses the new *GTEK'* for the multicast session. Since the leaving node(s) 302 does not have the new *GTEK'*, it will not be able to participate in the multicast session where the new *GTEK'* is required. Therefore this leave protocol advantageously provides forward secrecy in the secure communication among the remaining HR-MS*i* 304, 306, 308, 310 of the multicast session.

[0083] Table 1 shows the Multicast_Leave_MSG_#1 message attribute.

[0084] Table 1

Notation	Meaning
MulticastGrpID	Multicast Group ID
$T'_{\text{HR-MSX/BS}}$	Timestamp generated by HR-MSX/BS
$N'_{\text{HR-MSX/BS}}$	Freshly generated random number of 64bits by HR-MSX/BS
HR-MSX/BSAddr	Address of HR-MSX/BS
c'_i	symmetric key encryption using pre-shared key $MSKi$ of remaining multicast members HR-MSi
$\theta'_{\text{HR-MSi}}$	Key confirmation/MAC generated by HR-MSX/BS for remaining multicast members HR-MSi

[0085] The *GTEK* is used to encrypt data packets for the multicast service and it is shared amongst the HR-MSs that belongs to the multicast group. The *GTEK* is randomly generated by the HR-MSX/BS 300 (which may be the HR-BS or an appointed HR-MS if there is not HR-BS present). The *GTEK* may be encrypted with the pre-shared key *MSKi* in Multicast_Leave_MSG_#1 of both PKI-based and pre-shared key based leave protocol.

[0086] The *MSKi* is a key shared between the multicast members HR-MS*i* 304, 306, 308, 310 and the controller HR-MSX/BS 300. It is used as an encryption key and also as a MAC key. In the PKI-based approach, the *MSKi* can be randomly generated by HR-MSX/BS 300 (which may be the HR-BS or an appointed HR-MS if there is no HR-BS

present). In the pre-shared key approach, the *MSKi* is pre-established between HR-MS*i* 304, 306, 308, 310 and the controller HR-MSX/BS 300.

[0087] The *MSKi* may be refreshed/rekeyed periodically to maintain key freshness.

[0088] The HR-MSX/BS 300 may be the base station 200 of Figure 2. The remaining HR-MS*i* 304, 306, 308, 310 may be the plurality of communication terminals 206 of Figure 2.

[0089] In various embodiments, the base station 200 may further comprise a transceiver configured to receive an incoming message from the communication terminal not in the communication session. In this context, the communication session refers to the communication session before the change of participants.

[0090] In the context of various embodiments, the transceiver may be as defined above and may be the transceiver 212 of Figure 2. The incoming message may be defined as the message described herein.

[0091] As used herein, the term "receive" may interchangably be referred but not limited to as listen, or collect, or detect. For example, "receive" may further include to determine that the received message is correctly or incorrectly obtained. When correctly obtained, the received message is identical or at least substantially similar as the transmitted message. Such determining of a correct or incorrect message may be performed by error detections, for example, cyclic redundancy check (CRC). Further to this, the correctly obtained message may also need to contain an absolute power level or a relative power level to noise and interference above a particular threshold. The correctly obtained message may also need to indicate a time and or frequency offset below a particular threshold. In this context, a receiver means a node or terminal that receives voice or data service.

[0092] The transceiver 212 may be configured to check the received incoming message for message freshness.

[0093] As used herein, the term "message freshness" refers to a characteristic of a message being new or current if it was not sent in the past. Message freshness may be indicated by a nonce and/or time stamp in the message.

[0094] In various embodiments, the message comprising the key for secure communication in the communication session after the change of participants may be encrypted by a pre-shared authentication key.

[0095] In other embodiments, the transceiver 212 may be configured to include a certificate into the message. The message comprising the key for secure communication in the communication session after the change of participants may be encrypted and/or signed by a public key and a private key respectively shared by the communication terminals of the communication system. A message being further signed by a private key is to add integrity protection.

[0096] A certificate may be included into a message when the PKI-based approach is used. As used herein, the term "certificate" refers to a document that attests to the truth of something or the ownership of something. The term "attest" implies at least two entities which are involved in the use of a certificate. For example, a certificate is a digital certificate issued by a certification authority for mutual authentication and multicast key management.

[0097] In some embodiments, the message may be encrypted and/or signed by respective keys for secure communication in the communication session before or after the change of participants when it has been determined based on the incoming message that the communication terminal not in the communication session is joining the communication session with the plurality of communication terminals 206. In this context, the communication session refers to the communication session before the change of participants. For example, the "respective keys" may respectively refer to prekey/subkeys and new keying materials generated through a number used to derive the prekeys, for example, MC_nonce.

[0098] For example, the communication terminal not in the communication session joining the communication session with the plurality of communication terminals 206 may refer to the member joining a communication session 102 of Figure 1.

[0099] A non-limiting illustrative example of a multicast scenario when new nodes HR-MS*j* 600 joins the multicast group 604, 606, 608, 610 in IEEE 802.16n HR network is shown in Figure 6. The join (or joining) scheme/protocol may be of public key

infrastructure (PKI)-based approach or of the pre-shared key-based approach. It should be noted that the number of joining nodes can be more than 1, i.e. $1 \leq j \leq m$ where m is the number of joining nodes. A joining node may interchangably be referred to as a communication terminal joining the communication session.

[00100] The join protocol may be used create a new multicast key whenever there are multicast members joining the group to provide backward secrecy, i.e. new members are not able to decrypt previous secure multicast communications. For PKI-based approach, a secret pairwise key may also be established between HR-MSX/BS 602 and new member HR-MS*j* 600.

[00101] As used herein, the term "pairwise" is used to refer to a type of encryption key hierarchy pertaining to keys shared by only two entities or nodes.

[00102] For the PKI-based approach, the flow diagram for this scenario is depicted in Figure 7 and the flow chart for this scenario is shown in Figure 8.

[00103] **(Joining) Step 800**: New mobile station HR-MS*j* 600 first generates nonce $N_{\text{HR-MSj}}$. Next, HR-MS*j* computes the signature $\sigma_{\text{HR-MSj}}$ = SIGN(MulticastGrpID|$T_{\text{HR-MSj}}$|$N_{\text{HR-MSj}}$|HR-MSX/BSAddr|HR-MSjAddr) and sends the following message 700 to HR-MSX/BS 602:

$$\text{HR-MSj} \rightarrow \text{HR-MSX/BS} : \text{Join\_MG\_MSG\_\#1}$$

where Join_MG_MSG_#1 = MulticastGrpID|$T_{\text{HR-MSj}}$|$N_{\text{HR-MSj}}$|HR-MSX/BSAddr|HR-MSjAddr|$\sigma_{\text{HR-MSj}}$|Cert(HR-MSj).

[00104] **(Joining) Step 802**: HR-MSX/BS 602 first verifies the received timestamps and nonces for freshness and the certificate Cert(HR-MSj) and signature $\sigma_{\text{HR-MSj}}$. If the verifications are correct, then HR-MSX/BS 602 generates nonce $N'_{\text{HR-MSX/BS}}$, *GTEK'* and *MSKj* and computes $\theta_{\text{HR-MSX/BS}}$ = *MAC*(*GTEK'*|$N'_{\text{HR-MSX/BS}}$|HR-MSX/BSAddr|MulticastGrpID) and $\theta_{\text{HR-MSj}}$ = *MAC*(*MSKj*|*GTEK'*|$N'_{\text{HR-MSX/BS}}$|$N_{\text{HR-MSj}}$|HR-MSX/BSAddr|HR-MSjAddr). HR-MSX/BS 602 then uses HR-MS*j*'s 600 public key to encrypt and obtain $c_j = \varepsilon_{\text{HR-MSj\_PK}}$(*MSKj, GTEK', MSKj_lifetime, GTEK'_lifetime,* HR-MSjAddr, HR-MSX/BSAddr). HR-MSX/BS 602 also encrypts using the existing *GTEK* and obtains $c' = \varepsilon_{GTEK}$(*GTEK', GTEK'_lifetime,* HR-MSX/BSAddr, $N'_{\text{HR-MSX/BS}}$).

Finally, HR-MSX/BS 602 computes signature $\sigma'_{\text{HR-MS}j}$ = SIGN(MulticastGrpID|$T'_{\text{HR-MSX/BSAddr}}$|$N'_{\text{HR-MSX/BSAddr}}$|HR-MSjAddr|HR-MSX/BSAddr|$N_{\text{HR-MS}j}$|c_j|$\theta_{\text{HR-MS}j}$) and sends the following messages 702, 704 to HR-MS*i* 604, 606, 608, 610 for $1 \leq i \leq n$ and HR-MS*j* 600, respectively:

HR-MSX/BS → HR-MSi : Multicast_Join_MSG_#2

HR-MSX/BS → HR-MSj : Multicast_Join_MSG_#3

where Multicast_Join_MSG_#2 = MulticastGrpID|$T'_{\text{HR-MSX/BS}}$|$N'_{\text{HR-MSX/BS}}$|HR-MSX/BSAddr|c'|$\theta_{\text{HR-MSX/BS}}$ and Multicast_Join_MSG_#3 = MulticastGrpID|$T'_{\text{HR-MSX/BS}}$|$N'_{\text{HR-MSX/BS}}$|HR-MSjAddr|HR-MSX/BSAddr|$N_{\text{HR-MS}j}$|c_j|$\theta_{\text{HR-MS}j}$|$\sigma'_{\text{HR-MS}j}$.

[00105] **(Joining) Step 804**: Each HR-MS*i* 604, 606, 608, 610 for $1 \leq i \leq n$ first verifies the received timestamp and nonce for freshness. If the verifications are correct, then each HR-MS*i* 604, 606, 608, 610 decrypts *c'* and obtains the new *GTEK'*, and *GTEK'_lifetime*. Next, each HR-MS*i* 604, 606, 608, 610 verifies $\theta_{\text{HR-MSX/BS}}$. If the verification is correct, then HR-MS*i* 604, 606, 608, 610 can commence secure multicast.

[00106] **(Joining) Step 806**: HR-MS*j* 600 first verifies the received timestamp and nonces for freshness and the signature $\sigma'_{\text{HR-MS}j}$. If the verifications are correct, then HR-MS*j* 600 decrypts c_j and obtains *MSKj*, *GTEK'*, *MSKj_lifetime* and *GTEK'_lifetime*. Next, HR-MS*j* 600 verifies $\theta_{\text{HR-MS}j}$. If the verification is correct, then HR-MS*j* 600 can commence secure multicast.

[00107] HR-MS*i* 604, 606, 608, 610 and HR-MS*j* 600 use the new *GTEK'* for the multicast session after the change of participants. Since HR-MS*j* 600 no longer have the key for the previous communication session before it joined this multicast session, it will not be able to participate in that previous communication session since the key required for the previous communication session is not the same as the new *GTEK'* for the multicast session after the change of participants. Therefore this join protocol advantageously provides backward secrecy in the secure communication among HR-MS*i* 604, 606, 608, 610 and HR-MS*j* 600 of the multicast session.

[00108] Table 2 shows the Join_MG_MSG_#1 message attribute (PKI-based appproach).

[00109] Table 2

Notation	Meaning
MulticastGrpID	Multicast Group ID
T_{HR-MSj}	Timestamp generated by HR-MSj
N_{HR-MSj}	Freshly generated random number of 64bits by HR-MSj
HR-MSX/BSAddr	Address of HR-MSX/BS
HR-MSjAddr	Address of HR-MSj
σ_{HR-MSj}	signature of message generated by HR-MSj
Cert(HR-MSj)	digital certificate of HR-MSj

[00110] Table 3 shows the Multicast_Join_MSG_#2 message attribute (PKI-based appproach).

[00111] Table 3

Notation	Meaning
MulticastGrpID	Multicast Group ID
$T'_{HR-MSX/BS}$	Timestamp generated by HR-MSX/BS
$N'_{HR-MSX/BS}$	Freshly generated random number of 64bits by HR-MSX/BS
HR-MSX/BSAddr	Address of HR-MSX/BS
c'	Symmetric key encryption of new GTEK' and its lifetime using current GTEK
$\theta_{HR-MSX/BS}$	Key confirmation/MAC generated by HR-MSX/BS

[00112] Table 4 shows the Multicast_Join_MSG_#3 message attribute (PKI-based appproach).

[00113] Table 4

Notation	Meaning
MulticastGrpID	Multicast Group ID
$T'_{HR-MSX/BS}$	Timestamp generated by HR-MSX/BS
$N'_{HR-MSX/BS}$	Freshly generated random number of 64bits by HR-MSX/BS
HR-MSjAddr	Address of HR-MSj
HR-MSX/BSAddr	Address of HR-MSX/BS
N_{HR-MSj}	Nonce generated by HR-MSj in Join_MG_MSG_#1 message
c_j	public key encryption using HR-MSj's public key HR-MSj_PK
θ_{HR-MSj}	Key confirmation/MAC generated by HR-MSX/BS for HR-MSj
σ'_{HR-MSj}	signature of message generated by HR-MSj

[00114] As defined above, the *GTEK* is used to encrypt data packets for the multicast service and it is shared amongst the HR-MSs that belongs to the multicast group. The *GTEK* is randomly generated by the HR-MSX/BS 602 (which can be the HR-BS or an appointed HR-MS if there is not HR-BS present). The *GTEK* may be encrypted by HR-MS*i*/HR-MS*j*'s public key in Multicast_Join_MSG_#3 in the PKI-based join protocol. The new *GTEK'* may be encrypted with the existing *GTEK* in Multicast_Join_MSG_#2 of the PKI-based join protocol.

[00115] The *MSKi/MSKj* is a key shared between the multicast members HR-MS*i* 604, 606, 608, 610/HR-MS*j* 600 and the controller HR-MSX/BS 602. It is used as an encryption key and also as a MAC key. In the PKI-based approach, the *MSKi/MSKj* may be randomly generated by HR-MSX/BS 602 (which can be the HR-BS or an appointed HR-MS if there is not HR-BS present). The *MSKi/MSKj* may be refreshed/rekeyed periodically to maintain key freshness.

[00116] The HR-MSX/BS 602 may be the base station 200 of Figure 2. The HR-MS*i* 604, 606, 608, 610 may be the plurality of communication terminals 206 of Figure 2.

[00117] In another example, for the pre-shared key-based approach, the flow diagram for this scenario (as described in Figure 6) is similarly depicted in Figure 7 and the flow chart for this scenario is shown in Figure 9.

[00118] **(Joining) Step 900**: New mobile station HR-MS*j* 600 first generates nonce $N_{\text{HR-MSj}}$. Next, HR-MS*j* 600 computes the MAC $\theta_{\text{HR-MSj}}$ = $MAC(MSKj|\text{MulticastGrpID}|T_{\text{HR-MSj}}|N_{\text{HR-MSj}}|\text{HR-MSX/BSAddr}|\text{HR-MSjAddr})$ and sends the following message 700 to HR-MSX/BS 602:

$$\text{HR-MSj} \rightarrow \text{HR-MSX/BS} : \text{Join\_MG\_MSG\_\#1}$$

where Join_MG_MSG_#1 = $\text{MulticastGrpID}|T_{\text{HR-MSj}}|N_{\text{HR-MSj}}|\text{HR-MSX/BSAddr}|\text{HR-MSjAddr}|\theta_{\text{HR-MSj}}$.

