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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 August 2006 (24.08.2006)

PCT

(10) International Publication Number
WO 2006/088751 A2

(51) International Patent Classification:
H04J 3/26 (2006.01)

(21) International Application Number:
PCT/US2006/004846

(22) International Filing Date:
10 February 2006 (10.02.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0503308.9 17 February 2005 (17.02.2005) GB

(71) Applicant *(for all designated States except US)*: **MOTOROLA, INC.** [US/US]; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KELLIL, Mounir** [DZ/FR]; 26, Avenue Des Dahlias, F-94240 L'Hay Les Roses (FR). **LACH, Hon-yon** [FR/FR]; 9 Rue De La Republique, F-94220 Charenton-le-Pont (FR). **OLIVEREAU, Alexis** [FR/FR]; 1/3 Rue Guy Mocquet, F-91400 Orsay (FR). **JANNETEAU, Christophe Jacques Philippe** [FR/FR]; 12, Rue Eugene Delacroix, F-78390 Bois D' Arcy (FR).

(74) Agent: **NICHOLS, Daniel K.**; Labs Patent Porfolio Manager, 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

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

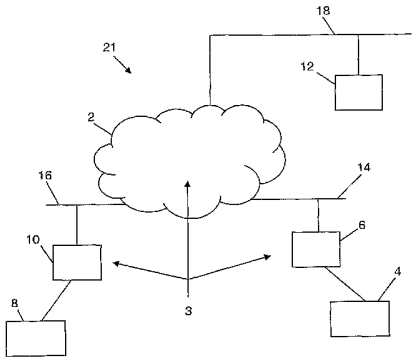
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** ACCESS CONTROL FOR MOBILE MULTICAST



(57) **Abstract:** An access control method for controlling access to a multicast delivery tree (3), in e.g. an IPv4 or an IPv6 network, comprising: performing, at a designated router (6, 10), authorization procedures for access to the delivery tree (3), the designated router (6, 10) being a multicast edge router of the multicast delivery tree. The designated router (6, 10) performs the authorization procedures by comparing authorization information received from a user (4, 8) with information received from a group manager (12). For sender access control, the verification information is based on a sender key provided by the group manager (12) to legitimate senders. For receiver access control, the verification information is based on a group key provided by the group manger (12) to a group of users. A derived value of the key, obtained by applying a derivation function to the key, may be used.

WO 2006/088751 A2

CML01661N

ACCESS CONTROL FOR MOBILE MULTICAST

Field of the Invention

The present invention relates to group communications over packet data networks. The present invention relates in particular, but not exclusively, to multicast according to the Internet Protocol, i.e. IP multicast, for use with the Internet or other networks.

Background of the Invention

Internet Protocol (IP) is a well established protocol for routing of data packets over packet data networks, for example the Internet. Examples of specific versions of IP are IPversion4 (IPv4) and IPversion6 (IPv6).

Multicast is a process whereby groups of users are formed, usually temporarily, and then each user in the group may send common data to some or all of the other members of the group. Protocols for multicast, i.e. transmission of given data from one provider to plural receivers are included in, or added to, the general IP protocols, and such multicast may be referred to as IP Multicast. Typical applications are multimedia conferences, video games and so on.

A multicast delivery tree (which may also be referred to as a multicast distribution tree) is established. The deliver tree comprises interconnected network nodes and routers, for example nodes in the Internet. At the edges of the delivery tree are edge routers which couple the delivery tree to a user's receiving and transmitting communication apparatus, or to a user's network

to which the user's receiving and transmitting communication apparatus is connected (e.g. a home network).

The IP and IP Multicast protocols are standardised by the Internet Engineering Task Force (IETF).

IP Multicast is an open model i.e. it provides public multicast addresses while keeping the receiver addresses unknown for the source as well as the multicast routers. Furthermore, in principle any host can send multicast traffic to any multicast address. This open model simplifies group management and enables IP multicast scaling to a large number of group members. However the lack of user access control mechanisms in the multicast routers according to this open model causes security deficiencies, i.e. access control is complicated and does not address all types of inappropriate access that may be attempted by malevolent or fraudulent users.

Multicast security issues may be considered as two main aspects: the first being end-to-end security i.e. protection of the multicast traffic content; the second being multicast infrastructure security i.e. security issues in the multicast delivery tree (the delivery tree comprising multicast routers in charge of transmitting and receiving multicast traffic from sources and receivers, and other nodes connected therebetween). Example of some security issues relating to access to the multicast delivery tree include:

1. Impersonation of multicast routers by malicious hosts
2. Joining illegitimately particular multicast groups
3. Sending bogus traffic to multicast groups (i.e. extra traffic and so called "Denial of Service" (DoS) attacks).

Measures to address the first problem are known in that it is sufficient to secure the control messages of the multicast routing protocols to ensure that the multicast tree has been correctly built as proposed for MOSPF (Multicast Open Shortest Path First), PIM-SM (Protocol Independent Multicast- Sparse Mode), and CBT (Core Based Tree). However, securing multicast routing protocols is not sufficient to protect the multicast distribution tree since it only ensures that the group membership subscription information maintained in the edge multicast routers are populated correctly. They do not have the ability to check whether a particular host is authorized to join a particular group, or whether a given host is authorized to send its traffic over the tree towards group receivers. The lack of access control mechanisms at the edge of the delivery/distribution tree produces a security hole in the multicast tree even though the multicast routing protocols are secure. Indeed, the lack of a security mechanism that prevents users from joining or sending data illegitimately may cause Denial of Service attacks due respectively to fake report messages and bogus multicast traffic. In brief, it is highly desirable to secure primarily the edge of the distribution tree.

The IP Multicast model does not currently provide any effective protection at the edge of the distribution tree. Such a protection is normally achieved through new mechanisms known as sender access control and receiver access control. From the viewpoint of the IP Multicast model, the access control service protects against several threats.

Specifically, sender access control aims at preventing unauthorized hosts from sending bogus multicast traffic. This is particularly challenging because the multicast model allows any user to send its multicast traffic without prior request to the multicast router. Therefore, an attacker can send

bogus multicast traffic to a multicast group even if it is secure. Also, although an ingress filtering mechanism eliminates the risk for remote attacks, an attacker localized within the same link as a legitimate sender can impersonate the legitimate sender (this may be referred to as "spoofing") and send bogus multicast traffic. Furthermore, the problem is particularly complicated in the basic IP Multicast model known as the "Any Source Model" (ASM) as the designated routers do not maintain state information about the senders. (ASM is described in S. Deering, "Host Extension for IP Multicasting", Internet RFC 1112, August 1989.). A further known aspect is the use of source filtering mechanisms as provided by the other IP Multicast Model known as the "Source-Specific Model" (SSM). (SSM is described in S. Bhattacharyya, "An Overview of Source-Specific Multicast (SSM)", Internet RFC 3569, July 2003; and also in N. Wang and G. Pavlou, "Scalable IP Multicast Sender Access Control for Bi-directional Trees" in Networked Group Communication, Proceedings of the 3rd International Workshop on Networked Group Communication (NGC'2001), London, UK, pp. 141-158, November 2001.) This scheme does not do not resolve the "spoofing" issue because the scheme uses sender's IP address-based filtering, which cannot prevent spoofing attacks originating from the network of a legitimate source.

With respect to receiver access control, it is significant that the receivers exchange router membership control messages with the multicast edge router. Current approaches attempt to secure the control messages originating from the receiver, this is the case for example with the *"Internet Group Management Protocol"* (IGMP) which is designed for IPv4 (IGMP is described in B. Cain, S. Deering, B. Fenner, I. Kouvelas, and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002), and *"Multicast Listener Discovery"* (MLD) which is designed for IPv6 (MLD is

described in Rolland Vida and al., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", Internet RFC 3810, June 2004). However, despite the security considerations of those protocols, an illegal host can still send bogus subscriptions that generate the following:

(i) wastage in resources and risk of denial of service attacks as well as unnecessary extension of the distribution tree towards networks where there are no legitimate hosts; and

(ii) excessive bandwidth consumption in the subnet of the attacker, as fake Report messages may open vulnerabilities to multicast traffic overload and potential risk for denial of service attacks in the subnet of the attacker.

Various approaches have been proposed to address the above deficiencies. Before reviewing them, it will aid understanding to clarify the fact that in the prior art, and even in other security-related works, access control, authentication, and authorization terms are usually unintentionally interchanged. In brief, the authentication refers typically to the action of establishing the identity of users. The access control assumes that the authentication succeeds before the access control can be enforced as described in R. S. Sandhu and P. Samarati, "Access control: principle and practice," IEEE Communications Magazine, vol. 32, no. 9, pp. 40–48, 1994. The access control aims at protecting system resources (e.g. computer, data networks, multicast tree, etc.) against unauthorized access as described in as described in R. Shirey, "Internet Security Glossary", RFC 2828, May 2000. The authorization represents rather the right (or a permission) that is granted to a system entity to access a system resource as described in as described in R. Shirey, "Internet Security Glossary", RFC 2828, May 2000.

