1-1-2005

A secure multicast architecture and protocol for MOSPF

Junqi Zhang
Macquarie University

Yi Mu
University of Wollongong, ymu@uow.edu.au

Vijay Varadharajan
Macquarie University

A secure multicast architecture and protocol for MOSPF

Abstract

Multicast Open Shortest Path First (MOSPF) is an en hancement to unicast routing protocol OSPF. It has been widely used in many multicast applications for years. How ever, its security is still a major concern in some applica tions. Much work has been done on data protection, but only a few works have been done on member access con trol mechanisms. In this paper, we present a new secure multicast architecture and protocol for MOSPF from the perspective of member access control. Our new model in cludes a variant of previous access control mechanism and a novel distributed encryption scheme. This architecture in particular meets the access control security needs of dense multicast routing protocol in MOSPF, simplifies the access control process, and increases scalability and flexibility in revocation and reauthorization.

Keywords

Secure, Multicast, Architecture, Protocol, for, MOSPF

Disciplines

Physical Sciences and Mathematics

Publication Details

Mu, Y., Zhang, J. & Varadharajan, V. (2005). A secure multicast architecture and protocol for MOSPF. In M. Hamza, P. Prapinmonkolkarn & T. Angkaew (Eds.), Proceedings of the IASTED International Conference Networks and Communication Systems (pp. 120-125). Anaheim, California, USA: ACTA Press.

A SECURE MULTICAST ARCHITECTURE AND PROTOCOL FOR MOSPF

J. Zhang
Department of Computing
Macquarie University
North Ryde, NSW 2109, Australia
email: janson@ics.mq.edu.au

V. Varadharajan
Department of Computing
Macquarie University
North Ryde, NSW 2109, Australia
email: vijay@ics.mq.edu.au

Y. Mu
School of Information Technology
and Computer Science
University of Wollongong
Wollongong, NSW 2522 Australia
email: ymu@uow.edu.au

ABSTRACT

Multicast Open Shortest Path First (MOSPF) is an enhancement to unicast routing protocol OSPF. It has been widely used in many multicast applications for years. However, its security is still a major concern in some applications. Much work has been done on data protection, but only a few works have been done on member access control mechanisms. In this paper, we present a new secure multicast architecture and protocol for MOSPF from the perspective of member access control. Our new model includes a variant of previous access control mechanism and a novel distributed encryption scheme. This architecture in particular meets the access control security needs of dense multicast routing protocol in MOSPF, simplifies the access control process, and increases scalability and flexibility in revocation and reauthorization.

KEY WORDS

MOSPF, Access Control, Multicast

1 Introduction

Multicasting provides an efficient communication mechanism in both private networks and Internet for large-scale content distribution, such as audio and video conferences, web casting, interactive game and video on demand. There are three basic types of multicast routing protocols: distance vector, link state and shared trees [1]. MOSPF belongs to the category of link state [2, 3]. MOSPF is also called dense-mode multicast routing protocol, because it requires some form of flooding of datagrams to the network to find multicast routes. This protocol is suitable for areas with dense concentrations of group members.

MOSPF is widely used in multicast but the security issues are still a concern where confidential and high value content are being transferred. Based on the properties of the multicast, the components that should be secured include[4, 5]: multicast distribution tree protection, end-to-end data protection through cryptographic operations and member access control. The end-to-end data protection includes data integrity, source authentication and data confidentiality. The main method used to protect the data is group key encryption, in which the multicast traffic is encrypted with a symmetric key and all authorized group members are given the decryption key. Many schemes were proposed to provide the efficient re-keying for the group key management protocol [6, 7]. These methods can become very complicated because the membership is dynamic. In addition, as mentioned in [4], there are some other related issues where encryption of communications may not be possible for legal reasons; furthermore, even where data confidentiality is provided, it may be possible to do traffic analysis depending on the layer where encryption is done.