[00119] **(Joining) Step 902**: HR-MSX/BS 602 first verifies the received timestamps and nonces for freshness and $\theta_{\text{HR-MSj}}$. If the verifications are correct, then HR-MSX/BS 602 generates nonce $N'_{\text{HR-MSX/BS}}$, *GTEK'* and computes $\theta_{\text{HR-MSX/BS}} = MAC(GTEK'|N'_{\text{HR-MSX/BS}}|\text{HR-MSX/BSAddr}|\text{MulticastGrpID})$ and $\theta_{\text{HR-MSj}} = MAC(MSKj|GTEK'|N'_{\text{HR-}}$

$_{MSX/BS}|N_{HR\text{-}MSj}|$HR-MSX/BSAddr|HR-MSjAddr). HR-MSX/BS 602 then encrypt and obtain $c_j = \varepsilon_{MSKj}(GTEK', GTEK'\_lifetime,$ HR-MSjAddr, HR-MSX/BSAddr). HR-MSX/BS 602 also encrypts using the existing *GTEK* and obtains $c' = \varepsilon_{GTEK}(GTEK', GTEK'\_lifetime,$ HR-MSX/BSAddr, $N'_{HR\text{-}MSX/BS}$). Finally, HR-MSX/BS 602 sends the following messages 702, 704 to HR-MS*i* 604, 606, 608, 610 for $1 \leq i \leq n$ and HR-MS*j* 600, respectively:

HR-MSX/BS → HR-MSi : Multicast_Join_MSG_#2

HR-MSX/BS → HR-MSj : Multicast_Join_MSG_#3

[00120] where Multicast_Join_MSG_#2 = MulticastGrpID$|T'_{HR\text{-}MSX/BS}|N'_{HR\text{-}MSX/BS}|$HR-MSX/BSAddr$|c'|\theta_{HR\text{-}MSX/BS}$ and Multicast_Join_MSG_#3 = MulticastGrpID$|T'_{HR\text{-}MSX/BS}|N'_{HR\text{-}MSX/BS}|$HR-MSjAddr|HR-MSX/BSAddr$|N_{HR\text{-}MSj}|c_j|\theta_{HR\text{-}MSj}$.

[00121] **(Joining) Step 904**: Each HR-MS*i* 604, 606, 608, 610 for $1 \leq i \leq n$ first verifies the received timestamp and nonce for freshness. If the verifications are correct, then each HR-MS*i* 604, 606, 608, 610 decrypts *c'* and obtains the new *GTEK'*, and *GTEK'_lifetime*. Next, each HR-MS*i* 604, 606, 608, 610 verifies $\theta_{HR\text{-}MSX/BS}$. If the verification is correct, then HR-MS*i* 604, 606, 608, 610 can commence secure multicast.

[00122] **(Joining) Step 906**: HR-MS*j* 600 first verifies the received timestamp and nonces for freshness. If the verifications are correct, then HR-MS*j* 600 uses *MSKj* to decrypt c_j and obtains *GTEK'* and *GTEK'_lifetime*. Next, HR-MS*j* 600 verifies $\theta_{HR\text{-}MSj}$. If the verification is correct, then HR-MS*j* 600 can commence secure multicast.

[00123] Similar to the join protocol for the PKI-based approach, HR-MS*i* 604, 606, 608, 610 and HR-MS*j* 600 use the new *GTEK'* for the multicast session after the change of participants. Since HR-MS*j* 600 no longer have the key for the previous communication session before it joined this multicast session, it will not be able to participate in the previous communication session where the key required for the previous communication session is not the same as the new *GTEK'* for the multicast session after the change of participants. Therefore this join protocol advantageously

provides backward secrecy in the secure communication among HR-MS*i* 604, 606, 608, 610 and HR-MS*j* 600 of the multicast session.

[00124] Table 5 shows the Join_MG_MSG_#1 message attribute (pre-shared key-based appproach).

[00125] Table 5

Notation	Meaning
MulticastGrpID	Multicast Group ID
T_{HR-MSj}	Timestamp generated by HR-MSj
N_{HR-MSj}	Freshly generated random number of 64bits by HR-MSj
HR-MSX/BSAddr	Address of HR-MSX/BS
HR-MSjAddr	Address of HR-MSj
θ_{HR-MSj}	MAC generated by HR-MSj

[00126] Table 6 shows the Multicast_Join_MSG_#2 message attribute (pre-shared key-based appproach).

[00127] Table 6

Notation	Meaning
MulticastGrpID	Multicast Group ID
$T'_{HR-MSX/BS}$	Timestamp generated by HR-MSX/BS
$N'_{HR-MSX/BS}$	Freshly generated random number of 64bits by HR-MSX/BS
HR-MSX/BSAddr	Address of HR-MSX/BS
c'	Symmetric key encryption of new GTEK' and its lifetime using current GTEK
$\theta_{HR-MSX/BS}$	Key confirmation/MAC generated by HR-MSX/BS

[00128] Table 7 shows the Multicast_Join_MSG_#3 message attribute (pre-shared key-based appproach).

[00129] Table 7

Notation	Meaning
MulticastGrpID	Multicast Group ID
$T'_{HR\text{-}MSX/BS}$	Timestamp generated by HR-MSX/BS
$N'_{HR\text{-}MSX/BS}$	Freshly generated random number of 64bits by HR-MSX/BS
HR-MSjAddr	Address of HR-MSj
HR-MSX/BSAddr	Address of HR-MSX/BS
$N_{HR\text{-}MSj}$	Nonce generated by HR-MSj in Join_MG_MSG_#1 message
c_j	symmetric key encryption using pre-shared key $MSKj$
$\theta_{HR\text{-}MSj}$	Key confirmation/MAC generated by HR-MSX/BS for HR-MSj

[00130] The *GTEK* may be encrypted with the pre-shared key *MSKi/MSKj* in Multicast_Join_MSG_#3 in the pre-shared key-based join protocol. The new *GTEK'* may be encrypted with the existing *GTEK* in Multicast_Join_MSG_#2 of the pre-shared key-based join protocol.

[00131] In various embodiments, the base station 200 may further comprise a transceiver configured to receive a request for the key for secure communication in the communication session after the change of participants from any communication terminal in the communication session after the change of participants.

[00132] For example, a "request for the key" may be made to help a communication terminal (or a MS) with a lost key to retrieve the key through unreliable communication.

[00133] For example, the message comprising the key for secure communication in the communication session after the change of participants may comprise a message comprising a parameter of the key for secure communication in the communication session after the change of participants; and wherein the transceiver may be configured to send the message to the requesting communication terminal in the communication session after the change of participants.

[00134] As used herein, the term "parameter of the key" may refer, for example, to information about the remaining lifetime of the key or a current counter for the key. The term "parameter of the key" may interchangably be referred to as "keying material".

[00135] In some embodiments, the message comprising the parameter of the key for secure communication in the communication session after the change of participants may be encrypted and/or signed by by respective keys for secure communication in the

communication session before the change of participants. The term "respective keys" is as defined above.

[00136] In the following example of multicast security for 802.16n GridMAN standards, the keying material may be defined by a 160-bit MAK, 128-bit MCNonce and 16-bit MTEK.

Multicast Key Derivation

[00137] The traffic encryption keys and message authentication code (MAC) keys used in a secure multicast operation (identified by MulticastGrpID) are derived from a hierarchy using three keying material: the 160-bit Multicast Authentication Key (MAK) as a root, a 128-bit nonce MCNonce, and a 16-bit counter COUNTER_MTEK for rekying traffic encryption keys.

MAK

[00138] The 160-bit Multicast Authentication Key (MAK) is the pre-established shared key that is shared among authorized devices of a multicast service. It can be transported via Extensible Authentication Protocol (EAP) methods or other methods that provide stronger or equivalent cryptographic strength than 160-bit.

MCMAC-MTEK Prekey Derivation

[00139] The MCMAC-MTEK Prekey is an immediate sub key derived from the MAK using MulticastGrpID and MCNonce as follows:

MCMAC-MTEK Prekey = Dot16KDF(MAK, MulticastGrpID| MCNonce|| "MCMAC-MTEK prekey", 160)

Where:

- MulticastGrpID is the identifier used for the multicast service.
- MCNonce is a randomly generated number by HR-BS, for example, the base station 200 of Figure 2, or network entity to ensure different sets of MCMAC and MTEK keys are derived after rekeying.
- Dot16KDF is a hashing function defined in the IEEE 802.16 standard.

[00140] The MCMAC-MTEK Prekey is used to derive Multicast Cipher-based Message Authentication Code (MCMAC) key; and Multicast Traffic Encryption (MTEK) Key.

MCMAC Key Derivation

[00141] The 128-bit MCMAC key is derived from MCMAC-MTEK Prekey and used for message authentication for the multicast messages sent during secure multicast operation.

[00142] MCMAC key is derived as follows:

MCMAC_KEY_D = Dot16KDF(MCMAC-MTEK Prekey, "MCMAC_KEYS", 128)

MTEK Derivation

[00143] The 128-bit MTEK is the multicast transport encryption key used to encrypt data for secure multicast operations.

[00144] MTEK is derived as follows:

MTEKi = Dot16KDF(MCMAC-MTEK Prekey,MSAID|COUNTER_MTEK=i|"MTEK", 128)

MAK Context

[00145] The MAK Context is kept at all members of the multicast group, including the HR-BS, in order to maintain the Finite State Machine of the secure multicast operation. For example, all members of the multicast group may be the the plurality of communication terminals 206 of Figure 2 and the HR-BS may be the base station 200 of Figure 2. The context is as follows in Table 8:

[00146] Table 8 – The MAK context

Parameter	***Size (bit)***	***Usage***
MAK	160	Shared by HR-MSs in a multicast group
MAK Lifetime	32	MAK Lifetime
MulticastGrpID	16	Identifies the Multicast Group

MCNonce	128	A random number used to derive the MCMAC-MTEK Prekey
MCMAC_KEY_D	128	The key which is used for signing DL MAC control messages.
MCMAC_PN_D	24	Used to avoid DL replay attack on the control connection before this expires, reauthorization is needed. The initial value of MCMAC_PN_D is zero and the value of MCMAC_PN_D is reset to zero whenever MAK_COUNT is increased.
Next available counter_MTEK	16	The counter value to be used in next MTEK derivation, after derivation this is increased by 1.

PKMv3 Message code for secure multicast key management

[00147] Table 9 shows the new message codes required for secure multicast key management.

[00148] Table 9 – PKMv3 message types

Code	***Message Type***	***MAC control message name***
1	PKMv3 Reauth-Request	AAI-PKM-REQ
2	PKMv3 EAP-Transfer	AAI-PKM-REQ/AAI-PKM-RSP
3	PKMv3 Key_Agreement-MSG#1	AAI-PKM-RSP
4	PKMv3 Key_Agreement-MSG#2	AAI-PKM-REQ
5	PKMv3 Key_Agreement-MSG#3	AAI-PKM-RSP
6	PKMv3 TEK-Request	AAI-PKM-REQ
7	PKMv3 TEK-Reply	AAI-PKM-RSP
8	PKMv3 TEK-Invalid	AAI-PKM-REQ/AAI-PKM-RSP
12	PKMv3 MulticastKey-Request	AAI-PKM-REQ
13	PKMv3 MulticastKey-Response	AAI-PKM-RSP
14	PKMv3 MulticastKey-Update	AAI-PKM-RSP

[00149] The following describes protocols for a HR-MS to request the keying material and for a HR-BS to update the keying material to members of the multicast group in multicast security for 802.16n GridMAN standards.

Multicast Key Request / Response

[00150] The Multicast Key Request Procedure takes place whenever an HR-MS wishes to derive up-to-date Multicast Keys of a secured multicast group from the serving HR-BS. Figure 10 shows the flow diagram for MulticastKey-Request.

[00151] The Multicast Key Request Procedure is described by the following steps:

[00152] **(Request) Step 1002**: Mobile station HR-MS 1000 first generates Timestamp_HR-MS and Nonce_HR-MS. Next, HR-MS 1000 transmits a MulticastKey-Request message 1006 using with the nonce, timestamp, multicast group ID, the serving HR-BSID and its MAC address to the HR-BS 1004. The message is protected by the CMCAC_HR-MS digest tuple using the current CMAC_KEY_U.

[00153] **(Request) Step 1008**: HR-BS 1004 first verifies the received timestamps and nonce for freshness. If the verifications are incorrect, the request 1006 is silently dropped. Otherwise, HR-BS 1004 generates Nonce_HR-BS and Timestamp_HR-BS. If needed, a new set of keys are generated or obtained by generating a new parameter, for example, MC_nonce; and the MCMAC-MTEK Prekey and all sub keys are computed. HR-BS 1004 then transmits an encrypted MulticastKey-Response message 1010 to the HR-MS 1000 containing the MC_Nonce, remaining lifetime of the MAK, the current COUNTER_MTEK, Nonce_HR-BS, Timestamp_HR-BS and the received Nonce_HR-MS, its own BSID and MAC address of the requesting HR-MS 1000. This message 1010 may be encrypted using the current (or existing) traffic encryption key (TEK) for confidentiality and protected by a CMAC_HR-MS digest tuple using the current CMAC_KEY_D. These keys refer to pre-established keys between the HR-BS 1004 and the HR-MS 1000.

[00154] **(Request) Step 1012**: HR-MS 1000 first verifies the received timestamp and nonces for freshness. The MulticastKey-Response message 1010 may be verified using the CMAC_HR-MS digest tuple. If the verifications fail, the MulticastKey-Response

message 1010 is silently dropped. Otherwise, the message 1010 is decrypted with the current TEK, and the up-to-date MCMAC and MTEK keys can be derived for the multicast operation.

[00155] For example, the HR-MS 1000 may be any of the plurality of communication terminals 206 of Figure 2, the HR-BS 1004 may be the base station 200 of Figure 2, and the MulticastKey-Request may be the MKM protocol 100 for requesting for a key 110 of Figure 1.

Multicast Key Request Message format

[00156] The HR-MS 1000 transmits the PKMv3 MulticastKey-Request message as a first step for an HR-MS initiated multicast key request. The MulticastKey-Request message 1006 identifies the multicast group, the serving HR-BSID and MAC address of the requesting HR-MS 1000.

[00157] The message 1006 may include a Nonce_HR-MS generated by the requesting HR-MS 1000 and a Timestamp_HR-MS for freshness. The CMAC Digest attribute (i.e., CMAC_PN_U and CMAC value) may be transmitted for CMAC verification, which is computed from CMAC_KEY _U.

[00158] Code: 12

[00159] The message attributes are shown in Table 10.

[00160] Table 10 – PKMv3 MulticastKey-Request message attribute

Attribute	***Contents***
MulticastGrpID	Multicast Group ID
Timestamp_HR-MS	Timestamp generated by HR-MS
Nonce_HR-MS	Nonce generated by HR-MS
HR-BSID	HR-BSID
HR-MS MAC address	48-bit MAC address
CMAC_HR-MS	Message digest calculated by HR-MS

[00161] In some examples, the attributes "Timestamp_HR-MS", "Nonce_HR-MS", "HR-BSID" and/or "HR-MS MAC address" may be hashed. As used herein, the term "hashed" refers to being represented in a digested form, normally reflected by a hash value.

Multicast Key Response Message format

[00162] The HR-BS 1004 transmits the PKMv3 MulticastKey-Response message 1010 to an HR-MS 1000 for disseminating information necessary for derivation of the multicast keys of a multicast group. The message 1010 is transmitted in response as a second step 1008 to the HR-MS initiated multicast key request event.

[00163] The message 1010 may include a Nonce_HR-MS sent by the requesting HR-MS 1000 in the MulticastKey-Request message 1006, a Nonce_HR-BS generated by the HR-BS 1004 and a Timestamp_HR-BS for freshness. The multicast group ID, MAC address of the requesting HR-MS 1000, HR-BSID may be included in the message 1010 for verification. The MAK lifetime, MC_Nonce and COUNTER_MTEK may be included in the message 1010 for the requesting HR-MS 1000 to derive the multicast keys.

[00164] The message 1010 may be encrypted with the current TEK for MAK confidentiality, and contain the CMAC Digest attribute (i.e., CMAC_PN_D and CMAC value) for CMAC verification, which is computed from CMAC_KEY _D. These keys refer to pre-established keys between the HR-BS 1004 and the HR-MS 1000.

[00165] Code: 13

[00166] The message attributes are shown in Table 11.

[00167] Table 11 – PKMv3 MulticastKey-Response message attribute

Attribute	***Contents***
MulticastGrpID	Multicast Group ID
Timestamp_HR-BS	Timestamp generated by HR-BS
Nonce_HR-BS	Nonce generated by HR-BS
HR-MS MAC address	48-bit MAC address

HR-BSID	HR-BSID
Nonce_HR-MS	Nonce sent by HR-MS
MC_Nonce	The number used to derive the MCMAC-MTEK Prekey
MAK Lifetime	Remaining Multicast Authentication Key Lifetime
COUNTER_MTEK	The current COUNTER_MTEK in use
CMAC_HR-BS	Message digest calculated using CMAC key by HR-BS

[00168] In some examples, the attributes "Timestamp_HR-BS", "Nonce_HR-BS", "HR-MS MAC address" and/or "HR-BSID" may be hashed. As used herein, the term "hashed" is as defined above.