To summarise, once an entity wishing to access particular resources has been successfully authenticated (e.g. by the entity providing the requested

resources), the access control can be enforced using an authorization procedure as a procedural means (to achieve the access control).

The access control to the multicast tree typically involves three entities: *group manager*, host, and router. The group manager is a security entity that is responsible for managing multicast groups. In a general scenario of an access control to the delivery tree, the group manager performs user authentication and authorization to subscribe to particular multicast groups. A successful authorization process at the group manager ends by providing the user with the *authorization information* (e.g. credentials).

Once the user (sender or receiver) gets the required authorization information, it could present that information to the multicast router of its network (the designated router (DR)), the designated router being a multicast edge router of the multicast distribution tree of a user in the given multicast group. The DR then performs a user authorization procedure based on the received authorization information. In this situation, user authentication procedure at the DR side may be optional in case such a procedure has already been performed by the group manager. A necessary condition that makes such a scenario working is that both the multicast router and the user know the group manager (e.g. group manager's certificate is trusted by both the user and the multicast router).

In brief, the access control to the delivery tree is effectively at least partially distributed between the group manager and the designated router. Note that it is possible that the *authentication information,* authenticating the user's request sent to the designate router, could represent as well its authorization information during the authorization procedure at the designated router. This is why part of the prior art unintentionally interchanges authentication, authorization, and access control although the

common goal of the proposed approaches is to define access control mechanisms at the edge of the distribution tree.

To avoid ambiguities in the description of the prior art, the terms "authorization information", and "authorization procedure" will be used in the description of the existing access control solutions.

Some of the main approaches that address the access control to the delivery tree are described in the following.

US 20020091926 A1 addresses the receiver access control problem for IGMP (IPv4). US 20020091926 A1 discloses definition of a "User Authentication Server" that registers valid receivers and attributes a password- as authorization information- to each of them. The *"Provider Edge Router"* (PE), which is a local area network (LAN) router stores a state for each receiver in order to maintain the forwarding state for multicast groups. However, this approach does not support sender access control. In addition, it does not work in IPv6 (i.e. with MLD) and does not address the receiver mobility problem.

A. Van Moffaert and O. Paridaens, "Security issues in Internet Group Management Protocol version 3 (IGMPv3)", draft-irtf-gsec-igmpv3-security-issues-01.txt, February 2002, (Work in Progress), discloses an IGMP message authentication approach. A Multiparty Security Association (also called Group Security Association: GSA) and its corresponding shared key (GSA key) are set up among IGMP entities (routers and hosts) participating to the same multicast group (source, multicast address). The GSA along with the GSA key are established based on an extension to the GDOI protocol which is described in Mark Baugher and al., "The Group Domain of Interpretation", RFC 3547, July 2003. When a host whishes to join a given multicast group, it sends an authenticated IGMP report message, where the authentication

information (generated based on the GSA key) represents as well the authorization information. However, this approach does not address the sender access control issue, since the IGMP router cannot identify valid sources. Besides, this approach does not address the user exclusion issue, which introduces risks for improper use of IGMP router resources by valid users. In addition, this approach may not work in mobile environment since a user may move into a network where the IGMP router does not support the GDOI protocol.

B. Coan et al., "HASM: Hierarchical Application-Level Secure Multicast", Internet draft draft-coan-hasm-01.txt, October 2002 (Work in Progress) discloses a Hierarchical Application-Level Secure Multicast (HASM) approach. The approach suggests securing and extending IGMP control messages. The approach involves an Authentication and Authorization server (A/A server) issuing a ticket containing user identity, a session key to be shared between the A/A and that user, and an expiration time. The ticket is encrypted with a key shared between the A/A server and the edge router, and sent to the user along with a session key using a secure channel. When a user wishes to join a multicast group as a receiver, it generates a timestamp that it encrypts using the session key, and sends it along with the ticket in a modified IGMP Report message to the edge router (the authorization information is then made of an encrypted timestamp and the ticket). However, this approach is exclusive to IGMP (IPv4). Also, the timer use is inconvenient. Furthermore, the edge router is vulnerable to denial of service attacks since a valid user (sender or receiver) can use the ticket improperly by launching bogus subscriptions (or traffic) for non-existing multicast groups. In addition, this approach may not work in mobile environment because the

ticket is encrypted with a key shared between the A/A server and the current edge router.

T. Hayashi et al., "Multicast Listener Discovery Authentication protocol (MLDA)", Internet draft draft-hayashi-mlda-02.txt, April 2004 (Work in Progress), discloses a Multicast Listener Discovery Authentication protocol (MLDA) approach. Various sub-types of Report messages and a new Query message called User Query are defined. The User Query is unicast to a particular user in order to authenticate it. In this solution the host that wishes to join a multicast group sends a specific MLDA Report message that requests for a "Challenge Value" from the MLDA router. A messaging procedure follows where the authorization information (user ID and password) is sent by the host to the MLDA router, leading to an authorization procedure at the MLDA router. However, this approach does not address the sender access control problem. In addition, this approach is specific to MLDv1 and relies on specific infrastructures which can introduce problems when a user changed domains.

C. Castelluccia and G. Montenegro, "Securing Group Management in IPv6 with Cryptographically Based Addresses" INRIA Technical Report no4523, July 2002, discloses a Group Cryptographically Based Addresses (G-CBA) approach. The Cryptographically Based Addresses concept is extended to group addresses. However, this approach is based on public key techniques, which are computationally expensive and require certificate infrastructures (because the authorization information has an SPKI (Simple Public Key Infrastructure) certificate format). Also, this approach does not support sender access control.

Summary of the Invention

The present inventors have realised that a combination of the following characteristics would be beneficial in an improved access control process for IP Multicast:

The process to have at least the option of being applicable to both sender access control and receiver access control.

The access control process to have the potential to be relatively quick, which would be particularly useful for mobile users.

A requirement for the user (sender or receiver) to provide information that proves that it is allowed attending multicast sessions.

In a first aspect, the present invention provides an access control, or authorization, method for controlling access to a multicast delivery tree, the method comprising: performing, at a designated router, authorization procedures for access to the delivery tree, the designated router being a multicast edge router of the multicast delivery tree.

The designated router may perform the authorization procedures by comparing authorization information received from a user with information received from a group manager.

When the access control (authorization) method is a sender access control method, the authorization information may be based on a sender key provided by the group manager to legitimate senders.

When the access control (authorization) method is a receiver access control method, the authorization information may be based on a group key provided by the group manager to a group of users.

The method may further comprise the use of a derived value of the key obtained by applying a derivation function to the key.

The derivation function may be a one-way hash function applied to the value of the key.

The derivation function may be specified to the user by the group manager.

The group manager may update the group key when a user leaves the multicast group.

The group manager may obsolete the group key when all the users in the multicast group leave the multicast group served by the delivery tree.

The group manager may send a list of authorized multicast groups to the designated routers.

The group manager may send a list of sender keys to the designated routers.

The group manager may send a list of derived group keys to the designated routers.

The sender key may be used to establish a secure channel between the sender and the designated router.

In a further aspect, the present invention provides a storage medium storing processor-implementable instructions for controlling a processor to carry out the above first aspect, including any of the various options mentioned above.

In a further aspect, the present invention provides a multicast group manager for a packet data network; the multicast group manager being arranged to provide authorization information to users and designated routers for implementing the method of the above first aspect, including any of the various options mentioned above.

In a further aspect, the present invention provides a multicast edge router of a multicast delivery tree in a packet data network; the router being arranged to perform authorization procedures to access the delivery tree according to the method of the above first aspect, including any of the various options mentioned above.

In a further aspect, the present invention provides a host for participating in multicast in a packet data network; the host being arranged to provide authorization information according to the method of the above first aspect, including any of the various options mentioned above. The host may be adapted to build the authorization information according to its current network location

The various aspects of the present invention tend to provide one or more of the following the following advantages.

The invention may be applied to both the IPv4 (IGMP) and the IPv6 (MLD) protocols.

Sender and receiver access control at the edge of the multicast distribution tree is provided.

The authorization/access control process has the potential to be low cost, for example when based on hash techniques, as this tends to significantly reduce both resource consumption for users, in particular mobile users, as well as tending to reduce the risk of denial of service attacks.

The processes tend to be suitable for the mobile environment since the authorization information, e.g. "Proof-of-Legitimacy", does not depend on user location or on certification schemes, and there is no need for a pre-established secure channel between users and multicast edge routers.

At least in certain aspects, the process tends to ensure user exclusion, which avoids improper use of multicast router resources by former group participants (senders and receivers).

