Developing and Simulating an IP Multicasting Service for Isfahan University's Network and Improving the Security of IGMP-AC Multicast System

masoumeh adhami1, fatemeh hasani2, iman halavati3, maryam okhovati1, azam bazrafshan1

1: Kerman University of Medical Sciences, Kerman, Iran
2: Kerman University of Medical Sciences, Kerman, Iran (Corresponding Author)
3: Research Center for Modeling in Health, Institute of Futures Studies in Health, Kerman University of Medical Sciences, Kerman, Iran
adhamimasomeh@yahoo.com

Abstract: Today, with the development of network applications, the need for bandwidth saving is increased and in this regard multicast service has gained great importance. One of the types of communication in computer networks is multicast where, the destination of sent packets is a group of receivers. Multicast is a useful network service which delivers the data to a group of users who are all members of a multicast group. It makes efficient use of network bandwidth, especially for multimedia streaming over the network for a group of users. Applications which can benefit multicast include video conferencing, TV, radio, Internet, distance learning and so on. Multicast uses its own special algorithms for routing multicast data. Multicast routing algorithms are divided into two groups of tree algorithms based on transmitter and a common tree algorithm. The aim of multicast routing is to find a tree that includes all routers in the network who have members. Several protocols have been designed based on these two algorithms among which, PIM, due to its benefits, is being used in practical implementation of IP multicasting. This protocol has two modes: PIM-DM which is based on sender tree algorithm and PIM-SM which is based on common tree algorithm. IP multicast model, despite all its advantages, is not yet widely implemented. One reason for this is insecurity of IP multicast service. In other words, in the classical model of IP multicasting, each entity can send information to the group and everyone can receive this information. The openness of joining and leaving services for groups in the IP multicasting underlies a wide range of attacks usually DOS attacks. In recent years, various solutions have been proposed to address these problems. In this work, in order to solve the security problems of IP multicasting services, we will review existing models and solutions and focusing on the access control structure of IGMP-AC and evaluating its advantages and disadvantages, a new structure will be suggested to address these deficiencies.

[Masomeh Adhami, Reza Malekpour Afshar, Iman Halavati, Maryam Okhovati, Fatemeh Hasani, Alireza Adhami, Forough Jahandari. **Developing and Simulating an IP Multicasting Service for Isfahan University's Network and Improving the Security of IGMP-AC Multicast System.** *Life Sci J* 2013;10(7s):1079-1084]. (ISSN: 1097-8135). http://www.lifesciencesite.com. 172

Keywords: IP multicasting, multicast routing algorithms, access control, authentication, key group

1. Introduction

As it can be seen in the following figure, if a number of receivers in the network has the same information requests, using a multicast service instead of unicast, conserves network bandwidth consumption. The number of internet-based applications that are based on multicast services is growing such as transferring audio and video from a live presentation to a remote audience, interactive gaming network, real time information of stock prices for shareholders and so on [Austerberry, 2005].

The idea of multicast in the third layer and IP network was first introduced in the doctoral dissertation of Deering [Deering, 1989]. The main aim of multicast routing is to find a way to send data from a transmitter to multiple receivers. The best structure for this scenario is tree structure because this structure enables parallel sending of packets to different recipients and in addition, minimizes the amount of duplicate data because new replicas only needed to be created where the branches are split. Therefore, the task of multicast routing is to find and create a tree which is rooted in the sender and covers all receivers. Technically, such a tree is called multicast tree.

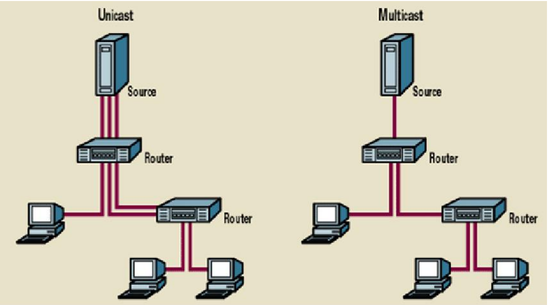


Figure 1: comparison of multicast and unicast services

Until now, many multicast routing protocols have been standardized by IETF including DVMRP [Waitzman, D., Partridge, C., Deering, S, 1988], PIM-SM 5 [Estrin, D., Wei, L., Farinacci, D., Helmy, A., Thaler, D., Deering, S., Handley, V., Sharma, P, 1995], and CBT [Ballardie, A, 1995]. Among different multicast routing protocols, PIM, due to its simplicity and other capabilities has more popularity in implementing intra-domain multicasting routing. PIM has its name from the fact that, it is independent from unicast routing protocols and can work with any other protocol such EIGRP - OSPF - BGP and so on [*Multicast routing: PIM sparse mode and other protocols*, White Paper, Spirent Communications, USA, November 2003]. Even in the case of static unicast routing, this protocol is still able to work.