[00169] In various embodiments, the transceiver 212 of Figure 2 may be configured to broadcast group formation information to communication terminals in the communication system; wherein the base station 200 may indicate that the group formation information is to be used for generating the incoming message; and wherein the determiner 218 may be configured to determine from the received incoming message whether the communication terminals are forming a communication session.

[00170] In the context of various embodiments, the term "broadcast" refers to sending out a message from one node, for example, the base station 200 of Figure 2, over an area, i.e. to all or multiple communication devices (e.g. using the same radio communication technology, e.g. according to the same communication standard, as the communication terminal or being part of the same communication network as the communication device) located in the area. As used herein, "multiple"communication devices may refer to a subset of communication terminals (or MSs) in the network.

[00171] As a further example, broadcast is when a single node is transmitting a message to all other nodes in a given address group. This broadcast can reach all hosts on the subnet, all subnets, or all hosts on all subnets. For example, based on the given address group, the BS, for example, the base station 200 of Figure 2, can pick any subset

of communication terminals (or MSs) to be the receiving communication terminals (or receiving MSs)

[00172] As used herein, the term "indicate" includes, but not be limited by, specify, show, imply, reveal, notify, publish, or register.

[00173] A non-limiting illustrative example of a multicast scenario for initial group (or communication session) formation in IEEE 802.16n HR network is shown in Figure 11. The initial group formation scheme/protocol may be of public key infrastructure (PKI)-based approach or of the pre-shared key-based approach.

[00174] The "controller" node HR-MSX/BS 1100 refers to either an appointed HR-MS node (HR-MSX) in the case where there is no Base Station (HR-BS) around or it can also refer to the Base Station node (HR-BS) in the case where an HR-BS is present.

[00175] The initial group formation protocol may be used to establish a multicast key for the multicast group when the group is initially formed. For the PKI-based approach, secret pairwise keys may also be established between the controller HR-MSX/BS 1100 and each multicast member HR-MS*i* 1102, 1104, 1106, 1108, 1110 in the initial group formation protocol.

[00176] The term "pairwise" is as defined above.

[00177] For the PKI-based approach, the flow diagram for this scenario is depicted in Figure 12 and the flow chart for this scenario is shown in Figure 13. The number of multicast group members is n.

[00178] **(Initial group formation) Step 1300**: HR-MSX/BS 1100 sends the multicast group information 1200 to all potential members of the multicast group comprising of HR-MS*i* 1102, 1104, 1106, 1108, 1110 for $1 \leq i \leq n$:

$$\text{HR-MSX/BS} \rightarrow \text{HR-MSi}(1 \leq i \leq n) : \text{MulticastGrpInfo}$$

where MulticastGrpInfo = MulticastGrpID|HR-MSX/BSAddr|Cert(HR-MSX/BS).

[00179] **(Initial group formation) Step 1302**: Each HR-MS*i* 1102, 1104, 1106, 1108, 1110 for $1 \leq i \leq n$ first generates nonce $N_{\text{HR-MSi}}$. Next, HR-MS*i* 1102, 1104, 1106, 1108, 1110 computes the signature $\sigma_{\text{HR-MSi}}$ = SIGN(MulticastGrpID|$T_{\text{HR-MSi}}$|$N_{\text{HR-MSi}}$|HR-

MSX/BSAddr|HR-MSiAddr) and sends the following message 1202 to HR-MSX/BS 1100:

$$\text{HR-MSi} \rightarrow \text{HR-MSX/BS} : \text{Multicast\_MSG\_\#1}$$

where Multicast_MSG_#1 = MulticastGrpID|$T_{\text{HR-MSi}}$|$N_{\text{HR-MSi}}$|HR-MSX/BSAddr|HR-MSiAddr|$\sigma_{\text{HR-MSi}}$|Cert(HR-MSi).

[00180] (Initial group formation) Step 1304: HR-MSX/BS 1100 first verifies the received timestamps and nonces for freshness and the certificate Cert(HR-MSi) and signature $\sigma_{\text{HR-MSi}}$ for $1 \leq i \leq n$. If the verifications are correct, then HR-MSX/BS 1100 generates nonce $N_{\text{HR-MSX/BS}}$, *GTEK* and *MSKi* for $1 \leq i \leq n$ and computes key confirmation/message authentication code $\theta_{\text{HR-MSi}}$ = *MAC*(*MSKi*|*GTEK*|$N_{\text{HR-MSX/BS}}$|$N_{\text{HR-MSi}}$|HR-MSX/BSAddr|HR-MSiAddr). HR-MSX/BS 1100 then uses HR-MS*i*'s 1102, 1104, 1106, 1108, 1110 public key to encrypt and obtain $c_i = \varepsilon_{\text{HR-MSi\_PK}}$(*MSKi, GTEK, MSKi_lifetime, GTEK_lifetime,* HR-MSiAddr, HR-MSX/BSAddr). Finally, HR-MSX/BS 1100 computes signature $\sigma'_{\text{HR-MSi}}$ = SIGN(MulticastGrpID|$T_{\text{HR-MSX/BSAddr}}$|$N_{\text{HR-MSX/BSAddr}}$|HR-MSiAddr|HR-MSX/BSAddr|$N_{\text{HR-MSi}}$|c_i|$\theta_{\text{HR-MSi}}$) and sends the following message 1204 to HR-MS*i* 1102, 1104, 1106, 1108, 1110 for $1 \leq i \leq n$:

$$\text{HR-MSX/BS} \rightarrow \text{HR-MSi}(1 \leq i \leq n) : \text{Multicast\_MSG\_\#2}$$

where Multicast_MSG_#2 = MulticastGrpID|$T_{\text{HR-MSX/BSAddr}}$|$N_{\text{HR-MSX/BSAddr}}$|HR-MSiAddr|HR-MSX/BSAddr|$N_{\text{HR-MSi}}$|c_i|$\theta_{\text{HR-MSi}}$|$\sigma'_{\text{HR-MSi}}$.

[00181] (Initial group formation) Step 1306: Each HR-MS*i* 1102, 1104, 1106, 1108, 1110 for $1 \leq i \leq n$ first verifies the received timestamp and nonces for freshness and the signature $\sigma'_{\text{HR-MSi}}$. If the verifications are correct, then each HR-MS*i* 1102, 1104, 1106, 1108, 1110 decrypts $c_i = \varepsilon_{\text{HR-MSi\_PK}}$(*MSKi, GTEK, MSKi_lifetime, GTEK_lifetime,* HR-MSiAddr, HR-MSX/BSAddr) and obtains *MSKi*, *GTEK*, *MSKi_lifetime* and *GTEK_lifetime*. Next, each HR-MS*i* 1102, 1104, 1106, 1108, 1110 verifies $\theta_{\text{HR-MSi}}$. If the verification is correct, then HR-MS*i* 1102, 1104, 1106, 1108, 1110 can commence secure multicast.

[00182] HR-MS*i* 1102, 1104, 1106, 1108, 1110 use the *GTEK* for the multicast session.

[00183] Table 12 shows the MulticastGrpInfo message attribute (PKI-based appproach).

[00184] Table 12

Notation	Meaning
MulticastGrpID	Multicast Group ID
HR-MSX/BSAddr	Address of HR-MSX/BS
Cert(HR-MSX/BS)	Digital certificate of HR-MSX/BS

[00185] Table 13 shows the Multicast_MSG_#1 message attribute (PKI-based appproach).

[00186] Table 13

Notation	Meaning
MulticastGrpID	Multicast Group ID
T_{HR-MSi}	Timestamp generated by HR-MS*i*
N_{HR-MSi}	Freshly generated random number of 64bits by HR-MS*i*
HR-MSX/BSAddr	Address of HR-MSX/BS
HR-MSiAddr	Address of HR-MS*i*
σ_{HR-MSi}	signature of message generated by HR-MS*i*
Cert(HR-MSi)	Digital certificate of HR-MS*i*

[00187] Table 14 shows the Multicast_MSG_#2 message attribute (PKI-based appproach).

[00188] Table 14

Notation	Meaning
MulticastGrpID	Multicast Group ID
$T_{\text{HR-MSX/BSAddr}}$	Timestamp generated by HR-MSX/BS
$N_{\text{HR-MSX/BSAddr}}$	Freshly generated random number of 64bits by HR-MSX/BS
HR-MSiAddr	Address of HR-MS*i*
HR-MSX/BSAddr	Address of HR-MSX/BS
$N_{\text{HR-MSi}}$	nonce generated by HR-MS*i* in Multicast_MSG_#1 message
c_i	public key encryption using HR-MSi's public key HR-MSi_PK
$\theta_{\text{HR-MSi}}$	Key Confirmation/Message Authentication Codes (MACs) generated by HR-MSX/BS
$\sigma'_{\text{HR-MSi}}$	signature of message for HR-MS*i* generated by HR-MSX/BS

[00189] As defined above, the *GTEK* is used to encrypt data packets for the multicast service and it is shared amongst the HR-MSs that belongs to the multicast group. The *GTEK* is randomly generated by the a key provider of HR-MSX/BS 1100. The *GTEK* may be encrypted by HR-MS*i*'s public key in Multicast_MSG_#2 in the PKI-based initial group formation protocol.

[00190] The *MSKi* is a key shared between the multicast members HR-MS*i* 1102, 1104, 1106, 1108, 1110 and the controller HR-MSX/BS 1100. It is used as an encryption key and also as a MAC key. In the PKI-based approach, the *MSKi/MSKj* may be randomly generated by the key provider. The *MSKi* may be refreshed/rekeyed periodically to maintain key freshness.

[00191] The HR-MSX/BS 1100 may be the base station 200 of Figure 2. The HR-MS*i* 1102, 1104, 1106, 1108, 1110 may be the plurality of communication terminals 206 of Figure 2.

[00192] In another example, for the pre-shared key-based approach, the flow diagram for this scenario (as described in Figure 11) is similarly depicted in Figure 12 and the flow chart for this scenario is shown in Figure 14.

[00193] **(Initial group formation) Step 1400**: HR-MSX/BS 1100 sends the multicast group information 1200 to all potential members of the multicast group comprising of HR-MS*i* 1102, 1104, 1106, 1108, 1110 for $1 \leq i \leq n$:

$$\text{HR-MSX/BS} \rightarrow \text{HR-MSi}(1 \leq i \leq n) : \text{MulticastGrpInfo}$$

where MulticastGrpInfo = MulticastGrpID|HR-MSX/BSAddr.

[00194] (Initial group formation) Step 1402: Each HR-MS*i* 1102, 1104, 1106, 1108, 1110 for $1 \leq i \leq n$ first generates nonce $N_{\text{HR-MSi}}$. Next, HR-MS*i* 1102, 1104, 1106, 1108, 1110 computes the MAC $\theta_{\text{HR-MSi}} = MAC(MSKi|\text{MulticastGrpID}|T_{\text{HR-MSi}}|N_{\text{HR-MSi}}|\text{HR-MSX/BSAddr}|\text{HR-MSiAddr})$ and sends the following message 1202 to HR-MSX/BS 1100:

$$\text{HR-MSi} \rightarrow \text{HR-MSX/BS} : \text{Multicast\_MSG\_\#1}$$

where Multicast_MSG_#1 = $\text{MulticastGrpID}|T_{\text{HR-MSi}}|N_{\text{HR-MSi}}|\text{HR-MSX/BSAddr}|\text{HR-MSiAddr}|\theta_{\text{HR-MSi}}$.

[00195] (Initial group formation) Step 1404: HR-MSX/BS 1100 first verifies the received timestamps and nonces for freshness and $\theta_{\text{HR-MSi}}$ for $1 \leq i \leq n$. If the verifications are correct, then HR-MSX/BS 1100 generates nonce $N_{\text{HR-MSX/BS}}$, *GTEK* and computes $\theta'_{\text{HR-MSi}} = MAC(MSKi|GTEK|N_{\text{HR-MSX/BS}}|N_{\text{HR-MSi}}|\text{HR-MSX/BSAddr}|\text{HR-MSiAddr})$. HR-MSX/BS 1100 then encrypt and obtain $c_i = \varepsilon_{MSKi}(GTEK, GTEK\_lifetime,$ HR-MSiAddr, HR-MSX/BSAddr). Finally, HR-MSX/BS 1100 sends the following message 1204 to 1102, 1104, 1106, 1108, 1110 for $1 \leq i \leq n$:

$$\text{HR-MSX/BS} \rightarrow \text{HR-MSi}(1 \leq i \leq n) : \text{Multicast\_MSG\_\#2}$$

where Multicast_MSG_#2 = $\text{MulticastGrpID}|T_{\text{HR-MSX/BSAddr}}|N_{\text{HR-MSX/BSAddr}}|\text{HR-MSiAddr}|\text{HR-MSX/BSAddr}|N_{\text{HR-MSi}}|c_i|\theta'_{\text{HR-MSi}}$.

[00196] (Initial group formation) Step 1406: Each HR-MS*i* 1102, 1104, 1106, 1108, 1110 for $1 \leq i \leq n$ first verifies the received timestamp and nonces for freshness and decrypts c_i using *MSKi* and obtains *GTEK* and *GTEK_lifetime*. Next, each HR-MS*i* 1102, 1104, 1106, 1108, 1110 verifies $\theta_{\text{HR-MSi}}$. If the verification is correct, then HR-MS*i* 1102, 1104, 1106, 1108, 1110 can commence secure multicast.

[00197] HR-MS*i* 1102, 1104, 1106, 1108, 1110 use the *GTEK* for the multicast session.

[00198] Table 15 shows the MulticastGrpInfo message attribute (pre-shared key-based appproach).

[00199] Table 15

Notation	Meaning
MulticastGrpID	Multicast Group ID
HR-MSX/BSAddr	Address of HR-MSX/BS

[00200] Table 16 shows the Multicast_MSG_#1 message attribute (pre-shared key-based appproach).

[00201] Table 16

Notation	Meaning
MulticastGrpID	Multicast Group ID
T_{HR-MSi}	Timestamp generated by HR-MSi
N_{HR-MSi}	Freshly generated random number of 64bits by HR-MSi
HR-MSX/BSAddr	Address of HR-MSX/BS
HR-MSiAddr	Address of HR-MSi
θ_{HR-MSi}	message authentication code (MAC) generated by HR-MSi

[00202] Table 17 shows the Multicast_MSG_#2 message attribute (pre-shared key-based appproach).

[00203] Table 17

Notation	Meaning
MulticastGrpID	Multicast Group ID
$T_{HR-MSX/BSAddr}$	Timestamp generated by HR-MSX/BS
$N_{HR-MSX/BSAddr}$	Freshly generated random number of 64bits by HR-MSX/BS
HR-MSiAddr	Address of HR-MSi
HR-MSX/BSAddr	Address of HR-MSX/BS
N_{HR-MSi}	nonce generated by HR-MSi in Multicast_MSG_#1 message
c_i	symmetric key encryption using pre-shared key $MSKi$
θ'_{HR-MSi}	key confirmation/MAC generated by HR-MSX/BS

[00204] The *GTEK* may be encrypted with the pre-shared key *MSKi* in Multicast_MSG_#2 in the pre-shared key-based initial group formation protocol.

[00205] The initial group formation protocol may be the MKM protocol 100 for forming an initial communication session 106 of Figure 1.

[00206] In various embodiments, the determiner 208 of Figure 2 may be configured to determine whether at least one of the communication terminals in the communication session after the change of participants requires to be updated with the key for secure communication in the communication session after the change of participants.

[00207] In the context of various embodiments, the term "update" refers to inform, bring up to date, or being kept informed.

[00208] For example, in Multicast Key Update / Rekey as shown in Figures 15 and 16, the Multicast Key Update Procedure takes place whenever a HR-BS 1500 decides to refresh the keying material and disseminate it via unicast to an HR-MS 1502 or multicast to members of the multicast group 1600. This may be due to an expiration of the current MCMAC-MTEK Prekey or current MTEK, or a multicast key update following a location update by an idle HR-MS, or a change in the group membership, e.g. a new HR-MS joins or leaves the multicast group.