The processes tend to reduce or remove the use of digital signatures.

The processes tend to reduce the risk of denial of service attack.

The processes tend to be particularly suitable or advantageous in the mobile environment.

Brief Description of the Drawings

Embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

FIG. 1 is a schematic illustration of a network arrangement coupled to the Internet to which embodiments of the present invention may be applied;

FIG. 2 is a message sequence chart showing messages sent between a receiver host, a designated router and a group manager of the network arrangement of FIG. 1;

FIG. 3 is a message sequence chart showing messages sent between a sender host, a designated router and a the group manager of the network arrangement of FIG. 1; and

FIG. 4 is a schematic illustration of a network arrangement coupled to the Internet to which embodiments of the present invention may be applied in the case of a distributed group manager.

Description of Preferred Embodiments

FIG. 1 is a schematic illustration of a network arrangement 1 coupled to the Internet 2 to which embodiments of the present invention may be applied. In this example the elements of the network arrangement are all compliant with IP. The network arrangement comprises a receiver host 4, a first designated router (DR) 6, a sender host 8, a second DR 10, and a group manager (GM) 12. The first DR 6 is coupled to the Internet 2 via a first link 14. The second DR 10 is coupled to the Internet 2 via a second link 16. The GM 12 is coupled to the Internet via a third link 18. The first DR 6 is further coupled to the receiver host 4. The second DR 10 is further coupled to the sender host 8.

The first DR 6 and the second DR 10 are respective multicast edge routers of the multicast delivery tree 3, which comprises these edge routers plus other nodes (not shown) including connected nodes of the Internet 2.

The receiver host 4 and the sender host 8 are mobile nodes compliant with Mobile IP, embodied for example in the form of mobile telephones, portable computers with wireless connectivity, and so on. Each of the hosts 4, 8 is functionally capable of receiving and transmitting in multicast, however for clarity the receiver host 4 will be described only with respect to receiving multicast data, and the sender host 8 will be described only with respect to sending multicast data.

The GM 12 is an IP node, for example a server (also referred to as Group Controller and Key Server (GCKS)) , and has functionality for managing one or more multicast IP groups as defined in the Multicast Group Security Architecture, which is described in T. Hardjono et al., "Multicast Group Security Architecture", Internet RFC 3740, March 2004.

Details of the process steps carried out by these entities in various embodiments will be described later below with reference to FIGS. 2 and 3.

However, an overview of the embodiments, including various process steps and network mechanisms created or introduced as part of the embodiments, will be described first, as follows.

Processes are implemented that provide sender and receiver access control in the multicast edge routers of the multicast tree (e.g. in DR 6 and DR 10). This is different to all the prior art approached described earlier above. These processes are based on verification/validity information provided by legitimate senders and receivers. This verification/validity information is labelled "Proof-of-Legitimacy" in the following description. In case of a sender, such information is constructed based on a Sender Key (SK) provided by the GM 12 to each legitimate sender when the sender carries out its registration process. In case of receivers, the Proof-of-Legitimacy information is the derived value of a Group Key (GK). Such a Group Key is provided by the GM and shared by a group of receivers. The GM generates a single GK either per multicast address or couple (source address, multicast address).

Another provision is the derived value of a Key. The Key is represented by the notation "K", and the derived value of the Key is represented by the notation "K-derived value". The derived value of the key may be any value obtained by applying a one-way hash function on the value of the key K. Details of one-way hash functions are described for example in R. Rivest, "MD5 Digest Algorithm", Request for Comments 1321, April 1992; and in D. Eastlake and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", Request for Comments 3174, September 2001, both of which references are incorporated herein by reference. This enables the K value to be secured against any non-trusted entity (e.g. malicious hosts, routers, etc). The derivation function (e.g. Hash (K)) may be specified by the GM 12 to the users

(e.g. the receiver host 4 and the sender host 8) during the registration of the respective user.

For receiver exclusion, the GM 12 obsoletes (e.g. deletes, or stores in an archive file, or some other appropriate action) the corresponding GK when all the receivers leave a given multicast group (corresponding either to a multicast address or a "couple" comprising a source address and a multicast address). Also, when a receiver leaves a given multicast group (multicast address or a couple), the GM 12 may update the GK for all the remaining receivers of the affected multicast group. This obsoletes the *Proof-of-legitimacy* of receivers that left their groups.

To ensure sender exclusion, the GM 12 and DR 10 may interact together so that they remove the multicast addresses from the list of addresses the sender is authorized to transmit traffic to. If there are no more multicast addresses registered for a given sender, the GM invalidates the corresponding SK key, whereas the DR removes the security association with that sender. Such a security association is established in advance based on the SK key.

Further details of the GM 12 are as follows. In the network arrangement 1 of FIG. 1, the GM 12 is a centralized GM. However, in other embodiments a distributed form of GM may be used, as will be explained in more detail later below with reference to FIG. 4. The GM 12, and where appropriate distributed GMs as will be described, perform the following tasks:

1. User authentication and authorization processes,
2. Key management functionalities for GK and SK (e.g. *Group Controller Key Server* (GCKS), as described further in Mark Baugher and al., "The

Group Domain of Interpretation", RFC 3547, July 2003, which reference is incorporated herein by reference.

3. Provide legitimate users with the required keying materials (GK, SK) to build their *Proof-of-Legitimacy* Information.
4. Give the rights to send for users (one SK key for each legal sender).
5. Maintain a data structure holding the SK key of each sender, its corresponding SK-derived value, and the list of multicast addresses to which the sender wishes to send multicast traffic.

Further details of the Proof-of-Legitimacy information are as follows. The Proof-of-Legitimacy information is constructed along the lines in which Proof of Membership terminology is described and used in T. Hardjono and B. Cain, "Key establishment for IGMP authentication in IP multicast", ECUMN, Colmar, France, October 2000, which reference is incorporated herein by reference. However, since such a terminology deals with the receiver access control problem exclusively, the issue is extended here to sender access control by replacing the word "Membership" by "Legitimacy", as the sender does not use group membership functionalities.

Further details of the designated routers, e.g. the first DR 6 and the second DR 10 are as follows. The DR is the last-hop router in the multicast delivery tree, or an elected subnet multicast router. In the case of senders, the DR forwards the sender's multicast traffic to upstream routers. In case of receivers, the DR is an MLD or IGMP router that maintains membership state information (e.g. registered multicast address and sources).

The embodiments may be applied to both IPv4 and IPv6 protocols. In particular, the receiver access control mechanisms are applicable to both IGMP (IPv4) and MLD (IPv6).

In the case of receiver access control, reference is made in the following embodiments to the list of source addresses tied to a single multicast address as a list of couples (Multicast Address, Source Address). Similarly, in case of sender access control, reference is made in the following embodiments to a list of multicast addresses corresponding to the same source as a list of couples (Source Address, Multicast Address).

In the following embodiments, it is assumed that when a given host wishes to attend a multicast session (as a sender or receiver), it first registers with the GM 12 to obtain securely the required keying materials (GK: for receivers, SK: for senders) to build its Proof-of-Legitimacy Information. When the host leaves a multicast group, it notifies the GM (this is a *deregistration Process*). The GM can also exclude a host at any time by triggering the deregistration process for that host. Registration and deregistration processes may include user authentication and authorization by the GM 12, and may be defined in different ways, for example based on processes described in Mark Baugher and al., "The Group Domain of Interpretation", RFC 3547, July 2003, which reference is incorporated herein by reference.

In the following embodiments, a secure (Group or Unicast) Channel may be established between the GM 12 and the DRs 6, 10, for message exchange.

In the following embodiments, when a given source (i.e. host) registers with the GM 12, it may request to join the multicast group as a source, i.e. as a sender host. If the GM 12 accepts this request, the GM 12 sends the source the

appropriate keying material (if any) along with a Sender Key (SK). Such a key serves as a Proof-of-Legitimacy and is used to establish a secure channel between the sender and DR.

A first embodiment, being a receiver access control process, will now be described with reference to FIG. 2, which is a message sequence chart showing messages sent between the receiver host 4, the first DR 6, and the GM 12.

The first phase of the receiver access control process is as follows.

When a given host, in this example the receiver host 4, wishes to join a multicast group address, it sends to the first DR 6, at step 40, a Report message (IGMP or MLD) along with a *Challenge_Group_Request* message. This *Challenge_Group_Request* message contains the following information:

- A *Timestamp* (Tsp): generated by the receiver
- A *Leave* option set to "0".
- The identity of GM (GMid).
- A Challenge Value (CV_h).
- The multicast address (and list of source addresses if any) it wishes to join.
- *Proof-of-Legitimacy Information.* This information represents the result of a hash function (*Value_h*) applied on the concatenation of the following:
  - The corresponding GK-derived value
  - *Subnet-based Identifier* (*Sid*): it identifies user's location. This identifier may represent the IP address of the user, or the *subnet's IP address* in IPv4 (respectively: the combination of the *Global Routing Prefix* with *subnet ID* in IPv6, where the global routing prefix is a (typically hierarchically-structured) value

assigned to a site (a cluster of subnets/links) and the subnet ID is an identifier of a link within the site).

