MSCIT Dissertation

Scalable Secure Multicast Using Extended IGMP

Prepared By : Desmond Chiu

Academic Supervisor : Rocky Chang

Contents

Appendix

Abstract

As multicast applications are deployed for mainstream use, there is a high demand on the security functions to be provided by the underlying multicast framework. Hence, security enhancement of IP multicast is required for multicast communication. This dissertation describes a scalable secure multicast framework to address the scalability problem occurred in the multicast scenario by extending the current Internet Group Management Protocol (IGMP) v3. The extended IGMP will provide security functions such as authentication and authorisation of the multicast senders and receivers, support encryption of the IP multicast datagram, in order to prevent unauthorised access.

Acknowledgement

I must take this opportunity to express my special thanks to my academic supervisor Dr. Rocky K.C.Chang for his guidance and valuable advice during the preparation of the dissertation. Besides, I must give my sincere thanks to my wife, who has been in full support during my study of the master course.

Chapter 1. Introduction

There is an indication that the use of multicast on wide-area communication is on demand and nowadays many applications may be developed to take advantage of the multicast, such as multimedia conference, videocasting, etc. The use of multicast can save the network bandwidth by broadcasting the datagram only once and allowing the members of the multicast group to access the data. At present, any host can join a specific multicast group by sending the required membership report to its nearest designated multicast router and then receive all the multicast datagrams sent to the group. There is no authentication nor authorisation of the group members. Any attackers can capture the multicast data and access the data easily, as there is no encryption of the data throughout the transmission path. As multicast application is becoming popular, security issue for multicasting becomes very important.

To address the multicast security problem, we should distinguish several differences between the secure unicast and secure multicast. First, secure unicast involves only two communicating parties while a group of dynamic members are taking part in the secure multicast group communication. Second, when protocol level is considered, the messages are directed to a known address for unicast while the messages can only be directed to some virtual multicast group address for multicast. Third, the most important of all, the nature of security association between communicating parties are different for the two cases. Under secure unicast, in order for two parties to communicate securely through an insecure network, they have to set up a security association between them. The security association may be a set of keying materials shared only by the two communicating parties. There is no need to update the security association and it may be static during the communication session between the two parties. However, for the case of multicast, instead of a pair of two parties, any parties may form a group and share the security association among the communicating parties. Since non-members of the group may join or members of the group may leave, the security association must be dynamic to cater for the change in the group membership. Hence, the multicast security protocol must ensure that a party is only allowed to participate in the group communication during those periods when it is authorised to do so. In view of these, it results in the need of an effective group access control protocol to be implemented to constrain a group's accessibility.

1.1 Literature summary on multicast security

The security issue in multicast has attracted much research works over the past few years, in order to make multicasting a secure platform for various application. The active research topics [11] may include the building up of a secure multicast architecture, group key management scheme, authentication algorithm and multicast transit traffic control.

The multicast architecture put emphasis on the research of required entities in the secure multicast environment and the way how a distribution tree can be formed so that multicast packets can flow along the tree to reach every authorized group members in a secure way. For instances, Iolus framework as proposed by Suvo Mittra [1], try to construct a multicast framework to handle the secure groups by using geographically distributed entities. It proposes a high-level infrastructure for secure multicast, and addresses the problems of key updates and reliable data transmission by partitioning a multicast group into a hierarchy of subgroups, each with relatively few members. Another example is the Nortel framework [12], which introduces two planes corresponding to the network entities and functions important to multicasting and to security. The key management plane consists of two hierarchy-levels in the form of a single 'trunk region' and one or more 'leaf region' for interconnections. These are papers focusing on the framework for secure multicasting.

As mentioned in the previous paragraph, secure multicast group communication requires an effective group access control protocol so that only authorised group members can use the correct key in decrypting the received multicast data. Hence, group key management scheme, which help to maintain the group access scheme for the multicast infrastructure, is quite an hot issue and important component of the secure multicast. So far many group key management schemes have been proposed, such as the Naïve key management scheme [11], which make use of a centralized group controller to share a secret key with each of the group members. Also well known is the Hierarchical Tree-Based management scheme [13], which use a logical hierarchy of key-encrypting keys and reliable multicast for group key management, such that it incurs messages and computational cost logarithmic to the size of the group. Another is the Group Key Management Protocol (GKMP) [14], which provides the ability to create and distribute keys within arbitrary-sized groups without the intervention of a global/centralized key controller, etc.

Another area of research topic is the authentication algorithm. This topic covers how the registered group members (both sender and receivers) can be identified by the multicast group controller, as well as the packet source level identification which is the process to identify the sender of a received packet. There are so many proposed packet source authentication schemes, examples may include the Naïve Authentication scheme and the Multiple MAC scheme [13]. The Naïve scheme is the most intuitive solution which makes use of the private key digital signature on each data packets, while the Multiple MAC scheme will make use of several secret keys for the operations. For the group member identification, there are proposals to extend the IGMP to have a secure version to support the end system authentication. For example, IGMP v2 [6] is to be modified for adding user authentication of senders and receivers, in which they are required to be authenticated before successfully joining the group, based entirely on the user account used to join the multicast group. Moreover, new messages are proposed to be added to IGMP so that it can authenticate the end system by interacting with those authentication servers.

To monitor the multicast group communication, the control on the multicast transit traffic is also a hot topic of research [2]. In an open network such as Internet, unauthorised sender can send multicast data

towards a restricted group in a misbehave manner. Although these unauthorised data will not eventually be perceived by those receivers if proper multicast authentication and authorisation are in place, it would put a burden on the multicast traffic and cause degradation on the transmission capacity of the multicast infrastructure. In order to prevent such unauthorised data from flooding the network, research has been done to detect the authorisation of multicast packets by using authorisation stamps included in every multicast data packets for checking purpose. If abnormal packets are detected, alerts packets will be generated and routers will be informed to block such unauthorised packets from spreading.

1.2 Scalability problem

With reference to a multicast communication system, the scalability can be measured by a number of parameters, but among those the most significant will be the total number of group members being affected and the total number of key update messages required to maintain the security during member join or leave scenario. Hence, within the scope of this work, the scalability of the system will be referred to these two metrics and a system is considered to be more scalable if it will have either smaller total number of group members being affected or total number of key update message required during a member join or leave scenario. The term "scalability problem" refer to the case where the specific action of one member will affect all the members of the entire multicast group and the multicast communication protocol cannot deal with the entire group as a whole.

With the scalability as mentioned above, a scalable multicast communication system should require an efficient and effective multicast key distribution mechanism. However, the essential problem of multicast key distribution is the scalability problem when distributing the group key or member-specific key during the multicast session. For a specific multicast group, the number of members N joining the group may be very large, the following two scenarios will help us to realize the mentioned problem :

(1) ***Key Exchange on a member join***

A multicast group security control mechanism must ensure that a member is only allowed to participate and receive the multicast data after it has joined the group. Suppose the group already has N members with existing group key Kgrp, if an additional member joins the group, in order to prevent the joining member from having the chance to access the previously multicasted data, a new group key K'grp has to be generated to the joining member and distributed to the existing members. In other words, all the members N will be required to process a key change when a new member joins.

(2) ***Key Exchange on a member leave***

The group security control mechanism must ensure that a member is not allowed to access the multicast data after it has left the group either voluntarily or forced by the system policy. As in the case of member join, a new group key K'grp has to be generated, and must be distributed to the

remaining N-1 members securely. This means that the new group key K'grp must be encrypted by some secret key which is only shared among the N-1 members but not the leaving member. However, there is no an efficient way to distribute the new group key as the only secret is the previous group key Kgrp which is shared among the N members. In order to distribute the new group key K'grp to the remaining N-1 members, those individual member-specific keying material associated with each of the member must be utilized to distribute the key securely. This is very inefficient as each of the N-1 members must be considered individually if there are totally N members when a member leave the group, especially when the group is large or has a highly dynamic membership.

These are the inherent problems on the multicast group communication, which must be handled by the underlying key management scheme or the communication architecture. In this paper, a new architecture, which is proposed to overcome these problems, can handle the multicast communication scenario more efficiently and effectively.

1.3 Summary of work

To support the authentication of multicast senders and receivers, and the integrity of multicast data packets, as well as to address the scalability problem mentioned earlier, this paper propose to extend the Internet Group Management Protocol (IGMP) v3 [5] by adding more new messages so that it can communicate with some external entities. In this paper, an extended IGMP communication architecture is defined, along with the necessary shared key materials for the new architecture. As far as authentication is concerned, it adopts the "RADIUS Extension for Multicast Router Authentication" protocol as the communication protocol, although with some minor modifications. The extended IGMP would function as a communication layer between the multicast hosts and other multicast entities, and is designed not to tie to a particular multicast framework or any group key management scheme, but to support them as much as possible. For measurement and comparison purpose, the work is based on the paper "A Framework for Scalable Secure Multicasting" by Suvo Mittra, in which a secure scalable framework architecture for multicasting is proposed. For the performance evaluation, some essential metrics are outlined as a measure to see how scalable the new extended IGMP architecture is.

1.4 Overview of chapters

Chapter 2 begins with an overview on the Iolus framework by Suvo Mittra, and those additional entities to be added for the extended IGMP architecture. This will also explain how authentication and key distribution can be supported, through the IGMP extension.

Chapter 3 will outline the new messages and explain in details the operation of the extended protocol, with the help of the IGMP state diagrams. The protocol scalability will be addressed and see how the extended protocol can be made compatible to the earlier versions.

Chapter 4 will focus on the performance issue of the extended protocol. It will be analysed in terms of the security issue and the scalability issues. The performance result will be based on some of the essential metrics and is to be compared among single domain multicasting, Iolus framework and Iolus framework with the extended IGMP architecture.

Chapter 5 will make a conclusion to the work and propose some future work that can be done to extend the capability of the Extended IGMP.

Chapter 2. Framework Architecture

2.1 Framework overview

In order to explain the concept of the proposed Extended IGMP architecture and compare the performance against the existing multicast framework, the Iolus framework as proposed by Suvo Mittra [1] is chosen as the reference for the description of the Extended IGMP architecture. The secure Iolus framework architecture is shown in Fig.1, in which the whole internetwork is divided into different virtual domains. The distribution of domains is supposed to follow the geographical distribution of the internetwork such that a specific domain will serve the internetwork nodes belonging to a certain geographical area. A virtual domain defines only a group of members taking part in multicasting activities, it is not representing any physical boundaries as identified in the internetwork. Actually, the secure framework can be applied to any size of network, and there is no restriction on the area to be covered by a virtual domain.

For each virtual domain it will be associated with a Group Security Agent (GSA for short), as indicated by the circles in Fig.1, which is to maintain the security of the multicast data. There is a root Group Security Agent (called the root GSA), which is the top level security agent containing the up-to-date security information for every multicast group. Other GSAs will exchange information with the root GSA in order to refresh their security information.

To create a single multicast group communication channel, the GSA also serves to connect different virtual domains with each other by forwarding multicast data. There will be a multicast routing protocol running on each GSA so that a distribution tree can be created among the GSA, as indicated by the thick black line linking up the GSAs. The distribution tree will determine the routing path of the multicast data. However, since the security framework is designed to be independent of the underlying multicast routing protocol, the choice of routing protocol will not be a concern as long as there exists a routing path between different GSAs for the virtual domains in which multicast data need to be delivered.

In fact, there will be no global encryption key for the whole multicast group. Scalability of the framework is achieved by having each virtual domain to be relatively independent of each other, as each virtual domain has its own security agent, message encryption key and even different multicast routing protocol for each domain. That means, members joining or leaving a specific multicast group will be effectively joining or leaving the nearest virtual domain, without any effects to members in the other virtual domains already joined the multicast group, thus it helps to localize the disturbance caused by the specific action of the group members.

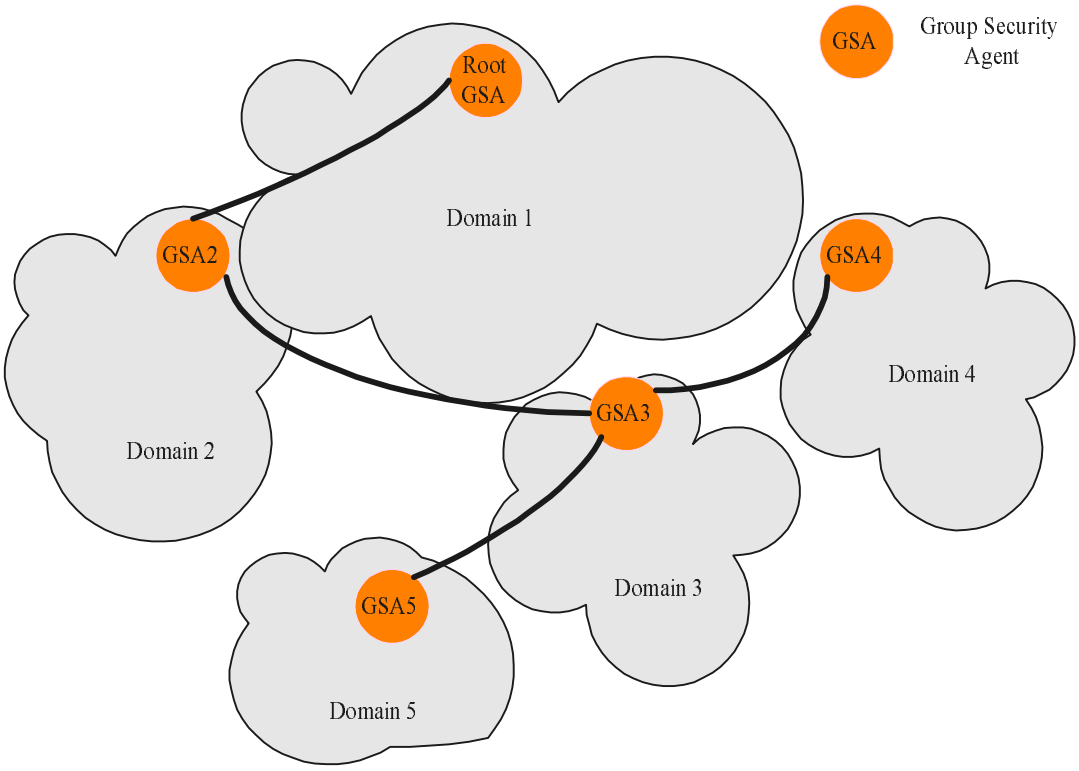


Fig. 1 Iolus Framework Architecture

With the deployment of the Extended IGMP Architecture, there will be some minor changes within the virtual domain. As shown in Fig. 2, two more entities which are the Authentication Server (AS for short) and the Multicast router will be taking part in the secure multicast group communications.

Inside each virtual domain there will be one or more AS local to the domain, which is to authenticate the multicast host on user basis. The rectangular box will be those multicast routers inside the virtual domain and may have direct communication with the Group Security Agent. Their relative positions are shown in Fig. 2 respectively. Different organisation can have their own AS, provided that they are configured with the multicast router in place. The existence of AS is to allow individual organisation to have administration and security control over the usage of multicast group communication. The GSA and the ASs will be queried by the multicast router separately for authentication of the joining and leaving process. For a multicast host to gain access to the multicast group, the host must be successfully authenticated by both the GSA and a AS within the virtual domain. The detailed mechanism will be explained Chapter 3.

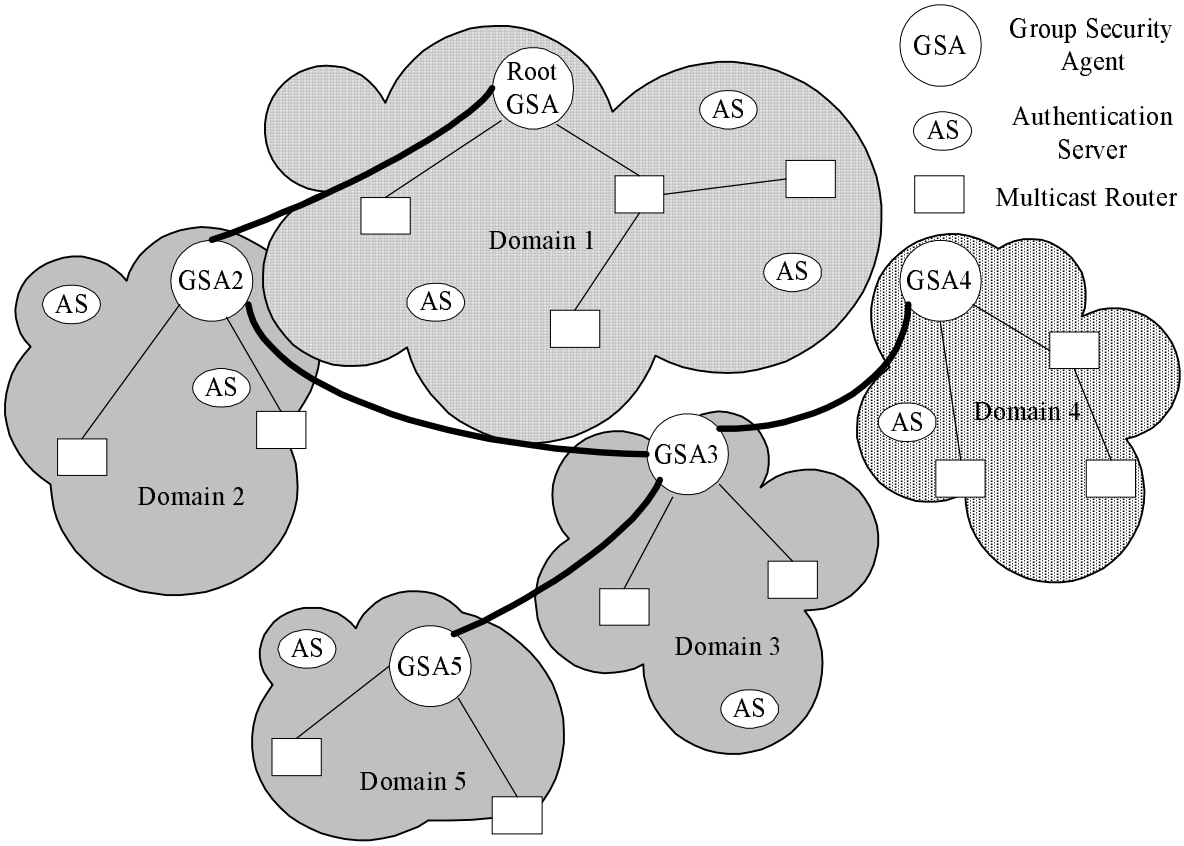


Fig. 2 Iolus Framework with Extended IGMP Architecture

Hence, the function of the Group Security Agent includes the following:

(1) Authentication of the Multicast Host and Multicast Router

For a multicast host to join a specific multicast group, the host must first be authenticated by the group security agent and obtain a valid certificate in order to be granted the access to join the group. For multicast router to join the multicast group successfully, it must be authenticated by some kinds of secret key.

(2) Forwarding the Multicast Data

When a multicast sender in a virtual domain send the encrypted data to the multicast group, only the local members of the virtual domain can receive those encrypted data and decrypted using the subgroup key for the virtual domain. In order to let the other virtual domain to receive the multicast data, the GSA must have to forward the multicast data to other virtual domain following the routing tree.

(3) Generation and Distribution of Encryption Key

Whenever a multicast host successfully join or leave the virtual domain, a new subgroup key for the virtual domain must be generated by the GSA and to be distributed to the members.

The function of the Authentication Server includes the following :

(1) Authentication of user and Multicast Router

For a multicast host to join a specific multicast group, the user used to join the group must be authenticated by an authentication server which is managed by a local organisation.

(2) Logging of the user account transaction

The Authentication Server can be used to track the user account transaction history so that it can be audited later. Since the focus of this paper will be on the security issue, the logging function will be skipped here.

For each successfully created multicast group by the GSA, there will be an associated Multicast GSA Certificate to store the property of the group. It includes the initiator of the multicast group, group address, the encryption algorithm adopted ,etc… Whenever the certificate is created by any one of the GSAs, it will be immediately transmitted to the root GSA, and then distributed to other GSA for replication. Hence, a multicast host can request to join and to be authenticated by the GSA within its own virtual domain.

In the proposed Extended IGMP architecture, to facilitate the communication among the GSA, multicast hosts and multicast routers, a multicast group address called the All-GSA-Address is reserved for all the GSA under the multicast architecture. All the GSA will subscribe to the group whenever they start up. In case that a multicast host wants to communicate with the GSA under its virtual domain, it just sends to the All-GSA-Address.