[00209] As shown in Figure 15, for unicast to a single HR-MS member 1502 of the multicast group, the multicast key update procedure is as follows:

[00210] **(Multicast Key Update) Step 1504**: Based on a new MC_Nonce 1506 or COUNTER_MTEK, HR-BS 1500 dervies the new MTEK and/or MCMAC keys through the key management procedure as described hereinabove. HR-BS 1500 generates Nonce_HR-BS and Timestamp_HR-BS for freshness, and transmits an encrypted MulticastKey-Update message 1508 to the HR-MS 1502 with group indicator = 0. The message 1508 may contain the multicast group ID, MC_Nonce, COUNTER_MTEK, the remaining MAK lifetime, Nonce_HR-BS and Timestamp_HR-BS, its own BSID and MAC address of the target HR-MS. This message 1508 may be encrypted using the current TEK for confidentiality and protected by the CMAC_HR-MS digest tuple using the current CMAC_KEY_D. These keys refer to pre-established keys between the HR-BS 1500 and the HR-MS 1502.

[00211] **(Multicast Key Update) Step 1510**: HR-MS 1502 first decrypts the message 1508 using the current TEK, and verifies the CMAC_HR-MS, and the received timestamp and nonce for freshness. If the verifications are incorrect, HR-MS 1502

silently drops the message. Otherwise, HR-MS 1502 updates its MAK context and derives the new MCMAC-MTEK Prekey and all sub keys.

[00212] As shown in Figure 16, for multicast key update via unicast or multicast to all members of the group, the procedure is as follows:

[00213] **(Multicast Key Update) Step 1602**: Based on a new MC_Nonce or COUNTER_MTEK 1604, HR-BS 1500 derives the new MTEK and/or MCMAC keys through the key management procedure as described hereinabove.

[00214] HR-BS 1500 generates Nonce_HR-BS, and Timestamp_HR-BS for freshness, and transmits an encrypted MulticastKey-Update message 1606 to all HR-MSs 1600 of that multicast group with group indicator = 1. In other examples, the group indicator may not be required if the implementation in the MS is able to determine whether the message 1606 is received from a multicast or unicast channel. The message 1606 may contain the multicast group ID, MC_Nonce, COUNTER_MTEK, the remaining MAK lifetime, Nonce_HR-BS and Timestamp_HR-BS, its own BSID. This message 1606 may be encrypted using the current MTEK for confidentiality and protected by the MCMAC_HR-BS digest tuple using the current MCMAC_KEY. These keys refer to pre-established keys between the HR-BS 1500 and the HR-MS 1600.

[00215] **(Multicast Key Update) Step 1608**: Every HR-MS 1600 first decrypts the message 1606 using the current MTEK, and verifies the MCMAC_HR-MS, and the received timestamp and nonce for freshness. If the verifications are incorrect, HR-MS 1600 silently drops the message. Otherwise, HR-MS 1500 updates its MAK context and derives the new MCMAC-MTEK Prekey and all sub keys.

Multicast Key Update Message Format

[00216] The HR-BS 1500 transmits unsolicited PKMv3 MulticastKey-Update message 1508, 1606 to disseminate the most up-to-date multicast security parameters of a multicast group to one or many HR-MSs of the multicast group via unicast 1502 or multicast 1600, respectively.

[00217] The message 1508, 1606 may include a Nonce_HR-BS and Timestamp_HR-BS generated by the HR-BS for freshness. The message 1508, 1606 may include

MC_Nonce and COUNTER_MTEK for key derivation, and the remaining MAK lifetime. For verification, the message 1508 may include HR-BSID, and the MAC address of the target HR-MS 1502 if the message 1508 is unicast to the target HR-MS 1502. This is indicated by the group attribute.

[00218] If the message 1508 is unicast to a target HR-MS 1502, it may be encrypted with the current TEK for confidentiality, and contain the CMAC Digest attribute (i.e., CMAC_PN_D and CMAC value) for CMAC verification, which is computed from CMAC_KEY _D.

[00219] Otherwise the message 1606 is multicast to all HR-MSs 1600 and it may be encrypted with the current MTEK for confidentiality, and contain the MCMAC Digest attribute (i.e., MCMAC_PN and MCMAC value) for MCMAC verification, which is computed from MCMAC_KEY.

[00220] Code: 14

[00221] The message attributes are shown in Table 18.

[00222] Table 18 – PKMv3 MulticastKey-Update message attribute

Attribute	***Contents***
Group	Indicates if it is a unicast or multicast key update
MulticastGrpID	Multicast Group ID
Timestamp_HR-BS	Timestamp generated by HR-BS
Nonce_HR-BS	Nonce generated by HR-BS
HR-BSID	HR-BSID
HR-MS MAC address	48-bit MAC address of the target HR-MS (present if unicast)
MC_Nonce	The number used to derive the MCMAC-MTEK Prekey
COUNTER_MTEK	The current COUNTER_MTEK in use
MAK Lifetime	Remaining Multicast Authentication Key Lifetime
CMAC_HR-MS or MCMAC_HR-BS	Message digest calculated by HR-BS

[00223] In some examples, the attributes "Timestamp_HR-BS", "Nonce_HR-BS", "HR-BSID" and/or "HR-MS MAC address" may be hashed. As used herein, the term "hashed" is as defined above.

PKMv3 Message Code for Multicast Key Update Messages

[00224] Table 19 below shows the message code and group indicator field required for secure multicast key update via unicast or multicast flows.

[00225] Table 19 – PKMv3 Message Codes and Group Indicator for Multicast Key Update Messages

Code	***Group***	***Message Type***	***MAC control message name***
14	0	Unicast MulticastKey-Update	AAI-PKM-RSP
14	1	Multicast MulticastKey-Update	AAI-PKM-RSP

[00226] However, group indicators as described in Table 19 are not required if the implementation in the MS is able to determine whether the PKMv3 messages are received from a multicast or unicast channel.

[00227] The HR-BS 1500 may be, for example, the base station 200 of Figure 2. The HR-MS 1502, 1600 may be, for example, the plurality of communication terminals 206 of Figure 2.

[00228] In various embodiments, the key for secure communication in the communication session after the change of participants may be a multicast authentication key for secure communication in the communication session after the change of participants. The message comprising the key for secure communication in the communication session after the change of participants may be encrypted and/or signed by respective keys for secure communication in the communication session before the change of participants. The term "respective keys" is as defined above.

[00229] For example, key dissemination from HR-BS may be through unicast and multicast Communication as shown in Figures 17 and 18.

[00230] In unicast key dissemination (MAK Update) as depicted in Figure 17, the Multicast Authentication Key (MAK) Update Procedure takes place whenever a HR-BS 1700 decides to refresh the MAK and disseminate it via unicast to an HR-MS 1702, a member of the multicast group. This may be due to an expiration of the current MAK, or a change in the group membership, e.g. a new HR-MS joins the multicast group. The MAK Update Procedure is as follows:

[00231] **(MAK Update) Step 1704:** Based on the new group authentication key MAK', HR-BS 1700 derives the new MCMAC' and MTEK' keys through the key management procedure as described hereinabove. HR-BS 1700 generates nonce $N_{HR\text{-}BS}$, and timestamp $T_{HR\text{-}BS}$ for freshness, and transmits an encrypted MAK-Update message 1706 to the HR-MS 1702 containing the multicast group ID, the MAK and its remaining lifetime, nonce $N_{HR\text{-}BS}$ and timestamp $T_{HR\text{-}MS}$, its own BSID and STID of the HR-MS 1702. This message 1706 may be encrypted using the current TEK for confidentiality and protected by the $CMAC_{HR\text{-}MS}$ digest tuple using the current CMAC_KEY_D. These keys refer to pre-established keys between the HR-BS 1700 and the HR-MS 1702.

[00232] **(MAK Update) Step 1708:** HR-MS 1702 first decrypts the message 1706 using the current TEK, and verifies the $CMAC_{HR\text{-}MS}$, and the received timestamp and nonce for freshness. If the verifications are incorrect, HR-MS 1702 silently drops the message. Otherwise, HR-MS 1702 updates its MAK and derives the new MCMAC and MTEK keys.

[00233] The MAK-Update message is defined in Table 20.

[00234] Table 20: MAK-Update message attribute

MulticastGrpID	***Multicast Group ID***
$T_{HR\text{-}BS}$	Timestamp generated by HR-BS
$N_{HR\text{-}BS}$	Nonce generated by HR-BS
HR-BSID	HR-BSID
STID	STID of the target HR-MS
MAK	Multicast Authentication Key

MAK Lifetime	Remaining Multicast Authentication Key Lifetime
MC_nonce	The number used to derive the MCMAC-MTEK Prekey
$CMAC_{HR-MS}$	Message digest calculated by HR-BS
COUNTER_MTEK	The current COUNTER_MTEK in use

[00235] The message 1706 may include a nonce N_{HR-BS} and timestamp T_{HR-BS} generated by the HR-BS for freshness. The message 1706 may include HR-BSID and STID for further verification, the most up-to-date MAK, and the remaining lifetime.

[00236] The message 1706 may be encrypted with the current TEK for MAK confidentiality, and contain the CMAC Digest attribute (i.e., CMAC_PN_D and CMAC value) for CMAC verification, which is computed from CMAC_KEY _D.

[00237] In multicast key dissemination (MAK Group Update) as shown in Figure 18, the Multicast Authentication Key (MAK) Group Update Procedure takes place whenever a HR-BS 1700 decides to refresh the MAK and disseminate it via broadcast to all member of a multicast group 1800. This may be due to an expiration of the current MAK, or a change in the group membership, e.g. a new HR-MS joins the multicast group. The MAK Group Update Procedure is as follows:

[00238] **(MAK Update) Step 1802:** Based on the new group authentication key MAK', HR-BS 1700 derives the new MCMAC' and MTEK' keys through the key management procedure as described hereinabove and further illustrated in Figure 19. HR-BS 1700 generates nonce N_{HR-BS}, and timestamp T_{HR-BS} for freshness, and transmits an encrypted MAK-Group_Update message 1804 to all HR-MS 1800 of that multicast group, containing the multicast group ID, the MAK and its remaining lifetime, nonce N_{HR-BS} and timestamp T_{HR-BS}, its own BSID. This message 1804 may be encrypted using the current MTEK for confidentiality and protected by the $MCMAC_{HR-BS}$ digest tuple using the current MCMAC_KEY. These keys refer to pre-established keys between the HR-BS 1700 and the HR-MS 1800.

[00239] **(MAK Update) Step 1806:** Every HR-MS 1800 first decrypts the message 1804 using the current TEK, and verifies the $MCMAC_{HR\text{-}MS}$, and the received timestamp and nonce for freshness. If the verifications are incorrect, HR-MS 1800 silently drops the message 1804. Otherwise, HR-MS 1800 updates its MAK and derives the new MCMAC' and MTEK' keys.

[00240] The MAK-Group_Update message is defined in Table 21.

[00241] Table 21: MAK-Group_Update message attribute

Attribute	*Contents*
MulticastGrpID	Multicast Group ID
$T_{HR\text{-}BS}$	Timestamp generated by HR-BS
$N_{HR\text{-}BS}$	Nonce generated by HR-BS
HR-BSID	HR-BSID
MAK	Multicast Authentication Key
MAK Lifetime	Remaining Multicast Master Authentication Key Lifetime
MC_nonce	The number used to derive the MCMAC-MTEK Prekey
$MCMAC_{HR\text{-}BS}$	Message digest calculated by HR-BS
COUNTER_MTEK	The current COUNTER_MTEK in use

[00242] The message 1804 may include a nonce $N_{HR\text{-}BS}$ and timestamp $T_{HR\text{-}BS}$ generated by the HR-BS for freshness. The message 1804 may include HR-BSID for further verification, the most up-to-date MAK, and the remaining lifetime.

[00243] The message 1804 may be encrypted with the current group MTEK for MAK confidentiality, and contain the MCMAC Digest attribute (i.e., MCMAC_PN and MCMAC value) for MCMAC verification, which is computed from MCMAC_KEY.

[00244] The HR-BS 1700 may be, for example, the base station 200 of Figure 2. The HR-MS 1702, 1800 may be, for example, the plurality of communication terminals 206 of Figure 2.

[00245] The Multicast Key Update protocol or MAK update may be the MKM protocol 100 for updating a key 108 of Figure 1.

[00246] In a second aspect, a method of performing secure communication among communication terminals in a cellular mobile communication system is provided as shown in Figure 20. In the method 2000, the cellular mobile communication system comprises a communication network for providing a communication session for a plurality of communication terminals of the communication network. The cellular mobile communication system may be, for example, the cellular mobile communication system 202 of Figure 2; the communication network may be, for example, the communication network 204 of Figure 2; and the plurality of communication terminals may be, for example, the plurality of communication terminals 206 of Figure 2.

[00247] The method 2000 comprises determining whether there is a change of the participants of the communication session 2002; providing a key to be used for secure communication in the communication session after the change of participants 2004; and sending to the communication terminals participating in the communication session after the change of the participants a message comprising the key 2006.

[00248] Similar terms as used herein are as defined above. For example, the terms "change of the participants" and "communication session" are as defined above.

[00249] As a example, the method 2000 may comprise multicast join procedure for preserving backward secrecy for 802.16n GridMAN standards. In order to prevent newly joined communication terminals (or stations) from decrypting and accessing multicast traffic prior to the join event, multicast keys may be changed whenever new members join a multicast group. Figure 21 shows a flow diagram of the Join Event, in accordance to one embodiment.

[00250] In Figure 21, the Join Procedure 2100 includes the following steps:

[00251] **(Join Procedure) Step 2104**: The HR-MS 2102 requests to obtain keying material from the HR-BS 2106 for a multicast group as described herein above under the Multicast Key Request Procedure.

[00252] **(Join Procedure) Step 2108**: The HR-BS 2106 verifies HR-MS 2102 is a member of the multicast group. Multicast membership is usually managed at the upper

layer of the communication standard model. If it is a new member, HR-BS 2106 generates a new MC_Nonce and disseminates it through the MulticastKey-Update procedure as described herein above under the Multicast Key Update Procedure to all existing members of the multicast group via multicast 2110.

[00253] **(Join Procedure) Step 2112**: Both the existing multicast group members 2110 and new multicast group member HR-MS 2102 verifies the respective received message, obtains the new MC_Nonce and derives the MCMAC-MTEK Prekey and all sub keys.

[00254] **(Join Procedure) Step 2116**: HR-BS 2106 replies the requesting HR-MS 2102 with the new keying material in the MulticastKey-Response message 2114.

[00255] (Join Procedure) Step 2112 may be performed in parallel or after (Join Procedure) Step 2116.

[00256] The HR-BS 2106 may be, for example, the base station 200 of Figure 2. The HR-MS 2102, 2110 may be, for example, the plurality of communication terminals 206 of Figure 2.

[00257] The Multicast Key Update procedure may be the MKM protocol 100 for updating a key 108 of Figure 1. The Multicast Key Request procedure may be the MKM protocol 100 for requesting for a key 110 of Figure 1. The Joining Procedure may the MKM protocol 100 for a member joining a communication session 102 of Figure 1.

[00258] As another example, the method 2000 may comprise multicast leave procedure for preserving forward secrecy for 802.16n GridMAN standards. In order to prevent communication terminals (or stations) from decrypting and accessing future multicast traffic after leaving the multicast group, multicast keys may be changed whenever members leave a multicast group. Figure 22 shows the flow diagram of the Leave Event, in accordance to one embodiment.

[00259] In Figure 22, the leave procedure 2200 includes the following steps:

[00260] **(Leave Procedure) Step 2202**: Upon receiving the AAI-DSD-REQ from a leaving member HR-MS 2204 and thereafter sending the AAI-DSD-RSP for leaving a multicast group, HR-BS 2206 generates a new MC_Nonce 2208 and unsolicitedly sends the MulticastKey-Update message 2210 (as described herein above under the Multicast

Key Update Procedure) via unicast to each remaining HR-MS 2212 in the multicast group. In Step 2216, all sub-keys are generated by the HR-BS 2206 so that traffic messages may be encrypted with the new keys and/or sub-keys. It is noted that in other examples, Step 2216 may take place after the generation of MC_nonce 2208, and may taken before or in parallel with the MulticastKey-Update 2210.