- *Timestamp* (Tsp)
- *Leave* value

The details of the messages being sent at step 40 may be represented as:

Challenge_ Group_Request {Tsp,[Leave],[GMid], H(GK DerivedValue|Sid|Tsp| Leave)=Value_h,[Multicast Group @], [Source @s],CV_h]}

The second phase of the receiver access control process is as follows. When the first DR 6 receives the *Challenge_Group_Request* message, it first performs the following check:

- The Timestamp is invalid (obsolete), *OR*:
- The received *Leave* option is set to "0" *AND* DR has already a registered state for the received *Value_h* value as well as the multicast address (and source(s), if any) mentioned in user's request.

If so, the first DR 6 ignores the message. If the timestamp is valid and the second condition is not satisfied, the first DR 6 may cache the timestamp along with *Value_h* value. Then, at step 42, the first DR 6 may send a *Group_Request* message to the GM 12 using a secure channel. This Group Request message is to request the GK-derived value corresponding to the requested multicast address (and source(s), if any). The details of the *Group_Request* message being sent at step 42 may be represented as:

{Group_Request{Multicast Group @, [Source Address(es)]}}$_{SC}$

Note that the receiver may wish to join multiple groups corresponding to a single multicast address with specific sources, as described for example in S. Bhattacharyya, "An Overview of Source-Specific Multicast (SSM)", Internet RFC 3569, July 2003, i.e. each group may correspond to a couple (Multicast address, Sender address). This implies that the receiver holds as many GKs as there are reported sources for the same multicast address. In this case, the receiver generates the GK-derived value based on the different GK values of the reported sources (e.g. using a hash on the concatenation of the different GKs). In case GM has generated a per-Multicast address GK (i.e. sources are not specified, as described for example in S. Deering, "Host Extension for IP Multicasting", Internet RFC 1112, August 1989, then the receiver will hold a single GK for each reported Multicast address. In this case, the receiver generates the GK-derived value based on a single GK key.

The third phase of the receiver access control process is as follows. When the GM 12 receives the *Group_Request* message, the GM 12 checks whether the received multicast group address (and source address(es) if any) exists within its list of registered Multicast addresses (respectively: couples (Multicast Address, Source Address). If the Multicast group address is not registered, the GM responds the DR with a *Group_ Response* message notifying the failure. If the multicast group is registered but some sources are missing in its registered list, the GM 12 may send either a *Group_Response* message with a *"Valid"* Option mentioning the missing sources and the GK-derived value (calculated based on the existing sources) or the same message with a *"Fail"* option. If the verification succeeds, at step 44, the GM 12 sends a *"Group_Response"* message to the first DR 6. In this case, the

"Group_Response" message will hold a *"Valid"* notification as well as the corresponding GK-derived value. The details of the *"Group_Response"* message being sent at step 44 may be represented as:

{GroupResponse{Valid/Fail, [GK-DerivedValue], [Missing Information}}$_{SC}$

The fourth phase of the receiver access control process is as follows. After the first DR 6 has received the above described Group_Response message, the first DR 6 may send, at step 46, a Challenge_*Group_Response* message to the receiver host 4.

If the received Group_Response message includes a "Failure" notification, the Challenge_Group_Response message being sent holds a "Failure" option (and the missing sources if any). Otherwise, the DR may hashe the result of the concatenation of the following:

- GK-derived value sent by GM,
- The *Subnet-based Identifier (Sid)which is* deduced from the user's IP address),
- The *Leave* value sent by the reporting user
- User's *Timestamp*.

The DR 6 then compares the result with the hash value sent by the user (*Value_h*). If the two values match, the DR 6 accepts the user's request, and triggers a Group Membership Management procedure (e.g. updates the membership state information (and triggers the multicast routing module to

build the routing path in case *Leave*=0)). In addition, at this version of step 46, the DR 6 may send a *Challenge_Group_Response* message holding a *"Valid"* option (as well as the list of missing sources in case the GM 12 mentions them to the DR 6 in the *Group_Response* message with a *Valid* Option) to the receiver host 4. The Group_Response message additionally holds a hash of the concatenation of the current GK-derived value along with the challenge value sent by the receiver host 4. If the match check does not succeeds, then at this version of step 46, the DR 6 sends a *Challenge_Group_Response* message holding a *Fail* option, and the hash result calculated as in the case of the *Challenge_Group_Response* message with a *Valid* option, to the receiver host 4.

Thus the details of the *Group_Request* message being sent at step 46, including the various options as to fail or valid, may be represented as:

[Challenge_Group_Response{Valid/Fail, [H(GK-DerivedValue|CV_h)], [Missing Information]}]

In each of the above details of the messages being sent, i.e. in the representations given above for the details of the messages sent at each of steps 40, 42, 44 and 46, the information contained within [....] may be omitted without altering the basic operation of this particular embodiment, and the notation "SC" represents a secure channel. A secure channel may be any Security Association that ensures message encryption, and sender authentication, e.g. IPsec ESP with a non-null authentication algorithm is one example of a secure channel. A Group Security Assocation (GSA) may also be used to regroup multiple DRs with the GM. In this case the GM may use a key shared with all the DRs to encrypt exchanged messages. The authentication in

this case may be achieved through a multicast source authentication mechanism (e.g. TESLA) or using Digital Signature in case the public key of the signer (e.g. GM) is known by the DRs.

Upon the reception of a *Valid* option, the receiver host 4 may check router validity by verifying whether the hash value contained in the message is correct. This check enables the receiver host to determine that the request has been received by a legitimate DR. Furthermore, whether the match check of *value_h* succeeds or not, the DR 6 removes the corresponding *Value_h* and Timestamp from its cache once the check is completed.

Receiver exclusion is processed as follows. When the GM 12 notices that there are no more receivers for a given multicast group address or source, the GM 12 sends a Group_Respnse message to all the DRs associated with the GM 12. In this case, the Group_Response message may be sent by unicast or multicast. The Group_Response message contains a "Fail" option mentioning the removed multicast group address (and source if any). The GM 12 then obsoletes the corresponding GK key. If a given DR receives this Group_Response message, the DR deletes the states of the affected multicast address or couples (Multicast address, Source Address), and halts forwarding multicast traffic related to the removed state. This prevents old receivers from improperly consuming DR resources.

Recall that aside from the case where the GM deregisters a given receiver without a prior request from that receiver, any receiver can leave a given multicast group (multicast address or a couple (source address, Multicast address)) at will. In this situation, the receiver preferably sends a *Challenge_Group_Request* with a *"Leave"* option set to "1" and holding the same information as when joining the group. In addition, as a deregistration

procedure, the receiver mentions the multicast group it has left to the GM. The GM then updates the corresponding GK key for all the remaining receivers of the affected multicast group. This ensures that old receivers cannot provide valid *Proof-of-legitimacy* information for multicast groups they have left.

In addition, using periodic MLD/IGMP *Queries*, the DR can invalidate the *Proof-of-Legitimacy* of receivers that do not possess the current GK.

The situation of multiple receivers leaving the group is processed as follows. When multiple receivers sharing the same GK key leave the multicast group in a short time period, multiple GK rekeying may be performed by the GM 12. In this case, a receiver that is due to share the same GK may fail to join the group as it may receive successive Challenge_Group_Response messages with a Fail option indicating that the GK-Derived value is incorrect. The GM 12 may overcome this problem by supporting Batch Rekeying, as described in Qu Jin, Ge Jianhua, Jiang Ming, and Zhangzhang, "On batch rekeying based on membership dynamics model of multicast", pp. 145 –147, Proceedings of IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering (TENCON '02), 28-31 Oct. 2002, which reference is incorporated herein by reference. In such a case, the GK update may be spread over multiple leave events. This reduces the receiver's attempts to join the group.

A second embodiment, being a sender access control process, will now be described with reference to FIG. 3, which is a message sequence chart showing messages sent between the sender host 8, the second DR 10, and the GM 12.

When a user, in this example the sender host 8, wishes to join the multicast group as a sender, it is provided with a distinct Sender Key (SK) by the GM 12. This key is rendered obsolete by the GM 12 once the sender leaves all the multicast addresses it registered with the GM 12. Here it is assumed that the GM 12 maintains a list of all the senders (IDs such as: certificates, or shared secret key, etc), each with its corresponding Sender Key (SK), and the SK-derived value.