As shown in Fig. 3 is a detailed view for a typical virtual domain showing the GSA, Designated multicast router, the Multicast host and the Local authentication server. The multicast router directly attached to the subnet of the multicast host is referred as the Designated Multicast Router, since all the requests originated by the host are to be processed by this router. As mentioned before, there may be more than one authentication server AS inside a virtual domain, but only a AS is shown in the diagram for illustration purpose. Any multicast router should be configured with a AS, so that user basis authentication can be processed.

Shown also in the Fig.3 are two multicast hosts, host A is executing the multicast group joining mechanism while host B is executing the multicast group leaving mechanism. The numbers in the diagram show the relative sequence of occurrence of the new messages for each join or leave mechanism. The meaning of each new messages, which is defined in the extended IGMP v3, will be elaborated and described in more details later.

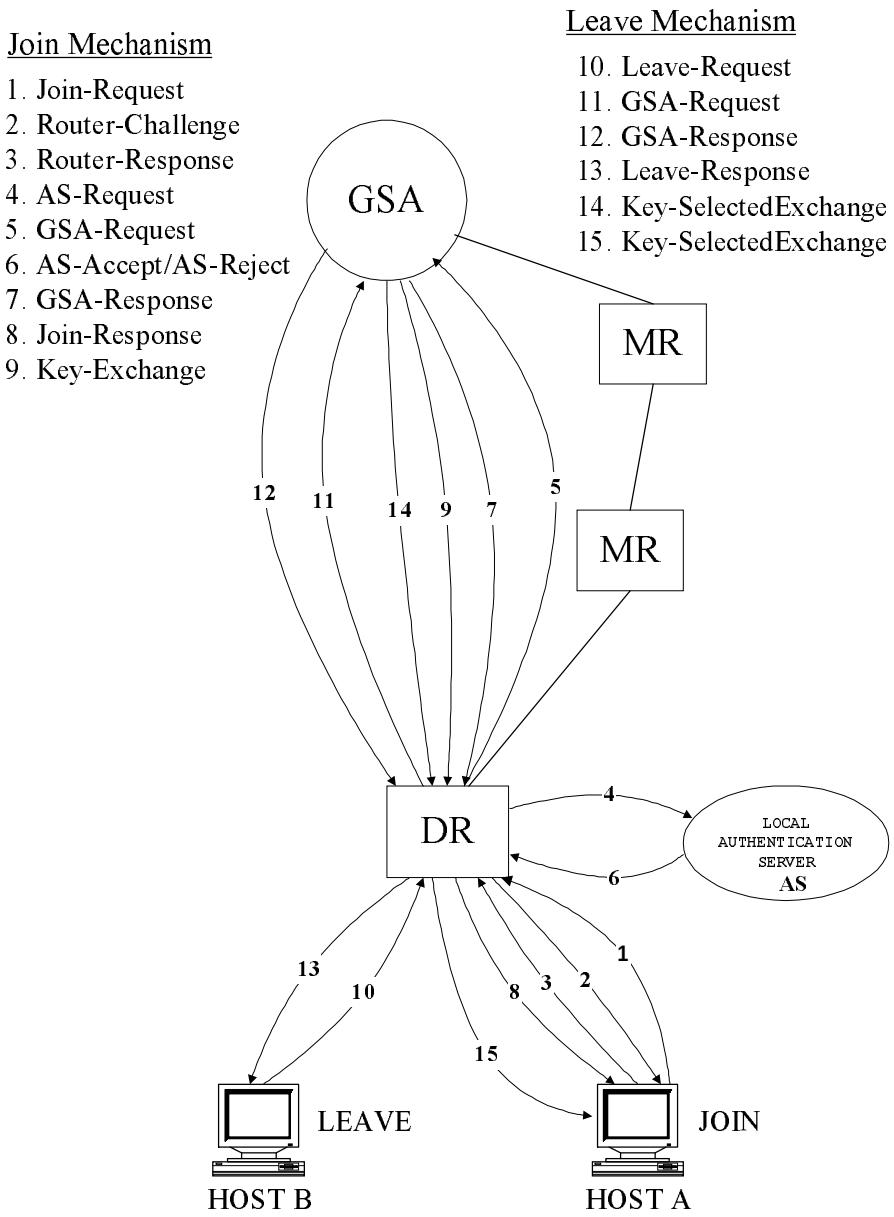


Fig. 3 Message Flow in Extended IGMP Architecture

2.2Authentication

The proposed multicast framework authentication is consisting of two levels. The first level, which is authenticated globally and handled by the GSA, will concern the eligibility of the host of sending/receiving the multicast data by subnet/IP address attributes. The initiator of the multicast group has to provide the security Access Control List (ACL) and once the multicast group is successfully created by the GSA, a copy of the (ACL) is stored in the GSA. The subsequent join or leave to the multicast group have to be authenticated by the GSA. In addition to the ACL, there will be a Group Creator List (GCL) stored in the GSA database. The GCL contains a list of multicast host by subnet/IP address attributes, for which they are granted to be a multicast group creator to initiate a multicast group. Both the ACL and the GCL will be replicated along the routing tree among the GSAs

so that authentication information can be exchanged.

The second level of authentication is on user basis. The user level authentication is carried out by the local authentication server AS, which is supposed to be maintained by an local administrator of individual organisation joining the multicast framework. In the Extended IGMP architecture, the RADIUS Extension for Multicast Router Authentication method [8], which is currently an internet draft, is chosen and used for user level authentication between the designated multicast router and the authentication server AS. The AS maintains the user access database and is to be queried by the designated multicast router. In order for an user to join the multicast group successfully, both the host which is used to join the group as well as the user account to login to the group must have the required permission and get successfully authenticated.

2.3 Key Distribution

It is assumed that a key controller (the role of GSA in the architecture) will be present in each virtual domain, whose main responsibility is to generate the required keys for the chosen group key management scheme.

With the available keys in place, the extended IGMP will help to communicate with the key controller, distribute and update the right keys to the right multicast hosts effectively and efficiently. To make the extended IGMP a flexible and usable multicast protocol, it can provide a general key distribution mechanism by supporting different kind of group key management scheme, such as the Naïve scheme, Tree-Based scheme and the One-Way function scheme. With such support features, the architecture will still be the same regardless of different key management schemes.

2.4 Routing of multicast data

Since the whole internetwork is divided into different virtual domains according to geographical area, and they are relatively independent of each other. One of the main functions of the GSA is to link them together and additional processing on the multicast data is needed so that all the independent virtual domain will come up as a whole.

The routing of multicast data can be viewed and treated in two levels. Firstly, with reference to the GSAs, there will be a routing tree connecting those GSAs for which there is one or more multicast hosts having successfully joined the virtual domain for a specific multicast group. The routing tree may be different for different multicast group since not exactly the same number of GSA will make their request to join the group. The formation of the routing tree depends on the routing protocol used, such as DVMRP, PIM, CBT etc, as long as there exists such routing path for transmission of multicast data by the GSAs. Secondly, for each virtual domain formed, it will have its own routing protocol to route the multicast data for a specific multicast group from the local GSA to the members of the group. Hence, for the multicast data within a virtual domain, it is handled by the routing

protocol implemented within the virtual domain. Different virtual domain may have their own choice of routing protocol as long as multicast data can reach the multicast host sending a valid IGMP membership report. Although those authenticated members may be multicast senders for the multicast group, as viewed inside for each virtual domain, one may be realized later that the only multicast sender for any multicast group as seen by other receivers will be the local GSA.

In other words, a multicast data packet must be forwarded from the originating virtual domain, following the routing path for the GSAs to the destination virtual domains. There the multicast data will be further routed by routing mechanism in each virtual domain and finally reach the target recipients.

Chapter 3. Detailed Operation

3.1 New message to extended IGMP

Several messages are proposed to be added to support the security functions, they are briefly described as below :

(1) Message type between DR and the host

(a) Join-Request

The message is to be sent by multicast host who intends to join a specific multicast group. The message will include those necessary information to be used to login to the multicast group session.

(b) *Router-Challenge*

The message is a response to the host when the DR receives the Join-Request message. The message includes an unpredictable number of variable length and the host is challenged to give back the response.

(c) Router-Response

The message is a response to the DR after the host receives the Router-Challenge. There should be a secret associated with each user account. When the host is challenged, it should generate the response by using the associated secret, based on the CHAP mechanism [9] for password authentication.

(d) Join-Response

The message is to be sent by the DR to the multicast host indicating the successfulness of the authentication process by both the GSA and the AS.

(e) Leave-Request

The message is to be sent by the multicast host member who intends to leave the multicast group.

(f) Leave-Response

The message is the response of the DR to the multicast host member after authentication process. On successful validation, the multicast host will be allowed to leave the group.

(g) Certificate-Query

The message is sent by the DR to query the certificates as held by the multicast host.

(2) Message type between DR and GSA

(a) GSA-Request

The message is generated by the DR and directed to the GSA. The message includes those necessary information of the host so that it can be authenticated or to be provided by the GSA.

(b) GSA-Response

This is the response to the DR from the GSA. The response indicates the successfulness of the authentication process or the information to be provided by the GSA. On successful authentication, a new set of shared key for the virtual domain as well as other important parameters will be returned.

(3) Message type between DR and AS

(a) AS-Request

The message is generated by the DR, which includes those necessary information to be authenticated by the AS. The message is UDP based and same as the RADIUS extension protocol format.

(b) AS-Accept

This is the response to the DR from the AS to indicate that the previous request is accepted upon successful authentication. The message is UDP based and same as the RADIUS extension protocol format.

(c) AS-Reject

This is the response to the DR from the AS to indicate that the previous request is rejected due to failed authentication. The message is UDP based and same as the RADIUS extension protocol format.

(4) Message for key exchange

(a) Key-Exchange

The message is either originated by the GSA or the DR to call for a change of shared keys. The target recipient of the message may be a specific host, a specific router or a group address, but all depends on the destination IP address. Under some circumstances, a Key-Exchange message on multicast router may trigger another Key-Exchange message to be produced.

(b) Key-SelectedExchange

The message is either originated by the GSA or the DR to call for a change of shared keys with selected target hosts. The message can specify the target hosts inclusively or exclusively, depending on how the message is initiated. Under some circumstances, a Key-SelectedExchange message on a multicast router may trigger another Key-SelectedExchange message or Key-Exchange message to be produced.

(c) Key-Query

The message is originated by the multicast host to query the current shared keys as used inside the virtual domain. The message is targeted at the DR.

(5) Addition of membership report type

The extension of the IGMP protocol require the existence of the following membership reports as shown below. Two type of membership reports are identified :

(a) Extended Membership Report

It is exactly the same functionality as the current V3 membership report. It is used by the multicast host to express its interest in particular group or reflect the change in the interface state of the host. However, an additional field "Parent Router Address" is added to the existing

format, so that an host is able to indicate the router responding to its requests.

(b) Certified Membership Report

The certified membership report is used by the multicast host to prove its identity to the designated multicast router when under query. The inclusion of the Multicast Host Certificate and the User certificate in the group record enable the designated multicast router to authenticate the membership of the sender . Upon receiving the certified membership report, the designated multicast router will check the presence of both of the Certificates. If exists, it will check and verify the digital signature included in the certificate by using the public key of the GSA in the virtual domain and the public key of the local AS. Only under successful authentication of the membership report will the designated multicast router consider the sending host as a valid member. Any certified membership report fails in the verification process will be silently discarded by the designated multicast router and a re-authentication of the host will be invoked. When the certified membership report is sent to the DR, it is encrypted by using the public key of the DR to prevent unauthorised capturing of the certificates.

3.2 Keying materials under extended IGMP architecture

The extended IGMP is designed to support both general group key distribution algorithms and authentication purpose. To implement such functionalities, a well-defined set of keying materials must be employed to deliver the security functions. Those keying materials defined under the framework are described here in order to have a good understanding on the security architecture :

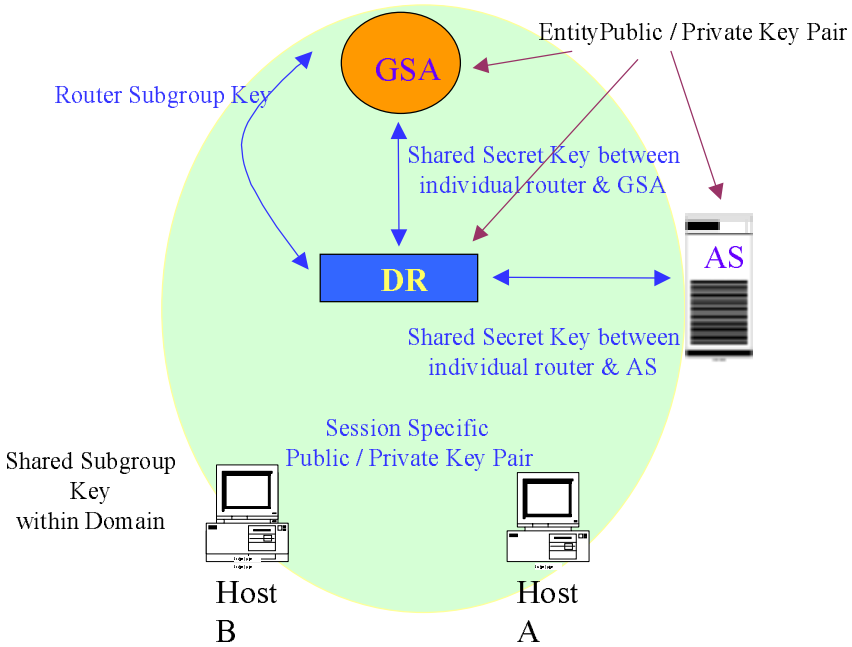


Fig. 4 Keying Materials in Extended IGMP Architecture

(1) Subgroup key under virtual domain

For each virtual domain, it will be associated with a subgroup key Kgrp for the encrypted communication within the domain. The key Kgrp is shared between a specific GSA and all the routers / hosts under the virtual domain. Whenever messages are sent by the GSA or DR directed to the group members, the messages are encrypted by Kgrp. The encryption algorithm for the keying material Kgrp may be different in each virtual domain, since they are relatively independent of each other. The subgroup key Kgrp will be updated under the situation (a) Whenever there is a new member joined to the multicast group; (b)Whenever there is a existing member leaving the multicast group; (c) Periodically requested to be updated by the Key-Exchange message sent by GSA, in order to maintain the security of the multicast group.

(2) Random key for raw multicast data

To minimise the encryption/decryption bandwidth (which concerns the number of time or complexity in data encryption or decryption) when transmitting the encrypted multicast data packets, a random key Krand is generated by the sender per multicast data packet and is used to encrypt the raw multicast data. The random key is then encrypted by the subgroup key Kgrp and also included in the packet for transmission. During forwarding of the whole multicast data packets, it is possible to authenticate the source of message by partial decryption of data packets.

(3) Router subgroup key within virtual domain

It is the key Kmr shared between all the multicast routers and the GSA. Whenever the messages are sent by the GSA and targeted to all the multicast routers under the virtual domain, they are encrypted by the router subgroup key Kmr. The router subgroup key Kmr will be periodically updated by the Key-Exchange message sent by GSA.

(4) Shared group key between different GSA

There will be a shared group key Kgsa among the GSAs constructing the GSA routing tree for a specific multicast group. Whenever multicast data is forwarded along the routing tree, it should be encrypted with Kgsa. To prevent the key being comprised, it should be periodically updated among the GSAs.

(5) Shared secret between individual multicast router and GSA

There will be a shared secret key K_{S_GSA} between each multicast router and the GSA for authentication of GSA-Request and GSA-Response message. The shared secret key is never disclosed to the network and is solely used in the generation of Request Authenticator and the Response Authenticator, the same as those used in the RADIUS authentication protocol.

(6) Shared secret between individual multicast router and AS

There will be a shared secret key K_{S_AS} between each multicast router and the AS for authentication of Router-Request, Router-Accept and Router-Reject message. The shared secret key is never disclosed to the network and is solely used in the generation of Request Authenticator

and the Response Authenticator, the same as those used in the RADIUS authentication protocol.

(7) Private/Public key for each multicast entity

The public key infrastructure is incorporated into the multicast framework such that there will be a private/public key pair for each multicast entity, including the multicast host, router, GSA as well as the local AS. Each entity will hold its private key secretly and announce its public key to other concerned entities. Upon the startup of any multicast router, it should exchange its public key information with the nearby GSA and the AS respectively, so that the subsequent communication can be secured.

For the GSA, AS and the multicast routers, they will be associated with a entity specific private / public key pair respectively, this means that each of them will have one unique key pair for its own for secure communication. On the other hand, for the multicast routers and hosts, they will be associated with session specific private / public key pair respectively, this means that the keys will be generated per session basis. In other words, both routers and hosts can have different key pairs at the same time, since a router can take parts in different multicast group sessions and a host can join in different multicast groups simultaneously.

The table below shows a summary of the keying materials

Keying materials	Protocol specifying the key	Entities sharing the key	Generated by	Used for	Life time	Remarks
Subgroup key Kgrp	Extended IGMP	GSA, all joined MRs, and all group members wiithin a specific domain	GSA	Encrypted communication among GSA, MRs, and all group members	Periodically updated	Each virtual domain will have a different subgroup key
Router subgroup key Kmr	Extended IGMP	GSA, all joined MRs, within a specific domain	GSA	Encrypted communication among GSA, and all joined MRs	Periodically updated	Each virtual domain will have a different router subgroup key
Secret key $K_{S\text{-}GSA}$	RADIUS Extension for Multicast Router Authentication Protocol	Between individual MR and the GSA	Configured upon setup	Authentication between individual MR and the GSA	Span the life time of the configuration	

Keying materials	Protocol specifying the key	Entities sharing the key	Generated by	Used for	Life time	Remarks
Secret key $K_{S\text{-}AS}$	RADIUS Extension for Multicast Router Authentication Protocol	Between individual MR and the AS	Configured upon setup	Authentication between individual MR and the AS	Span the life time of the configuration	
Entity specific public/private keys	Extended IGMP	The public key portion is shared among GSA, MRs, and AS	The private key portion is generated by GSA, MRs, and AS respectively	Authentication of entities and for encrypted communication	Span the life time of the entities respectively	
Session specific public/private keys	Extended IGMP	The public key portion is shared among the parent MR, and the specific member	The private key portion is generated by MRs, and the group members respectively	Authentication of entities and for encrypted communication	Span only the multicast communication session for a specific group	A host has to generate the key pair during session setup
Random key Krand	Extended IGMP	None	Group members	Encryption of multicast data	Span on the message life time	
Inter domain key Kgsa	Extended IGMP	Among all the GSAs	GSA	Encrypted communication among GSAs	Relies on the multicast framework	

3.3 Detailed operation of the secure multicast protocol

The following is the notation used in the description of the mechanism :

$[XYZ]_A$ or $\{XYZ\}_A$	the message XYZ is encrypted by the key A.
S[XYZ] or S{XYZ}	the message XYZ is sent by S without any encryption
$S[XYZ]_A$ or $S\{XYZ\}_A$	the message is sent by S and the message XYZ is encrypted by the key A.
Krand	Random key generated per message.
Kgrp, K'grp	Subgroup Key for the virtual domain
Kmr	Subgroup router key for the virtual domain
Kgsa	Shared key among GSA along the GSA routing tree
Pk_GSA	Public key of GSA
Pk_S_DR	Public key of DR for a specific multicast group session
Pk_E_DR	Public key of DR (Entity Specific)
Pk_AS	Public key of AS
Pk_host	Public key of host for a specific host session

3.3.1 Join mechanism

The join mechanism is initiated by a Join-Request sent to the designated multicast router. Several types of join are proposed in the architecture, and they are identified by the Join Type field in the Join-Request message :

(1) Multicast Receiver

Host requests only join as a receiver to receive the multicast data

(2) Multicast Sender

Host requests to send data to or receive data from the multicast group

(3) Multicast Group Creator

Host requests to create the multicast group, send data to or receive data from the multicast group

Referring to the Fig.3, suppose Host A is going to join the multicast group G, it sends the Join-Request to the All-Router-Address. As DR is the directly attached designated multicast router to the subnet of host A and so it will process the request. To start the authentication process, DR generates a random challenge which is an unpredictable number of variable length, and reply with the Router-Challenge message to A.

Host A :

Host A [Join-Request] ⟶ All-Router-Address

DR :

DR [Router-Challenge] ⟶ Host A

Upon receiving the Router-Challenge message, the host should respond with the Router-Response message, which should contain the corresponding CHAP-based [9] response value of the challenge, and encrypted using the public key of designated multicast router DR.

Host A :

Host A $[\text{Router-Response}]_{Pk\_S\_DR}$ ⟶ All-Router-Address

After receiving the message, DR will generate the GSA-Request to the GSA and the AS-Request to the local authentication server (AS). The GSA-Request will be sent to the All-GSA-Address, with attached IP Address of the originating host for subnet/IP level authentication. The AS-Request will be sent to the AS, with attached challenge/response pair for user authentication. Basically, the communication protocol between the GSA and DR is similar to the one between the AS and the DR, as both of them are based on the RADIUS message format. The communication channel that the DR makes with the GSA or the AS is secured by the public/private key encryption, in addition to the separate shared key that is used in the Radius extension protocol.