Because of the above reasons, research was done to develop group access control schemes as an additional security mechanism [5, 8, 9]. In this paper, we propose a new secure multicast scheme and protocol for MOSPF based on a broadcasting encryption scheme.

The rest of this paper is organized as follows. Section 2 introduces the security architecture for multicast and the Internet Group Management Protocol (IGMP) and reviews the proposed member access control schemes. Section 3 describes the MOSPF protocol architecture. Section 4 gives the novel distributed encryption scheme that is used in the scheme. Section 5 presents our new secure multicast architecture and protocol for MOSPF. Finally, in section 6, we give some concluding remarks.

2 Security Architecture for Multicasting

This section briefly reviews security architecture, Internet Group Management protocol and related proposed work [10, 11, 5, 9].

The multicast security (MSEC) working group of the Internet Engineering Task Force (IETF) presents a multicast security architecture reference framework (Figure 1). This Reference Framework is used to classify functional areas, functional elements, and interfaces. In Figure 1, the boxes are the functional entities and the arrows are the interfaces between them.

There are three sets of functional entities and three

functional areas. The three sets of functional entities are the Policy Server, Group Controller and Key Server (GCKS), Sender and Receiver.

The three functional areas are Multicast data handling, Group key Management, and the Multicast security policies. Multicast data handling covers problems concerning the security-related treatments of multicast data by the sender and the receiver. Typically, the data needs to be encrypted by group key and authenticated in a secure multicast group. Group Key Management is concerned with the secure distribution and refreshment of keying material. The keying material refers to the cryptographic key belonging to a group, the state associated with the keys and the other security parameters related to the keys. The multicast security policies cover aspects of policy in the context of multicast security and must provide the rules for operation for the other elements of the Reference Framework. Our new secure multicast architecture and protocol for MOSPF will follow this reference framework.

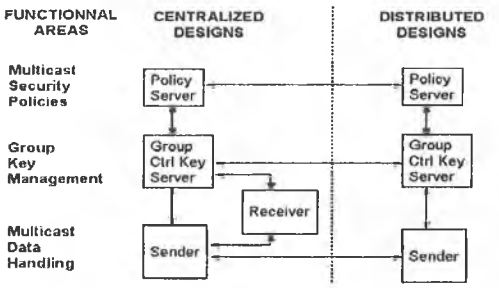

Figure 1. Multicast Security Architecture Reference Framework

2.1 IGMP Protocol

The Internet Group Management Protocol (IGMP) is the protocol through which hosts exchange information with their local routers. This protocol is specified in [11]. It is used by IPv4 systems (hosts and routers) to report their IP multicast group memberships to any neighboring multicast routers. IGMP lets a router keep track of IP membership on its local LANS by 2 types IGMP messages: sending IGMP host membership queries and receiving IGMP host membership reports.

We note that the multicast provides an open group model. This open model has many beneficial aspects, but it also causes security issues, as it cannot control membership to a set of authorized hosts. Security problems include eavesdropping, theft of service, denial of service and possibly cryptanalysis. The next section will discuss possible solutions to addressing these issues.

2.2 Member Access Control Schemes

As mentioned before, the open group model properties of the multicast may cause serious security problems. On the other hand, the traditional methods used to cryptographically encrypt information cannot solve these problems. To solve these security problems, we need to control the ability of hosts to join the multicast group. There are three functions required for multicast receiver access control. It includes group policy specification functions, access request functions and access control functions [4, 9]. The proposed solutions can be found in [5, 9, 12]. Depending upon the type of revocation provided, these multicast receiver authorization solutions are classified into three types: centralized, ACL supported and time-limited.