The first phase of the sender access control process is as follows. When a given host, here the sender host 8, wishes to send its multicast traffic to one or multiple multicast group addresses, it sends, at step 50, a *Challenge_Group_Request* message to the second DR 10. This message contains the following information:

- A *Timestamp* (Tsp): generated by the sender (Optional value)
- A *Leave* value (optional). If this option is used, it is set to "0" by the new sender.
- The identity of GM (GMid).
- The list of multicast addresses it wishes to send traffic to.
- *Proof-of-Legitimacy Information*. This information represents the result of a hash function (*Value_h*) applied on the concatenation of the following:
  - The corresponding SK value
  - *Subnet-based Identifier* (*Sid*): it identifies sender's location (as in case of receiver).
  - *Timestamp* (Tsp) (Optional for senders)
  - *Leave* value (Optional for senders)
- An SK-derived value.
- A Challenge Value (CV_h)

The details of the messages being sent at step 50 may be represented as:

Challenge_Group_Request {[Tsp], [Leave], [GMid],H(SK|Sid|[Tsp]|[Leave])=Value_h, [Multicast Group @(s)], SK-Derived Value, [CV_h]}

The second phase of the sender access control process is as follows. When the DR 10 receives a *Challenge_Group_Request* message from a new sender (not a registered IP source address), in this example the sender host 8, the DR 10 may first perform the following check:

- The Timestamp is invalid (obsolete), *OR*:
- The DR has already a registered state for the received SK-derived value, *OR*
- *Leave* value (if any) is set to "1"

If so, the DR 10 ignores the message, and may respond to the sender with a *Challenge_Group_Request* message holding a *Fail* option. Otherwise, the DR 10 may cache the timestamp (if any) along with *Value_h, and* SK-derived value and may send, at step 52, a *Group_Request* message to the GM 12. This message is sent using a secure channel. The message requests the SK value from the GM 12. This message holds the multicast address(es) as well as the SK-derived value received from the sender host 8. Note that, if the DR 10 receives multicast traffic from a new source, it discards this traffic and may respond to that source with a *Challenge_Group_Response* message holding a *Fail* option, indicating that a *Challenge_Group_Request* message is missing. The

details of the *Group_Request* message being sent at step 52 may be represented as:

{Group Request {Multicast Group @(s), SK-derived Value}}$_{SC}$

The third phase of the sender access control process is as follows. When the GM 12 receives the *Group_Request* message, it checks whether the received multicast group address(es) and the SK-derived value exist within its list of registered SK-derived values. Table 1 shows an example of an SK-related data structure within the GM 12. If one of the Multicast addresses is missing or the SK-derived value is not registered, the GM 12 may respond to the DR with a *Group_Response* message notifying the failure. If however the verification succeeds, then at step 54, the GM 12 sends a *Group_Response* message to the DR 10. The Group response message holds a *Valid* notification along with the SK value corresponding to the received SK-derived value.

SK-derived Value	Corresponding SK key	Multicast @s
D(SK1)	SK1	Mcast @1 Mcast @2 Mcast @3
d(SK2)	SK2	Mcast @1
. . .	. . .	. . .

Table 1

If there are some missing multicast addresses, but the SK-derived value is correct, then the GM sends a different *Group_Response* message to the DR 10

rather than the message with a *Fail* option. This alternative Group Response message holds a *Valid* option and mentions the missing multicast addresses. Thus overall the details of the *Group_Response* message being sent at step 54 may be represented as:

{Group Response{Valid/Fail, [SK], [Missing Information]}}$_{SC}$

The fourth phase of the sender access control process is as follows. If the DR 10 receives a *Group_Response* message with a *Fail* option, it sends a *Challenge_Group_Response* message to the sender host 8. The Challenge_Group_Response message holds a *Fail* option (and mentions the missing Multicast group addresses if any). The DR 10 also removes the information cached on reception of the *Challenge_Group_Request* message. If the DR 10 receives a *Group_Response* message with a *Valid* option, it hashes the result of the concatenation of the following:

- SK value sent by GM,
- User's *Sid*
- Timestamp (if any)
- *Leave* value (if any)

Then, the DR 10 compares the result with the *Value_h* it received from the sender host 8. If the two values match, the DR 10 accepts the sender host (e.g. it creates the corresponding state information), removes the corresponding *Timestamp*, and keeps the related SK-derived value. Table 2 shows an example of SK-related state in the DR 10.

(Sender @, Multicast @)	Corresponding SK-derived	...

CML01661N

	Value	
(S1, Mcast @1)	d(SK1)	
(S1, Mcast @2)	d(SK1)	
(S1, Mcast @3)	d(SK1)	...
.	.	.
.	.	.
.	.	.

Table 2

Then the DR 10 optionally sends, at step 56, a *Challenge_Group_Response* message to the sender host 8. The Challenge_Group_response message holds a *Valid* option (and mentions the missing multicast addresses if any). If the match test fails, the DR 10 sends instead, at step 56, a *Challenge_Group_Response* message with a *Fail* option to the sender host 10, and removes the information cached upon the reception of the *Challenge_Group_Request* message. The *Challenge_Group_Response* message also holds a Hash of the concatenation of the SK value (if any) with the challenge value sent by the host. Thus overall the details of the *Challenge_Group_Response* message sent at step 56 may be represented as:

[Challenge_Group_Response{Valid/Fail, [H(SK|CV_h)], Missing Information]}]

If the sender host 8 receives a *Challenge_Group_Response* message with a *Fail* option, it registers with the GM 12 as a sender before it sends its *Challenge_Group_Request* message. If the sender host receives a *Challenge_Group_Response* message with a *Valid* option, it may check the DR's validity by verifying whether the hash value contained in the message is

correct. This check enables the sender host 8 to determine that its request has been received by a legitimate DR.

In each of the above details of the messages being sent, i.e. in the representations given above for the details of the messages sent at each of steps 50, 52, 54 and 56, the information contained within [....] may be omitted without altering the basic operation of this particular embodiment, and the notation "SC" represents a secure channel. A secure channel may be any Security Association that ensures message encryption, and sender authentication, e.g. IPsec ESP with a non-null authentication algorithm is one example of a secure channel. A Group Security Assocation (GSA) may also be used to regroup multiple DRs with the GM. In this case the GM may use a key shared with all the DRs to encrypt exchanged messages. The authentication in this case may be achieved through a multicast source authentication mechanism (e.g. TESLA) or using Digital Signature in case the public key of the signer (e.g. GM) is known by the DRs.

After the new sender is validated, at step 58, the DR 10 and the sender host 8 establish a secure channel (either for message authentication, or message encryption, or both), based on the shared SK value, and preferably including anti-replay protection. The secure channel may be established either in a peer-to-peer fashion (e.g. IPsec ESP) or using a Group Security Association (GSA) that may regroup the DR 10 and all other registered senders.

For multicast data transmission, the valid sender, i.e. in this example the sender host 8, includes a security header (e.g. an authentication and encryption header: IPsec ESP) in its multicast packet. When the DR 10 intercepts multicast traffic from a given sender, it checks whether it has a registered state for the received multicast address and for that sender. If it is

not the case, it discards the packet and may send a *Group_Challenge_Response* message with a *Fail* option to the sender. Otherwise, the DR 10 may trigger the appropriate security check procedure for sender's packets (e.g. the authentication procedure). If that check succeeds, the DR 10 forwards the packet to upstream tree routers. Elsewhere, the packet may be silently discarded.

One way of adding Multicast addresses will now be described. If a valid sender wishes to transmit multicast traffic for additional multicast addresses, it sends the DR a *Challenge_Group_Request* mentioning only the added multicast addresses, and optionally: a *Leave* value set to"0". In such a case, the sender may use the secure channel to send its request. Then, the DR may perform the sender access control process with the group manager, and if the process succeeds, the DR adds the requested multicast addresses to its state information, and there may be no need to change the secure channel with the sender. Otherwise, the DR may send a *Challenge_Group_Response* message to the sender, with the Challenge_Group_Response message holding a *Fail* option.

One way of cancelling Multicast addresses will now be described. When a valid sender wishes to halt data transmission for some multicast addresses, it sends a *Challenge_Group_Request* to the DR. the message is sent over the secure channel. The message mentions the multicast addresses that have been left, and a *Leave* value set to "1". The DR then removes the affected multicast addresses of the corresponding SK-derived value from the corresponding state information. If there are no more multicast addresses for the corresponding SK-derived value, the DR cancels the secure channel with the affected sender, removes the corresponding entry from the sate

information, and sends to this sender a *Challenge_Group_Response* message with a *Fail* option to indicate that the secure channel between them has been cancelled.