[00261] **(Leave Procedure) Step 2214**: Each remaining multicast group member HR-MS 2212 verifies their respective received messages and derives the new multicast keys to continue secure multicast communications.

[00262] The HR-BS 2206 may be, for example, the base station 200 of Figure 2. The HR-MS 2212, 2204 may be, for example, the plurality of communication terminals 206 of Figure 2.

[00263] The Multicast Key Update procedure may be the MKM protocol 100 for updating a key 108 of Figure 1. The Leave Procedure may the MKM protocol 100 for a member leaving a communication session 104 of Figure 1.

[00264] The phrase "at least substantially" may include "exactly" and a variance of +/- 5% thereof. As an example and not limitation, the phrase "A is at least substantially the same as B" may encompass embodiments where A is exactly the same as B, or where A may be within a variance of +/- 5%, for example of a value, of B, or vice versa.

[00265] While the invention has been particularly shown and described with reference to specific embodiments, it should be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention as defined by the appended claims. The scope of the invention is thus indicated by the appended claims and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced.

CLAIMS

1. A base station of a cellular mobile communication system, the cellular mobile communication system comprising a communication network for providing a communication session for a plurality of communication terminals of the communication network, the base station comprising:

a determiner configured to determine whether there is a change of the participants of the communication session;

a key provider configured to provide a key to be used for secure communication in the communication session after the change of participants; and

a transceiver configured to send to the communication terminals participating in the communication session after the change of the participants a message comprising the key.

2. The base station as claimed in claim 1, wherein the change of the participants of the communication session comprises at least one of the plurality of communication terminals in the communication session leaving the communication session, or a communication terminal not in the communication session joining the communication session with the plurality of communication terminals.

3. The base station as claimed in claim 1 or 2, wherein the communication session is a multicast session.

4. The base station as claimed in any one of claims 1 to 3, wherein the message is encrypted using an authentication key or an encryption key.

5. The base station as claimed in any one of claims 1 to 4, wherein the base station is an appointed communication terminal.

6. The base station as claimed in any one of claims 1 to 5, wherein the communication network is a communication network according to a 802.16 communication standard.

7. The base station as claimed in any one of claims 1 to 6, wherein the communication network is a communication network according to the 802.16n communication standard.

8. The base station as claimed in any one of claims 1 to 7, wherein the transceiver is configured to include a nonce into the message.

9. The base station as claimed in any one of claims 1 to 8, wherein the key for secure communication in the communication session after the change of participants is a multicast traffic encryption key for secure communication in the communication session after the change of participants.

10. The base station as claimed in any one of claims 2 to 9, wherein the message comprising the key or its parameters for secure communication in the communication session after the change of participants is encrypted and signed by a pre-shared authentication key when it has been determined that the at least one of the plurality of communication terminals in the communication session is leaving the communication session.

11. The base station as claimed in any one of claims 1 to 10, further comprising a transceiver configured to receive an incoming message from the communication terminal not in the communication session.

12. The base station as claimed in claim 11, wherein the transceiver is configured to check the received incoming message for message freshness.

13. The base station as claimed in claim 11 or 12, wherein the message comprising the key for secure communication in the communication session after the change of participants is encrypted by a pre-shared authentication key.

14. The base station as claimed in claim 11 or 12, wherein the transceiver is configured to include a certificate into the message.

15. The base station as claimed in claim 14, wherein the message comprising the key for secure communication in the communication session after the change of participants is encrypted and signed by a public key and a private key respectively shared by the communication terminals of the communication system.

16. The base station as claimed in claim 11 or 12, wherein the message is encrypted and signed by respective keys for secure communication in the communication session before or after the change of participants when it has been determined based on the incoming message that the communication terminal not in the communication session is joining the communication session with the plurality of communication terminals.

17. The base station as claimed in any one of claims 1 to 16, further comprising a transceiver configured to receive a request for the key for secure communication in the communication session after the change of participants from any communication terminal in the communication session after the change of participants.

18. The base station as claimed in claim 17, wherein the message comprising the key for secure communication in the communication session after the change of participants comprises a message comprising a parameter of the key for secure communication in the communication session after the change of participants; and wherein the transceiver is configured to send the message to the requesting communication terminal in the communication session after the change of participants.

19. The base station as claimed in claim 18, wherein the message comprising the parameter of the key for secure communication in the communication session after the change of participants is encrypted and signed by respective keys for secure communication in the communication session before the change of participants.

20. The base station as claimed in any one of claims 11 to 15, wherein the transceiver is configured to broadcast group formation information to communication terminals in the communication system; wherein the base station indicates that the group formation information is to be used for generating the incoming message; and wherein the determiner is configured to determine from the received incoming message whether the communication terminals are forming a communication session.

21. The base station as claimed in any one of claims 1 to 8, wherein the determiner is configured to determine whether at least one of the communication terminals in the communication session after the change of participants requires to be updated with the key for secure communication in the communication session after the change of participants.

22. The base station as claimed in claim 21, wherein the key for secure communication in the communication session after the change of participants is a multicast authentication key for secure communication in the communication session after the change of participants.

23. The base station as claimed in claim 21 or 22, wherein the message comprising the key for secure communication in the communication session after the change of participants is encrypted and signed by respective keys for secure communication in the communication session before the change of participants.

24. A method of performing secure communication among communication terminals in a cellular mobile communication system, the cellular mobile communication system comprising a communication network for providing a communication session for a plurality of communication terminals of the communication network, the method comprising:

determining whether there is a change of the participants of the communication session;

providing a key to be used for secure communication in the communication session after the change of participants; and

sending to the communication terminals participating in the communication session after the change of the participants a message comprising the key.