This feature makes it easy to implement multicast service in any network using these protocols without the need to change and reconfigure the current unicast routing.

Multicast IP, despite all its advantages is not yet widely implemented. One reason for this is insecurity of multicast IP structure where there is no access control for receivers and transmitters of multicast groups [Islam, S., William Atwood, J, 2007].

2. Material and Methods

Nowadays, the widely accepted multicast structure is an open model based on PIM-SM and IGMP for IPv4 and MLD for IPv6. Although, this model, because of its scalability and simplicity is the best model to be used by an ISP to provide multicast service, but in this model, each entity can send information to a group and everyone can receive this information and there is no management mechanism or security feature in this model.

After through study on this structure, we concluded that, in this structure, there is no method to provide security for multicast data. In other words, after authenticating of members, the data will be revealed and sent to them without any keys distributed among them. Furthermore, the important security services which have great importance in group communications and join and leave events such as forward secrecy and backward secrecy are not considered in this structure and therefore it is vulnerable to some attacks. All these operations are under group key management operations that is one of the most important parts of a secure group communication system. Therefore, it is clear that, in order to overcome these shortcomings in the access control structure of IGMP-AC, using a key management approach is required. Therefore, our main goal is to select a method for key management and provide suggestions for using this structure. By using a convenient method for managing keys, security shortcomings of this structure will be eliminated.

The common way for information security is using encryption. An encryption algorithm receives input data (such as a group message) and transforms it through an encryption key.

2.1. Classification of Group Key Management Protocols

Different methods and protocols have been proposed in the field of group key management that can be divided into four main groups as following [Adusumilli, P., Xukai, Z., Ramamurthy, B, 2005; Mittra, S, 1997; Amir, Y., Kim, Y., Nita-Rotaru, C., Schultz, J. L., Stanton, J., Tsudik, G, 2004; Chan, H., Gligor, V. D., Perrig, A., Muralidharan, G., 2005; Kim, Y., Perrig, A., Tsudik, G, 2004].

- Centralized Group Key Distribution Protocol (CGKD)
- Decentralized group key management protocol (DGKM)
- Distributed group key agreement protocol (DGKA)
- Distributed group key distribution protocol (DGKD)

An overall evaluation suggests that, each of the above group key management protocols are suitable for a particular application and there is no protocol to address all security requirements [Kaufman, C, 2008].

2.2. Key Management based on Access Control Polynomial

This method is based on an innovative access control polynomial (ACP) [Kaufman, C, 2008] over a finite field which is especially suitable for dynamic environments where members frequently enter and leave the group. This method, not only satisfies different security requirements, but also is secure against various attacks.

First, the ACP is created so that, the information is distributed in a way that only the authorized receivers with an ID in the form of $x - f(\mathrm{SIDi}\,, \mathrm{z})$ are able to acquire the information. Thus, we have the following assumptions:

- q Is a large prime number which forms f_q.
- f: $\{0, 1\}^* \rightarrow \{0, 1\}_q$ is a hash function.
- There is a reliable central server.
- Any valid user, Ui, will be provided by a password (SID_i) which is an integer smaller than q and is known only for central server and the user. Allocating *SID* to a user can take place during the registration process.

ACP is a polynomial on F_q [X] as follows:

$$A(x) = \prod_{i\in\varphi}(x - f(\ SIDi\,, z)) \qquad \text{Eq.1}$$

Where, φ is the group, SID_i is the password of members of φ, and z is a random integer from Fq that changes each time A(x) is recalculated. It is clear that, in this polynomial, when x is replaced with $f(SIDi\,,z)$ by a valid user having a SID_i in Group φ, the value of A(x) is equal to zero and otherwise, it has a random value.

For multicasting, an encryption key like K for all users in the group φ is calculated by server through the following polynomial:

$$P(x) = A(x) + K \qquad \text{Eq.2}$$

Then the$(z, P(x))$, where K is hidden in combination with constant value of A(x) is multicast and any valid member of group can obtain the key, K, with SID_i value using the following equation.

$$K = P(f(SIDi\,,z)) \qquad \text{Eq.3}$$

Characteristics and capabilities of ACP method are as follows [Zou, X., Shun Dai, Y., Bertino, E, 2008]:

- ACP is a simple and scalable method for implementing group communications. In addition, it features the flexibility to adapt with different access control and key management patterns.
- ACP is secure against various attacks.
- ACP is suitable for highly dynamic environments with frequent entry and exit of members. Canceling the user membership is also simple and efficient.
- ACP users do not need to be synchronized.