One way of excluding a sender will now be described. When a sender terminates data transmission for some multicast addresses, it notifies the GM. The GM can also exclude a sender from particular multicast groups (Multicast group addresses) according to one or more predetermined or operator controlled reasons (e.g. Group Policy rules). In both cases, the GM removes the affected Multicast group address(s) from the list of Multicast group address(s) registered for the leaving sender. If there are no more registered Multicast group addresses for the leaving sender, the GM invalidates the corresponding SK key.

If some multicast addresses remain registered for a given SK-derived value, the GM sends a *Group_Response* message to all the multicast routers it has a SA with. The message may be sent by unicast or multicast. The message holds a *Valid* option mentioning the removed multicast group address(s) (as missing multicast addresses) and their corresponding SK-derived value. If the GM needs to obsolete a given SK-derived value, it may send (either in a unicast or multicast fashion) a *Group_Response* message with a *Fail* option mentioning the invalidated SK-derived value to all the multicast routers it has a SA with.

If a given DR receives the above *Group_Response* message with a *Valid* option and has a registered SK-derived value affected by that message, it deletes the state information of the affected couples (Source Address, Multicast address), where the source address is the one that corresponds to the affected SK-derived value, and the multicast address is listed in the

received *Group_Response* message. Then, if some multicast addresses are still registered for the affected SK-derived value, the DR may transmit a *Challenge_Group_Response* message to the sender. The message has a *Valid* option indicating the excluded multicast addresses (as missing multicast addresses). If the DR either notices that there are no more registered multicast addresses for the corresponding sender (i.e. no more couples (Source address, Multicast address)), or it receives a *Group_Response* with a *Fail* option mentioning that a SK-derived value it holds is obsolete, it cancels the secure channel (e.g. SA) with the affected sender and sends to this sender a *Challenge_Group_Response* message with a *Fail* option to indicate that the secure channel between them has been cancelled (i.e. Invalid SK-derived value).

All these options prevent old senders from improperly transmitting traffic to multicast addresses they have left.

In other embodiments, a further option that may be added is to provide further ways for the system to function; for example so that the GM securely and occasionally sends (e.g. on session setup) to the multicast routers (e.g. the DRs) a list of authorized groups (e.g. a list of couples (optional source address, multicast address)), and/or a list of SK keys, and/or a list of GK-derived values that the GM manages. This allows the DR for e.g. to immediately invalidate (e.g. remove, ignore, etc.) user requests (*Challenge_Group_Request*) holding fake information (e.g. group addresses, SK keys, etc). In this situation, the DR may not need to send a *Group_Request* message to the GM.

Further aspects, options and analysis relevant to both the above embodiments, and more generally to other embodiments of either receiver or sender access control, will now be discussed.

The risk of denial of service attacks is reduced since fake *Challenge_Group_Request* messages are quickly identifiable. Also, the access control mechanisms being based on large-scope authorization information-Proof-of-Legitimacy- (scope of the information = scope of the multicast group), render the processes particularly suitable for the mobile environment. In particular, the above embodiments avoid the use of digital signature-based and pre-shared secret (user-DR)-based techniques, which tend not to be suitable for the mobile environment where fast handover is desirable.

An example of a common Group Key defined in the Multicast security literature that behaves in apart like the Group Key used in the above embodiments is the *Traffic Encryption Key* (TEK). This key is used by the sender to encrypt data traffic and by receivers to decrypt sender's data. The TEK key could be updated each time a multicast user (sender or receiver) joins or leaves the group to ensure respectively *backward* and *forward secrecies*. When such a key is already used for data encryption, it may further be utilized as the Group Key of the above described access control embodiments, with attendant cost efficiency arising from sharing of resource or overhead.

Some ways of providing anti-replay protection are as follows. In the case of receiver access control, replay attacks may be easily identified and prevented since the DR ignores the replayed *Challenge_Group_Request* messages holding Value_h values already cashed by the DR and destined to registered multicast addresses (and sources).

The following scenarios may be envisaged in the case of sender access control. Case 1: The valid source has a registered SK-derived value at the DR - replay attacks related to an unmodified copy of a Challenge_Group_Request message are detected by the DR. This is done either by using the secure

channel with the valid sender or by the DR noticing that it has already registered state information for the corresponding SK-derived value (if the secure channel has not been established yet). Case 2: The validity of the secure channel between the valid source and DR expires - if the secure channel with a valid sender has been cancelled (e.g. the valid sender moves to a new subnet), the DR overcomes the replay attacks related to old sender's *Challenge_Group_Request* message by identifying either obsolete timestamps or a non-matching *Value_h* (i.e. an illegitimately modified timestamp). If the timestamp is not used, the DR may trigger the establishment process of the secure channel with the attacker. However, such a process will fail since the attacker does not know the SK corresponding to the SK-derived key of the *Challenge_Group_Request* message intercepted by the attacker.

Another point in general is in relation to a possibility for the DR to transmit challenge values. If such a challenge value is sent by the DR in specific messages such as Router Advertisement, MLD/IGMP Queries, etc, the host can use such a value to build the hosts Value_h.

In the above embodiments the GM 12 is a centralized GM. However, in other embodiments, the GM may be a distributed GM. FIG. 4 is a schematic illustration of a network arrangement 21 coupled to the Internet 2 to which embodiments of the present invention may be applied in the case of a distributed GM. The same elements as were present in the network arrangement 1 of FIG. 1 are included again and indicated by the same reference numbers as in FIG. 1. However, network arrangement 21 further comprises a first local GM 20, which together with the receiver host 4, the first DR 6 and the first link 14 is located in a first domain 22; and a second local GM 24, which together with the sender host 8, the second DR 10 and the

second link 16 is located in a second domain 26. The first local GM 20 is coupled to the GM 12 via a first inter-GM signalling link 28. The second local GM 24 is coupled to the GM 12 via a second inter-GM signalling link 30.

Examples and/or further details of the content of the different messages used in the above described processes will now be given in Tables 3 to 6. Other information may be added in addition to that shown below. For example, fields may be added to enable the DR to distinguish between sender and receiver messages.

Table 3 below shows a message content for a Challenge_Group_Request:

Field	Description	Source	Receiver
Timestamp (Tsp)	Up to date time value.	Optional	Mandatory
Leave:	0: Request to join multicast group(s) / transmit data to multicast address(es) 1: Request to leave multicast group(s) / halt data transmission to multicast address(es)	Optional	Optional
GMid:	A unique GM identifier such as its IP address (IPv4 or IPv6).	Optional	Optional
Value_h:	It represents the hash of (GK-derivedValue| Sid| Tsp| Leave) in case of a receiver, or (SK| Sid) in case of a sender.	Mandatory	Mandatory
Multicast Address(es):	Single IP Multicast address (IPv4 or IPv6) of the group the receiver wishes to join or a list of IP Multicast addresses (IPv4 or IPv6) to which the sender wishes to send its traffic.	Optional	Optional
Source Address(es):	It represents a list of IP source addresses (IPv4 or IPv6) from which the receiver wishes to receive multicast traffic.	Not used	Optional
SK-derived value	It represents the SK-derived value of the sender.	Mandatory	Not used
CV_h	Challenge value sent by the user in case it needs to verify that its	Optional	Optional

	Challenge_Group_Request message was received by a multicast router that has a Secure Channel with GM.		
Destination Address	Case of receiver: All (subnet)_MLDv2_Routers (case of IPv6), or All Subnet_IGMPv3_Routers (case of IPv4), or the reported multicast address in case of former versions of MLD (i.e.v1) and IGMP (i.e. v1 and v2) Case of sender: All_Link_scope_Multicast_Routers multicast address in case of senders (IPv4 or IPv6).	Optional	Optional

Table 3

The use of "Multicast Address", "Source Address(es)", and "Destination Address" fields are optional. For example, there is no need for these options if other protocols that already hold this information (such as MLD/IGMP in the case of receivers) are being used between the users and the multicast routers. In such a case, the Report contains the required information and there is no need to add it in the *Challenge_Group_Request* message.

Table 4 below shows a message format for a Challenge_Group_Response:

Field	Description	Sender	Receiver
Valid/Fail:	0: Valid 1: Invalid GK-derived Value 2: Invalid SK-derived value 3: Group Manager Unknown 4: Invalid Value_h 5: Challenge_Group_Request	Mandatory	Mandatory

	missing 6: Multicast Group address missing (case of sender)		
Hash Result	The result of a hash applied on (GK-derived Value/SK |CV_h)	Optional	Optional
Missing Information	The list of missing multicast addresses (and source addresses if any) (case of receiver) or List of missing Multicast group addresses (case of sender).	Optional	Optional
Destination Address:	IP Multicast (All-System) address or IP unicast (user) Address (IPv4 or IPv6)	Mandatory	Mandatory

Table 4

Table 5 below shows a message format for a Group Request:

Field	Description	Sender	Receiver
Sender Id:	It represents the SK-derived value	Mandatory	Not used
Multicast Address:	It represents the Multicast address the receiver wishes to join, or the multicast address to which the sender wishes to send its traffic (IPv4 or IPv6)	Mandatory	Mandatory
Source Address(es): (Optional)	Reserved for receivers. It represents the list of IP source addresses (IPv4 or IPv6) from which the receiver wishes to receive the multicast traffic from.	Not used	Optional
Destination Address:	GM's IP address (IPv4 or IPv6)	Mandatory	Mandatory

CML01661N

Table 5

Table 6 below shows a message format for a Group response:

Field	Description	Sender	Receiver
Valid/Fail:	0: Valid 1: SK value Invalidated 2: Missing Multicast Address (s) 3: Invalid SK-derived Value 4: Missing sources	Mandatory	Mandatory
Authorization Information	GK-derived Value (receiver) or SK Value (sender), list of missing sources, or list of missing multicast addresses	Optional	Optional
Missing Information	List of missing sources, or list of missing multicast addresses	Optional	Optional
Destination Address	Either a specific Multicast address (all multicast routers having an SA with GM) or multicast router's IP Address (IPv4 or IPv6)	Mandatory	Mandatory

Table 6

It will be appreciated that the present invention can provide useful implementations of user exclusion. For example, in the above embodiments, each time the receiver joins a multicast group it needs to provide the Designated Router (DR) with a valid *Proof-of-Legitimacy* information. Similarly, each time a sender wishes to sends its traffic to a new multicast group, it needs to provide valid *Proof-of-Legitimacy* information to the Designated Router. The Proof-of-Legitimacy may be any security information

that enables the multicast router to process user access control. Besides, when a user (sender or receiver) leaves the multicast group, the group manager obsoletes (e.g. deletes) the Proof-of-Legitimacy information for that user so that the user cannot re-join the group without a new Proof-of-Legitimacy.

It will also be appreciated that the present invention provides efficient and secure sender and receiver access control mechanisms for, e.g. IP Mobile Multicast communications. The access control in the multicast edge router of the delivery tree is achieved through authorization procedures that may be based on hash functions. Such functions can avoid or reduce the use of process-heavy digital signatures, can reduce the risk of denial of service attacks, and is suitable for mobile environments.

The above described embodiments may be implemented by configuring or adapting any suitable apparatus, for example conventional mobile hosts (nodes) such as mobile telephones and portable computers, and, where required, conventional equipment and software providing conventional edge routers and group managers. Alternatively, or in addition, the processes described may be implemented by processor-implementable instructions implemented by a processor and/or stored on a suitable storage medium, such as computer memory, hard disk, floppy disk, ROM, PROM etc.

The above described embodiments relate to specific network arrangements in which the present invention may be applied. However, it will be appreciated that the present invention may be applied to other network arrangements, provided some form of edge router is available for to carry out authentication processes.

Also, in the above embodiments many optional process steps are included that improve the efficiency of the processes described. However, it will be appreciated that in other embodiments such steps may be omitted, or

modified, or replaced by other steps. Accordingly, particular steps in the embodiments, singly or in combination, should not be considered as essential to any or all aspects of the present invention.

5

CML01661N

CLAIMS

1. An access control method for controlling access to a multicast delivery tree, the method comprising:

performing, at a designated router, authorization procedures for access to the delivery tree, the designated router being a multicast edge router of the multicast delivery tree.

2. A method according to claim 1, wherein the designated router performs the authorization procedures by comparing authorization information received from a user with information received from a group manager.

3. A method according to claim 1 or 2, wherein the access control method is a sender access control method, and the authorization information is based on a sender key provided by the group manager to legitimate senders.

4. A method according to claim 1 or 2, wherein the access control method is a receiver access control method, and the authorization information is based on a group key provided by the group manager to a group of users.

5. A method according to claim 3 or claim 4, comprising use of a derived value of the key obtained by applying a derivation function to the key.

6. A method according to claim 5, wherein the derivation function is a one-way hash function applied to the value of the key.

7. A method according to claim 5 or claim 6, wherein the derivation function is specified to the user by the group manager.

8. A method according to claim 4, 5 or 6, wherein the group manager updates the group key when a user leaves the multicast group served by the delivery tree.

9. A method according to claim 4, 5 or 6, wherein the group manager obsoletes the group key when all the users in the multicast group leave the multicast group served by the delivery tree.

10. A method according to any of claims 1 to 9, wherein the group manager sends a list of authorized multicast groups to the designated routers.

11. A method according to any of claims 3 or 5 to 9, wherein the group manager sends a list of sender keys to the designated routers.

12. A method according to any of claims 3 or 5 to 9, wherein the group manager sends a list of derived group keys to the designated routers.

13. A method according to any of claims 3 to 12, wherein the sender key is used to establish a secure channel between the sender and the designated router.

14. A method according to any of claims 1 to 13, wherein the delivery tree is provided by an IPv4 or an IPv6 network.

15. A storage medium storing processor-implementable instructions for controlling a processor to carry out the method of any of claims 1 to 14.

16. A multicast group manager for a packet data network; the multicast group manger being arranged to provide authorization information to users and designated routers for implementing the method of any of claims 1 to 14.

17. A multicast edge router of a multicast delivery tree in a packet data network; the router being arranged to perform authorization procedures to access the delivery tree according to the method of any of claims 1 to 14.

18. A host for participating in multicast in a packet data network; the host being arranged to provide authorization information according to the method of any of claims 1 to 14.

19. A host according to claim 18, wherein the host is adapted to build the authorization information according to its current network location

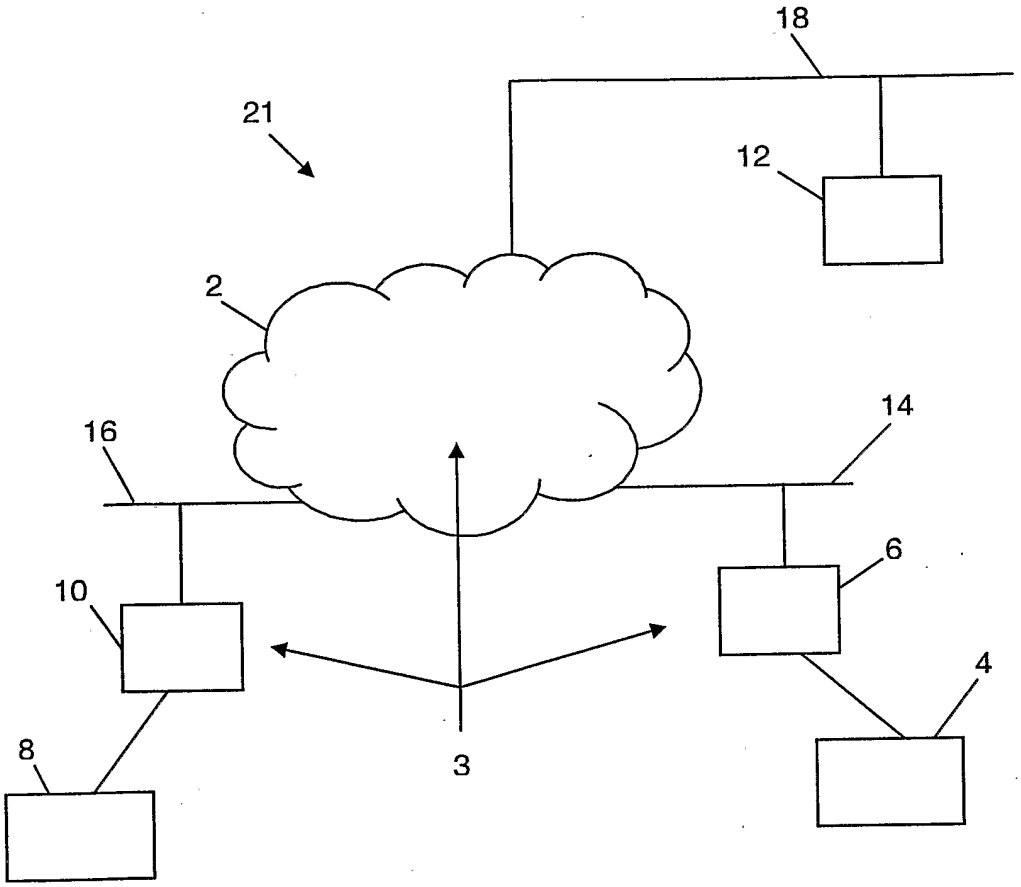


FIG. 1

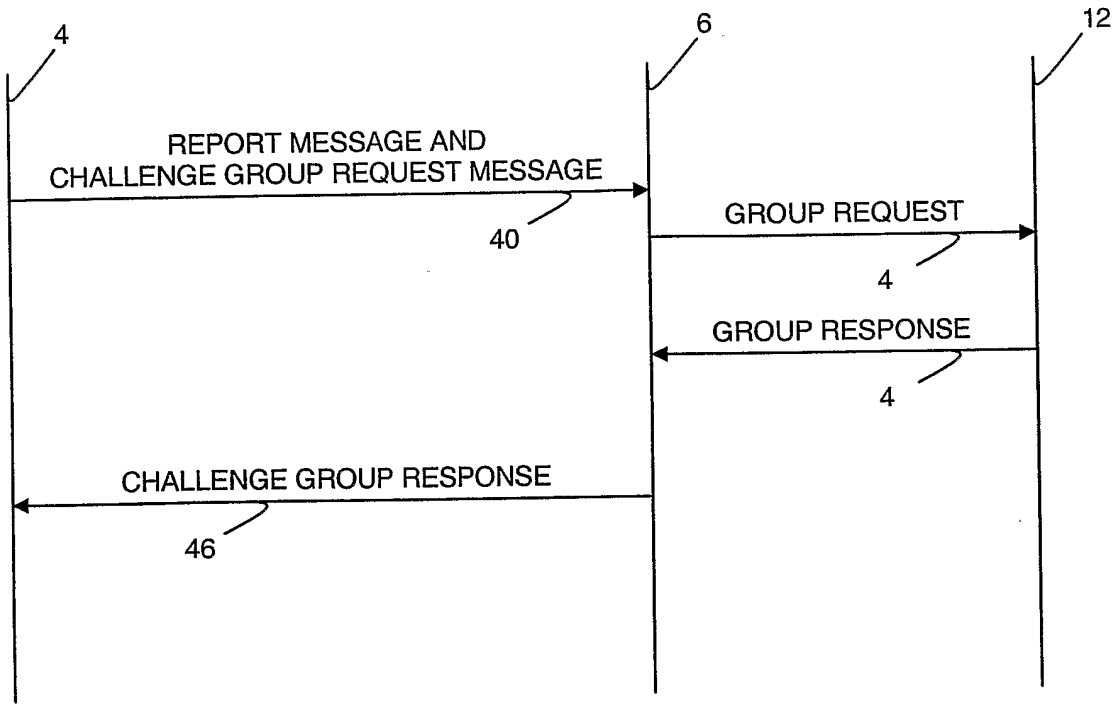

4
6
12
REPORT MESSAGE AND
CHALLENGE GROUP REQUEST MESSAGE
40
GROUP REQUEST
4
GROUP RESPONSE
4
CHALLENGE GROUP RESPONSE
46

FIG. 2

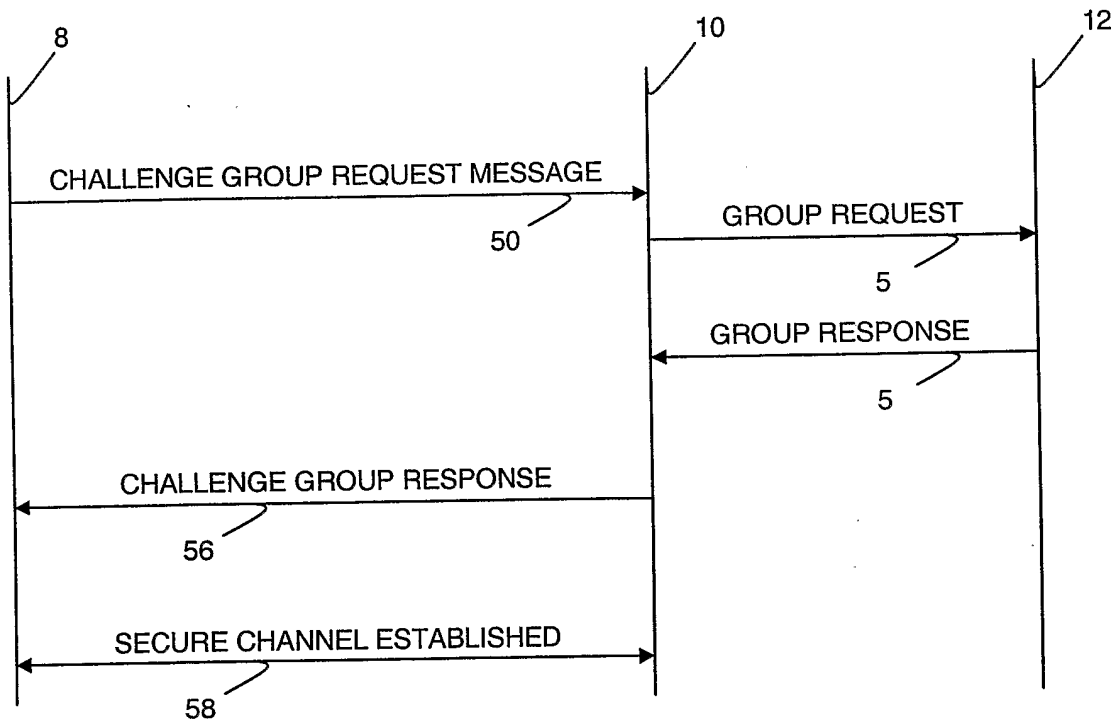

8
10
12
CHALLENGE GROUP REQUEST MESSAGE
50
GROUP REQUEST
5
GROUP RESPONSE
5
CHALLENGE GROUP RESPONSE
56
SECURE CHANNEL ESTABLISHED
58

FIG. 3

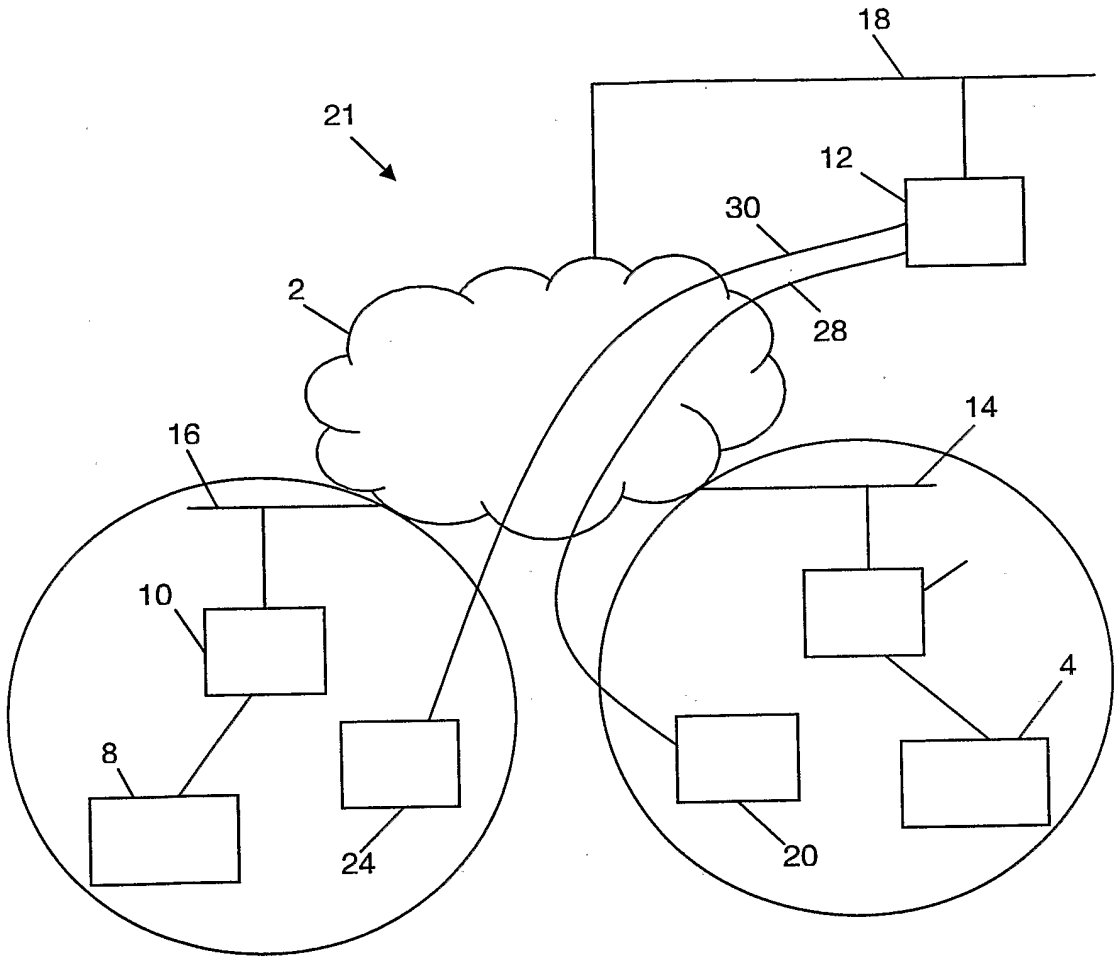


FIG. 4