DR :

DR [GSA-Request]$_{Pk\_GSA}$ ⟶ GSA

DR [AS-Request]$_{Pk\_AS}$ ⟶ AS

The GSA will authenticate the router DR, using the request authenticator included in the message as well as checking its own database. If DR is a valid and trusted router, GSA will proceed to check the followings according to the Join Type as specified in the Join-Request; If the host request to be a multicast sender or receiver and there already exists a Multicast GSA Certificate for the said multicast group G, it will check the host IP address against the Access Control List (ACL) included in the certificate, to determine whether the host is allowed to join the group; or else if the host request to be a multicast group creator and there is no such Multicast GSA Certificate for the said multicast group G, it will check the host IP address against its Group Creator List (GCL) stored in its database, to determine whether the host is allowed to create the new multicast group G. If the host is authorized to do so, the GSA will create the Multicast GSA Certificate for the multicast group G, and form the ACL as submitted by the requesting host.

Upon authentication, the GSA will reply with the GSA-Response message to DR, encrypted using the entity specific public key of DR, with the code indicating the result of the authentication. If successful, the GSA will also reply with a new subgroup key K'grp for its virtual domain, together with any other keys used in the group key management scheme, and with the Multicast Host Certificate attached.

On the other side, the AS will authenticate the user account used to join the multicast group G, using the Radius Extension for the Multicast Router Authentication Protocol. Upon successful authentication, the AS will reply with the AS-Accept message, with the User Certificate attached, otherwise a AS-Reject message will be returned.

After authentication,

GSA :

GSA [GSA-Response]$_{Pk\_E\_DR}$ ⟶ DR

Authentication Server :

AS { AS-Accept | AS-Reject }$_{Pk\_E\_DR}$ ⟶ DR

DR will wait for the reply from the GSA and the AS server, and upon receiving the GSA-Response message and the response message from the AS, DR will reply with the Join-Response to host A. On successful authentication, the Multicast Host Certificate, User Certificate, the new subgroup key K'grp and together with any other keys used in group key management scheme will be attached and sent to host A. DR will keep a copy of the new subgroup key K'grp for the virtual domain. The DR will put the joining host's IP address, its session public key into its router member database, and set the validity period equal to the least of those specified in the certificates. If DR is the first time to join the multicast group G, it will also be given the Multicast Host Certificate for the router, to certify its authenticity.

DR :

DR [Join-Response]$_{Pk\_Host\ A}$ ⟶ Host A

At the same time, if the multicast group G is not a newly formed group, GSA will multicast the Key-Exchange message to its own virtual domain, in order to update the existing subgroup key Kgrp to K'grp, and the message is encrypted using the existing subgroup key Kgrp.

GSA :

GSA [Key-Exchange]$_{Kgrp}$ ⟶ Virtual Domain

For the ideal case, all the subgroup members should have updated their new subgroup key to K'grp. Afterwards, the GSA will then flood the new multicast data encrypted using the new subgroup key. In case the host can't receive the multicast Key-Exchange message, it will be not able to decode the incoming multicast data. In such case, the host should send a Key-Query message to the directly attached DR, the DR then reply with the Key-Exchange message using unicast, upon verification of the host. This mechanism ensure that no host will miss the new subgroup key even when they actually lost the multicast Key-Exchange message.

Whenever a multicast host successfully join a particular multicast group in the virtual domain, its IP address, session public key as well as the effective validity period of its certificates will be registered in the router member database of its designated multicast router. Shown as below is the proposed router member database record :

Host IP Address	Session Public Key of Host	Validity Period of Host Certificates
xxx.xxx.xxx.xxx	xxxxxxxxxxxxxxxx	xxxxxxxxxx
xxx.xxx.xxx.xxx	xxxxxxxxxxxxxxxx	xxxxxxxxxx
xxx.xxx.xxx.xxx	xxxxxxxxxxxxxxxx	xxxxxxxxxx

Where

Host IP Address

IP Address of the host successfully authenticated by the GSA and AS

Session Public Key of Host

The public key is provided by the joining host, and is generated by session basis

Effective Validity Period of Host Certificates

It is the least of the two validity period for the Multicast Host Certificate and the User Certificate respectively

3.3.2 Multicast data transmission mechanism

Whenever there is a sender S within a virtual domain intends to multicast data to the multicast group,

the mechanism is shown as below :

(1) The sender S must first join/create the multicast group G by joining to its nearest virtual domain and get successfully authenticated, and obtain the Multicast Host Certificate capable of sending multicast data.

(2) If the GSA of the virtual domain is not a member on the GSA routing tree for multicast group G, it will generate the IGMP membership report with attached Multicast GSA Certificate, in order to join the GSA routing tree for the group.

(3) The sender multicast the data to the All-GSA-Address, with the following formats :

$$S\{ [\text{Multicast Data}]_{Krand} + \{[Krand]_{Kgrp} + \text{Multicast Host Certificate}\}_{Pk\_GSA} \}$$

$$\longrightarrow \text{All-GSA-Address}$$

(4) The GSA of the virtual domain receive the message, decrypt part of the whole message using its private key, authenticate the sender by the Multicast Host Certificate. The GSA then re-encrypts the message using the subgroup key Kgrp, and multicast to its own virtual domain,

$$GSA\{ [\text{Multicast Data}]_{Krand} + [\text{Krand + Digital Signature of GSA}]_{Kgrp} \}$$

$$\longrightarrow \text{Virtual Domain}$$

(5) As a member of the GSA routing tree, it will forward the multicast data to the next GSA. The GSA of the message originating domain then re-encrypt the message using the GSA group key Kgsa, with attached digital signature of sending GSA ,

$$GSA\{ [\text{Multicast Data}]_{Krand} + [\text{Krand + Digital Signature of GSA}]_{K\_gsa} \}$$

$$\longrightarrow \text{GSA routing tree}$$

The encrypted multicast data will flow along the GSA routing tree until all the GSA receives the multicast data packets.

(6) At the same time the GSA in the other virtual domain will listen for multicast data originated from other GSAs. If there is any, it will decrypt the message using Kgsa, authenticate the message using the digital signature included in the message. On successful verification, it will re-encrypt the data using the subgroup key of its own virtual domain, as in the case of (4).

3.3.3 Leave mechanism

The leave mechanism is initiated by a Leave-Request sent to the designated multicast router. Referring to Fig 3, suppose host B is currently a member of the multicast group G and is going to leave the group, it will send the leave group message Leave-Request to the All-Router-Address. Upon receiving the message, the designated multicast router will authenticate the message using the

Multicast Host Certificate and the User Certificate as attached. If the sender of the Leave-Request message is a valid member, then the designated multicast router will issue the GSA-Request (with request_type code set to LEAVE) message to the GSA, for requesting a new subgroup key K'grp for its virtual domain and any other keys for the group key management scheme. The GSA will then reply with the GSA-Response , with the response code indicating the result of leave verification.

Host B :

Host B $[\text{Leave-Request}]_{Pk\_S\_DR}$ ⟶ All-Router-Address

DR :

DR $[\text{GSA-Request}]_{Pk\_GSA}$ ⟶ GSA

GSA :

GSA $[\text{GSA-Response}]_{Pk\_E\_DR}$ ⟶ DR

Upon receiving the GSA-Response from the GSA, the DR will reply with the Leave-Response back to the host no matter the leave is granted or not, with response code indicating the successfulness of the leave request.

DR :

DR $[\text{Leave-Response}]_{Pk\_Host\ B}$ ⟶ Host B

In response to the GSA-Request for leave, the GSA will generate a new subgroup key K'grp and any other required keys for the remaining members, it will multicast the Key-SelectedExchange message with the IP address of the leaving member included, targeted to All-Router-Address following the GSA-Response, encrypted using the router subgroup key Kmr shared between the GSA and all the routers within the virtual domain.

(on successful verification on leave)

GSA :

GSA $[\text{Key-SelectedExchange}]_{Kmr}$ ⟶ All-Router-Address

To update the subgroup key of the multicast group members left behind in the virtual domain, the multicast router which is the designated router of the leaving member, as a response to the received Key-SelectedExchange message, will broadcast another Key-SelectedExchange message into its subnet, which contains n copies of the new subgroup key K'grp (assuming n remaining members under router's subnet) each encrypted with a different member's public key.

MR of the leaving member:

MR [Key-SelectedExchange]$_{Kgrp}$ ⟶ Leaving member's subnet

Each member of the subnet then decrypt the whole message using the old subgroup key Kgrp, then extract the new subgroup key by using its private key and update the subgroup key record accordingly. The leaving member can't extract the new subgroup key as it do not have the required private key information.

For the other MRs inside the virtual domain, they will just broadcast another Key-Exchange message with the new subgroup key K'grp attached, and encrypted only once by the old subgroup key, as a response to the received Key-SelectedExchange message.

Other MRs :

MR [Key-Exchange]$_{Kgrp}$ ⟶ Other subnets

Group members on the other subnets then obtain the new subgroup key K'grp by decrypting the Key-Exchange message by using their existing subgroup key Kgrp.

3.3.4 Key query mechanism

There is a threshold counter to record the number of failed decryption for the received multicast data. Whenever the threshold value is exceeded, it may be caused by outdated subgroup key or any other invalid keys being held by the host. In such case, the host should send the Key-Query to the DR, with attached Multicast Host Certificate and User Certificate, encrypted by the session public key of DR.

Host :

Host [Key-Query]$_{Pk\_S\_DR}$ ⟶ All-Router-Address

Upon successful authentication by the DR, if it has the requested key information, it should send the updated keys through the Key-Exchange message, unicasted to the requesting host.

DR: (Successful)

DR [Key-Exchange]$_{Pk\_Host}$ ⟶ Host

However, if the DR do not hold the key information, it should initiate a GSA-Request message to the GSA, for requesting the key information.

DR :

DR [GSA-Request]$_{Pk\_GSA}$ ⟶ GSA

GSA :

GSA [GSA-Response]$_{Pk\_E\_DR}$ ⟶ DR

Upon receiving the required key information, DR will send it back to the requesting host with a unicasted Key-Exchange message.

DR :

DR $[\text{Key-Exchange}]_{Pk\_Host}$ ⟶ Host

On the other hand, if it is failed upon authentication by the DR, it should lead to the re-authentication of the host by sending Router-Challenge message :

DR: (Failed)

DR [Router-Challenge] ⟶ Host

3.3.5 Re-authentication of membership

The membership of the multicast host is required to be re-authenticated whenever the DR found that the identity of the joined multicast host need to be challenged again. When reauthentication takes place, the DR will initiate a Router-Challenge message to the expiring host as in the member join process. The host should response with the Router-Response message upon receiving the challenge message. The mechanism that follows will be the same as the case for the member join mechanism. On successful re-authentication of the multicast host, it will be given the new Multicast Host Certificate and User Certificate with refreshed validity period. The virtual domain subgroup key Kgrp may not be changed as it depends on the current Kgrp used by the GSA.

The re-authentication will occur under the following circumstances:

(1) Expiration of the host record in the router member database

When the Host get successfully authenticated, it will be given the Multicast Host Certificate and User Certificate in which the validity period is defined. The directly attached DR will keep the least of the two validity period for each joined multicast group members in the router member database. Whenever there is a member whose validity period is going to be expired in the database, the designated multicast router will execute the re-authentication process.

(2) Certified membership report failed on authentication

Upon receipt of extended Membership Report, the DR will look up the address of the multicast host and check against its router member database. If failed, the DR will initiate the Certificate-Query to the sending host, requesting the Certified Membership Report from the host, in order for the DR to verify its identity. However, in case of unsuccessful authentication of received multicast host certificates in the certified membership report, the re-authentication procedure will follow.

(3) Failed authentication of Key-Query

Upon receipt of Key-Query message from the multicast host, the DR will authenticate the sender by the Multicast Host Certificate and the User Certificate as attached. If any of the certificates fails, the DR will force the re-authentication of the sending host.

However, in the case any multicast host fails in the re-authentication process, this means that the host must be removed from the multicast group in which it is currently a member. In such circumstances, the GSA of the virtual domain will generate a new subgroup key K'grp for the multicast group and initiate the Key-SelectedExchange message as in a member leave mechanism, so that the failing host will be forced to leave the multicast group.

3.4 Protocol Scalability

With the addition of new IGMP messages, the function of the designated multicast router is extended to membership authentication, key distribution and exchange, rather than normal routing of multicast data. As the multicast group members under the subnet of a multicast router increase, the loading on the designated multicast router will become heavier and may lead to degradation of performance.

To make the protocol more scalable and to prevent the designated multicast router from performance degradation, the protocol is designed such that load-balancing can be achieved among several multicast routers existing in the same subnet. That is, those non-querier routers, although they will not take parts in sending query messages, they should take active role in authenticating membership and multicast key distributions. As such, the task of membership authentication and key distributions can be evenly distributed among the available multicast routers on the same subnet supporting the extended IGMP versions.

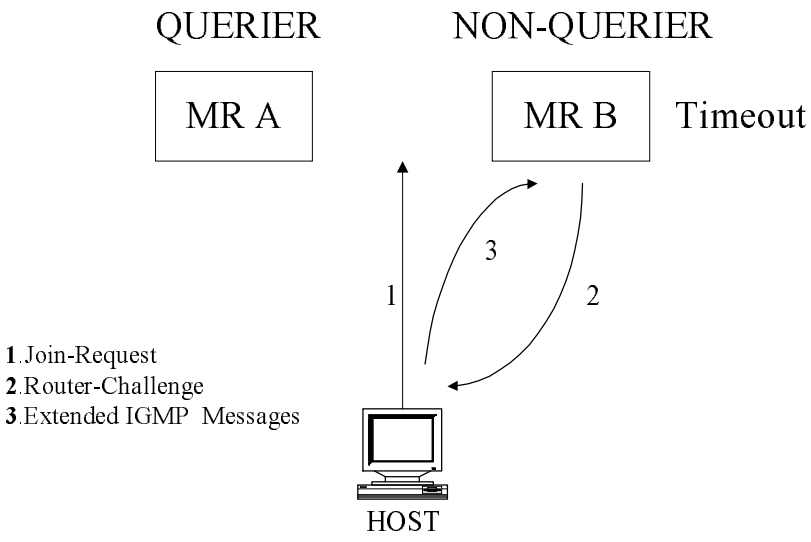


Fig. 5 Co-Existence of Multicast Routers

Mechanism :

Referring to Fig.5 as above, when both the multicast routers receive the Join-Request message on the subnet, it will not respond immediately but it sets the delay timer for the group to a random value

selected from the range [0, Max Response Time], with Max Response Time as specified in the Join-Request packet. Suppose the group's delay timer of router B expires, the router should respond with the Router-Challenge message. If any router receives another router's Router-Challenge message while it has a delay timer running, it stops its timer for the group under monitoring and not to send the challenge message, in order to suppress duplicate response to the same Join-Request message.

After the host receives the challenge response from router B, it will assume the responding router as its parent router and all the subsequent extended IGMP message will quote router B as the parent router address if necessary. In case when the host do not know the responding router in advance, it should set the "parent router address" to All-Router-Address. In the other words, multicast routers should only respond to those messages with either the "parent router address" addressed to their own IP address, or "parent router address" set to All-Router-Address.

By using these mechanisms, the designated multicast router can be off-loaded by adding more multicast routers to the same subnet, to share the additional requests due to an increase in the membership.

To maintain the co-operation among the multicast routers on the same subnet, each router should identify its own router member state for the multicast group concerned. The state transition diagram per multicast group per attached subnet is shown in Fig. 6 as below :

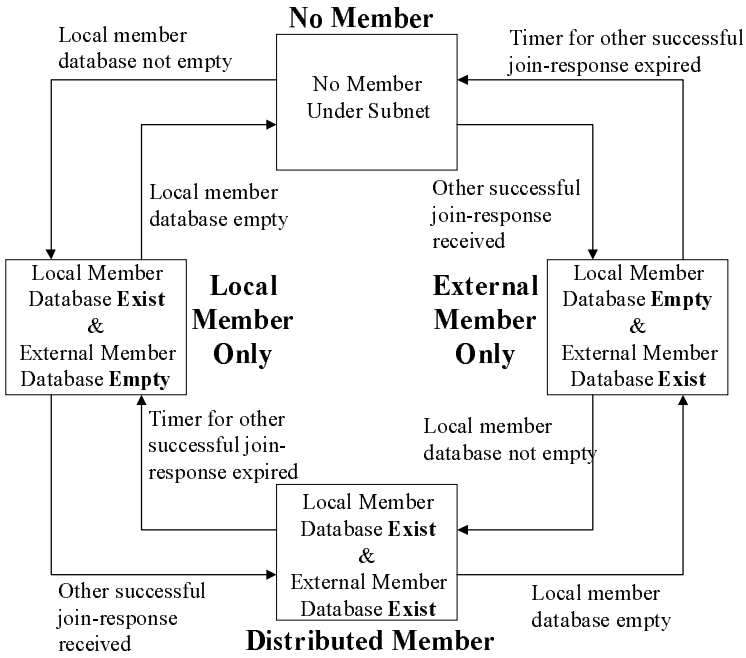


Fig. 6 Router Member State Diagram

1. No Member

Router member database is empty in both local router and external router. There is no need to forward multicast data packet into the subnet.

2. Local Member Only

There are only member records in local router member database and the external router member database is empty. This means that at present the local router is the parent router of all the group members.

3. External Member Only

There are only member records in external router member database and the internal router member database is empty. This means that at present the local routers are NOT one of the parent routers.

4. Distributed Member

There are member records in both local and external router member database. This implies that there is more than one parent router existing in the subnet.

Events triggering a change in state :

a. Local Member Database Empty

When there is no member record in the local member database.

b. Local Member Database Not Empty

When there is member record in the local member database.

c. Other Successful Join-Response Received

When a router receive a successful Join-Response message sent by other routers.

d. Timer for Presence of Other Successful Join-Response Expired

It occurs when the timer for presence of other Join-Response message is expired, indicating that there has been a sufficient long period of time for which Join-Responses sent from other routers are not detected.

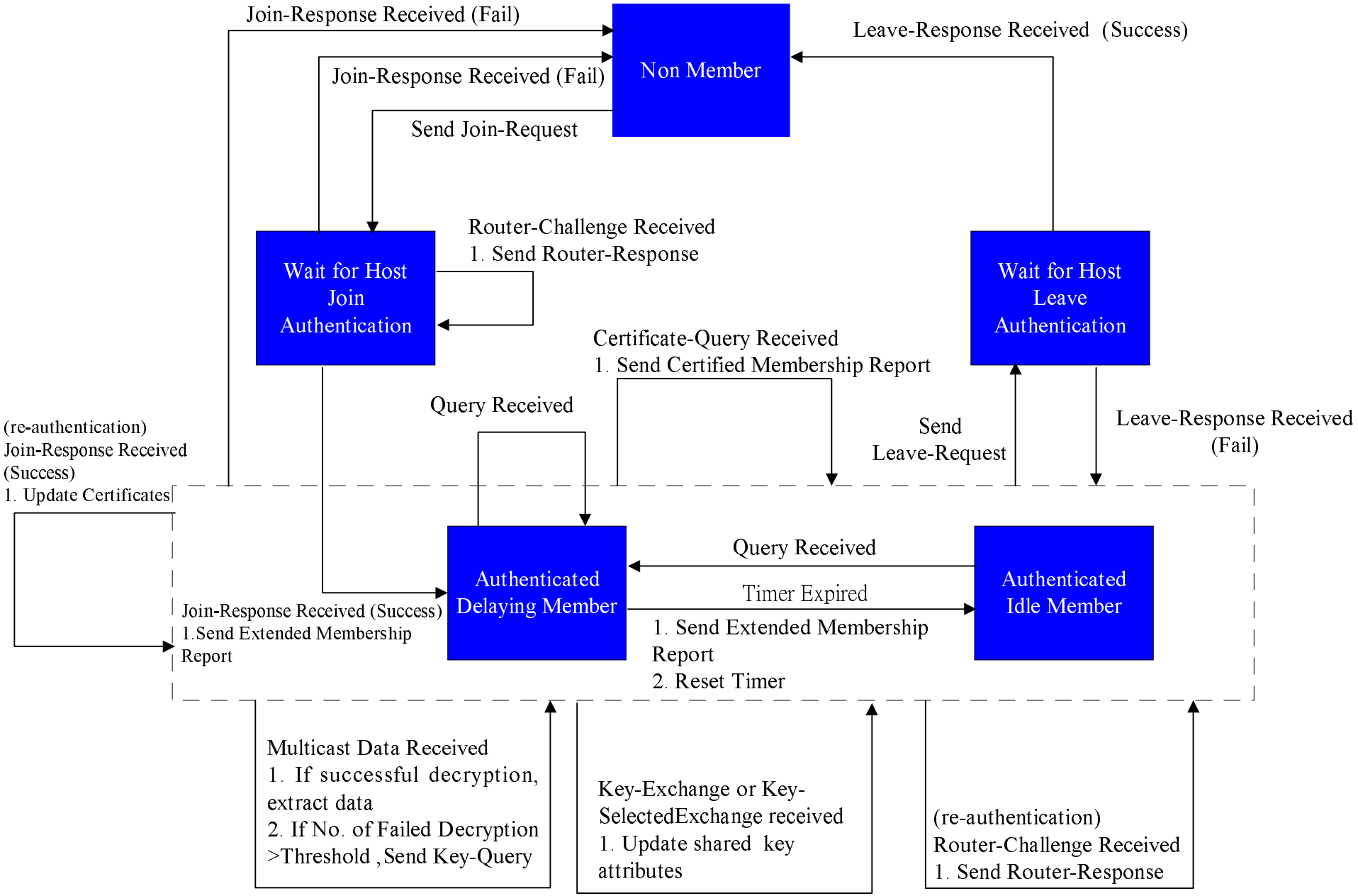


Fig. 7 Extended IGMP Host State Diagram

3.5 IGMP State Diagram

3.5.1 Host state diagram

Host behavior is more formally specified by the state transition diagram. The host state diagram for current IGMP v3 is shown in Fig. 8 as below for our reference. For the extended IGMP, some additional states have to be added in order to fulfill the required functionalities. The host state diagram for the proposed extended IGMP is shown in Fig.7 for our discussion.