In [5], Hardjono and Cain present an approach that makes use of the existing Group Key management protocol for host members of a group to deliver the IGMP keying material to the host and the multicast distribution tree to deliver the necessary keying material to the multicast routers. The receiver host sends a join request including the access token to the router, and the router verifies the access token in the token list. In [12], Ballardie and Crowcroft present a version of IGMP that allows receivers to be authorized before joining the group. The architecture includes the group owner (the initiator), the authorization server, the routers and the receiver hosts. The group owner (the initiator) distributes the ACLs to the authorization servers. The receiver host sends a request to an authorization server to obtain an authorization stamp. When the receive host joins this group, it sends a join request to the router with this authorization stamp. Then the router forwards the receiver host's request to the authorization server for approval. In [9], Judge and Ammar proposed a comprehensive architecture GOTHIC for providing group access control.

2.2.1 Gothic Architecture

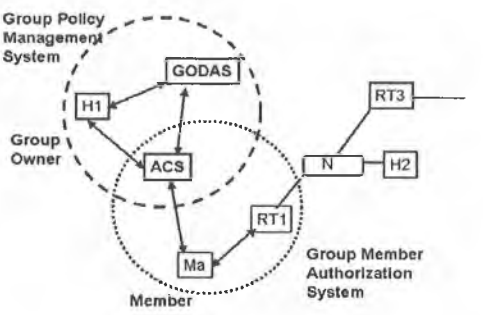

Figure 2. Gothic Architecture

In this section, we briefly describe the Gothic architecture proposed in [9]. Our new scheme extends the Gothic architecture and provides a novel group key management scheme that enables the management of multicast groups to be efficient. The Gothic includes two systems: the group policy management system and the group

member authorization system (Figure 2). The group policy management system performs group policy specification functions. It includes three components: the group owner, the group owner determination and authentication system (GODAS), and the access control server (ACS). The group owner provides the security policy for the group and the list of the authorized members to the ACS. The group owner determination and authentication system (GODAS) provide the system to verify that the host is the group owner. The group member authorization system carries out access request functions and access control functions. This system involves the interaction among the host, the router and the ACS.

This system works as follows. First, the group owner contacts the ACS, and the ACS performs the authentication and authorization. Then the group owner provides the group policy to the ACS. Next, the receiver hosts request a capability from the ACS. These capabilities are identity based and time limited. After this, the receiver host can send a join request along with the capabilities that it received from its ACS to the router. The router host authenticates the receiver host and verifies the capabilities. Finally, the receiver host is allowed to join the group.

3 MOSPF (Multicast Open Short Path First) Architecture

In this section, we will briefly introduce the MOSPF architecture [3]. Figure 3 shows a sample a MOSPF configuration (Nx-the network, RTx- the router, M-the member, H-the host, number is the cost from the routers to network).

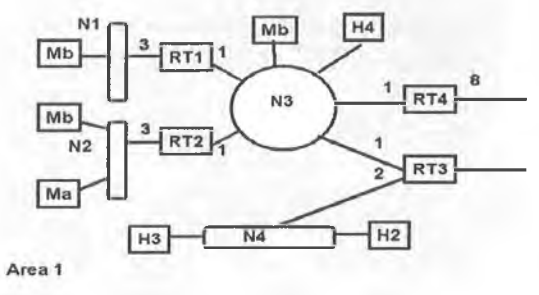

Figure 3. MOSPF Architecture

MOSPF is an extension to OSPF unicast routing protocol. OSPF routers use link state advertisements (LSAs) to understand all available links in the network and route datagram along least cost paths. MOSPF includes multicast information in OSPF link state advertisements (LSAs) to construct multicast distribution trees. All MOSPF routers maintain an up-to-date image of the topology of the entire network. The path of the multicast datagram depends on both the datagram's source network and destination multicast group. Group membership LSAs are flooded throughout the OSPF routing domain so MOSPF routers can compute outgoing interface lists. The MOSPF routers use the Dijkstra algorithm to compute shortest path tree for each group.