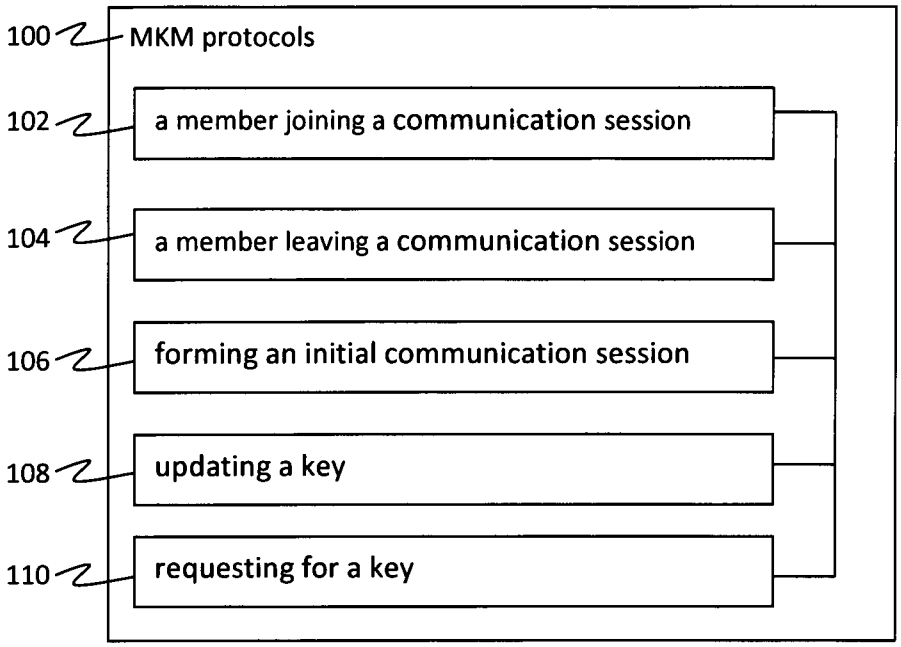

Figure 1

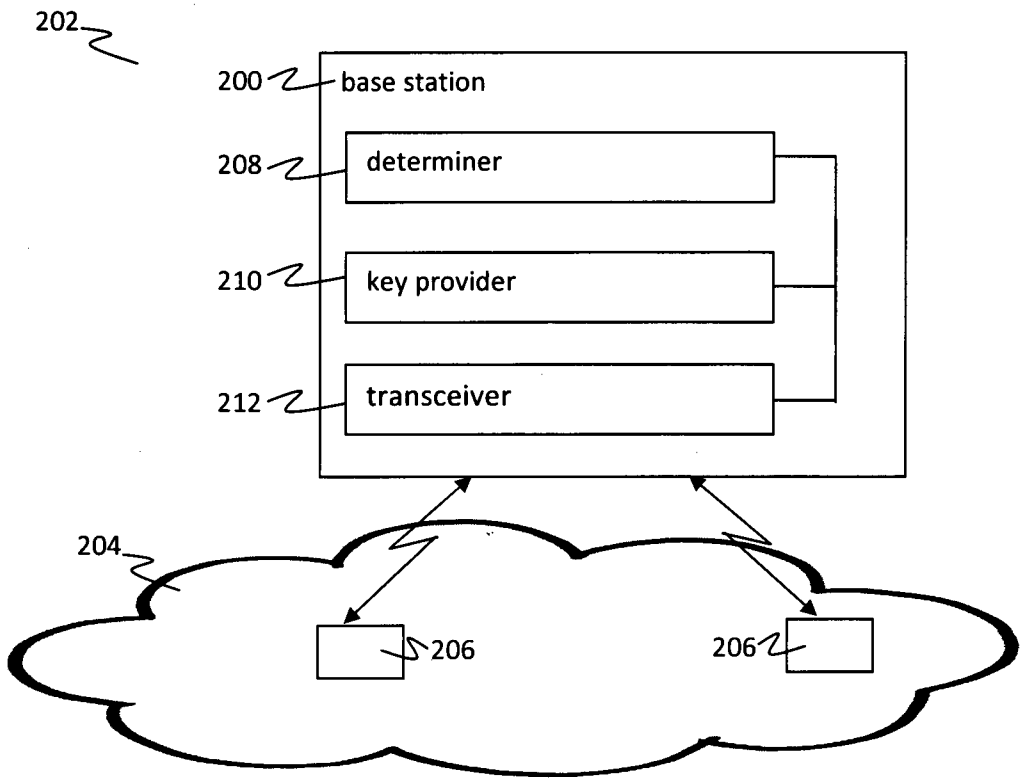

Figure 2

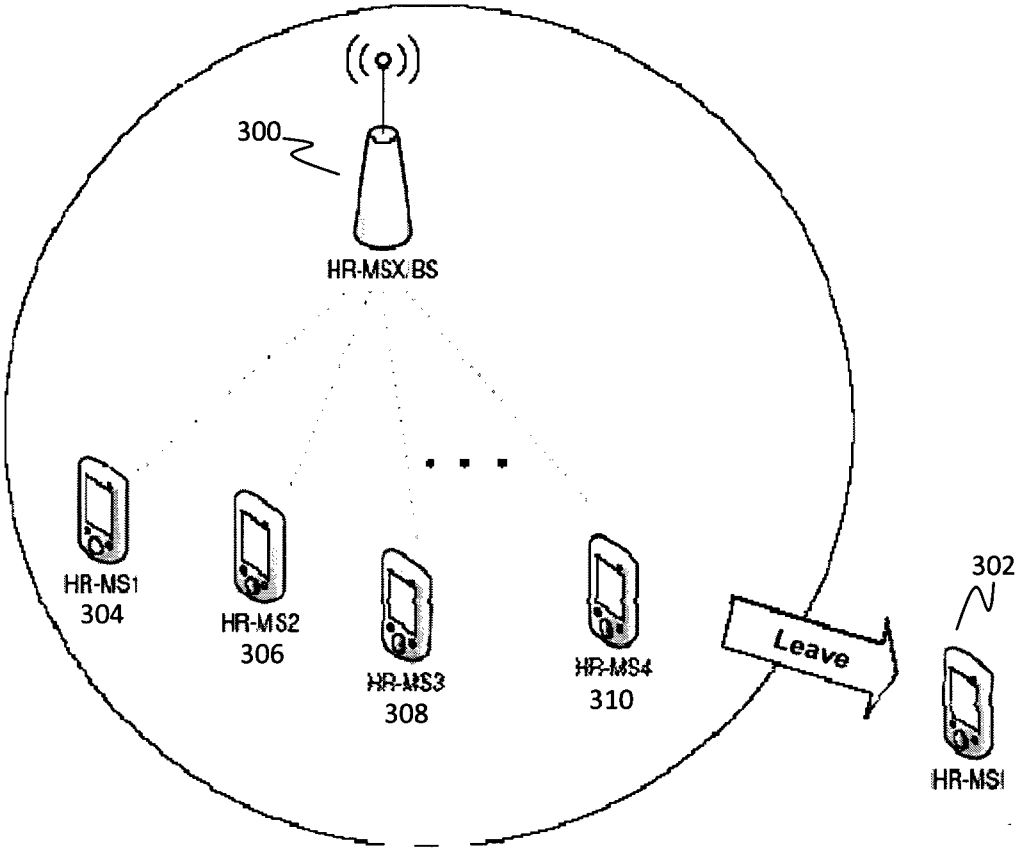

Figure 3

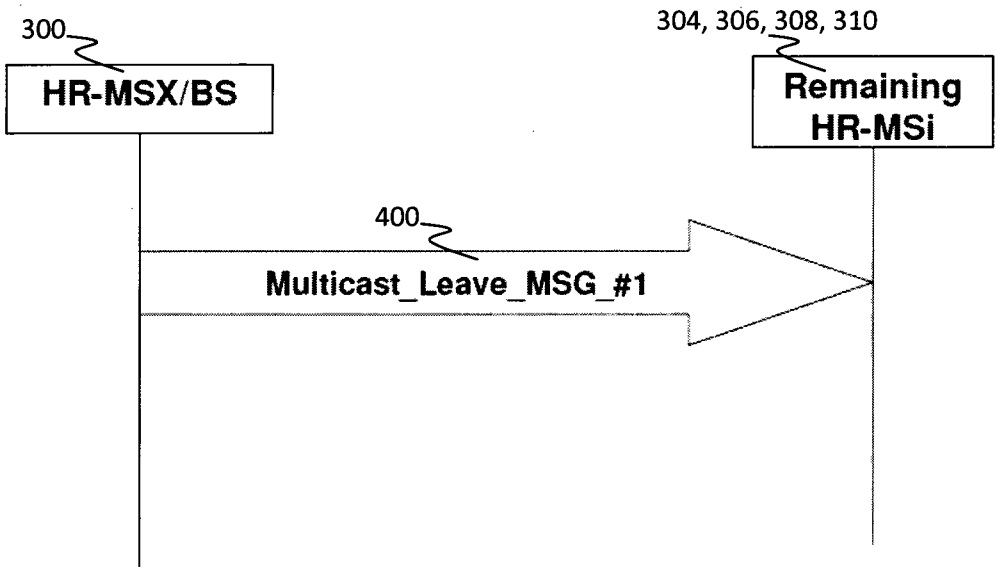

Figure 4

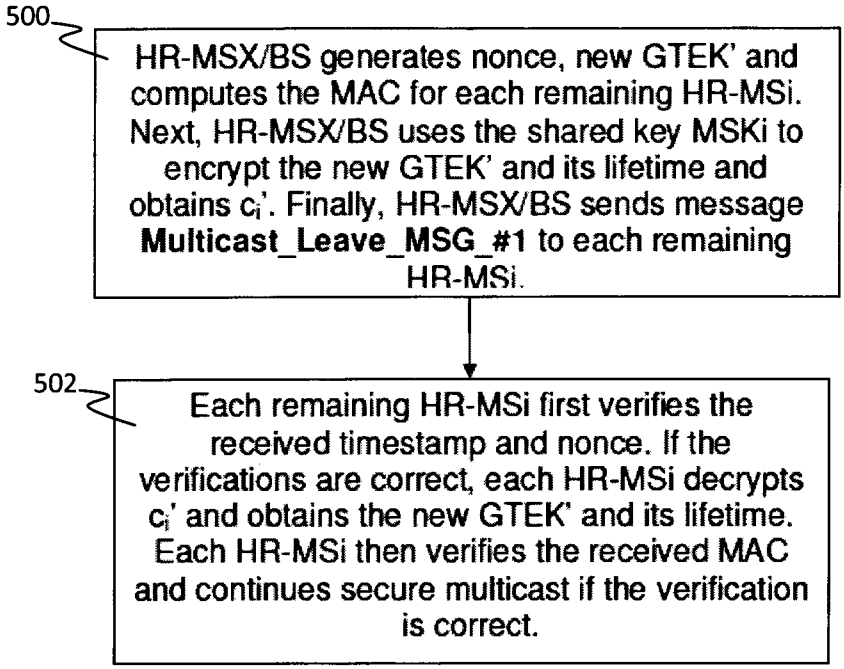

Figure 5

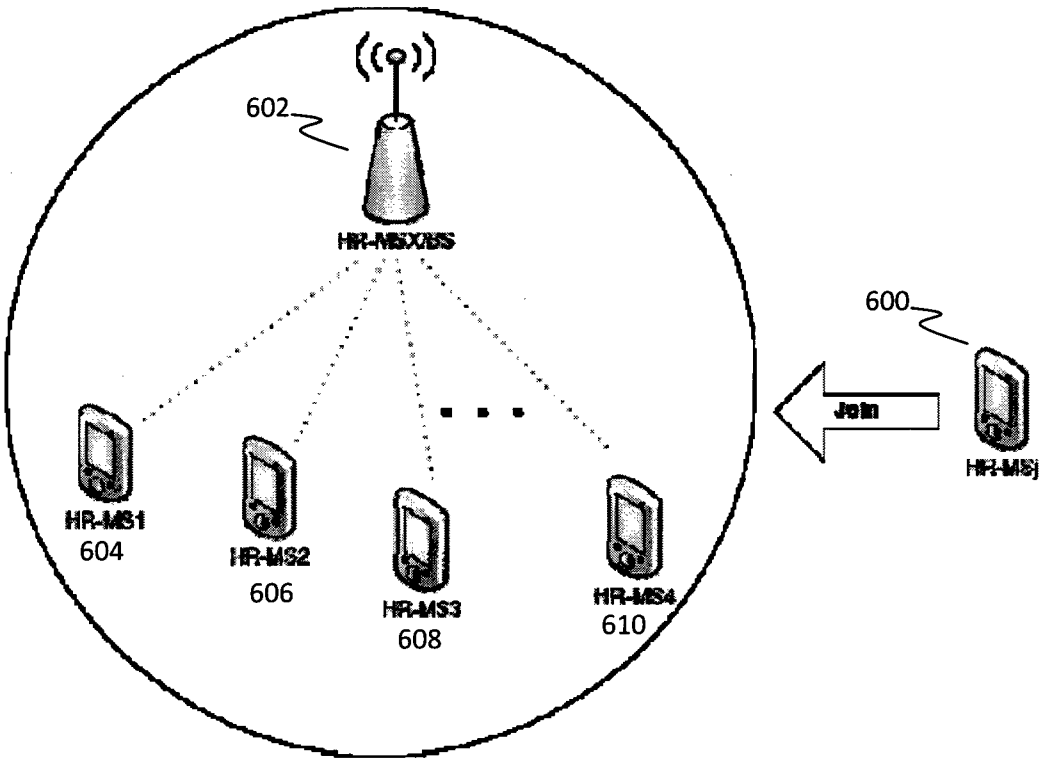

Figure 6

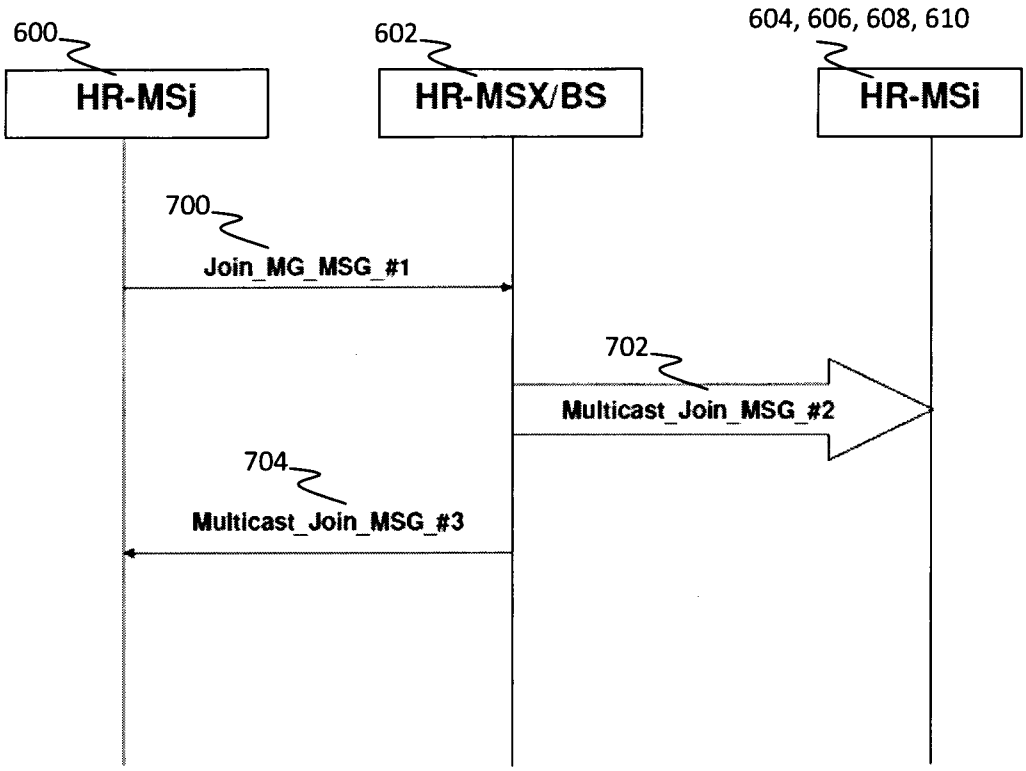
600
HR-MSj
602
HR-MSX/BS
604, 606, 608, 610
HR-MSi
700
Join_MG_MSG_#1
702
Multicast_Join_MSG_#2
704
Multicast_Join_MSG_#3

Figure 7

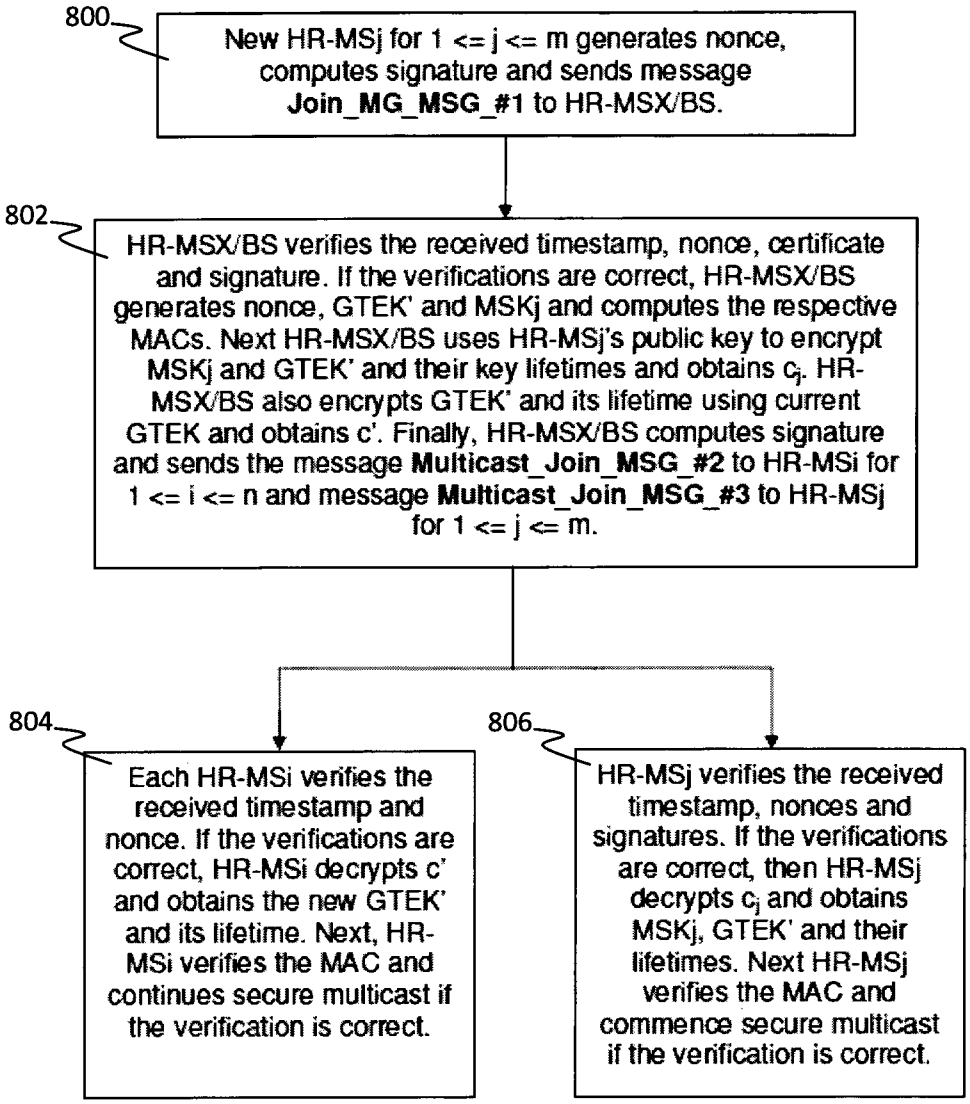
800
New HR-MSj for 1 <= j <= m generates nonce, computes signature and sends message Join_MG_MSG_#1 to HR-MSX/BS.
802
HR-MSX/BS verifies the received timestamp, nonce, certificate and signature. If the verifications are correct, HR-MSX/BS generates nonce, GTEK' and MSKj and computes the respective MACs. Next HR-MSX/BS uses HR-MSj's public key to encrypt MSKj and GTEK' and their key lifetimes and obtains cj. HR-MSX/BS also encrypts GTEK' and its lifetime using current GTEK and obtains c'. Finally, HR-MSX/BS computes signature and sends the message Multicast_Join_MSG_#2 to HR-MSi for 1 <= i <= n and message Multicast_Join_MSG_#3 to HR-MSj for 1 <= j <= m.
804
Each HR-MSi verifies the received timestamp and nonce. If the verifications are correct, HR-MSi decrypts c' and obtains the new GTEK' and its lifetime. Next, HR-MSi verifies the MAC and continues secure multicast if the verification is correct.
806
HR-MSj verifies the received timestamp, nonces and signatures. If the verifications are correct, then HR-MSj decrypts cj and obtains MSKj, GTEK' and their lifetimes. Next HR-MSj verifies the MAC and commence secure multicast if the verification is correct.

Figure 8

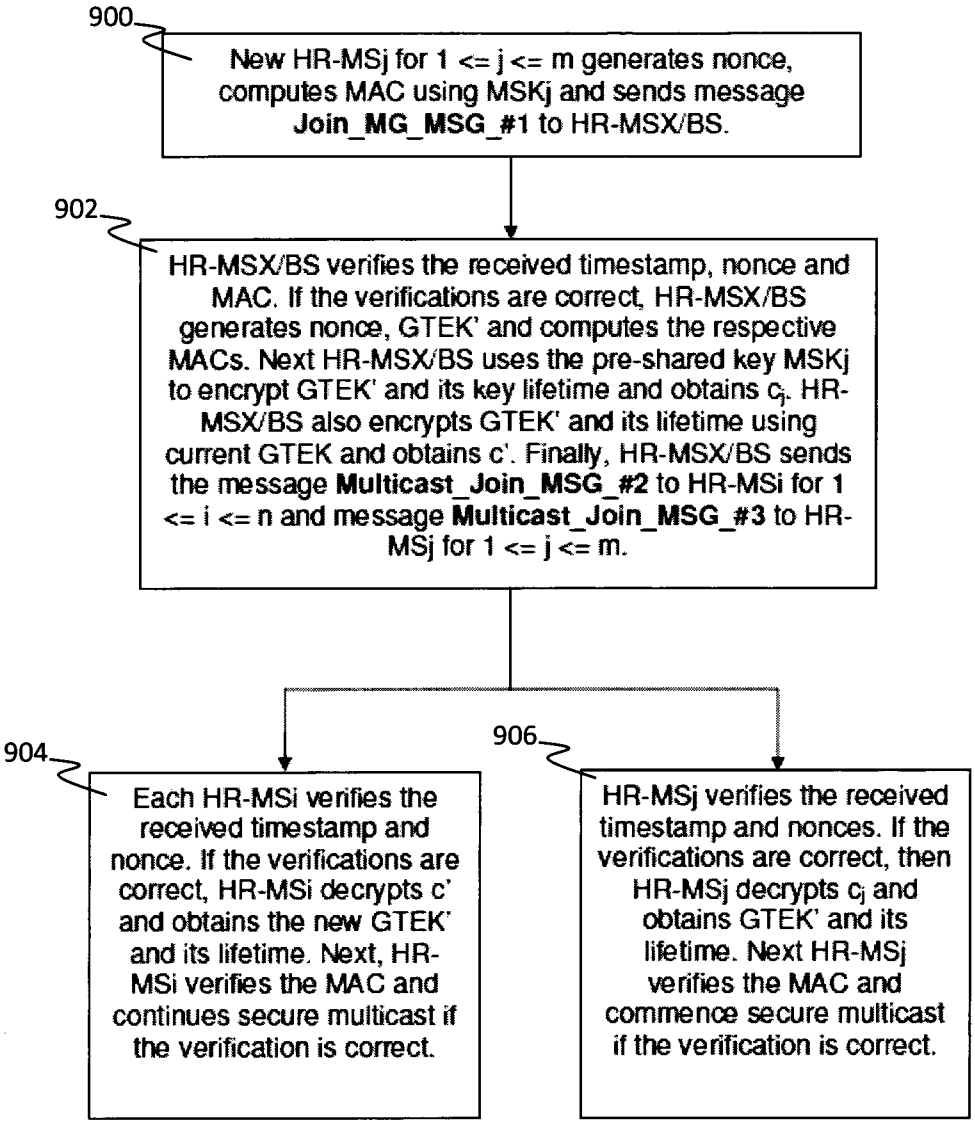
900
New HR-MSj for 1 <= j <= m generates nonce, computes MAC using MSKj and sends message Join_MG_MSG_#1 to HR-MSX/BS.
902
HR-MSX/BS verifies the received timestamp, nonce and MAC. If the verifications are correct, HR-MSX/BS generates nonce, GTEK' and computes the respective MACs. Next HR-MSX/BS uses the pre-shared key MSKj to encrypt GTEK' and its key lifetime and obtains cj. HR-MSX/BS also encrypts GTEK' and its lifetime using current GTEK and obtains c'. Finally, HR-MSX/BS sends the message Multicast_Join_MSG_#2 to HR-MSi for 1 <= i <= n and message Multicast_Join_MSG_#3 to HR-MSj for 1 <= j <= m.
904
Each HR-MSi verifies the received timestamp and nonce. If the verifications are correct, HR-MSi decrypts c' and obtains the new GTEK' and its lifetime. Next, HR-MSi verifies the MAC and continues secure multicast if the verification is correct.
906
HR-MSj verifies the received timestamp and nonces. If the verifications are correct, then HR-MSj decrypts cj and obtains GTEK' and its lifetime. Next HR-MSj verifies the MAC and commence secure multicast if the verification is correct.