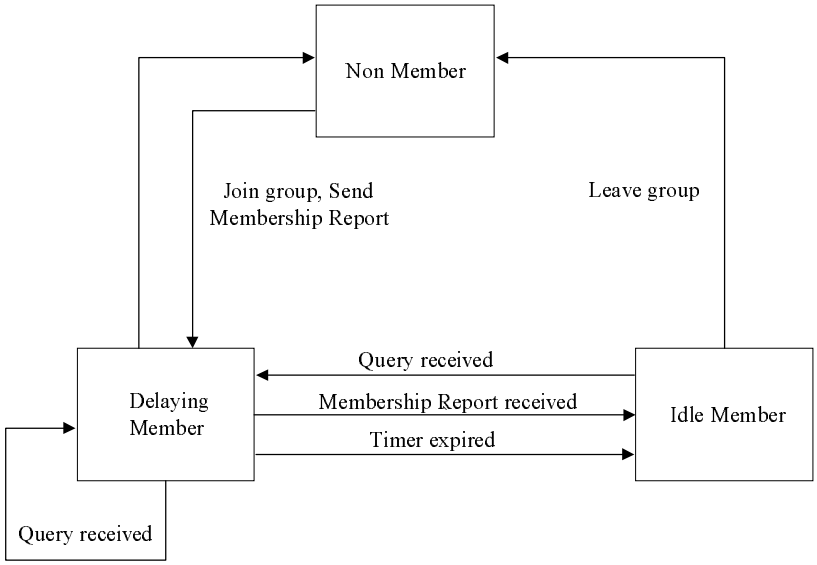


Fig. 8 Current IGMP v3 Host State Diagram

Regarding to the host state diagram in Fig. 7 for the extended IGMP, a host may be in one of five possible states with respect to any single IP multicast group on any single network interface :

(a) Non Member

When the host does not belong to any multicast group on the interface. This is the initial state for all memberships on all network interfaces.

(b) Wait for Host Join Authentication

This is a waiting state. The host in this state is waiting for the reply of the Join-Request initiated earlier.

(c) Authenticated Delaying Member

After the host receive the Join-Response message and successfully obtain the Multicast Host Certificate and User Certificate, it will fall into this state. Host in this state may be able to send or receive multicast data, depending on the kind of Multicast Host Certificate obtained. A report delay timer will be running for that membership.

(d) Authenticated Idle Member

When the host belongs to a specific multicast group on the interface and does not have a report

delay timer running for that membership.

(e) Wait for Host Leave Authentication

This is a waiting state. The host in this state is waiting for the reply of the Leave-Request initiated earlier.

There are several significant events that may or may not cause IGMP state transitions :

(a) Send Join-Request

It occurs when the host decides to join a specific group on the interface. It may occurs only in the Non Member state.

(b) Join-Response received

It occurs when there is a reply from the designated multicast router for the Join-Request or due to the re-authentication of the host. It may lead to different host state depending on the successfulness of the Join-Response message.

(c) Router-Challenge received

The receipt of Router-Challenge message will cause the corresponding action of the host, but it will remain in the previous state.

(d) Send Leave-Request

It occurs when the host decides to leave a joined multicast group on the interface. It may occur only when the host is in either states, Authenticated Delaying Member or Authenticated Idle Member.

(e) Leave-Response received

It occurs when there is a reply from the designated multicast router for the Leave-Request. It may lead to different host state depending on the successfulness of the Leave-Response message.

(f) Query received

The same event as in the existing IGMP version 3.

(g) Timer expired

The same event as in the existing IGMP version 3.

(h) Multicast Data received

Whenever the host receives multicast data packets targeted to the joined multicast group, it will decrypt the packets using the shared key materials and extract the data if possible.

(i) Key-Exchange or Key-SelectedExchange received

The receipt of the above message will cause the host to update the shared keys, but remain in the previous state.

(j) Membership-Query received

The message is sent by the designated multicast router to query the host's authenticated membership.

There are several possible action that may be taken in response to the above events:

(a) Send Router-Response

The multicast host should send the Router-Response as a reply to the designated multicast router on

receipt of the Router-Challenge.

(b) Send Membership Report

It occurs when the host in the Authenticated Member state want to receive multicast data by sending the extended membership report to the designated multicast router.

(c) Extract Data

The multicast host should decrypt the multicast data packets, using the current shared keys .

(d) Send Key-Query

When the number of failed decryption is greater than a certain threshold value, this may due to outdated shared keys, the multicast host should send the Key-Query to the designated multicast router for a refresh.

(e) Update shared keys

On receipt of the Key-Exchange or Key-SelectedExchange, the multicast host should update the corresponding shared keys.

(f) Update Certificates

On receipt of the successful Join-Response due to the re-authentication procedure, the multicast host should update its Multicast Host Certificate and User Certificate.

(g) Send Certified Membership Report

The certified membership report will contain both the Multicast Host Certificate and the User Certificate to be verified by the designated multicast router, and is encrypted by the public key of the DR.

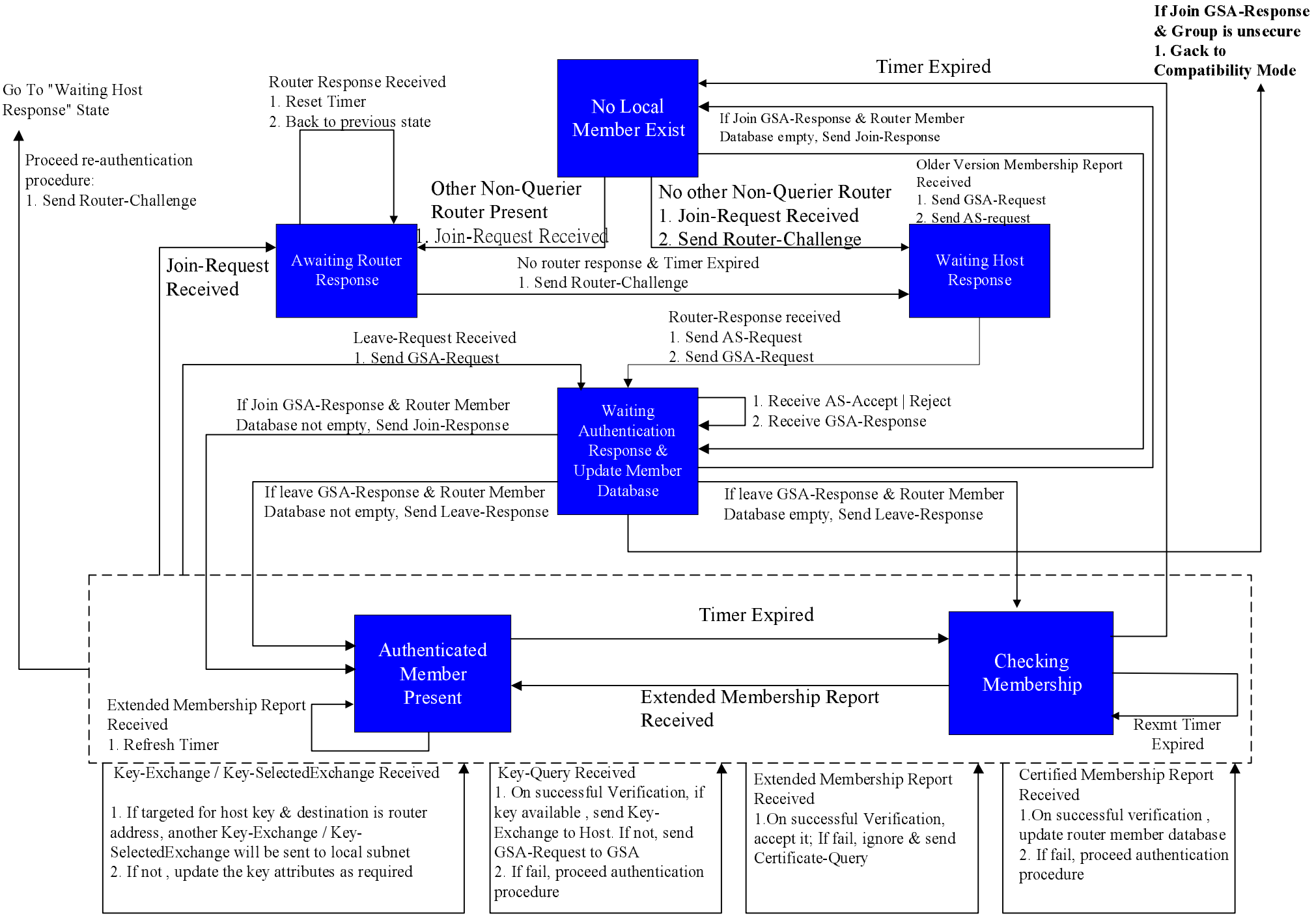


Fig. 9 Extended IGMP Router Querier State Diagram

3.5.2 Router state diagram

Router behavior is more formally specified by the state transition diagram. The router state diagram for current IGMP v3 is shown in Fig. 10 as below for our reference. For the extended IGMP, some additional states have to be added in order to fulfill the required functionalities. The router state diagram for the proposed extended IGMP is shown in Fig. 9 for our discussion.

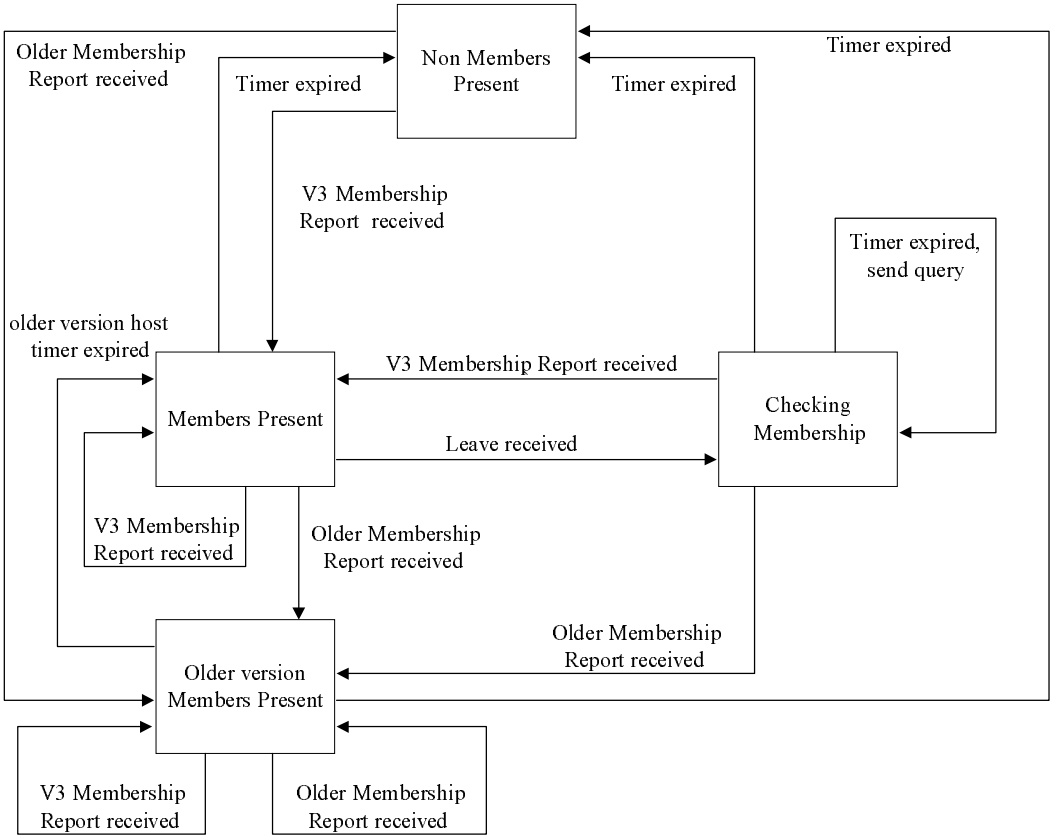


Fig. 10 Current IGMP v3 Router State Diagram

Regarding to the router state diagram in Fig. 9 for the extended IGMP, a router may be in one of the following state with respect to any single IP multicast group on any single attached network:

(a) No Member Present

When there are no multicast hosts on the network having been successfully authenticated and joined as group member at present. This is the initial state for all groups on the router.

(b) Waiting Host Response

This is a waiting state. The router in this state is waiting for the reply of the Router-Challenge initiated earlier.

(c) Waiting Authentication Response and Update Member Database

It is the state in which the router is waiting for the reply from the GSA and the local AS. Upon receipt of the reply messages, the router has to update its router member database according.

(d) Authenticated Member Present

Whenever a multicast host is successfully authenticated by the GSA and the AS, the router will come into this state, to indicate that there is at least a joined member for the group.

(e) Checking Membership

Whenever the router has verified a granted Leave-Request and the router member database is empty, or the timer is expired for a membership report, the router will come into this state to check whether there is any multicast host still interested in the group.

(f) Awaiting Router Response

The waiting state for the presence of other router response when other non-querier router exists. This state is required for the load-balancing between different routers.

There are significant events that may or may not cause router state transition:

(a) Join-Request received

Whenever a router receives the Join-Request message, it will come into the 'Waiting Host Response' state.

(b) Router-Response received

Whenever a router receives the Router-Response message reply to a previous Router-Challenge, it will come into the 'Waiting Authentication Response and Update Member Database' state.

(c) Received AS-Accept or AS-Reject

It is the response from the local AS. The message indicates whether the previous request is accepted or rejected.

(d) Leave-Request received

Whenever a router receives the Leave-Request, it will come into the Waiting Authentication Response and Update Member Database state. It occurs when the previous router state is either Authenticated Member Present or Checking Membership.

(e) When the router is in the Waiting Authentication Response and **Update Member Database base, there will be 4 possible events that will trigger the router state transition:**

(1) If a join GSA-Response is received and its router member database is not empty after updating, this indicates that there still exists authenticated member under the router's subnet, so router will come into 'Authenticated Member Present' state.

(2) If a join GSA-Response is received and its router member database is empty after updating, this indicates that there still no authenticated member under the router's subnet, so router will come into 'No Member Present' state.

(3) If a leave GSA-Response is received and its router member database is not empty after updating, this indicates that there still exists authenticated member under the router's subnet, so router will come into 'Authenticated Member Present' state.

(4) If a leave GSA-Response is received and its router member database is empty after updating, this indicates that there may be no authenticated member under the router's subnet, so router will come into 'Checking Membership' state to query for membership.

(5) If a join GSA-Response is received and the multicast group is unsecured, router will come into 'Authenticated Member Present' state without further authentication. It is for the compatibility with previous IGMP versions, to allow old version IGMP hosts to join the unsecured group as well.

(f) Membership Report received

The router will have a different response to the received membership report, depending on its current state. If the router is in

(1) 'No Member Present' state

It will cause the router to initiate the GSA-Request and AS-Request, to check whether the group is secure or not. This is to maintain the compatibility with existing IGMP versions.

(2) 'Authenticated Member Present' or 'Checking Membership' state

If the group is secure, it will check the sender IP address against its router member database, and accept it on successful verification. If failed, it will ignore it and send the Certificate-Query message. However, if the group is unsecured, it will accept as valid reports without going through verification.

(g) Key-Exchange / Key-SelectedExchange received

When the router receive the Key-Exchange / Key-SelectedExchange, it must be originated from the GSA. The reason code in the message indicate the reason why an update in subgroup key is needed. There are 2 possible cases :

(1) Reason code indicate "Member Join" or "Periodically Update"

The message should be targeted at the whole virtual domain, the router will only need to update its own subgroup key.

(2) Reason code indicate "Member Leave"

The message should be targeted only at the All-Router-Address , only the routers can decrypt the message using router subgroup key Kmr, and update its own subgroup key. The router should broadcast the Key-SelectedExchange message into router's subnet, to update remaining member's subgroup key.

(h) Key-Query received

Whenever the router receives the Key-Query, it will authenticate the sending host by the attached certificates. Upon successful verification, it will initiate the Key-Exchange to update host's subgroup key. If failed, it will execute the re-authentication procedure.

(i) Certified Membership Report received

Whenever the router receive the certified report, it will decrypt the message using its private key, authenticate the certificates as attached. On successful verification, it will add the sender information into its router member database. If failed, it will execute the re-authentication procedure.

(j) Re-authentication of Host

This action is triggered by either of the following events :

(1) Expiration of the host record in the router member database

(2) Certified membership report failed on authentication

(3) Failed authentication of Key-Query

There are several possible actions that may be taken in response to the above events :

(a) Send Router-Challenge

This is a response to the sending host when the router receives the Join-Request.

(b) Send AS-Request

This is a request to the local AS when the router receive the Router-Response, or when the router receive membership reports in the 'No Member Present' state.

(c) Send GSA-Request

This is a request to the GSA when the router receive the Router-Response or Leave-Request, or when the router receive membership reports in the 'No Member Present' state.

(d) Send Join-Response

This is a response to the previous received Join-Request.

(e) Send Leave-Response

This is a response to the previous received Leave-Request.

(f) Update subgroup key Kgrp

This is a response to the received Key-Exchange message.

(g) Send Key-SelectedExchange

This is a response to the received Key-Exchange message for reason code "leave", when the leaving member is located in the router's subnet.

(h) Send Key-Exchange

This is a response to the received Key-Query message after successful verification, or a response to the Key-Exchange message for reason code "leave", when the leaving member is not located in the router's subnet.

(i) Send Certificate-Query

This is a response to the failed authentication of the received membership report, when the multicast group is secure.

3.6 Compatibility

For the sake of discussion, the IGMP V3 protocol with the extended messages as described is referred to as Secure IGMP v3. Those multicast router and host supporting the Secure IGMP v3 is called the Secure IGMP router and host respectively. Secure IGMP hosts and routers are interoperable with hosts and routers that have not yet been upgraded to Secure IGMP v3. This compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within the network, but without sacrifying the security functions added to a particular multicast group.

3.6.1 Secure IGMP host interoperability with older version Queriers

An Secure IGMP host may be placed on a network where the Querier router has not yet been upgraded to Secure IGMP router. Under this scenario, the security functions will not be implemented on any multicast group and the Secure IGMP host will function as a IGMP v3 host. The Secure IGMP host will support those compatibility in a subnet where older version queriers and hosts exist, as in the case of existing IGMP v3, with some minor modifications of the state transition diagram to the existing IGMP v3 as shown. All Secure IGMP host will start to join a specific multicast group by sending the Join-Request to the All-Router-Address, when the Join-Request times out on its interface, by assuming there is no Secure IGMP router present, it will fall into IGMP v3 mode of operation and follow the transition in the state diagram as shown in Fig. 11.