Each MOSPF router in the distribution tree for each source/destination combination bases its forwarding decision on forwarding cache. A forwarding cache entry is built from local group database and datagram's shortest path tree. The local group database records the group membership of the router's directly attached networks. This local group database is built from the Internet Group Management Protocol (IGMP). In multi-access network, one router is selected as Designated Router (DR); this Designated Router originates a network links advertisement on behalf of the network and becomes adjacent to all other routers on the network. The router updates the local group database when the membership state is changed. The datagram's shortest path tree depicts the intermediate hops taken by a multicast datagram when it is sent from the source to the individual group members. This shortest path tree is built on demand. It is built by using the router-LSAs and network-LSAs in the link states database and having the source network as root. The branches that do not include the router and transit networks are pruned from the tree.

For our new secure multicasting protocol, we need to add the encryption key into the LSA control messages, so that all the routers can store the encryption key to verify the prospective members.

4 Key Generation Algorithm

Our approach involves the proposal of a dynamic group key management scheme that enables secure and efficient updating of group members. We achieve this by constructing a public key that is associated with several associated private keys. Our proposal for secure multicasting is based on our earlier work on key distribution described in [13].

4.1 Preliminaries

The security of our scheme is based on the difficulty of computing discrete logarithms, and the protocols are based on the polynomial functions and a set of exponentials.

Let N be a composite of two large primes,p, q, $\mathbb{Z}_N^*$ be a multiplicative group of order $\phi(N) = (p-1)(q-1)$, and $g \in \mathbb{Z}_{\phi(N)}$ be a generator, Let $x_i \in_R \mathbb{Z}_q$ for $i = 0, 1, 2, ..., n$ be a set of integers. A polynomial function of order n is constructed as follows: $f(x) = \prod_{i=1}^{n}(x - x_i) \equiv \sum_{i=0}^{n} a_i x^i \bmod \phi(N)$, where the a_i are coefficients: $a_0 = \prod_{j=1}^{n}(-x_j)$, $a_1 = \sum_{i=1}^{n}\prod_{i\neq j}^{n}(-x_j)$,..., $a_{n-2} = \sum_{i\neq j}^{n}(-x_i)(-x_j)$, $a_{n-1} = \sum_{i=1}^{n}(-x_j)$, $a_n = 1$. Note that $f(x_j) = \sum_{i=0}^{n} a_i x_j^i = 0$. We can use this property to construct a broadcasting encryption system. Note that we

require $\phi(N)$ to be a composite of a large set of primes in order to generate keys.

Having the set $\{a_i\}$, we can then construct the corresponding exponential functions,

$$\{g^{a_0}, g^{a_1}, g^{a_2}, ..., g^{a_n}\} \equiv \{g_0, g_1, g_2, ..., g_n\}.$$

4.2 System Setup

The construction of the encryption and decryption keys is done as follows:

- Select n distinct random numbers $x_i \in \mathbb{Z}_{\phi(N)}$ for $i = 1, 2, \cdots, n$, which form a set X_n and a subset $X_m \subset X_n$.
- Compute $A = \prod_{j=1}^{n}(\prod_{i=0}^{n-1} g_i^{x_j^i}) \bmod N$. Note that A is computed once only. We will see later, a dynamic further updates of the system do not require recomputation of A.
- Select an integer $b \in \mathbb{Z}_{\phi(N)}$ and compute its multiplicative inverse b^{-1} such that $bb^{-1} = 1 \bmod \phi(N)$.
- Compute $\bar{x}_j = b^{-1} \sum_{i \neq j}^{n} x_i^n \bmod \phi(N)$, for $j = 1, 2, ..., n$.
- Compute $\hat{x}_j = s_j x_j^n$, where

$$s_j = s_1' s_2' \cdots s_n', \; s_j s_j' = s_j' \bmod \phi(N), \; s_j, s_j' \in \mathbb{Z}_{\phi(N)}.$$

We note that this construction requires $\phi(N)$ to be a composite of many primes; therefore, $\phi(N)$ must be properly chosen to suit this construction.

These values satisfy the equality:

$$A^s g^{sb\bar{x}_j} g^{s\hat{x}_j} = 1 \bmod N, \quad \forall j \in \{1, 2, \cdots, n\}.$$

A is kept by the authorized server and will be used as the encryption key. Since the encryption key is not public, there is no need for us to protect it against any illegal modification.