In this method, users only need to store a secret values and calculating the key does not need high computing and processing power. Therefore, it can be implemented in devices with low computational power such as sensors.

First, we consider the following assumptions:

- AAA server is used as a trusted server in ACP method.
- All AR routers are considered as trusted entities.
- Group key is only distributed between receivers and transmitters do not need group key.
- Each member of the group (receivers) has its own SID.
- AR, in addition to the previously received states, has to keep the group key too.
- It is assumed that, greport is from the messages of Diameter protocol.

In order to shed a light on how to apply the ACP method on access control structure of IGMP-AC we suppose that, a user with SID_i has sent a new application for membership in secure group of (g_or_gs) or to leave it to the related AR. The authenticity and access control processes of this user are performed based on the access control structure of IGMP-AC. After verification of authenticity of user by AAAS, the success or failure message of user's authenticity will be sent to AR and AAAS must calculate the new group key based on SID of new user. In this step, it is required to send $(z, P(x))$ to members. Here, AAAS, using greport message, sends $(z, P(x))$ value to all ARs. Moreover, in this message, the group key will be sent to all ARs in an encrypted form with a key shared between AAAS and each (K_c)AR. The diagram of the new state of AAAS in our proposed structure is shown in the following figure.

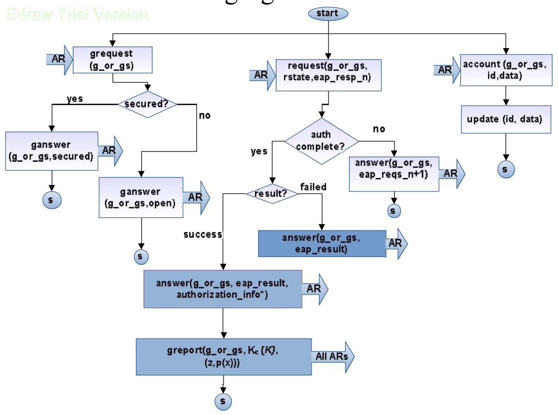

Edraw Trial Version
start
AR
grequest (g_or_gs)
secured?
yes
no
ganswer (g_or_gs,secured)
AR
s
ganswer (g_or_gs,open)
AR
s
AR
request(g_or_gs, rstate,eap_resp_n)
auth complete?
yes
no
result?
failed
success
answer(g_or_gs, eap_reqs_n+1)
AR
s
answer(g_or_gs, eap_result)
AR
answer(g_or_gs, eap_result, authorization_info*)
AR
greport(g_or_gs, Kc {K}, (z,p(x)))
All ARs
s
AR
account (g_or_gs, id,data)
update (id, data)
s

Figure 2: The state diagram of AAAS

As it can be seen, in addition to the greport message which is added to this structure, the rstate value is added in the request (g_or_gs - rstate - eap_resp_n) message that comes from AR. AR, receiving greport message, obtains new key and sends aresult (g_or_gs , (z, p (X))) message to group members (receivers) in the related subnet (Fig.3).

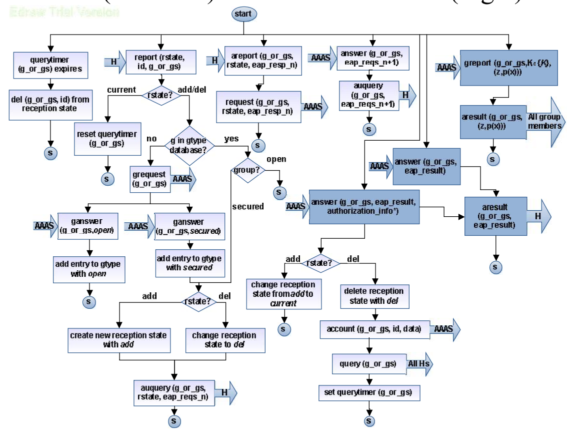

Edraw Trial Version
start
querytimer (g_or_gs) expires
del (g_or_gs, id) from reception state
s
H
report (rstate, id, g_or_gs)
rstate?
current
add/del
reset querytimer (g_or_gs)
s
no
g in gtype database?
yes
grequest (g_or_gs)
AAAS
group?
open
secured
s
AAAS
ganswer (g_or_gs,open)
add entry to gtype with open
s
AAAS
ganswer (g_or_gs,secured)
add entry to gtype with secured
rstate?
add
del
create new reception state with add
change reception state to del
auquery (g_or_gs, rstate, eap_reqs_n)
H
s
H
areport (g_or_gs, rstate, eap_resp_n)
request (g_or_gs, rstate, eap_resp_n)
AAAS
s
AAAS
answer (g_or_gs, eap_reqs_n+1)
auquery (g_or_gs, eap_reqs_n+1)
H
s
AAAS
greport (g_or_gs,Kc {K}, (z,p(x)))
aresult (g_or_gs, (z,p(x)))
All group members
s
AAAS
answer (g_or_gs, eap_result)
AAAS
answer (g_or_gs, eap_result, authorization_info*)
aresult (g_or_gs, eap_result)
H
s
rstate?
add
del
change reception state from add to current
s
delete reception state with del
account (g_or_gs, id, data)
AAAS
query (g_or_gs)
All Hs
set querytimer (g_or_gs)
s

Figure 3: Diagram of AR State

As noted before, our goal of providing a new structure is adding some important group security services such as security of group data, forward secrecy, and backward secrecy in access control structure of IGMP-AC. This goal can be achieved by distribution of a key between members of the group and renewing this key with entering and leaving of members which we have achieved by using ACP key management mechanism in this structure. It is clear that, the addition of these services requires more computations, more message exchange, and more memory in the hosts, routers and servers, and generally, it the whole structure will become more complicated. Our results indicated that, by achieving higher security we can ignore these complexities.

Table 1: Comparison of IGMP-AC and proposed structures

	IGMP-AC structure	Proposed structure
Authenticating, licensing, and audit services of group members	✓	✓
The use of encryption and data secrecy services	✓	×
Forward secrecy service for the data exchanged within group	✓	×
Backward secrecy service for the data exchanged within group	✓	×
Computational complexity in the host in order to obtain group key	N/A	O(n)
Amount of memory required in the host in order to obtain group key	N/A	O(1)
Amount of memory required in the router	N/A	O(1)
Computational complexity in the server in order to obtain group key	N/A	O(n^2)
Amount of memory required in the server in order to obtain group key	N/A	O(n)

As shown in this table, our proposed structure has added essential security services to the structure of IGMP-AC access control. These services contribute to improve the security of exchanged data within group and only members can access to these data that had current group key.

3. Results

3.1. Simulating IP multicasting in Isfahan Industrial University (IUT) and evaluating its performance

Since our goals is developing an IP multicast service to be implemented in a real network (IUT network) we have tried to develop a network by benefitting simulation environment that reflects the topology of a real network through which, we can investigate the protocols and their IP multicast performance under conditions close to reality.

3.2. Selecting the Routing Protocol

As it is mentioned before, IP multicasting uses special routing protocols for routing multicast packets. We also mentioned that, between different multicast routing protocols, PIM protocols, due to their simplicity and other capabilities have higher popularity in implementation of intra-domain multicasting routing. Therefore, we used PIM-SM protocol in our scenario and in the following we will explain our results.

PIM has its name from the fact that, it is independent from unicast routing protocols and can work with any other protocol such EIGRP - OSPF - BGP and so on [*Multicast routing: PIM sparse mode and other protocols*, White Paper, Spirent Communications, USA, November 2003]. Even in the case of static unicast routing, this protocol is still able to work [*Multicast routing: PIM sparse mode and other protocols*, White Paper, Spirent Communications, USA, November 2003].

Another feature of PIM is that, it will not exchange multicast routing updates between routers and therefore, it will not produce high signaling traffic.

Another feature of PIM is its lower complexity compared to other multicasting protocols and is easy to implement.

In general, PIM-SM protocol has following advantages over PIM-DM protocol:

- Only one tree is created per group
- Only routers that are on the branches of tree are involved in maintaining the multicast tree information
- Reducing the amount of data stored on the router for each group and increased extensibility
- Capability of creating tree based on the sender in a receiver-oriented manner and the possibility of switching to this tree
- Presence of a common root for registration and management of membership of receptors
- Presences of a common root for management and control the senders of a group
- High scalability for networks with small, medium and large sizes

There are some problems for protocols based on common-tree algorithms as following:

1. Increasing the packets receiving latency in the receivers

2. Traffic congestion around the junction of the common roots due to the sending of packets through it
3. low error tolerance of created tree due to the presence of common roots as the only point of failure

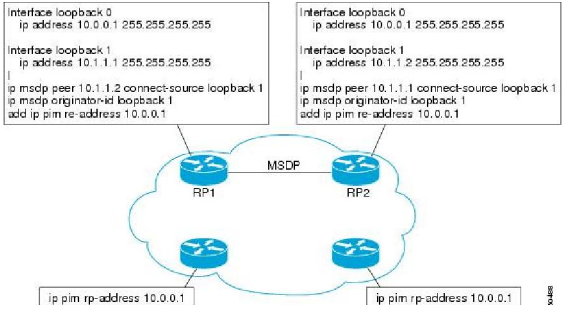
SPT Switchover

In order to solve the first two problems of PIM-SM, there is the potential that, receivers receive sent packets from the shortest path between sender and receiver (SPT) rather than from common tree (RPT).