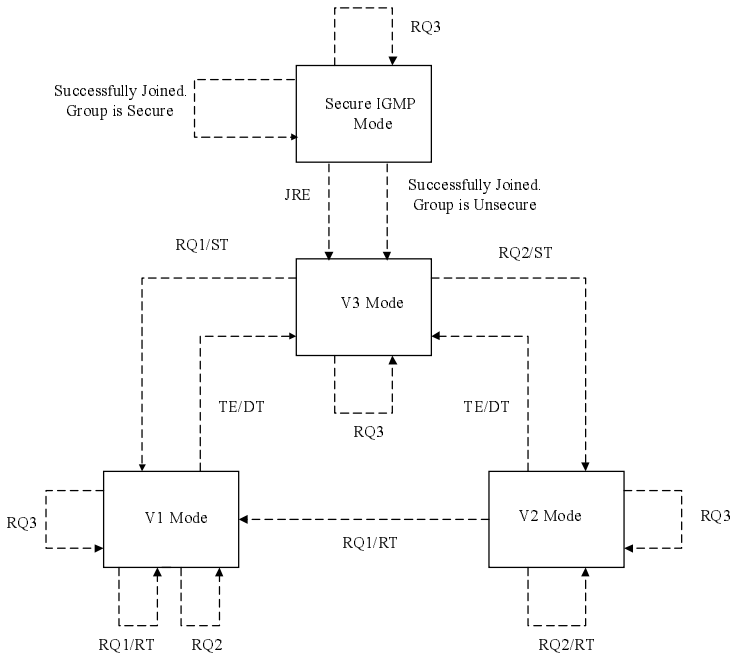


Fig. 11 Extended IGMP Host Compatibility State Transition Diagram

Actions

ST : start Older Version Querier Present Timer

DT : delete Older Version Querier Present Timer

TE : Older Version Querier Present Timer expires

RT : reset Older Version Querier Present Timer

Events

JRE : Join-Request timeout counter is exceeded

RQ1 : Receive IGMPv1 Host Membership Query

RQ2 : Receive IGMPv2 Host Membership Query

RQ3 : Receive IGMPv3 Host Membership Query

States

Secure IGMP Mode

An Secure IGMP v3 router is the present querier on an interface. The host uses Secure IGMP v3 messages

V3 Mode

An IGMPv3 router is the present querier on an interface. The host uses IGMPv3 Membership Reports

V2 Mode

An IGMPv2 router is the present querier on an interface. The host uses IGMPv2 Membership Reports and IGMPv2 Leave Group messages.

V1 Mode

An IGMPv1 router is the present querier on an interface. The host uses IGMPv1 Membership Reports.

3.6.2 Secure IGMP host Interoperability with older version hosts with secure IGMP router

It is also possible for the Secure IGMP router to take the role as a querier with a coexistence of different IGMP version on different hosts on the same subnet. Under this scenario, the Secure IGMP router will support the secure group as well as unsecured group multicasting.

(a) Unsecured Group

If the group is unsecured, this means that all the old versions of IGMP host can join and leave as before. Secure IGMP host will try to join the group securely using the Join-Request message, but it will be informed by the Join-Response message that the group is unsecured, as indicated by the subkey algorithm identifier. The Secure IGMP host will then switch to v3 mode, as shown in previous Fig. 11, and follows the state transitions.

(b) Secure Group

If the group is secure, this means that the host must be authenticated before granting the

permission to join the group. The host must be running in the Secure IGMP mode in order to exchange secure message with the Secure IGMP router, and it will not switch to other mode although there are other old versions IGMP host in the network.

3.6.3 Secure IGMP router interoperability with older version of host

Secure IGMP router may be placed on a network where there are hosts that have not yet been upgraded to Secure IGMP v3. Under this scenario, the security function will not be available to those group which is created as unsecured, but provide security to those secure group. The Secure IGMP router will support those compatibility in a subnet where older version hosts exist, as in the case of existing IGMP v3, with some minor modifications of the router state transition diagram to the existing IGMP v3 as shown. All the Secure IGMP router will treat any multicast group as secure initially, but in case it is reported that the group is unsecured after authenticated by the GSA, it will fall into IGMP v3 mode operation and follow the transition in the state diagram as shown in Fig. 12, with respect to a single multicast group.

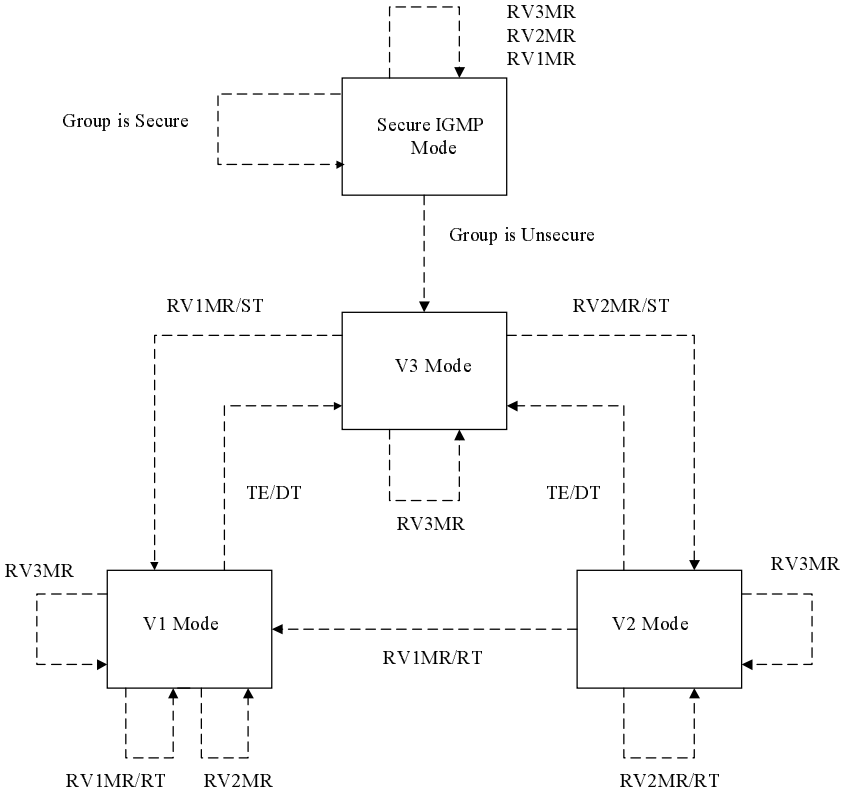


Fig. 12 Extended IGMP Router Compatibility State Transition Diagram

Actions

ST : start Older Host Present Timer

DT : delete Older Host Present Timer

TE : Older Host Present Timer expires

RT : reset Older Host Present Timer

Events

RV1MR : Receive Version 1 Membership Report

RV2MR : Receive Version 2 Membership Report

RV3MR : Receive Version 3 Membership Report

States

Secure IGMP mode

A router operates using the Secure IGMP v3 messages

V3 Mode

A router operates using only IGMPv3 messages for this group.

V2 Mode

An IGMPv2 Membership Report has been heard for this group within the last Older Host Present Timeout seconds. A router operates using only IGMPv2 messages for this group.

V1 Mode

An IGMPv1 Membership Report has been heard for this group within the last Older Host Present Timeout seconds. A router operates using only IGMPv1 messages for this group.

3.6.4 Secure IGMP router in the presence of older version Queriers

It is possible to place Secure IGMP router on a network where at least one router on the network has not yet been upgraded to Secure IGMP v3, but it must be administratively assured that the Secure IGMP router is taking the role as the querier on the subnet, since it must be the designated multicast router to send membership queries on the subnet and make authentication request to the GSA and the local AS for member join or leave process, although it does allow older version IGMP routers acting as the non-queriers on the same subnet.

Implementation Issue

The proposed multicast framework is designed to add security functions to the multicast environment, while maintaining the interoperability with existing unsecure group multicasting. The compatibility of the secure IGMP v3 with older versions of IGMP also help to ease the implementation of secure multicasting by phases. It allows the following implementation scenarios :

(a) Hosts can be using the secure IGMP v3, in coexistence with other older version IGMP hosts, without the implementation of secure IGMP router, the GSA or the local AS.

(b) With the readiness of the GSAs, AS, and the Secure IGMP router within a virtual domain, both

secure group and unsecured group multicasting are supported. For secure multicasting, it is possible with mixed Secure IGMP router and Unsecure IGMP router appearing in the same virtual domain, since only the secure routers can communicate with the GSA and AS in order to decrypt or encrypt the multicast data accordingly.

Chapter 4. Performance Issue

4.1 Security consideration

With regards to the security of the multicast communication, a prevention-based approach is adopted rather than the detection-based approach. For the prevention-based approach, specific control algorithms are in place to make sure that potential threats to the group communication are minimised as much as possible. The security issue can be viewed in different aspects, namely the authentication, non-repudiation and data integrity.

(a) Authentication

The authentication process will be consisted of two levels, one is subnet level while the other is user basis. The subnet level authentication is implemented through the use of Access Control List and Group Creator List stored in the GSA database, while the user basis authentication is handled by the authentication servers. Multicast routers will take the role as an authentication request initiator on behalf of the joining or leaving hosts, and to give the response accordingly. Upon successful authentication, the joining host will be given certificates to prove its identity and eligibility of the joined multicast group. To minimise the probability that a given set of certificates are stolen for unauthorised use, the certificates will have certain life time and re-authentication is required to have the certificates refreshed.

(b) Non-repudiation

Critical messages from different entities are not forgeable as the messages themselves will be digitally signed by the corresponding sending entity, so that the identity of the sender can be verified before processing the messages. Besides, a forged Membership Report in the proposed framework is useless. Since the identity of sending host of the membership report will be checked against the router member database of the parent multicast router, any unauthorised joining host will invoke the re-authentication procedure executed by the multicast router. Moreover, to prevent the intruders from sending out Leave-Request message on behalf of the authenticated multicast host members, it is required that the Leave_Request message should also be authenticated before dropping off the authenticated members from the router member database.

(c) Data Integrity

All the eligible multicast senders for a particular multicast group will be supposed to send their multicast data packets towards the GSA for verification. As seen by all the receivers for the multicast group in interest, all the multicast data packets will be originated and digitally signed by the GSA. Receivers will authenticate the message by using the public key of the GSA before further processing the message, and should ignore the message packets in case of any discrepancy.

The algorithm ensures that the multicast data will not be altered in any way during the transit path.

(d) Confidentiality

All the critical messages is encrypted by the secret or public key, which can only be decrypted by the target recipients. For multicast data, it is supposed to be encrypted by the subgroup key of the virtual domain, so that only the valid members of the group can have the subgroup key for data decryption. In order to secure the communication and minimise the probability of key compromisation, the shared subgroup key for the virtual domain as well as the shared router group key are to be updated periodically. Moreover, to avoid the private key of the multicast router and the joining hosts to be easily link-attacked by unauthorised capturing of the data packets over a long period, the public / private key pair for both of the multicast routers and the joining hosts are generated per session basis. The use of different private keys for the same entity to enable secure communication help to reduce the vulnerability for being attacked. Even when being compromised, this would only cause partial disruption to the specific session without other effects on the remaining sessions.

4.2 Scalability consideration

One of the main objectives of the framework is to provide scalability to the multicast environment. As discussed before, the essential problem lies in the nature of the multicast key distribution and it makes the multicasting mechanism not scalable. By using a simulation model, a comparison will be made among the following 3 different multicast scenarios :

(1) A single multicast domain
(2) Iolus framework
(3) Iolus framework with extended IGMP architecture

A single multicast domain is the case where all the members form a single multicast group. There are no virtual partitions between members and they all subscribe to the same multicast group. Iolus framework is the case where all the members are divided into different virtual domain groups, members only have to join their local domain groups in order to become member of a specific multicast group. Finally, the Extended IGMP architecture, although it is flexible enough to be independent of the underlying multicast framework, the Iolus framework is chosen with added Extended IGMP architecture support, to show what will be benefited from such architecture.

To measure the degree of scalability for the above architecture, the following metrics are used for the comparison purpose:

For Join Mechanism

(a) Members affected during a Join

(b) Total messages required for key exchange during a Join

For Leave Mechanism

(a) Members affected during a Leave

(b) Total messages required for key exchange during a leave

A simulation model for our proposed architecture with Iolus as the reference framework, which is developed to analyse the member-join and member-leave scenario respectively, is shown in Fig. 13. The model assume that there are maximum N members for a particular group G, and totally there are D virtual domains. Moreover, there are hosts in randomly chosen virtual domains going to join the group G by sending the Join-Request message to one of the multicast routers within the domain. On the other hand, there are members in randomly chosen virtual domains requesting to leave the group G.

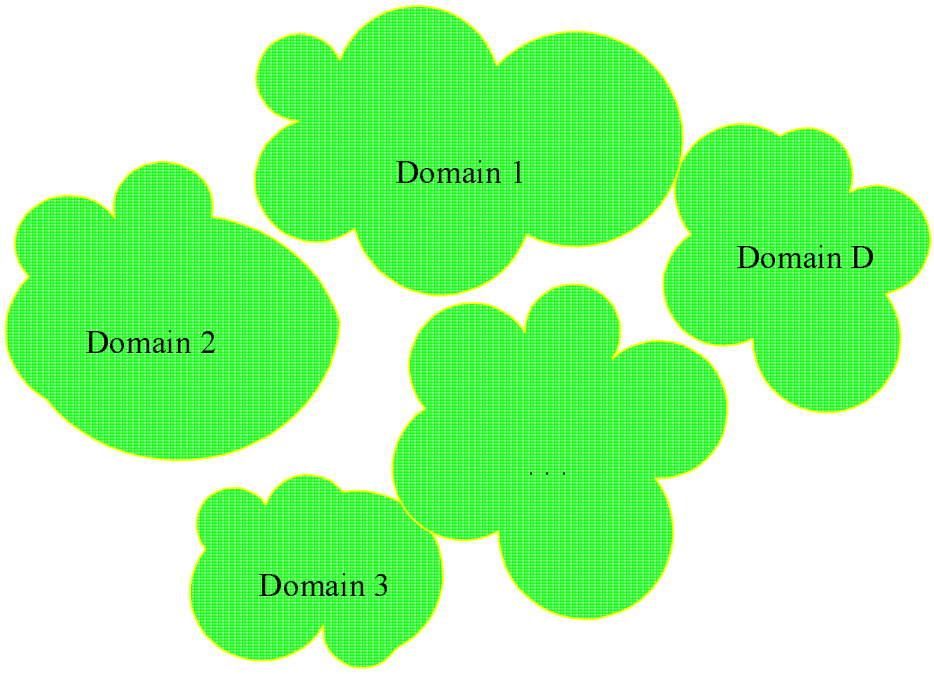


Fig. 13 Simulation Model

The mode can be further described by the following parameters and notations:

d_J - a random number denoting the domain in which a host will join the multicast group

G

d_L - a random number denoting the domain in which a member will leave the multicast group G

f_d (d) - where f_d is the function representing the number of group members inside the domain d

f_s (MR_{Ls}) - where f_s is the function representing the number of group members under the subnet of the router MR_{Ls}, where L is the domain the leave occurs and s is the subnet the leaving member resides

M_d - the total number of multicast routers inside the domain d

n - the total current group members for group G

For each member join or leave at different values of n, the number of members being affected, whose subgroup key need to be updated in order to maintain the security of the system, and the number of messages required to update the subgroup key have been counted.

Based on the comparison metrics, let $f_a(n)$ denotes the total number of members to be affected and $f_m(n)$ denotes the total key update messages required during a member join or leave scenario when the total number of members for group G equals n, the performance on the different multicast architecture will be discussed as below.

Join Scenario

For Join Scenario modeling, the following assumption is applied :

(a) Initially there are no member for the group G

(b) Members from randomly chosen virtual domain will join the group G

The modeling equations for the total number of members to be affected are :

For architecture (1), there is only one single domain for group G, obviously :

$$f_a(n) = n$$

For architecture (2) and (3) :

$$f_a(n) = f_d(d_J)$$

Based on the modeling equations, the value $f_a(n)$ is plotted against n by setting N=1000, D=10 and M_d=3 for all value of d. It can be seen that for each member join, less group members will be affected in both architecture (2) and (3) when compared with (1), and the significant difference is shown in

Fig 14. and it can be seen that it is about 10 times more scalable, and it can be shown that the degree of scalability will increase with a larger value of D.

For the number of messages required, totally 9 messages is to be processed for each member join. The messages serve to authenticate the membership of the host as well as to update the necessary key information. However, as far as the number of messages required for updating the required group keys of the affected members, it will be more or less the same for all architectures , since such key update messages will be multicasted to the affected members other than the joining host, and be encrypted using the old subgroup key.

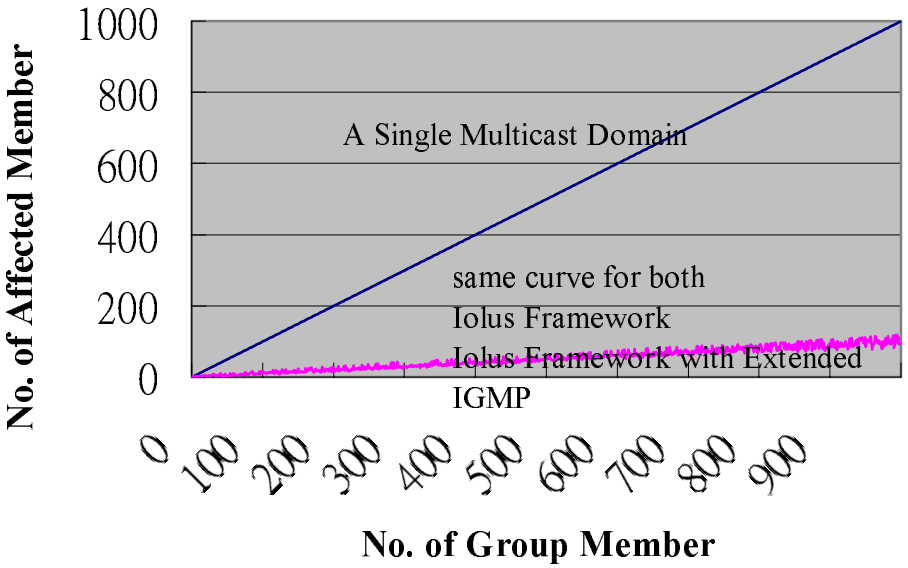


Fig. 14 Member Affected under Join Scenario

Leave Scenario

For leave scenario modeling, the following assumption is applied :

(a) Initially there are N member for the group G distributed randomly among the virtual domains

(b) Members will leave the group G in a randomly selected virtual domain

The modeling equations for the total number of members to be affected are :

For architecture (1), there is only one single domain for group G, obviously :

$$f_a(n) = n$$

For architecture (2) and (3) :

$$f_a(n) = f_d(d_L)$$

Assuming a key update message is required for an affected member, the modeling equation for the total number of key update message required are :

For architecture (1) :

$$f_m(n) = n$$

For architecture (2) :

$$f_m(n) = f_d(d_L)$$

For architecture (3) :

$$f_m(n) = f_s(MR_{Ls}) + \sum_{i=1}^{M_L} f_g(MR_{Li})$$

where $\sum_{i=1}^{M_L} f_g(MR_{Li}) = \begin{cases} 1 & \text{if subnet router still has group members} \\ 0 & \text{if subnet router has no group members} \end{cases}$

and L is the domain where member leave occurs
s is the subnet where the leaving member resides

Based on the modeling equations, the value $f_a(n)$ and $f_m(n)$ are plotted against n by setting N=1000, D=10 and M_d=3 for all value of d. For the member-leave scenario, the simulation result on the number of affected members is shown in Fig. 15. The curve follows the same shape as in Fig. 14, it is what we have expected since the effect of any member join or leave will only be confined to a particular virtual domain, without causing any disturbance to other members being served by other virtual domain.

The number of messages required for updating the group key of the affected members may be significantly larger than that in the case of member join, since there should be proportionally more key update messages required for those affected members. Although the number of key update messages required for the affected members is somehow closely related to the group key management scheme chosen for the multicast, but for comparison purpose, it is assumed that one message for key exchange must be required for each affected member, despite the fact that a leave key exchange

message for both architecture (2) and (3) has the capability to update key information for more than one group members.

The curve where $f_m(n)$ is plotted against n is shown in Fig. 16. For the Iolus framework architecture (2), it is shown that the number of key update message required is much less that those required in architecture (1). It is as expected because the key updates are confined only to the virtual domain where the leave occurs.