$\bar{x}_j$ and $\hat{x}_j$ are given to user j as its secret decryption key during the process of its registration. Hence the private decryption key doublet is $(\bar{x}_j, \hat{x}_j)$. Please note that computation of A is a one-time task. The server does not need to modify it during a system update.

4.3 Multicasting Encryption Protocol

The encryption key A is used to encrypt a session key that is then used to encrypt a message. All members in the group can decrypt the session key and then decrypt the message individually with their private keys. Let us suppose that M is the message to be encrypted and k is a session key.

The protocol is as follows:

- Select an integer $r \in_R \mathbb{Z}_{\phi(N)}$.
- Compute $\bar{g} = g^{sr} \bmod N$ and $\hat{g} = g^{sbr} \bmod N$.
- Compute the ciphertext $c = E_k(M)$ and $k' = kA^{sr} \bmod N$, where $E_k(.)$ denotes a symmetric key encryption function.
- Broadcast the 4-tuple $(\bar{g}, \hat{g}, c, k')$ to all subscribers.

To decrypt the session key, the user j computes $k'\hat{g}^{\bar{x}_j}\bar{g}^{\hat{x}_j} = k \bmod N$. k is then used for the decryption of the message.

5 A New Secure Multicast Architecture for MOSPF

In this section, we will present our new secure multicast architecture and protocol for MOSPF. As we discussed before, traditional methods are still prone to threats such as eavesdropping, theft of service, or denial of service. The proposed solutions are inadequate for large dynamic multicast group memberships. Our new secure multicast scheme for MOSPF is partly based on the Gothic architecture mentioned earlier; it includes two systems namely the group key and policy management system and the group member authorization systems (Figure 4).

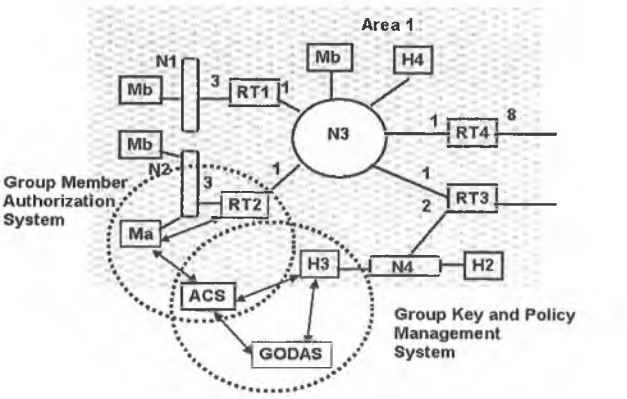

Figure 4. Secure Multicast Architecture for MOSPF

5.1 Group Key and Policy Management System

Except for the group policy specification functions mentioned before in the Gothic system, the group key and policy management system also performs the access control key generation and group session key generation functions. The group key and policy management system involves three parts: the group owner (for example, Host3 in Figure 4), the access control server (ACS) and the group owner determination and authentication systems (GODAS). The group owner generates group access control keys, group keys for the group. It also provides the list of authorized members and other security policy for the group to ACS. The multicast security policy can be referred to [14]. The access control server (ACS) is used to verify and authorize the prospective member, and it also involves in the group

member authorization system. The group owner determination and authentication systems (GODAS) can be used to verify that the host is the group owner [9].

The first solution makes use of group certificates (Figure 5). This is similar to traditional digital certificates.

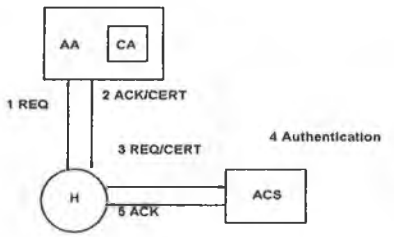

Figure 5. Group Owner Certificates

The second solution is the use of a group ownership service (Figure 6). This service is a query/reply protocol based service. It works in 4 different multicast environments. It includes the multicast address allocation architecture (MAAA), the source specific multicast (SSM), GLOP, and Session Announcement Protocol (SAP) / Session Description Protocol (SDP).