Figure 9

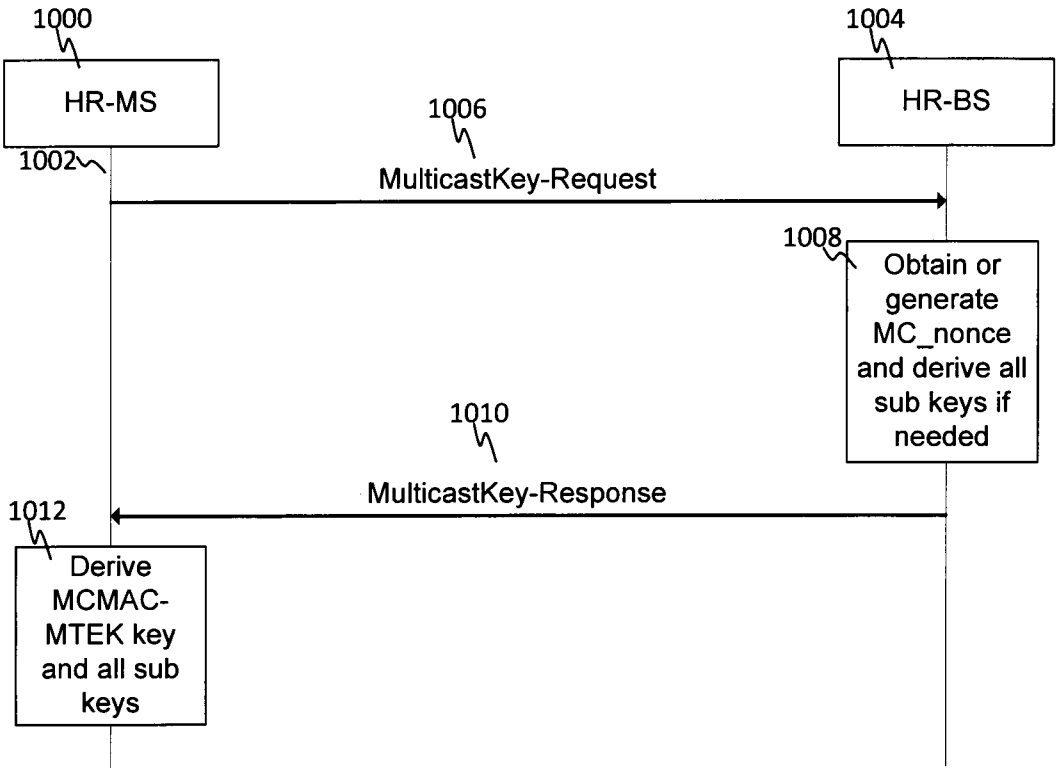

Figure 10

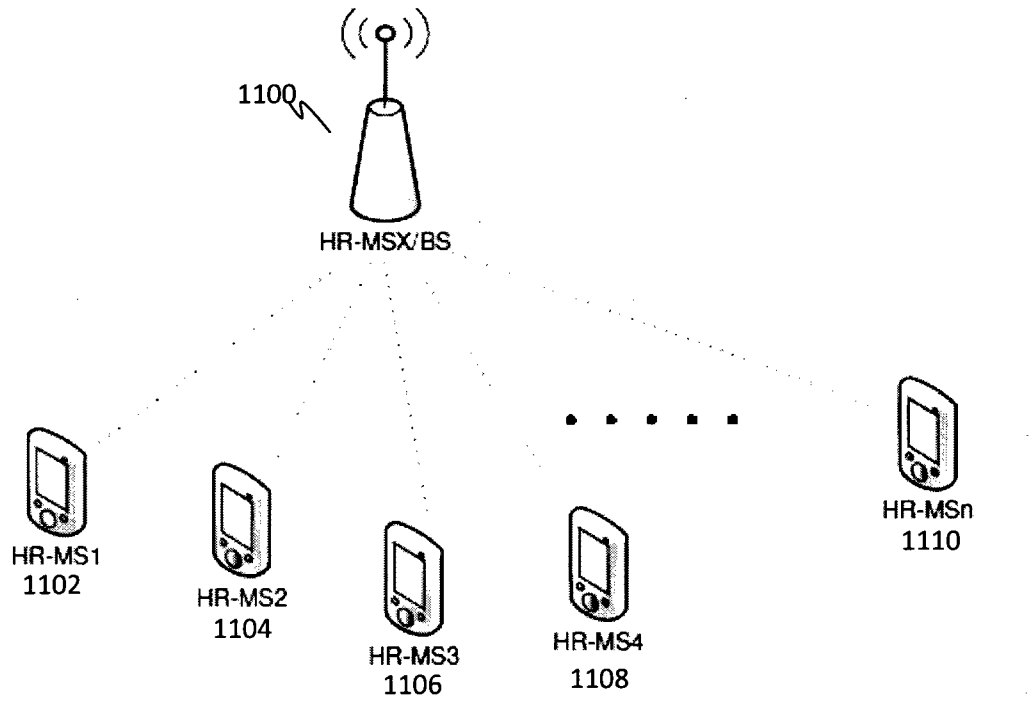

Figure 11

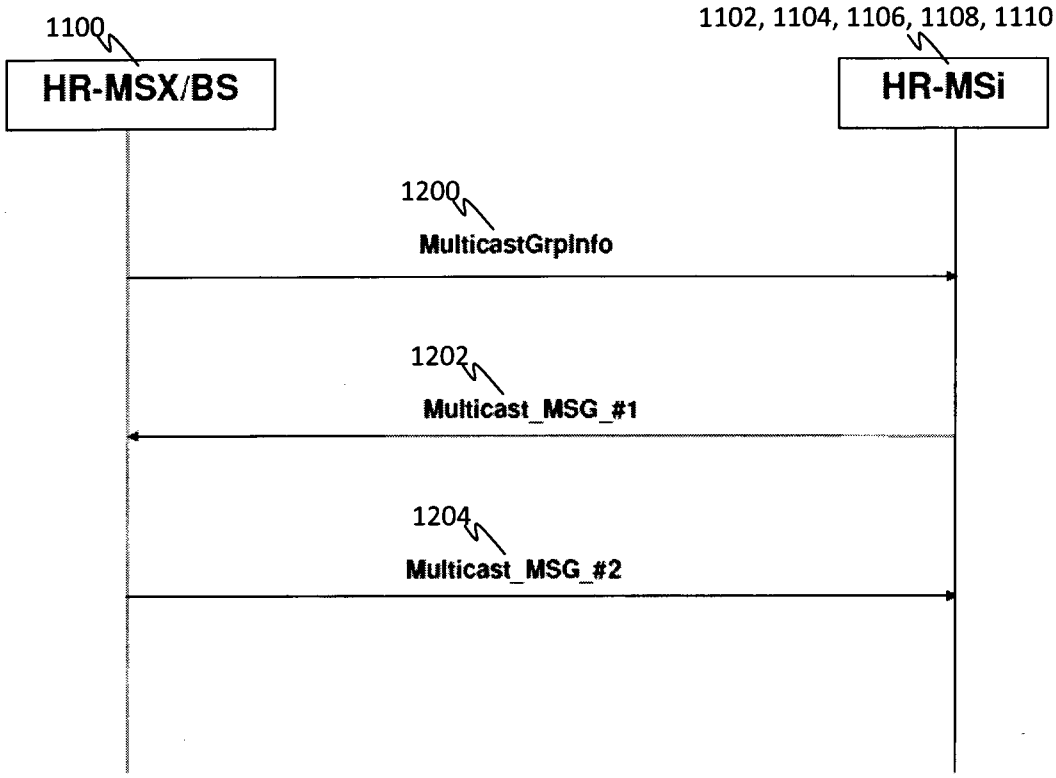
1100
HR-MSX/BS
1102, 1104, 1106, 1108, 1110
HR-MSi
1200
MulticastGrpInfo
1202
Multicast_MSG_#1
1204
Multicast_MSG_#2

Figure 12

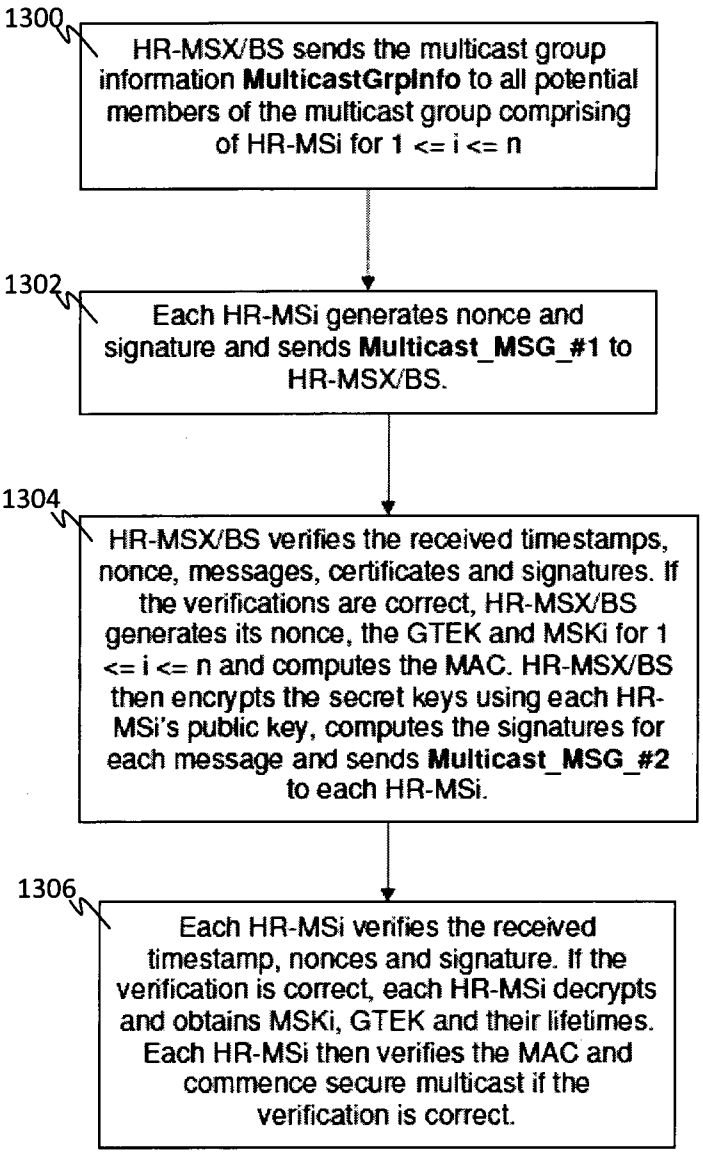
1300
HR-MSX/BS sends the multicast group information **MulticastGrpInfo** to all potential members of the multicast group comprising of HR-MSi for 1 <= i <= n
1302
Each HR-MSi generates nonce and signature and sends **Multicast_MSG_#1** to HR-MSX/BS.
1304
HR-MSX/BS verifies the received timestamps, nonce, messages, certificates and signatures. If the verifications are correct, HR-MSX/BS generates its nonce, the GTEK and MSKi for 1 <= i <= n and computes the MAC. HR-MSX/BS then encrypts the secret keys using each HR-MSi's public key, computes the signatures for each message and sends **Multicast_MSG_#2** to each HR-MSi.
1306
Each HR-MSi verifies the received timestamp, nonces and signature. If the verification is correct, each HR-MSi decrypts and obtains MSKi, GTEK and their lifetimes. Each HR-MSi then verifies the MAC and commence secure multicast if the verification is correct.

Figure 13

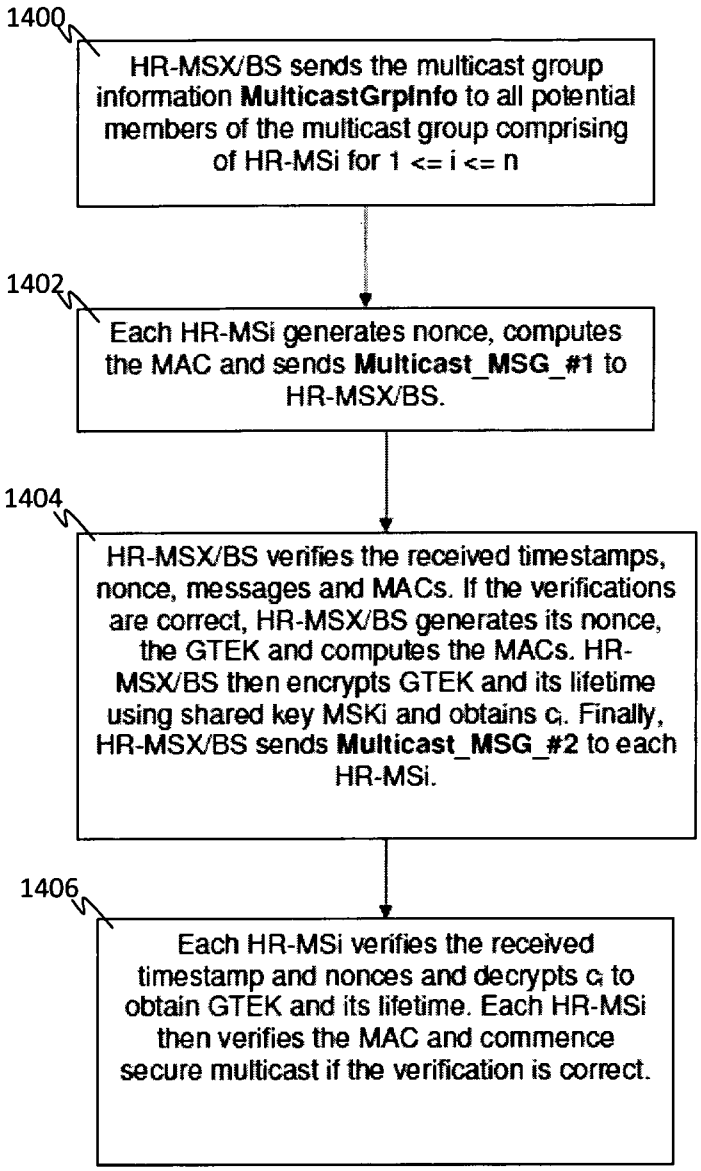
1400
HR-MSX/BS sends the multicast group information **MulticastGrpInfo** to all potential members of the multicast group comprising of HR-MSi for 1 <= i <= n
1402
Each HR-MSi generates nonce, computes the MAC and sends **Multicast_MSG_#1** to HR-MSX/BS.
1404
HR-MSX/BS verifies the received timestamps, nonce, messages and MACs. If the verifications are correct, HR-MSX/BS generates its nonce, the GTEK and computes the MACs. HR-MSX/BS then encrypts GTEK and its lifetime using shared key MSKi and obtains c_i. Finally, HR-MSX/BS sends **Multicast_MSG_#2** to each HR-MSi.
1406
Each HR-MSi verifies the received timestamp and nonces and decrypts c_i to obtain GTEK and its lifetime. Each HR-MSi then verifies the MAC and commence secure multicast if the verification is correct.