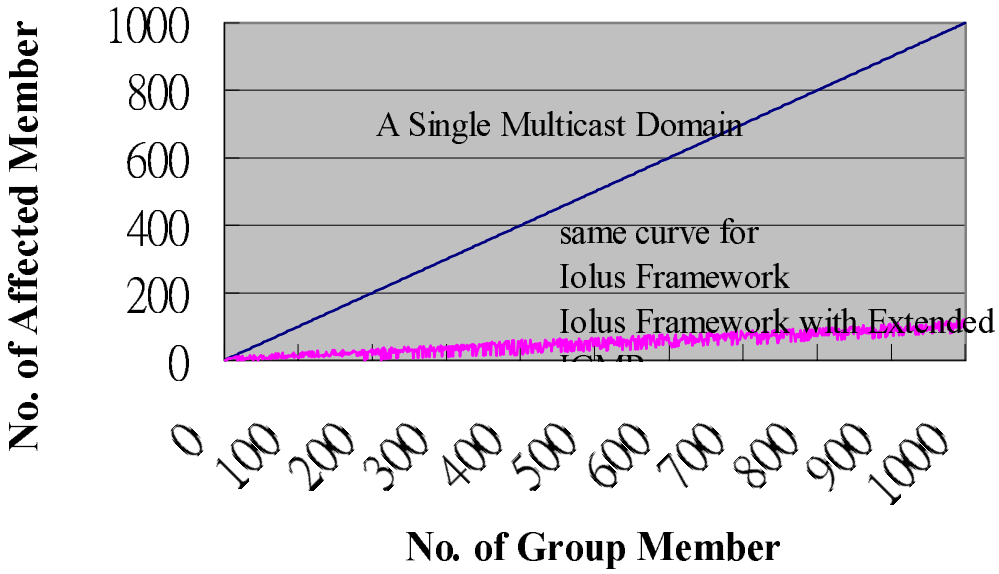


Fig. 15 Members Affected under Leave Scenario

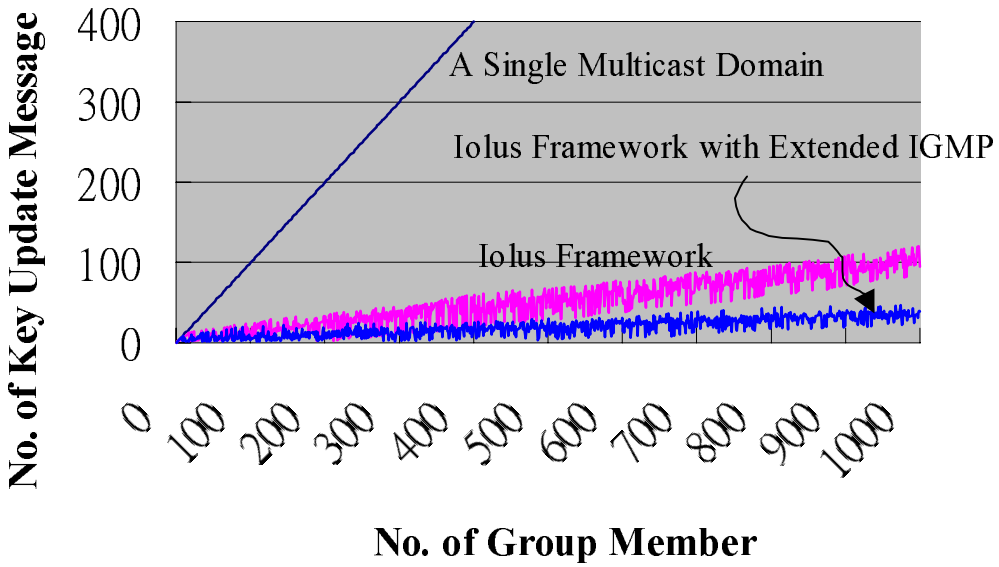


Fig. 16 Key Update Messages Required under Leave Scenario

With the added extended IGMP architecture (3) , the corresponding key update message required is even less than those required for architecture (2). The reason behind the result is that the virtual domain can be further subdivided into different multicast subnets with the help of extended secure multicast routers. With the key management capabilities of the routers, it is possible to use the most efficient and effective method to handle the key update mechanism for the affected members. For the leave scenario, the Key-SelectedExchange message, which is bandwidth consuming, is only required for the subnet where the leaving member is attached to. For the other subnets inside the same virtual domain, a broadcasted Key-Exchange message is enough for handling the key exchange for other affected members, which is the same as for a member-join scenario. These will lead to even more scalable architecture with the extend IGMP.

To visualise the scalability of the extended IGMP architecture for the key update message, the same simulation model is used with N=10,000 D=10 but with different number of M_d, which represent the number of multicast routers supporting the extended IGMP under each virtual domain. The number of key update messages $f_m(n)$ for a leave is plotted against the number of current group members n for the extended IGMP architecture only, and is shown in Fig. 17. Each of the curves represents a different number of multicast routers within each virtual domain, and is plotted using interpolation method. The result shows that the extended IGMP can be made more scalable by tuning the number of multicast routers present in each virtual domain, but not exceeding its limit. This is very useful in the reality when certain multicast group is very dynamic in terms of number of joining or leaving

members, as the network traffic can be accommodated by increments or decrements of multicast routers in the network infrastructure.

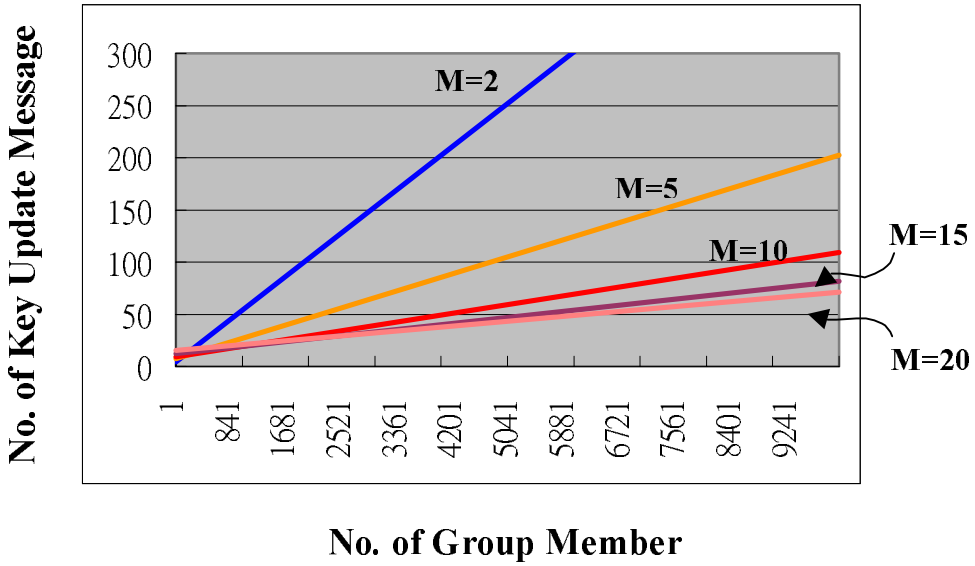


Fig. 17 Extended IGMP Scalability

Comparison between Iolus Framework and Extend IGMP

The main difference between the two proposed architectures lies on the mode of operation inside the virtual domain or subgroup scenario. The mode of operation may include the key distribution mechanism, authentication mechanism as well as the message flows.

When the message flow is considered, it is found that in the Iolus framework, hosts will communicate directly with the GSA, since all the authentication or join request will be sent to GSA, and there are no dependence on the underlying multicast routers. However, in the Extended IGMP, the hosts will take with GSA indirectly through the multicast routers using the extended protocol.

For the key distribution issue, what Iolus propose is to assign GSA as the sole key centre for the subgroup and to generate the symmetric key for each of the joining host. The member specific key is then unicasted to the corresponding member when they join the group. However, the Extended IGMP approach eliminates the necessities in transmitting the member specific key by using the public/private key architecture. In order to join, the host generates its own public/private key pair and only have to submit its public key which can be made well known to others. This thus reduces the risk being attacked for the multicast session. Besides, the key generation process can be off-loaded from the GSA by distributing the process down to the joining host. In addition, the Extended IGMP is

designed to support general key management scheme such as Naïve , Tree-based scheme, etc.

As far as authentication is concerned, it seems that the GSA need to handle both host as well as user authentication under the Iolus framework. This may be one of the drawback because the organisation must have own a GSA in order to take part in the multicast communication, which may be expensive for such specialised application. On the other hand, the Extended IGMP will have the user authentication incorporated into the protocol itself, organisation wish to join the multicast communication only need to maintain an user authentication server to keep track of the user accounts, thus providing a more cost effective and flexible management architecture.

Chapter 5. Conclusions and Future Work

At present, any host can join a specific multicast group by sending the required membership report, and then send or receive data associated with the group without any restrictions. Even though there are proposed group key management protocols or authentication mechanisms to be deployed in secure multicasting, there is no a well defined common multicast protocols to support them.

In this paper, a solution is proposed to extend the current IGMP v3 to enhance the support of the security functions, so that a well-defined protocol can be established between the multicast entities. The detail of the proposed protocol is described based on the Iolus Framework, with which a scalable architecture can be achieved. In the proposed Extended IGMP architecture, it introduces new types of messages to be used in the multicast group join or leave mechanism, together with a set of keying materials, to support authentication as well as different key management algorithms. The protocol also exhibits load-balancing feature on the multicast routers in order to make them more scalable to increasing number of group members. Based upon the simulation model and the performance result, it is shown that the approach will lead to scalable multicasting architecture in terms of group members being affected and the number of key update messages required to maintain the security of the multicast group communication.

Since the Extended IGMP architecture situated between the group members and the underlying multicast framework, it can hide the backend multicast framework from the joining or leaving members as long as the multicast routers can communicate with the hosts using Extended IGMP. Although Iolus is used as the reference framework in the description and performance comparison of the Extended IGMP architecture, it should be noted that it can be deployable to other frameworks as the only requirement is for the Extended IGMP multicast routers to be able to interact with some kinds of security controllers specific to the framework using the well-defined Extended IGMP messages.

The proposed extended IGMP only assume the requesting hosts to be authenticated by using the CHAP based mechanism in the current work. In fact, more research work can be carried out on the authentication mechanism for the client hosts so as to enhance the capability of the extended protocol.

Chapter 6. References

1. Suvo Mittra,"Iolus: A Framework for Scalable Secure Multicasting", Pro. ACM, SIGCOMM 1997, p277-288
2. Tony Ballardie and Jon Crowcroft, "Multicast-Specific Security Threats and Counter-Measures", IEEE Symposium on Network and Distributed System Security, p2-16, Feb 1995
3. Steve Deering, "Host Extensions for IP Multicasting", RFC 1112 , May 1989
4. W. Fenner, "Internet Group Management Protocol, Version 2", RFC 2236, Nov 1997
5. Steve Deering, Brad Cain and Ajit Thyagarajan, "Internet Group Management Protocol, Version 3", IETF Internet Draft <draft-ietf-idmr-igmp-v3-00.txt>, Feb 1999
6. Norihiro Ishikawa, Nagatsugu Yamanouchi and Osamu Takahashi, "IGMP Extension for Authentication of IP Multicast", IETF Internet Draft <draft-ishikawa-igmp-auth-01.txt>, Aug 5 1998
7. Carl Rigney, Allan C.Rubens, William Allen Simpson and Steve Willens, "Remote Authentication Dial in User Service (RADIUS)", IETF Internet Draft <draft-ietf-radius-radius-v2-00.txt>, Feb 1999
8. N. Yamanouchi, N. Ishikawa and O.Takahashi, "RADIUS Extension for Multicast Router Authentication", IETF Internet Draft <draft-yamanouchi-radius-ext-00.txt>, March 1998
9. W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, Aug 1996
10. Gary C. Kessier, "An Overview of Cryptography", Internet Publication <http://www.hill.com/library/staffpubs/crypto.html>, Information Technology Department at Hill Associate, May 1998
11. Matthew J. Mayer and Josyula R.Rao and Pankaj Rohatgi, "A survey of security issues in Multicast Communications", IEEE Network p12-23, Nov/Dec 1999
12. T. Hardjono, B.Cain, and N. Doraswamy, "A Framework for Group Key Management for Multicast Security" IETF Internet Draft <draft-ietf-ipsec-gkmframework-01.txt>, Feb 1999
13. D.M. Wallner, E.J.Harder, and R.C.Agee, "Key Management for Multicast : Issue and Architectures", IETF Internet Draft <draft-wallner-key-arch-01.txt>, Sep 1998
14. H. Harney, C.Muckenhirn, "Group Key Management Protocol (GKMP) Architecture", RFC 2094, July 1997

Appendix

A. Multicast Certificate

In the proposed security multicast framework, several certificates which are designed with reference to the multicast group access control methodology mentioned in [2], are defined to identify the membership of a multicast group and the eligibility of a particular type of membership. Moreover, it is also used in the trustee identification of the GSA and the DR during the authentication process. The details of different type of certificate are explained below :

1. User-Certificate

Description

It is to certify that the user account as submitted by the Join-Request is valid and granted the permission by the local AS.

User Certificate

VERSION NUMBER (1 Octet)
ISSUER NAME (32 Octet)
VALIDITY PERIOD (4 Octet)
MULTICAST GROUP ADDRESS (4 Octet)
HOST IP ADDRESS (4 Octet)
USER ID LENGTH (1 Octet)
USER ID
DIGITAL SIGNATURE OF AS

(1.1) Version Number

The current version of the authentication protocol used by AS.

(1.2) Issuer Name

The name of the AS issuing the user certificate. The issuer name is expressed in the Domain Name System syntax.

(1.3) Validity Period

The period over which the user certificate is valid during the multicast session.

(1.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(1.5) Host IP Address

The IP address of the requesting host.

(1.6) User ID Length

The length of User ID measured in octet

(1.7) User ID

The User ID can be of variable length, maximum up to 255 character

(1.8) Digital signature of AS

The user certificate must be digitally signed by the local AS in order to be valid.

Multicast Host Certificate

VERSION NUMBER (1 Octet)
ISSUER NAME (32 Octet)
VALIDITY PERIOD (4 Octet)
MULTICAST GROUP ADDRESS (4 Octet)
HOST IP ADDRESS (4 Octet)
HOST TYPE (1 Octet)
CERTIFICATE TYPE (1 Octet)
DIGITAL SIGNATURE OF GSA

2. Multicast Host Certificate

Description

It is to certify that the Subnet/IP address as submitted by the Join-Request is valid and granted the permission to join the multicast group by the GSA of the virtual domain.

(2.1) Version Number

The current version of the secure IGMP .

(2.2) Issuer Name

The name of the GSA issuing the Multicast host certificate. The issuer name is expressed in the

Domain Name System syntax.

(2.3) Validity Period

The period over which the Multicast host certificate is valid during the multicast session.

(2.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(2.5) Host IP Address

The IP address of the requesting host.

(2.6) Host Type

The field indicates the type of host the certificate is issued for :

Value	Type	Description
0x01	Terminal	For multicast host joining the multicast group
0x02	Router	For multicast router routing the multicast traffic

(2.7) Certificate Type

The field indicates the type of action the host as granted to perform by the Multicast host certificate :

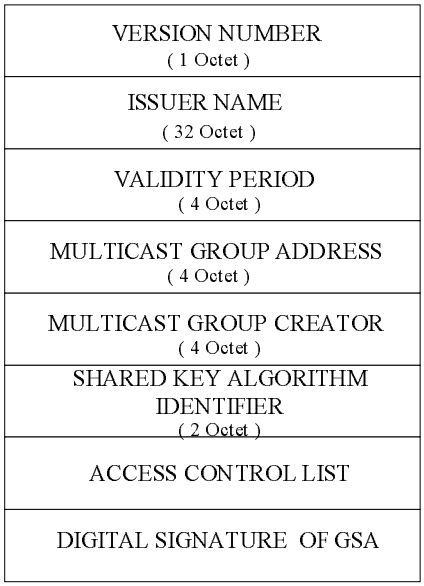
Value	Function
0x01	Multicast Receiver
0x02	Multicast Sender
0x03	Multicast Group Creator

3. Multicast GSA Certificate

Description

It is the certificate for a specific multicast group and is shared among the GSA for information replication. Once a multicast group is successfully created by a group creator, a corresponding Multicast GSA Certificate will be created by the GSA of the initiator ‘s virtual domain. The root GSA will be kept most-up-date and always hold the master copy and other GSA should synchronize with the root GSA periodically.

Multicast GSA Certificate



(3.1) Version Number

The current version of the GSA communication protocol .

(3.2) Issuer Name

The name of the GSA issuing the Multicast GSA certificate. The issuer name is expressed in the Domain Name System syntax.

(3.3) Validity Period

The period over which the Multicast GSA certificate is valid during the multicast session.

(3.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(3.5) Multicast Group Creator

The multicast group initiator is the host creating the multicast group for communication. The group initiator is represented by its IP address.

(3.6) Shared Key Algorithm Identifier

The identifier indicates the shared key encryption algorithm as adopted by the virtual domain owned by the GSA for the created multicast group. The value of the identifier represents exactly a specific algorithm.

(3.7) Access Control List

This is the Access Control List of the multicast group which records the accessibility of hosts.

The inclusion list includes those subnet/IP address, together with the join attributes on which the end systems are authorized to join the multicast group.

The exclusion list includes those subnet/IP address on which the end systems are not authorized to join the multicast group.

(3.8) Digital signature of GSA

The multicast GSA certificate must be digitally signed by the GSA issuing the certificate.

B. Message Format of Extended IGMP

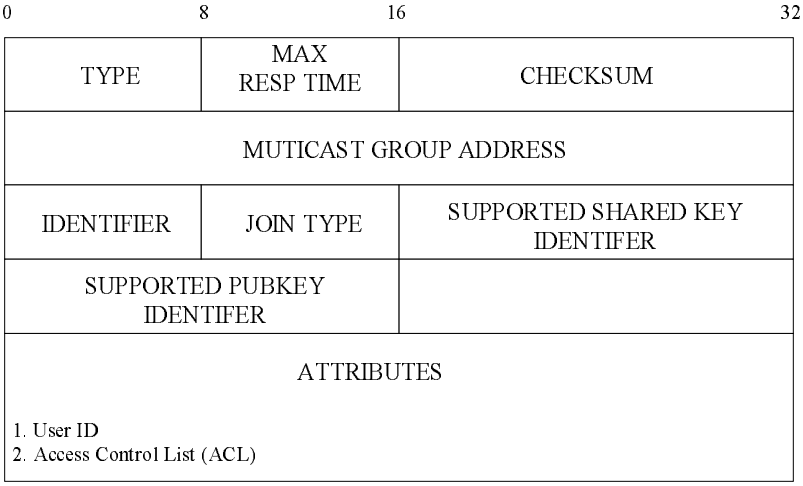
The new message format of Extended IGMP has made reference to the existing IGMP v3 as in [5] and the RADIUS extension protocol as in [8], the details of each message are explained as below:

1. Join-Request

Description

The message is to be sent by multicast host who intends to join a specific multicast group. The message is sent with destination IP address equal to All-Router-Address, and no encryption is needed.

Join-Request



(1.1) Type

Type field is set to 0x31

(1.2) Max Resp Time

It specifies the maximum response time allowed before the sender time out.

(1.3) Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the checksum field is set to zero. When receiving packets, the checksum must be verified before processing a packet.

(1.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(1.5) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier must be changed whenever the content of the request changes, and whenever a valid reply has been received for a previous request. For retransmissions, the Identifier must remain unchanged.

(1.6) Join Type

It identify the type of action the multicast host intends to perform :

Value	Action
0x01	Multicast Receiver
0x02	Multicast Sender
0x03	Multicast Group Creator

(1.7) Supported Shared Key Identifier

It identifies the shared key encryption algorithm in the virtual domain as supported by the multicast host. The identifier is a 16bit long variable, with each bit position indicating a particular encryption algorithm. A '1' in the particular bit position indicate the particular encryption algorithm is supported. For the multicast group creator, the identifier with zero value means that the multicast group should be created with security function turning off.

(1.8) Supported Pubkey Identifier

It identifies the public/private key encryption algorithm as supported by the multicast host. The identifier is a 16bit long variable, with each bit position indicating a particular encryption algorithm. A '1' in the particular bit position indicate the particular encryption algorithm is supported.

(1.9) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) UserID

It is the UserID of the user account which is used by the multicast host to login to the multicast group. The UserID will be authenticated by the local authentication server. The length of the UserID may up to 255 characters.