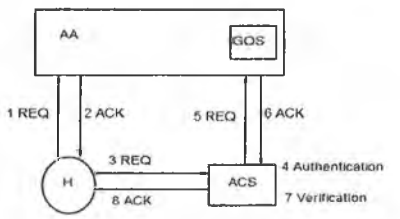

Figure 6. Group Ownership Service

5.2 Group Member Authorization System

Group member authorization system is the main part of controlling access to the group. This system performs the access request and access control functions. It allows a prospective group member authorized to become a group member. This system involves three components: a prospective member host, a router and the access control server (ACS). We assume that the presence of a public key infrastructure, otherwise we can use the digitally sign messages method [9]. The group owner generates the distributed encryption key pairs (A, s) and decryption keys ($\bar{x}$ and $\hat{x}$), as discussed in the last section. We also assume that there is one access control server (ACS) for the convenience of describing this protocol. The access control authorization protocol is described as follows.

5.3 Authorization Protocol

The group member authorization system includes the interaction between the host and ACS, and the interaction between the host and the router. This system also assumes the presences of the public key infrastructure (PKI).

- (K_{+h}, K_{-h}) denotes the prospective member hosts public key and private key pair
- (K_{+acs}, K_{-acs}) denotes ACS public key and private key pair.
- $(K_{+x}, CERT_{k_{+x}})$ denotes the trusted authority key and signed certificate

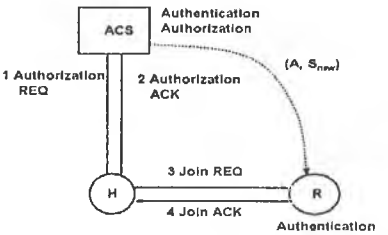

Figure 7. Basic Authorization protocol

The interaction between the prospective member and the ACS includes the following:

1. $H \rightarrow ACS : AR = [GID, CERT_{K_{+h}}]_{K_{-h}}$
2. $ACS \rightarrow H : AA = CAP = [[IP_H, DN_H, GID, T_{exp}, X_j, CERT_{K_{+acs}}]_{K_{-acs}}]_{K_{+h}}$

Here

- AR denotes authorization request
- CAP denotes Capability
- GID denotes the group ID
- AA denotes authorization acknowledgement
- DN denotes the host's distinguished name
- X_j denotes the member decryption key pair$[\hat{x}_j, \bar{x}_j]$

The interaction between the prospective member and the Router includes:

3. $H \rightarrow R : JR = CAP$
4. $R \rightarrow H : JA = Status$

Here

- JR denotes join request
- JA denotes join acknowledgement

First, the prospective member sends an authorization request to the access control server (ACS). This authorization request (AR) includes the group ID that the member want to join and his/her public key certificate, which is signed by his/her private key.

Second, the access control server authenticates the prospective member and decides if this prospective member can be authorized by checking the group policy from the policy server. Then the access control server returns an authorization acknowledgement (AA). If the request is

successful, the prospective member will receive the decryption key ($\bar{x}$ and $\hat{x}$), which is encrypted with the prospective member's public key.

Third, the access control server updates the encryption key (A, S) to (A, S_{new}). As we discussed before, we only need to change the S in this case. This can then be transferred to one of the MOSPF router as part of the link state advertisement (LSA) information. Based on the MOSPF routing protocol, all the routers of the area will store this information. We assume that the routing control messages are secure, which can use the OSPF digital signature [15].

Finally, the prospective member sends the join request to the router that is the designated router if the prospective member connected network has more than one router. Because the router already has the distributed encryption key, the router can verify whether the prospective member is qualified. If successful, the prospective member is accepted as a formal member.