Figure 14

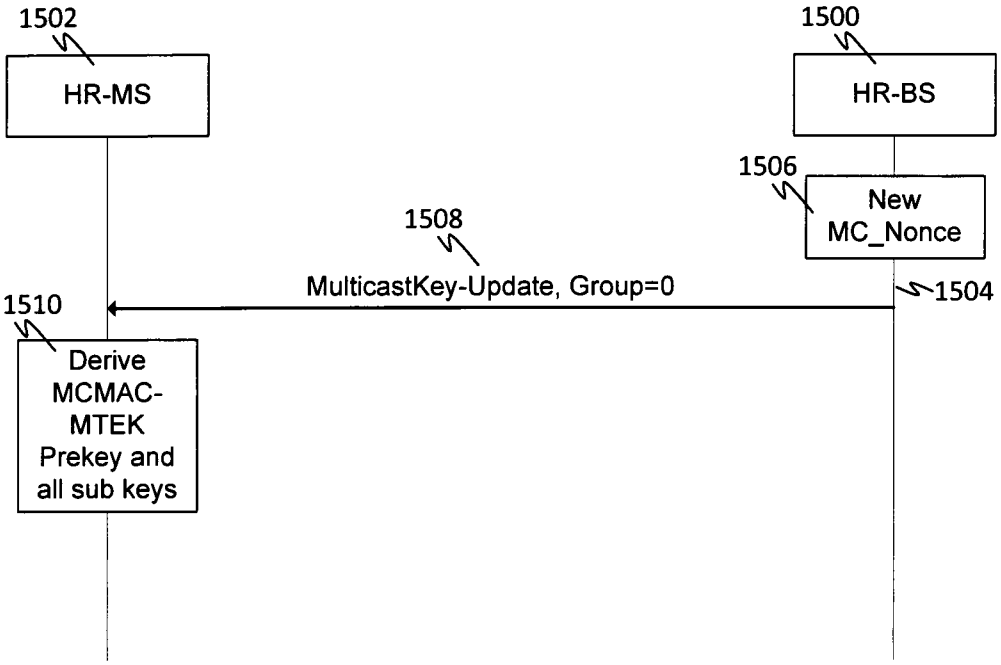

Figure 15

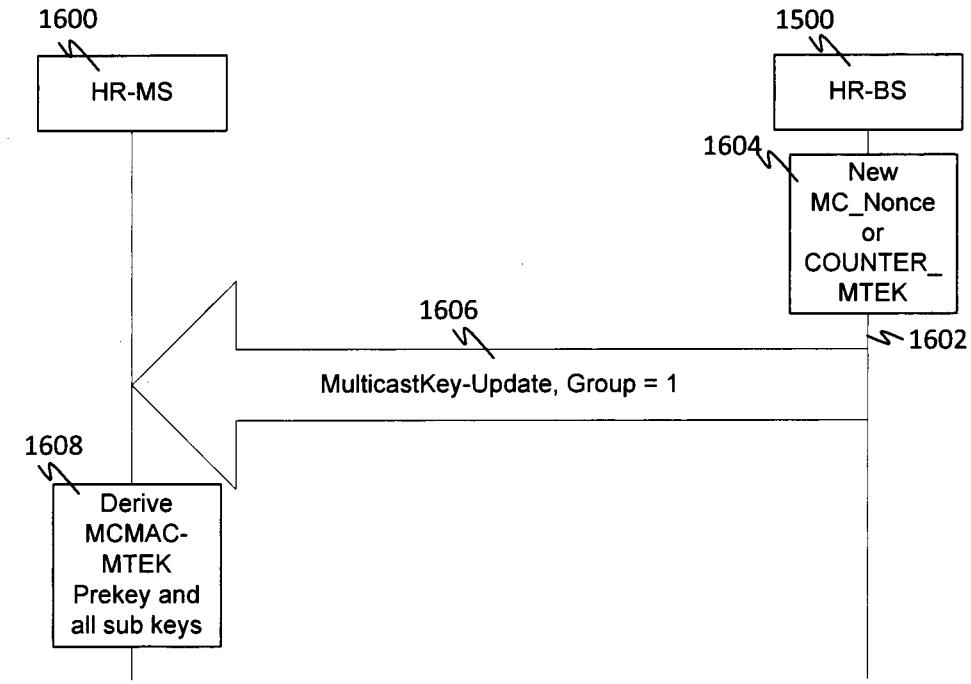

Figure 16

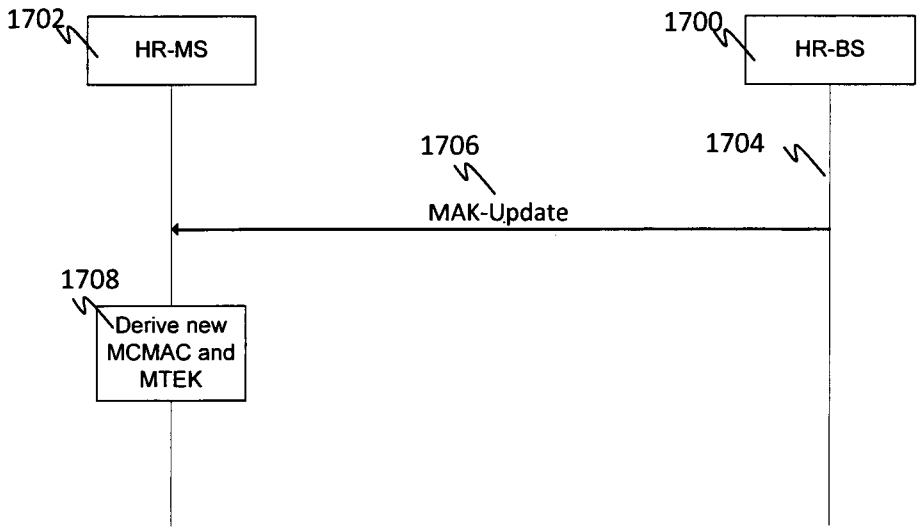

Figure 17

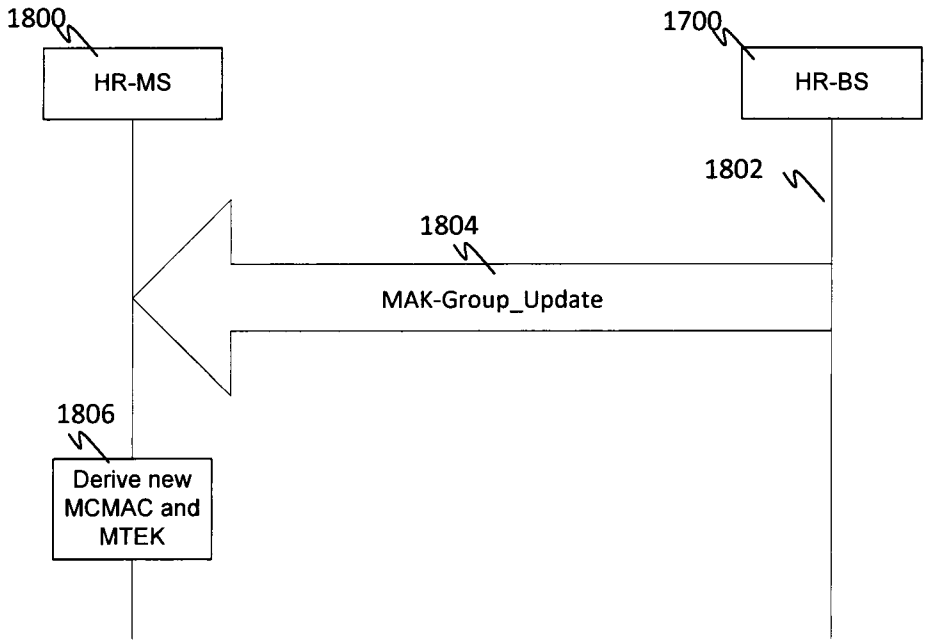

Figure 18

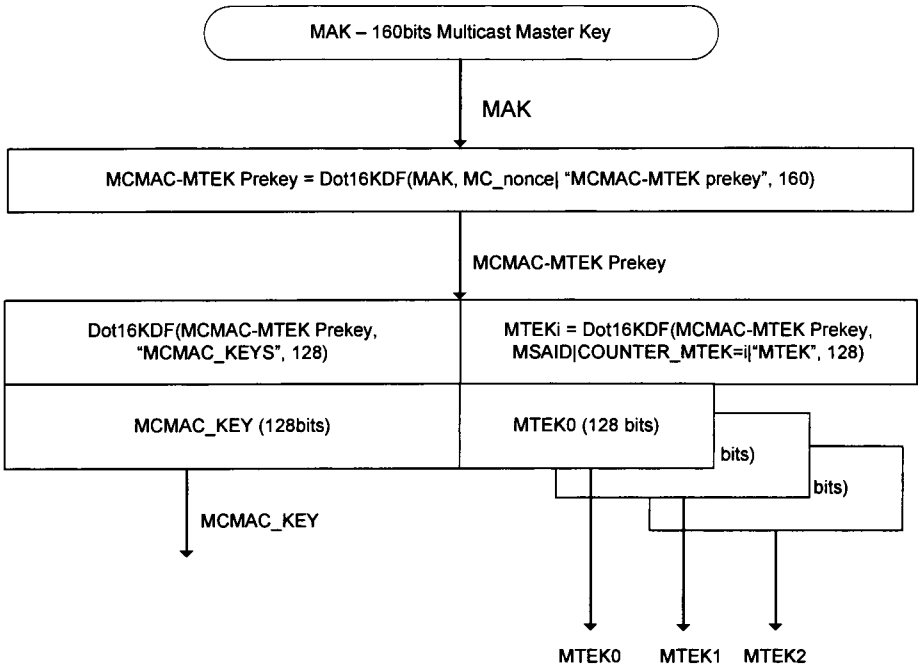

Figure 19

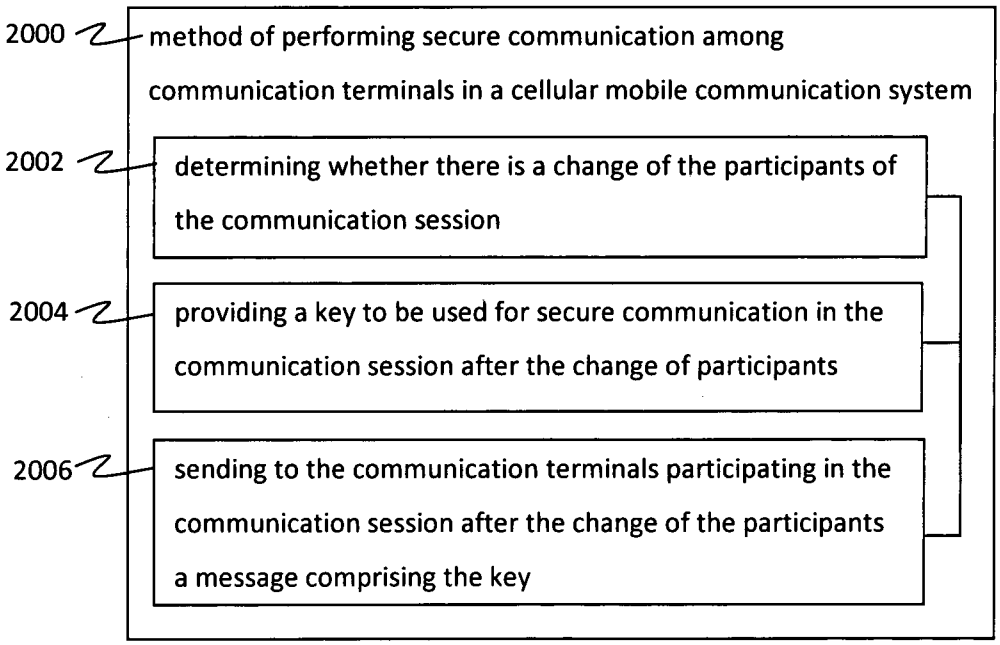

Figure 20

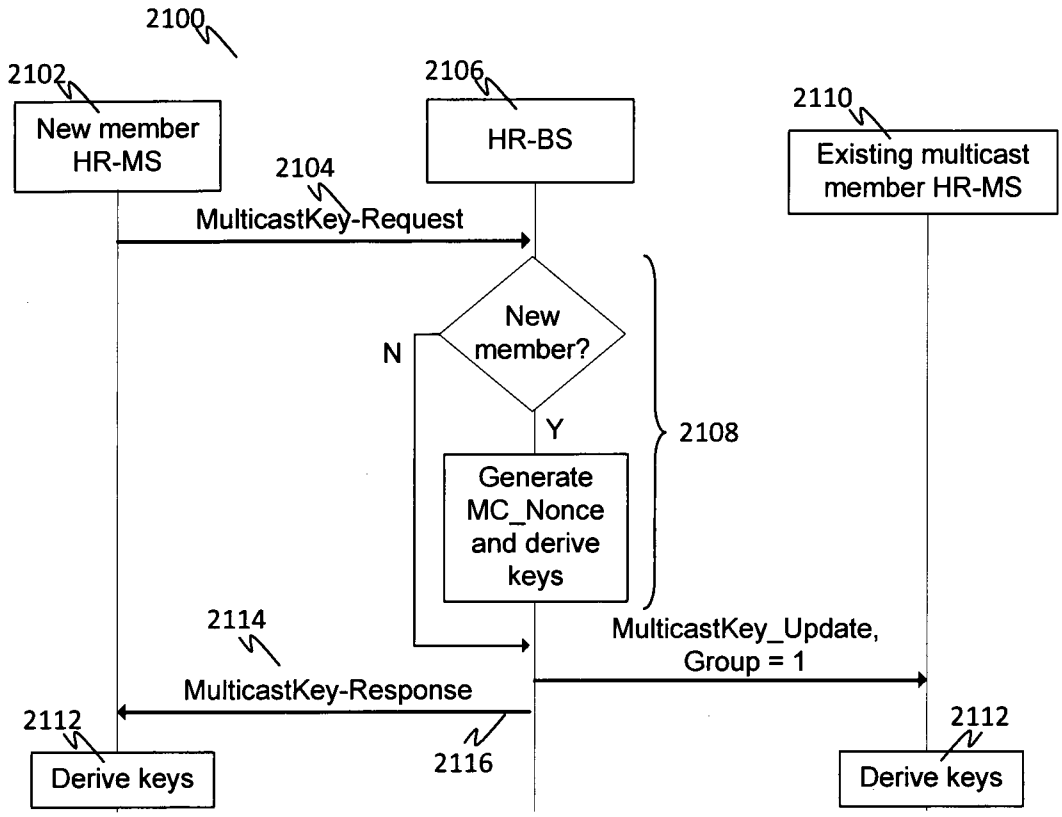

Figure 21

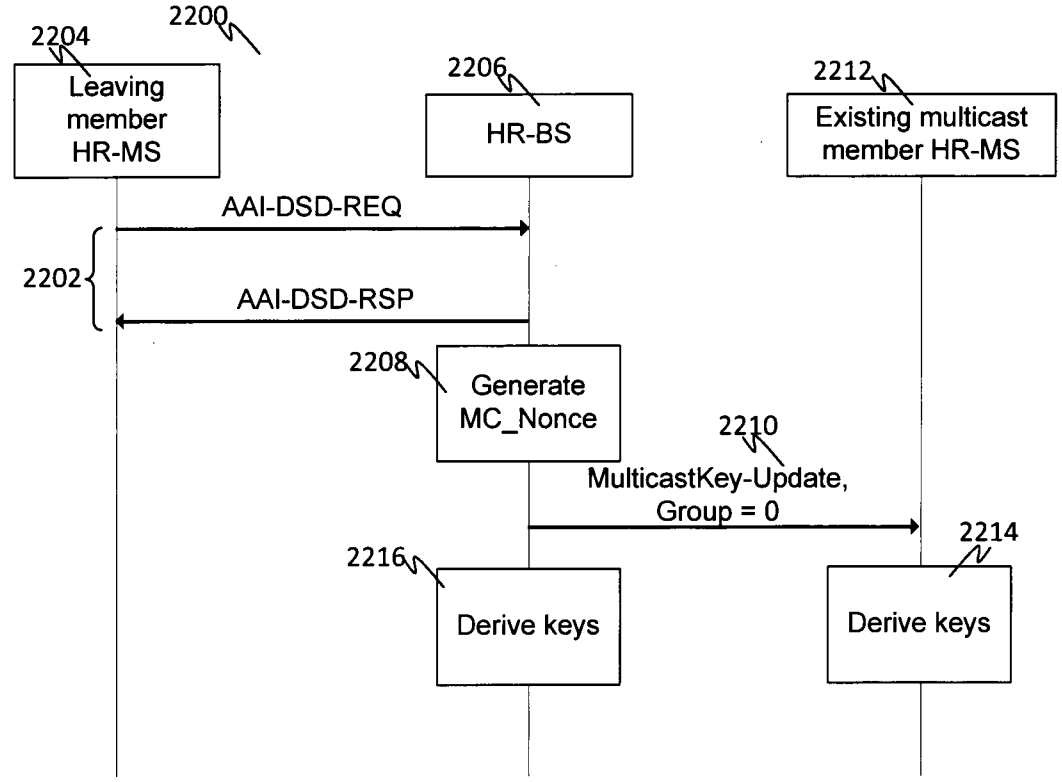

Figure 22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2012/000062

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04L 9/08 (2006.01) ***H04L 9/32*** (2006.01) ***H04W 12/04*** (2009.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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

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

EPODOC, WPI, GOOGLE PATENTS: secure communication, cellular mobile, authenticate, check+, multicast, clients, cipher and similar keywords

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/0257365 A1 (ANCHAN et al.) 07 October 2010 Abstract; Figs. 4 – 6B; paragraphs [0005], [0007], [0010], [0013], [0024], [0038], [0041], [0048] – [0056], [0060], [0064] – [0066]; claims 1, 2	1 – 24

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

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 May 2012	1 June 2012
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **ASHWIN EDAKANDI** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : +61 2 6225 6158

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SG2012/000062

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report	Patent Family Member					
US 2010257365	CN	102379134	EP	2415293	KR	20120015312
	WO	2010115129				

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX