2005

An ID-based Access Control Scheme for MOSPF

Junqi Zhang
Macquarie University

Vijay Varadharajan
Macquarie University

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

An ID-based Access Control Scheme for MOSPF

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 ID-based 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.

Disciplines

Physical Sciences and Mathematics

Publication Details

Mu, Y., Zhang, J. & Varadharajan, V. (2005). An ID-based Access Control Scheme for MOSPF. In X. Xue (Eds.), International Workshop on Network Architecture and Service Models (pp. 25-30). China: Fudan University Press.

An ID-based Access Control Scheme for MOSPF

Junqi Zhang* and Vijay Varadharajan
Department of Computing,
Macquarie University, NSW, Australia
E-mail: janson, vijay@ics.mq.edu.au
*Corresponding author

Yi Mu
School of Information Technology and Computer Science,
UOW, NSW, Australia
E-mail: 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 ID-based 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: Access Control; MOSPF; Multicast; Security.

1 INTRODUCTION

Multicasting provides an efficient communication mechanism in both private networks and Internet for large-scale content distribution, such as audio and videoconference, web casting, interactive game and video on demand. There are three basic types of multicast routing protocols: distance vector, link state and shared trees (Miller 1998). MOSPF belongs to the category of link state (Moy, 1994, 1998). 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 (Judge et al., 2003, Hardjono et al., 2000): 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 (Hardjono et al., 2000, Kruus et al., 1998). These methods can become very complicated because the membership is dynamic. In addition, as mentioned in (Judge et al., 2003), 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 (Hardjono et al., 2000, Shields et al., 1999, Judge et al., 2002). In this paper, we propose a new secure multicast scheme and protocol for MOSPF based on an ID-based distributed 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 (Hardjono, et al., 2000, 2002, Cain et al., 2002, Judge et al., 2002).

The multicast security (MSEC) working group of the Internet Engineering Task Force (IETF) presents a multicast

security architecture reference framework. This Reference Framework is used to classify functional areas, functional elements, and interfaces.

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 policy server represents both the entity and functions that is used to create and manage security policies specific to a multicast group. The Group Controller and Key Server (GCKS) represent both the entity and functions relating to the management of cryptographic keys used by a multicast group. The Sender is an entity that sends data to the multicast group. Based on the number of the senders, multicast is divided into two types, i.e. 1-to -N and M-to-N. For the 1-to-N multicast type, only one sender can transmit data to the group. For the M-to-N multicast type, many or all group members can transmit data to the group. The three functional areas are Multicast data handling, Group key Management, and the Multicast security policies.

Our new secure multicast architecture and protocol for MOSPF will follow this 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 (Cain et al., 2002). 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. The IGMP has the following rules: firstly, host sends an IGMP "report" to join a group; secondly, host does not send a report when it wants to leave a group; finally, multicast routers send IGMP queries to the all hosts group periodically to see whether any group members exist on their subnet works. If no response is received after a number of queries, the router assumes that there is no group member on the network.

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 (Judge et al., 2002, 2003). The proposed solutions can be found in (Hardjono et al., 2000, Judge et al., 2002, Ballardie et al., 1995). Depending upon the type of revocation provided, these multicast receiver authorization solutions are classified into three types: centralized, ACL supported and time-limited processor. However, at each step of the way, it must decide which one is the next task to map: it maps 'more important' tasks first when possible, where this is determined by the weight of a node.

In (Hardjono et al., 2000), 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 is in the token list. In (Ballardie et al., 1995), 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 (Judge et al., 2002), Judge and Ammar proposed a comprehensive architecture GOTHIC for providing group access control.

2.3 Gothic Architecture

In this section, we briefly describe the Gothic architecture proposed in (Judge et al., 2002). 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 1). 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.

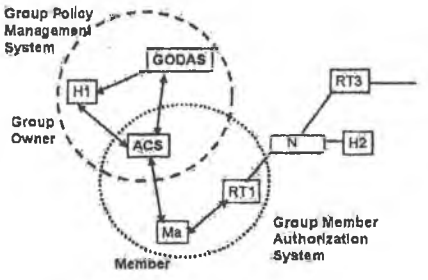

Figure 1 *Gothic Architecture*

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 (Moy 1994) Figure 2 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).

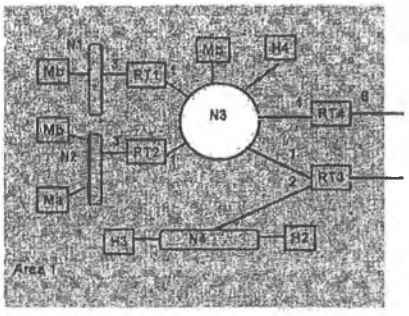

Figure 2 *MOSPF Architecture*

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 (Mu, et al., 2004)

4.1 System Set up

The Group controller and key Server (GCKS) need to set up the system such that all necessary parameters can be used during the multi-group services oriented application lifetime. GCKS selects the following parameters:

- a large prime $p = 2q + 1$ where q is also prime,
- an additive group $\mathbf{G}_1$ and a multiplicative group $\mathbf{G}_2$ (both have order p),
- a master secret key $s \in \mathbf{Z}$, and
- a number $P \in \mathbf{G}_1$.

Based on the ID-based encryption algorithm (Boneh, et al., 2001), the KDC computes the system public key $P_{pub} = sP$ which is then sent to all membership who have registered

with KDC. KDC also selects two strong public one-way functions H_1: {0, 1}* → G_1 and H_2: G_1 →{0, 1}*

4.2 Membership Registration

Any users who want to join the multicsat group have to register to the GCKS and become a member. We suppose that there is a secure channel between each user and the KDC. The user applies to join the group including his/her *ID*. The KDC authorizes a privileged user by send him/her with private key $S_{ID} = sQ_{ID}$ ($Q_{ID} = H_1(ID)$). After registration, user becomes membership.

4.3 Algorithm Construction

This scheme consists of the following 3 steps: Encryption Setup, Encryption and Decryption.

Encryption Setup

In order to deliver multicast services to corresponding members, the GCKS or sender needs to setup the following parameters.

Select a random number $r \in Z$.

- Compute $R = rP$
- Compute $x_i = \hat{e}(rQ_{IDi}, P_{pub})$.

Where $\hat{e}$ is the Weil pairing mapping.

- Compute the following polynomial function

$$f(x) = \prod_{i=1}^{m}(x - x_i) \bmod p = \sum_{i=0}^{m} a_i x^i \bmod p$$

Then we can obtain:

$$a_0 = \prod_{j=1}^{m}(-x_j)$$

$$a_1 = \sum_{i=1}^{m}\prod_{j=1, j\neq i}^{m}(-x_j)$$

$$\cdots\cdots$$

$$a_{m-2} = \sum_{i=1}^{m}\sum_{j=i+1}^{m}(-x_i)(-x_j)$$

$$a_{m-1} = \sum_{j=1}^{m}(-x_j)$$

$$a_m = 1$$

Note that $\{a_i\}$ satisfy $\sum_{i=0}^{m} a_i x_j^i = 0 \bmod p,\ j = 1, \cdots, m$

Construct the corresponding exponential functions $\{a_0 P, a_1 P, a_2 P, \cdots a_n P\} = \{P_0, P_1, P_2, \cdots P_m\}$

Encryption

Let $M_k \in \{0, 1\}^*$ be the multicast session key (TEK), then we can encrypt it as follows.

- Select a random number $R \in Z$ and a random number $D \in G_1$.
- Compute *(m+2)* tuple

$$T \leftarrow (R, M \oplus H_2(D), D + kP_0, kP_1, \cdots, kP_m)$$
$$= (R, M \oplus H_2(D), C_0, C_1, \cdots, C_m)$$

- Broadcast *T* to Multicast group

Decryption

When the members received the *T*, they can decrypt the correspondent session key (TEK) as follows.

$$\hat{e}(S_{IDi}, R) = x_i$$

$$C_0 + \sum_{j=1}^{m} x_i C_j = D + k(a_0 + a_1 x_i + \cdots + a_m x_i^m)P = D$$

$$C \oplus D = M_k$$

If a member does not register to the multicast group, s/he will not decrypt the session key. Therefore s/he could not get the session key. This is because for any x_i not belonging to multicast group, $\sum_{i=0}^{m} a_i x_j^i \neq 0 \bmod p$.

5 A NEW SECURE MULTICAST ARCHITECTURE FOR MOSPF

In this section, we will present our new secure multicast architecture and protocol for MOSPF. This scheme is based on the algorithm described in last section.

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 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 3).

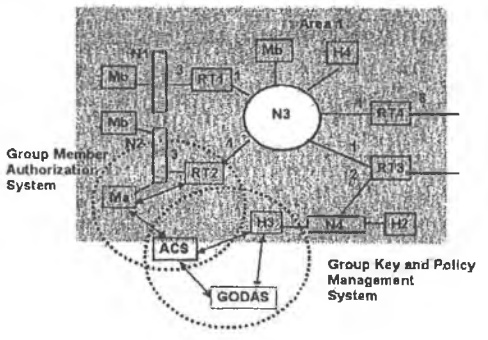

Figure 3 *Secure Multicast Architecture for MOSPF*

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 3 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 (McDaniel et al., 2000}. 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 (Judge, et al., 2002}. There are two different systems for providing such functionality.

The first solution makes use of group certificates (Figure 4). This is similar to traditional digital certificates.

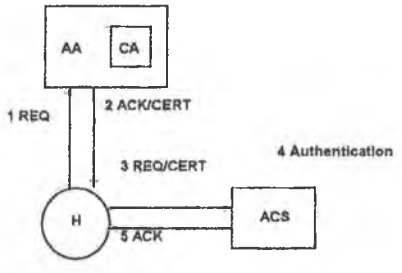

Figure 4 *Group Owner Certificates*

The second solution is the use of a group ownership service (Figure 5). 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).

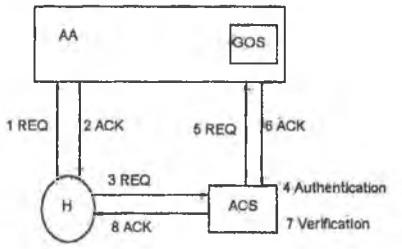

Figure 5 *Group Owner Service*

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 (Judge et al., 2002).

The group owner generates the distributed encryption key set $\{a_i\}$ and decryption key (s_{ID}), as discussed in the preceding 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

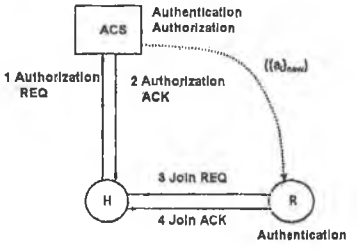

Figure 6 *Basic Authorization Protocol*

The interaction between the prospective member and the ACS includes the following (Figure 6):

1. $H \rightarrow ACS : AR = [GID, ID, CERT_{k+h}]_{k-h}$

2. $ACS \rightarrow H : AA = CAP = [IP_H, DN_H, GID, S_j, CERT_{k+acs}]_{k-acs}$

Here

- *AR* denotes authorization request
- *ID* denotes the prospective member ID
- *AA* denotes authorization acknowledgement
- *CAP* denotes Capability
- DN_H denotes the host's distinguished name
- *GID* denotes the group ID
- S_j denotes the member decryption key s_{ID}

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 check 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 (s_{ID}), which is encrypted with the prospective member's public key.

Third, the access control server updates the encryption key set ($\{a_i\}$) to ($\{a_i\}_{new}$). As we discussed before, the system needs to change the related parameter for encryption. These can then be transferred to one of the MOSPF routers 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 (Murphy et al., 1997).

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 (Hardjono et al., 2000, Judge et al., 2002, Ballardie et al., 1995). 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. 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

REFERENCES

Ballardie, A. and Crowcraft, J. (1995) "Multicast specific security threats and countermeasures," in ISOC Sysp. Net. and Distrib. Sys. Sec, San Diego, CA, Feb. 1995, pp. 2-16.

Boneh, D. and Franklin, M. "Identity-based encryption from the weil pairing," Advances in Cryptology-Crypto 2001, LNCS, vol. 2139, pp. 213– 229, 2001. Springer-Verlag.

Cain, B. Dearing, S. Kouvelou, I. and Thyagarajan, A. (2000) Internet Group Management Protocol, Version 3, RFC3376, IETF, October 2002.

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

Hardjono, T. and Tsudik, G. (2000) "Ip multicast security: Issues and directions," Annales de Telecom, pp. 324–340, July-August 2000.

Hardjono, T. and Weis, B. (2002) MSEC Architecture, draft-ietf-msec-arch- 00.txt,Oct 2002. Work in Progress.

Judge, P. and Ammar, M. (2003) "Security issues and solutions in multicast content distribution: A survey," IEEE Network, Jan./Feb. 2003.

Judge, Q. P. and Ammar, H. M. (2002) "Gothic: Group access control architecture for secure multicast and any cast," in IEEE INFOCOM, July 2002.

Kruus, S. P.and Macker, P. J. (1998) "Techniques and issues in multicast security," MILCOM 98, 1998.

McDaniel, P. Harney, H. Dinsmore, P. and Prakash, (2000) A. Multicast Security Policy, IETF, November 2000. http://www.ietf.org/internet-drafts/draftirtf-smug-mcast-policy-01.txt.

Miller, K. C. (1998) Multicast networking and Applications. Addison Wesley Longman, Inc., September 1998.

Moy, J. (1998) OSPF, version 2, RFC2328, IETF, April 1998.

Moy, J. (1994) Multicast Extensions to OSPF, RFC1584, IETF, March 1994.

Mu, Y. and Susilo, W. (2004) "Identity-based instantaneous broadcast system in mobile ad-hoc networks," in the 2004 International Workshop on Mobile Systems, E-commerce and Agent Technology, (USA), pp. 35–40, 2004.

Murphy, S. Badger, M. and Wellington, B. (1997) OSPF with digital signatures, RFC2154, IETF, Jun 1997.

Shields, C. and Garcia-Luna-Aceves, J. J. (1999) "Khip - a scalable protocol for secure multicast routing," in SIGCOMM, pp. 53–64, 1999.