5.4 Reauthorization and Revocation

The group member needs to refresh their membership state to coincide with the soft state of the IGMP group membership reports and of the routing protocol. In this scheme, the router can encrypt the control messages and only the qualified members have the decryption key in the group. The group owner can cancel the member who has left by changing the encryption key. On the other hand, the member who has left can also rejoin the group; the group owner only need to change the encryption key. We can see that this new scheme can achieve efficient revocation and reauthorization.

This new secure multicast architecture and protocol for MOSPF has the following advantages comparing to the previous proposals [5, 9, 12]. First, this scheme simplifies access control protocol process by adding a group control encryption key into the MOSPF LSA control messages. This is because the access control server does not need to transfer the prospective member's certificates to related routers every time. Next, the scheme is flexible and the group owner can revoke a member at any time; other proposed schemes can not do this, whether they use a capability like token or a time limited token. Furthermore, our scheme is scalable, when the group is dynamic with members joining and leaving frequently. This is a major advantage of our scheme over the previously proposed ones.

In this scheme, we assume that the router is trusted and can receive group messages. One can easily envisage a slight variation of the scheme which uses a hybrid method by employing group session key and the group key management protocols to enhance the system and to achieve higher levels of security.

6 Concluding Remarks

In this paper, we have presented a new secure multicast architecture and protocol for MOSPF. Our new scheme involves a novel distributed encryption scheme and simplifies the access control process. The proposed scheme has good scalability properties and achieves efficient revocation and reauthorization. Currently, we are in the process of conducting a simulation of our proposed scheme to analyse the performance issues.

References

[1] C. K. Miller, *Multicast networking and Applications* (Massachusetts: Addison Wesley Longman, Inc., September 1998).

[2] J. Moy OSPF, version 2, RFC2328, IETF, April 1998.

[3] J. Moy Multicast Extensions to OSPF, RFC1584, IETF, March 1994.

[4] P. Judge and M. Ammar, Security issues and solutions in multicast content distribution: A survey *IEEE Network*, Jan./Feb. 2003.

[5] T. Hardjono and B. Cain, Key establishment for igmp authentication in ip multicast, *IEEE European Conference on Universal Multiservice Networks (ECUMN)*, CREF, Colmar, France, 2000.

[6] T. Hardjono and G. Tsudik, IP multicast security: Issues and directions, *Annales de Telecom*, pp. 324 - 340, July-August 2000.

[7] P. S. Kruus and J. P. Macker, Techniques and issues in multicast security, *MILCOM 98* , 1998.

[8] C. Shields and J. J. Garcia-Luna-Aceves, KHIP - a scalable protocol for secure multicast routing, *SIGCOMM* , pp. 53 - 64, 1999.

[9] P. Q. Judge and M. H. Ammar, Gothic: Group access control architecture for secure multicast and any cast, *IEEE INFOCOM*, July 2002.

[10] T. Hardjono and B. Weis MSEC Architecture, draft-ietf-msecarch- 00.txt, Oct 2002. Work in Progress.

[11] B. Cain, S. Dearing, I. Kouvelou, and A. Thyagarajan Internet Group Management Protocol, Version 3, RFC3376, IETF, October 2002.

[12] A. Ballardie and J. Crowcraft, Multicast specific security threats and countermeasures, *ISOC Sysp. Net. and Distrib. Sys. Sec*, San Diego, CA, Feb. 1995, pp. 2-16.

[13] Y. Mu and V. Varadharajan, Robust and secure broadcasting, *Indocrypt 2001*, Lecture Notes in Computer Science, Springer 2001.

[14] P. McDaniel, H. Harney, P. Dinsmore, and A. Prakash Multicast Security Policy, IETF, November 2000. http://www.ietf.org/internet-drafts/draft-irtf-smug-mcastpolicy- 01.txt.

[15] S. Murphy, M. Badger, and B. Wellington OSPF with digital signatures, RFC2154, IETF, Jun 1997.