(b) Access Control List (Optional)

This control list is optional in the Join-Request. It only exists and valid for the Multicast Group Creator join type. The format of the Control List is shown as below:

Access Control List

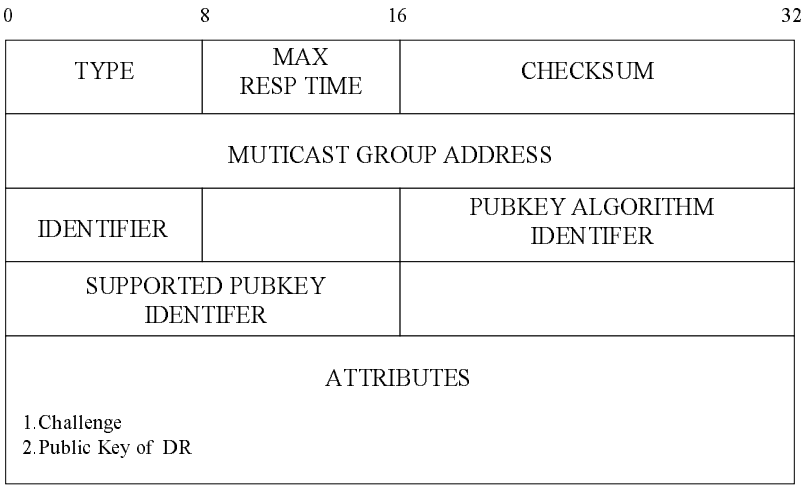
NO OF ASSIGNMENT (N) (1 Byte)
JOIN TYPE [1] (1 Byte)
HOST / SUBNET ADDRESS [1] (4 Byte)
FILTER MODE [1] (1 Byte)
. . . . .
JOIN TYPE [N] (1 Byte)
HOST / SUBNET ADDRESS [N] (4 Byte)
FILTER MODE [N] (1 Byte)

2. Router-Challenge

Description

The message is a response from the DR to multicast host who sends the Join-Request. The message is unicasted to the host, and no encryption is needed.

Router-Challenge



(2.1) Type

Type field is set to 0x32

(2.2) Max Resp Time

It specifies the maximum response time allowed before the sender time out.

(2.3) Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the checksum field is set to zero. When receiving packets, the checksum must be verified before processing a packet.

(2.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(2.5) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier is a copy of the Identifier field of the Join-Request message which caused this Router-Challenge.

(2.6) Pubkey Algorithm Identifier

The identifier indicate the public/private key encryption algorithm as adopted by the DR. The public key as attached in the attributes is generated based on this chosen algorithm. The value of the identifier represents exactly a specific algorithm.

(2.7) Supported Pubkey Identifier

It identifies the public/private key encryption algorithm as supported by the DR. The identifier is a 16bit long variable, which is exactly the same format as in Join-Request.

(2.8) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) Challenge

The joining host is given an unpredictable number of variable length and challenged to encrypt it and give back the result. The Challenge field contains the unpredictable number generated by the DR.

(b) Public key of DR

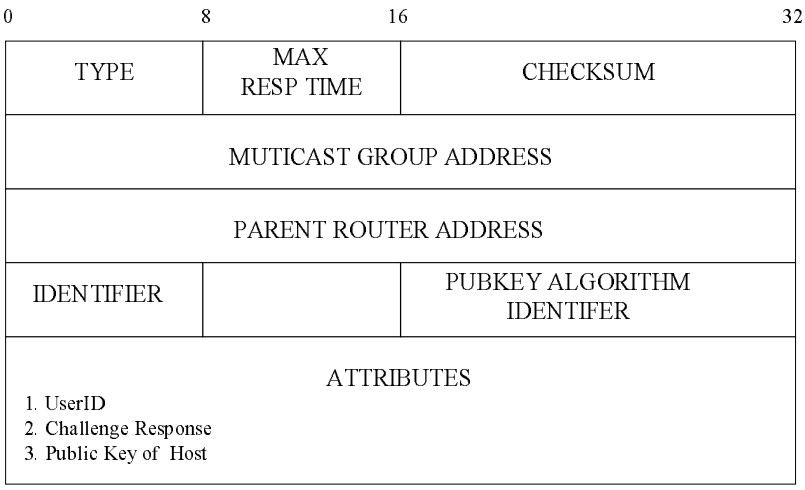
This is the public key of the designated multicast router used for encrypted communication between the designated multicast router and the multicast host.

3. Router-Response

Description

The message is a reply from multicast host to the DR, in receipt of the Router-Challenge. The message is directed to the DR, with destination IP address set to All-Router-Address, and encrypted using the public key of the DR.

Router-Response



(3.1) Type

Type field is set to 0x33

(3.2) Max Resp Time

It specifies the maximum response time allowed before the sender time out.

(3.3) Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the checksum field is set to zero. When receiving packets, the checksum must be verified before processing a packet.

(3.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(3.5) Parent Router Address

It is the IP address of the multicast router giving the Router-Challenge response to the Join-Request initiated by the host.

(3.6) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier is a copy of the Identifier field of the Join-Request message which caused this Router-Challenge.

(3.7) Pubkey Algorithm Identifier

The identifier indicate the public/private key encryption algorithm as adopted by the multicast host. The public key as attached in the attributes is generated based on this chosen algorithm. The value of the identifier represents exactly a specific algorithm.

(3.8) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) UserID

It is the User ID which is used by the multicast host to login to the multicast group. The User ID will be authenticated by the local authentication server.

(b) Challenge Response

The joining host is given an unpredictable number and challenged to encrypt it and give back the result. The Challenge Response field contains the encrypted challenge generated by the multicast host.

(c) Public key of Host

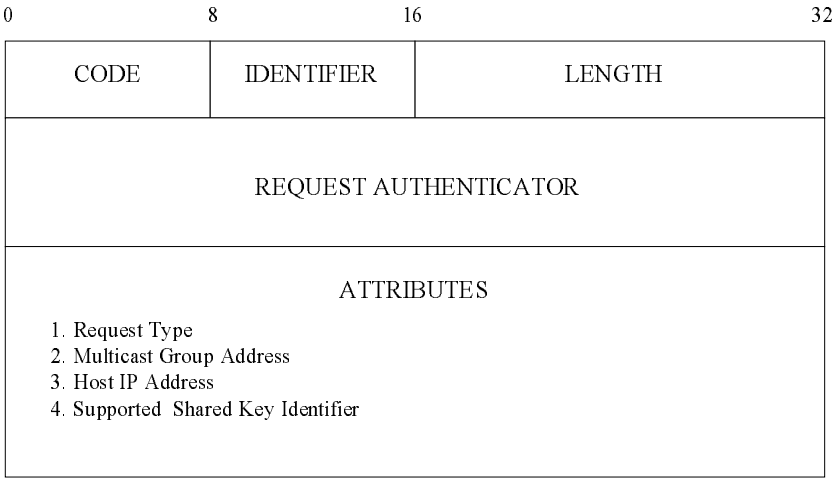
This is the public key of the multicast host used for encrypted communication between the designated multicast router and the multicast host.

4. GSA-Request

Description

The message is originated from the DR to the GSA, to make an authentication or key information request. The message is directed to the GSA, with destination IP address set to All-GSA-Address, and encrypted using the public key of the GSA.

GSA-Request



(4.1) Code

Code field is set to 0x01

(4.2) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier is a copy of the Identifier field of the Join-Request message or the Leave-Request which caused this GSA-Reqeust.

(4.3) Length

This part is the same as that of RADIUS. The length field is two octets. It indicates the length of the

packet including the Code, Identifier, Length, Authenticator and Attributes fields. Octets outside the range of the Length field should be treated as padding and should be ignored on reception. If the packet is shorter than the Length field indicates, it should be silently discarded.

(4.4) Request Authenticator

This part is the same as that of RADIUS. It is used to authenticate the messages between the requesting DR and the GSA. The authenticator is a 16 octets value containing one-way MD5 hash checksum calculated over a stream of octets consisting of the Code + Identifier + Length + 16 zero octets + attributes + shared secret (where + indicates concatenation). The most significant octet is transmitted first.

(4.5) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) Request Type

The value of the request type field indicates the type of request submitted to the GSA. Allowable value are :

Value	Request
0x01	Join as Multicast Receiver
0x02	Join as Multicast Sender
0x03	Join as Multicast Group Creator
0x04	Leave Multicast Group
0x05	Key Request

(b) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(c) Host IP Address

The IP address of the joining host. The GSA will authenticate the host based on this subnet/IP address.

(d) Supported Shared Key Identifier

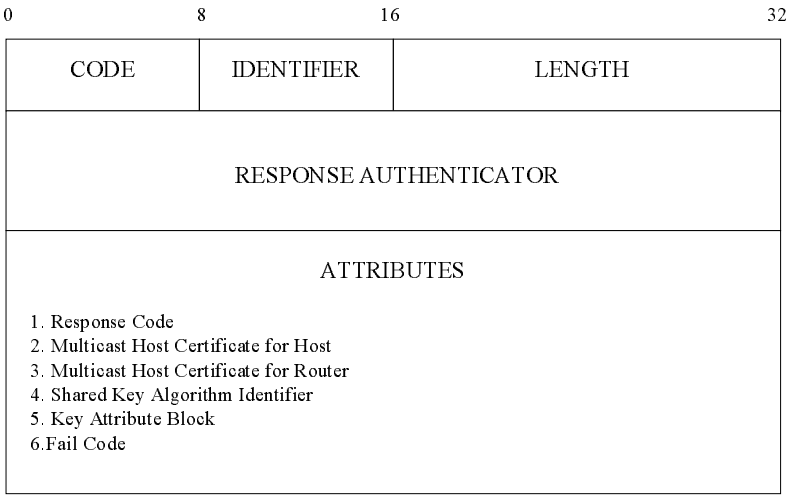
It identifies the shared key encryption algorithms in the virtual domain as supported by both the DR and the host. The identifier is a 16bit long variable, with each bit position indicating a particular encryption algorithm. A '1' in the particular bit position indicate the particular encryption algorithm is supported. For the multicast group creator, the identifier with zero value means that the multicast group should be created with security function turning off.

5. GSA-Response

Description

The message is a reply from the GSA to the DR, in receipt of the GSA-Resquest. The message is unicasted to the DR, , and encrypted using the public key of the DR.

GSA-Response



(5.1) Code

Code field is set to 0x02

(5.2) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier is a copy of the Identifier field of the GSA-Request message which caused this GSA-Response.

(5.3) Length

This part is the same as that of RADIUS. The length field is two octets. It indicates the length of the packet including the Code, Identifier, Length, Authenticator and Attributes fields. Octets outside the range of the Length field should be treated as padding and should be ignored on reception. If the packet is shorter than the Length field indicates, it should be silently discarded.

(5.4) Response Authenticator

This part is the same as that of RADIUS. It is used to authenticate the messages between the client and the authentication server. The authenticator is a 16 octets value containing one-way MD5 hash checksum calculated over a stream of octets consisting of the Code + Identifier + Length + request authenticator in the request packet + attributes + shared secret (where + indicates concatenation). The most significant octet is transmitted first.

(5.5) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) Response Code

The value of the response code field indicates the result of previous request. Allowable value are :

Value	Response
0x01	Success
0x02	Fail

(b) Multicast Host Certificate for Host

The Multicast host certificate for host is produced and digitally signed by the GSA as a certification that the requesting host has been successfully authenticated based on the subnet/IP address of the host.

(c) Multicast Host Certificate for Router (Optional)

The Multicast host certificate for router is produced and digitally signed by the GSA as a certification that the requesting router has been successfully authenticated. The certificate for the router only exist if the router has not been authenticated before.

(d) Shared Key Algorithm Identifier

The identifier indicate the shared key encryption algorithm as adopted by the GSA. The shared key as indicated in the attribute block is generated based on this chosen algorithm. The value of the identifier represents exactly a specific algorithm.

(e) Key Attribute Block

The block contains the necessary key information to be returned back to the DR on successful authentication of the requesting host.

(h) Fail Code

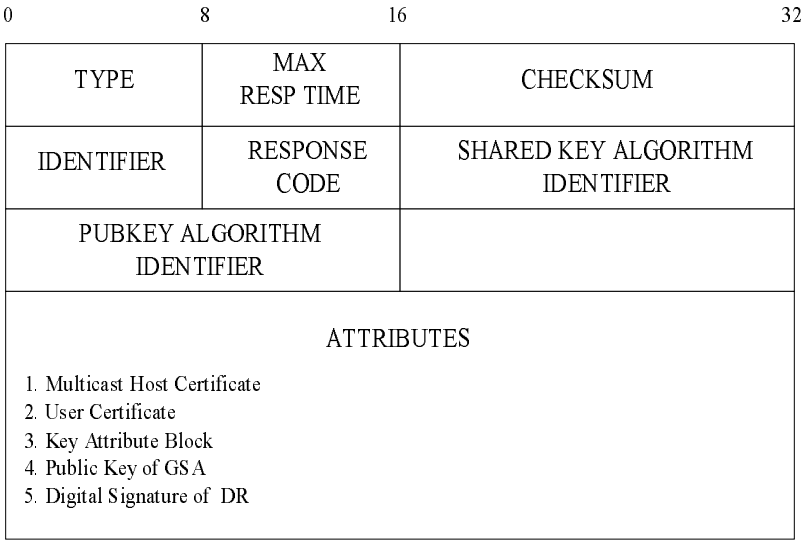
The value of the code represent the type of error occurred in the GSA authentication process, if the Response Code indicate a failure.

6. Join-Response

Description

The message is a reply from the DR to the multicast host who intends to join a specific multicast group. The message is unicasted to the host, and encrypted using the public key of the host.

Join-Response



(6.1) Type

Type field is set to 0x34

(6.2) Max Resp Time

It specifies the maximum response time allowed before the sender time out.

(6.3) Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the checksum field is set to zero. When receiving packets, the checksum must be verified before processing a packet.

(6.4) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier is a copy of the Identifier field of the Join-Request message which caused this Join-response.

(6.5) Response Code

The value of the response code field indicates the result of previous request. Allowable value are :

Value	Response
0x01	Success
0x02	Fail

(6.6) Shared Key Algorithm Identifier

The identifier indicate the shared key encryption algorithm as adopted by the GSA. The shared key as attached in the attributes is generated based on this chosen algorithm. The value of the identifier represents exactly a specific algorithm.

(6.7) Pubkey Algorithm Identifier

The identifier indicate the public/private key encryption algorithm as adopted by the GSA. The public key as attached in the attributes is generated based on this chosen algorithm. The value of the

identifier represents exactly a specific algorithm.

(6.8) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) Multicast Host Certificate

The Multicast host certificate for host is produced and digitally signed by the GSA as a certification that the requesting host has been successfully authenticated based on the subnet/IP address of the host.

(b) User Certificate

The user certificate is issued by the local authentication server to certify that the user account is authorised to join the mentioned multicast group.

(e) Key Attribute Block

The block contains the necessary key information to be returned back to the DR on successful authentication of the requesting host.

(g) Public Key of GSA

The public key of the GSA is distributed to the multicast host, so that the host can verify the message sent by GSA.

(h) Digital signature of DR

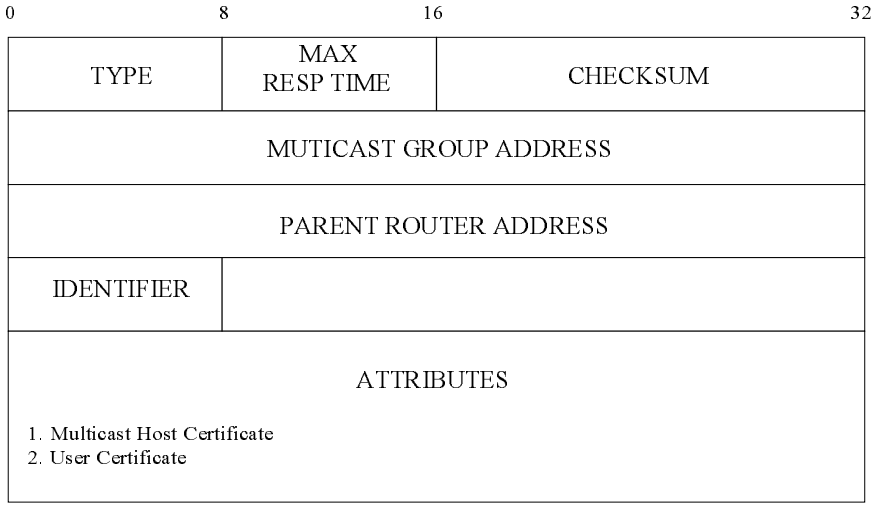
The whole message must be digitally signed by the DR in order to let the message can be authenticated by the multicast host.

7. Leave-Request

Description

The message is to be sent by multicast host who intends to leave a specific multicast group. The message is sent with destination IP address equal to All-Router-Address, and is encrypted using the public key of the DR.

Leave-Request



(7.1) Type

Type field is set to 0x35

(7.2) Max Resp Time

It specifies the maximum response time allowed before the sender time out.

(7.3) Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the checksum field is set to zero. When receiving packets, the checksum must be verified before processing a packet.

(7.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(7.5) Parent Router Address

It is the IP address of the multicast router giving the Router-Challenge response to the Join-Request initiated by the host.

(7.6) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier must be changed whenever the content of the request changes, and whenever a valid reply has been received for a previous request. For retransmissions, the Identifier must remain unchanged.

(7.7) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) Multicast Host Certificate

This is the certificate to certify that the host is authorised to join the corresponding multicast group

(b) User Certificate

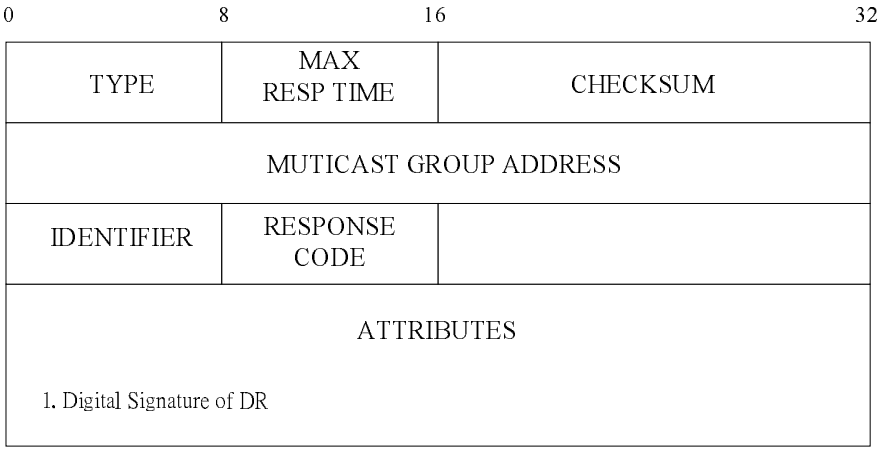
This is the certificate to certify that the user account is authorised to join the mentioned multicast group.

8. Leave-Response

Description

The message is a reply from the DR to the multicast host, in the receipt of Leave-Request. The message is unicasted to the multicast host, and is encrypted using the public key of the multicast host.

Leave-Response



(8.1) Type

Type field is set to 0x36

(8.2) Max Resp Time

It specifies the maximum response time allowed before the sender time out.

(8.3) Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the checksum field is set to zero. When receiving packets, the checksum must be verified before processing a packet.

(8.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(8.5) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier is a copy of the Identifier field of the Leave-Request message which caused this Leave-Response.

(8.6) Response Code

The value of the response code field indicates the result of previous request. Allowable value are :

Value Response

0x01 Success

0x02 Fail

(8.7) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

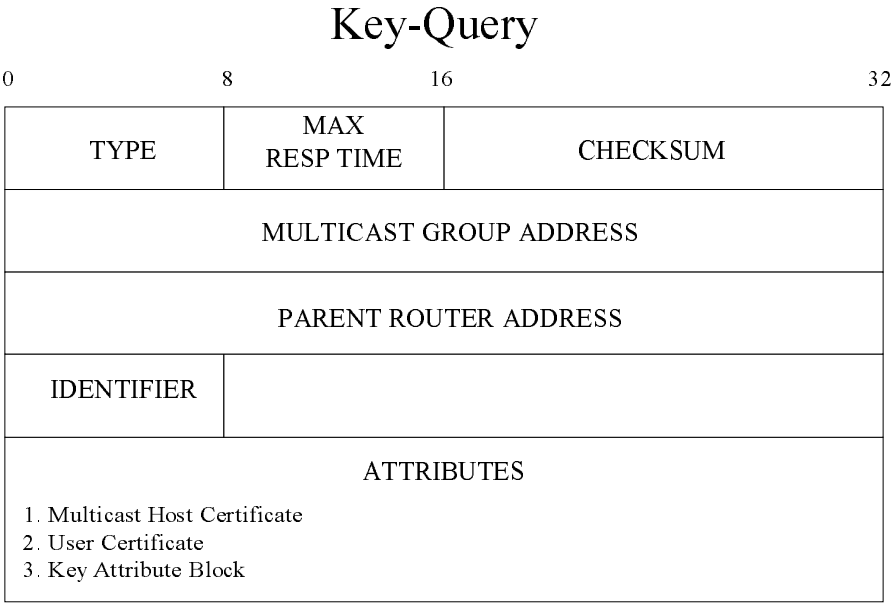
(a) Digital signature of DR

The presence of the digital signature of Router ensure that the message is originated from the trusted Designated multicast router.

9. Key-Query

Description

The message is to be sent by multicast host who intends to query the subgroup key for the virtual domain or any other keys used in group key management scheme. The message is sent with destination IP address equal to All-Router-Address, and is encrypted by the public key of DR.



(9.1) Type

Type field is set to 0x37

(9.2) Max Resp Time

It specifies the maximum response time allowed before the sender time out.

(9.3) Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the checksum field is set to zero. When receiving packets, the checksum must be verified before processing a packet.

(9.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(9.5) Parent Router Address

It is the IP address of the multicast router giving the Router-Challenge response to the Join-Request initiated by the host.

(9.6) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier must be changed whenever the content of the request changes, and whenever a valid reply has been received for a previous request. For retransmissions, the Identifier must remain unchanged.

(9.7) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) Multicast Host Certificate

This is the certificate to certify that the host is authorised to join the corresponding multicast group

(b) User Certificate

This is the certificate to certify that the user account is authorised to join the mentioned multicast group.

(c) Key Attribute Block

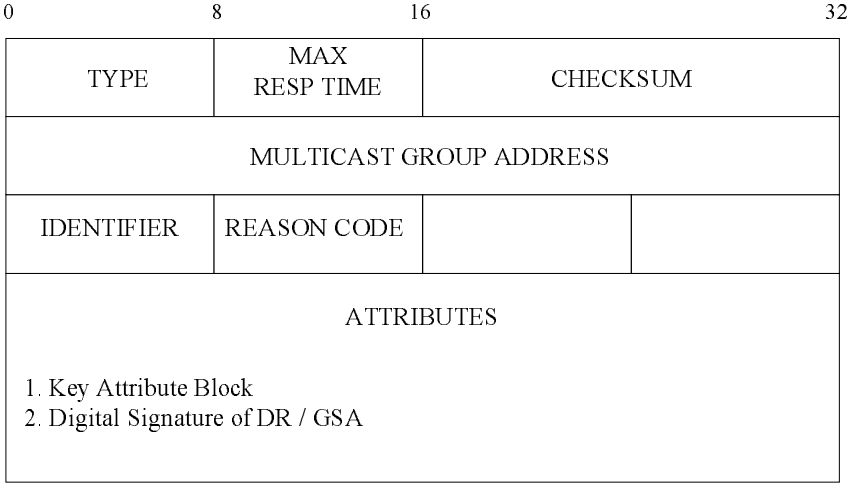
The block contains the key information to be queried by the host.

10. Key-Exchange

Description

The message can be originated by the DR or the GSA, in order to update the subgroup key or any other keys used in group key management scheme of the target receipient. The destination IP address may be a specific host address or a group address , depending on the receipient. When a multicast router receive a Key-Exchange message originated from GSA directed to it only, it will broadcast another Key-Exchange message to the members under its subnet.

Key-Exchange



(10.1) Type

Type field is set to 0x38

(10.2) Max Resp Time

It specifies the maximum response time allowed before the sender time out.

(10.3) Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the checksum field is set to zero. When receiving packets, the checksum must be verified before processing a packet.

(10.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(10.5) Identifier

The Identifier is one octet size, and aids in matching request and reply. If the message is a reply to the Key-Query, the Identifier should be a copy of the Identifier field of the Key-Query message. If the message is initiated by the DR or GSA, the Identifier field should be set to zero.

(10.6) Reason Code

The code indicate the reason why a change in subgroup key is needed.

Value	Reason
0x01	Member Join
0x02	Member Leave
0x03	Periodical Update
0x04	Host Query

(10.7) Key Type

The type code indicate what kind of key the message is referred to. The allowable type are :

Value	Key Type
0x01	Host shared key

0x02 Router group key

(10.8) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) Key Attribute Block

The block contains the necessary updated key information originated from GSA or DR.

(b) Digital signature of DR/ GSA

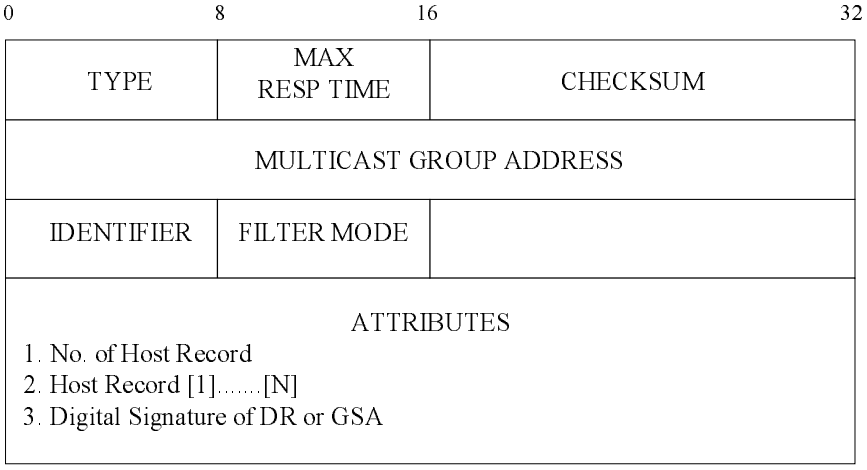
The whole message must be digitally signed by the DR or GSA in order to let the message to be verified by the multicast host.

11. Key-SelectedExchange

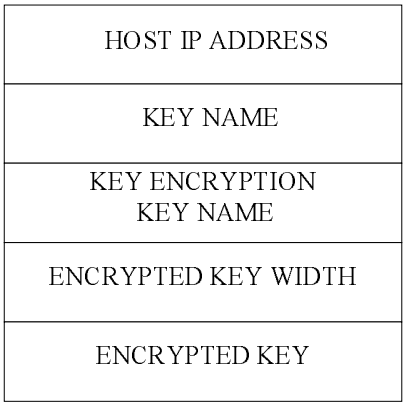
Description

The message can be originated by the DR or the GSA, in order to update the subgroup key or any other keys used in group key management scheme of the selected target receipient, which are already the members of a specific multicast group. The destination IP address may be a specific host address or a group address, depending on the receipent. When multicast routers receive a Key-SelectedExchange message originated from GSA directed to themselves, they will either broadcast a Key-Exchange or a Key-SelectedExchange message to the members under their subnets, in order to complete the key modification process.

Key-SelectedExchange



Host Record [N]



(11.1) Type

Type field is set to 0x39

(11.2) Max Resp Time

It specifies the maximum response time allowed before the sender time out.

(11.3) Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the checksum field is set to zero. When receiving packets, the checksum must be verified before processing a packet.

(11.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(11.5) Identifier

The Identifier is set to all zero as the message is initiated by the DR.

(11.6) Filter Mode

It indicates whether the listed IP address to be included or excluded.

Value	Filter mode
0x01	Inclusive
0x02	Exclusive

(11.7) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) No. of Host Record

The number of hosts to be the target receipient.

(c) Host Record

Each host record holds the required key information for a particular host. It consists of the IP address and a number of encrypted group keys. The keys in the host record are encrypted by the public key of the host, and can only be decrypted by using the private key of the target host of the same IP address.

(c) Digital signature of DR or GSA

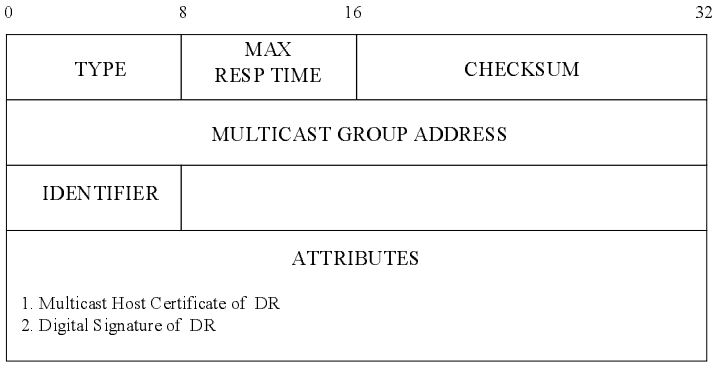
The presence of the digital signature of the DR ensure that the message is originated from the trusted Designated multicast router.

12. Certificate-Query

Description

The message is originated from the designated multicast router to the target host, to query the certificates held by the host, in order to verify its identity.

Certificate-Query



(12.1) Type

Type field is set to 0x40

(12.2) Max Resp Time

It specifies the maximum response time allowed before the sender time out.

(12.3) Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the checksum field is set to zero. When receiving packets, the checksum must be verified before processing a packet.

(12.4) Multicast Group Address

It is the Class D IP address assigned to the multicast group

(12.5) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole key query and reply process.

(12.6) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) Multicast Host Certificate of DR

This is the certificate to certify that the DR has been authorised to join the corresponding multicast group.

(b) Digital Signature of DR

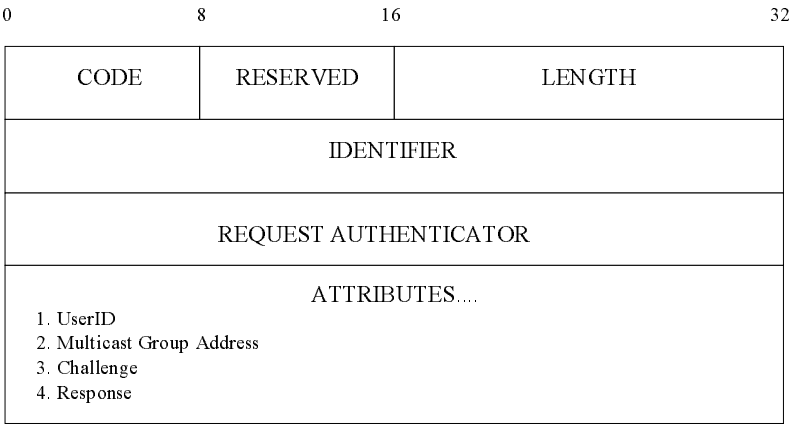
This is the digital signature signed by DR.

13. AS-Request

Description

The message is originated from the designated multicast router to the AS, in receipt of the Router-Response. The message is directed to the AS, and encrypted by using the public key of AS.

AS-Request



(13.1) Code

Code field is set to 0x01

(13.2) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier must be changed whenever the content of the request changes, and whenever a valid reply has been received for a previous request. For retransmissions, the Identifier must remain unchanged.

(13.3) Length

This part is the same as that of RADIUS. The length field is two octets. It indicates the length of the packet including the Code, Identifier, Length, Authenticator and Attributes fields. Octets outside the range of the Length field should be treated as padding and should be ignored on reception. If the packet is shorter than the Length field indicates, it should be silently discarded.

(13.4) Request Authenticator

This part is the same as that of RADIUS. It is used to authenticate the messages between the client and the authentication server. The authenticator is a 16 octets value containing one-way MD5 hash checksum calculated over a stream of octets consisting of the Code + Identifier + Length + 16 zero octets + Attributes + shared secret (where + indicates concatenation). The most significant octet is transmitted first.

(13.5) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) UserID

The UserID represent the user account used by the multicast host to join the multicast group.

(b) Multicast Group Address

It is the Class D IP address assigned to the multicast group.

(c) Challenge

The Challenge field contains the original unpredictable number generated by the DR.

(d) Response

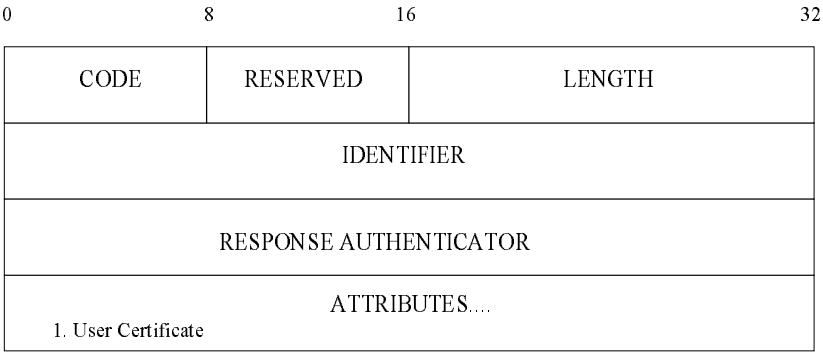
The Response field contains the encrypted response to the challenge generated by the multicast host.

14. AS-Accept

Description

The message is a reply from the AS to the designated multicast router in receipt of the AS-Request, if user authentication is successful. The message is directed to the DR, , and encrypted using the public key of the DR.

AS-Accept



(14.1) Code

Code field is set to 0x02

(14.2) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier is a copy of the Identifier field of the AS-Request message which caused this AS-Accept.

(14.3) Length

This part is the same as that of RADIUS. The length field is two octets. It indicates the length of the packet including the Code, Identifier, Length, Response Authenticator and Attributes fields. Octets outside the range of the Length field should be treated as padding and should be ignored on reception. If the packet is shorter than the Length field indicates, it should be silently discarded.

(14.4) Response Authenticator

This part is the same as that of RADIUS. It is used to authenticate the messages between the client and the authentication server. The authenticator is a 16 octets value containing one-way MD5 hash checksum calculated over a stream of octets consisting of the Code + Identifier + Length + Request authenticator in the AS-Request packet + Attributes + shared secret (where + indicates concatenation). The most significant octet is transmitted first.

(14.5) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) User Certificate

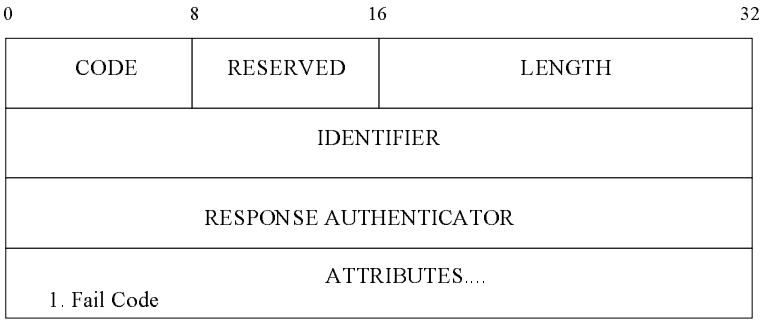
The user certificate is issued by the local authentication server to certify that the user account is authorised to join the mentioned multicast group.

15. AS-Reject

Description

The message is a reply from the AS to the designated multicast router in receipt of the AS-Request, if user authentication is failed. The message is directed to the DR, , and encrypted using the public key of the DR.

AS-Reject



(15.1) Code

Code field is set to 0x03

(15.2) Identifier

The Identifier is one octet size, and aids in matching request and reply for the whole authentication process. The Identifier is a copy of the Identifier field of the AS-Request message which caused this AS-reject.

(15.3) Length

This part is the same as that of RADIUS. The length field is two octets. It indicates the length of the packet including the Code, Identifier, Length, Response Authenticator and Attributes fields. Octets outside the range of the Length field should be treated as padding and should be ignored on reception. If the packet is shorter than the Length field indicates, it should be silently discarded.

(15.4) Response Authenticator

This part is the same as that of RADIUS. It is used to authenticate the messages between the client and the authentication server. The authenticator is a 16 octets value containing one-way MD5 hash checksum calculated over a stream of octets consisting of the Code + Identifier + Length + Request authenticator in the AS-Request packet + Attributes + shared secret (where + indicates concatenation). The most significant octet is transmitted first.

(15.5) Attributes

The attributes field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes. The following parameters are to be included in the message :

(a) Fail Code

The value of the code represent the type of error occurred in the user authentication process by the authentication server

16. Extended Membership Report

Description

The extended membership report is same as current V3 membership report except an additional field "Parent Router Address" is added. The field is used to distinguish which multicast router will be responsible to the request raised by the host and store the member database.

The format of the extended membership report is shown as below :

Extended Membership Report

TYPE	RESERVED	CHECKSUM
RESERVED		NUMBER OF GROUP RECORDS (N)
PARENT ROUTER ADDRESS		
GROUP RECORD[1]		
.....		
GROUP RECORD[N]		

GROUP RECORD

RECORD TYPE	RESERVED	NUMBER OF SOURCES (N)
MULTICAST ADDRESS		
SOURCE ADDRESS [1]		
.....		
SOURCE ADDRESS [N]		

17. Certified Membership Report

Description

The certified membership report is sent by the multicast host to the DR, to certify its identity when queried by the Certificate-Query message. The report is sent with destination IP address set to All-Router-Address and encrypted by the public key of DR.

When compared with the normal version 3 membership report, there are 3 more additional pieces of information :

(a) Public key of the sending host

The public key of the host is required so that the DR can add the host's information to its router member database in case of successful authentication.

(b) Multicast Host Certificate

The certificate is included in the group record to certify its membership by subnet/IP address basis. If the host has joined more than one group on the interface, each group record should have its own certificate.

(c) User Certificate

The certificate is included in the group record to certify its membership by user account basis. If the host has joined more than one group on the interface, each group record should have its own certificate.

The format of the certified membership report is shown as below :

Certified Membership Report

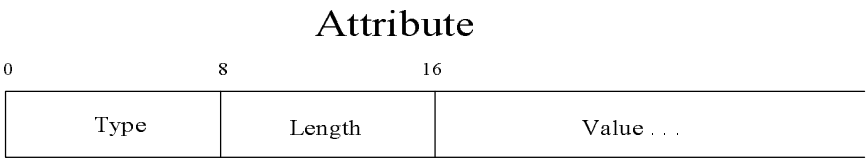
TYPE	RESERVED	CHECKSUM
RESERVED		NUMBER OF GROUP RECORDS (N)
PARENT ROUTER ADDRESS		
GROUP RECORD[1]		
.....		
GROUP RECORD[N]		
PUBLIC KEY OF HOST		

GROUP RECORD

RECORD TYPE	RESERVED	NUMBER OF SOURCES (N)
MULTICAST ADDRESS		
MULTICAST HOST CERTIFICATE		
USER CERTIFICATE		
SOURCE ADDRESS [1]		
.....		
SOURCE ADDRESS [N]		

18. Attribute Format

The Attributes field is variable in length, and contains a list of zero or more attributes. The attributes carry the specific authentication, authorization information and configuration details for the request and reply messages. A summary of the Attribute format is shown below. The fields are transmitted from left to right.



(A) Type

The type field is one octet long and indicates the meaning of the attribute as followed.

(B) Length

The length field is one octet long, and indicates the length of the attribute including the Type, Length and Value fields. If an Attribute is received with an invalid length field, the request or reply should be silently discarded.

(C) Value

The value field is zero or more octets and contains information specific to the Attribute. The format and length of the Value field is determined by the Type and Length fields.

19. Key Attribute Block

It defines the format of the key attributes to be passed between the entities. Since the protocol is designed to support different type of group key management scheme, a general parameter block for exchanging key information is needed. The subgroup key, which is used in a specific virtual domain, can be one of items in the key attribute block.

Key Attribute Block

KEY NAME [1]
KEY ENCRYPTION KEY NAME [1] (Optional)
ENCRYPTED /UNENCRYPTED KEY LENGTH [1]
ENCRYPTED /UNENCRYPTED KEY [1]
. . . . .
KEY NAME [N]
KEY ENCRYPTION KEY NAME [N] (Optional)
ENCRYPTED /UNENCRYPTED KEY LENGTH [N]
ENCRYPTED /UNENCRYPTED KEY [N]

(19.1) Key Name

Each key used in the extended IGMP is assigned a corresponding key name so that it can be referenced in the subsequent communication.

(19.2) Key Encryption Key Name

It is the name of the key used to encrypt the target key which is to be passed to the designated receipient.

(19.3) Encrypted / Unencrypted Key Length

It indicates the length of the key in the next field, for which the key is either encrypted or unencrypted.

(19.4) Encrypted / Unencrypted Key

It is the actual key to be passed in the attribute block, for which the key is either encrypted or unencrypted.

List of Additional Timer and **Couner Variables**

Additional Timers

(1) Maximum Response Time for messages

It defines the maximum allowed time before the sending message becomes expired. If there is no any response from the target recipient, the sender will time out the sending message. To cater the

different scenarios for both broadcast and unicast message, separate values can be identified :

(a) Maximum Response Time for broadcast message

(b) Maximum Response Time for unicast message

Additional Counters

(1) Robustness Variable

It allows the tuning for the expected packet loss on a subnet. If the subnet is expected to be lossy, the robustness variable may be increased. IGMP message is robust to (Robustness Variable –1) packet losses. To cater the different scenarios for both broadcast and unicast message, separate values can be identified :

(a) Robustness Variable for broadcast message

(b) Robustness Variable for unicast message

(2) Failed Decryption Threshold

It determines the maximum allowed failed decryption of multicast data messages experienced by an IGMP host before sending an IGMP Key-Query message.

(3) Join-Request Timeout Counter

It defines the maximum no. of timeout as experienced by the Join-Request messages sent by an IGMP host before going into the IGMP v3 compatible state.