Anycast RP

As mentioned, the presence of a common root in the network as the only failure point highly reduces the error tolerance of created errors. In PIM-SM, benefiting Anycast RP mechanism, we can establish load Balance AND redundancies in the network.

The following figure shows a typical configuration of Anycast RP [Kim, Y., Perrig, A., Tsudik, G., 2004]



```
Interface loopback 0
   ip address 10.0.0.1 255.255.255.255

Interface loopback 1
   ip address 10.1.1.1 255.255.255.255
|
ip msdp peer 10.1.1.2 connect-source loopback 1
ip msdp originator-id bopback 1
add ip pim re-address 10.0.0.1
```

```
Interface loopback 0
   ip address 10.0.0.1 255.255.255.255

Interface loopback 1
   ip address 10.1.1.2 255.255.255.255
|
ip msdp peer 10.1.1.1 connect-source loopback 1
ip msdp originator-id bopback 1
add ip pim re-address 10.0.0.1
```

```
ip pim rp-address 10.0.0.1
```

```
ip pim rp-address 10.0.0.1
```

Figure 4: Anycast RP configure

In addition, network routers have informed RP address through the following command.

ip pim rp-Address 10.0.0.1

Therefore, PIM-SM, using Anycast RP prevents traffic congestion around the connections of a RP and via configuring multiple RPs with one IP address in the network, creates redundancies and increases error enhances of the created tree.

Nowadays, the widely accepted multicast structure is an open model based on PIM-SM and IGMP for IPv4 and MLD for IPv6 [Hilt, S., Pansiot, J, 2000]. PIM-SM is a protocol that due to the aforementioned advantages, as well as lower complexity, is widely used in implementing intra-domain multicast IP implementation, especially in cases where the network size is medium or large and the receivers are scattered. Therefore we benefitted this protocol to develop our multicast service.

After selecting the multicast routing protocol, it comes to select a corresponding unicast routing protocol. As mentioned before, PIM protocols are able to work with any routing protocol thus, we can use any protocol. Here, we use Open Shortest Path First (OSPF) protocol which is widely supported by router manufacturers.

OSPF Protocols

The powerful and popular protocol of OSPF is described at RFC 2328. The protocol is a link-state protocol that works using Dijkstra algorithm. OSPF runs within an Autonomous System (AS) but is capable of connecting multiple systems to each other [Moy, J., *OSPF Version 2*, RFC 2328, April 1998]. Features of this protocol are as follows:

1. High convergence rate and supporting multiple paths with identical cost to the same destination
2. A fast protocol that is strong and expandable and can be used in thousands of operational networks
3. The protocol is designed in a way to support hierarchical networks

Using the third feature, we can divide large intra network communications into several smaller networks called region. Using above potential have several benefits such as following:

- Reduce routing operations
- Accelerating convergence rate
- Limiting network volatility in a region and preventing its spread to other parts of the network

4. Discussions

In this work we investigated IP multicasting service. As mentioned, among different types of multicast routing protocols, PIM protocols have higher popularity in implementation of intra domain multicast routing due to its simplicity and other capabilities.

Today, the widely accepted multicast structure is an open model based on PIM-SM and IGMP protocols for IPv4 and MLD protocol for IPv6. Although, this model, because of its scalability and simplicity is the best model to be used by an ISP to provide multicast service, but in this model, each entity can send information to a group and everyone can receive this information and there is no management mechanism or security feature in this model. In this work, in order to overcome the security shortcomings of this service, after the introduction we investigated the access control structure of IGMP-AC which through using AAA structure gives appropriate level of authentication, licensing, and auditing services. However, it is observed that, in this model, multicast data will be sent to receivers from AR in an overt fashion after authentication and this threatens the data security.

Our proposed structure, using ACP Group Key Management in IGMP-AC access control structure adds the features of data secrecy, forward and backward secrecy and so in. Finally these two structures were compared and evaluated. Therefore we concluded that, our proposed structure provides very good security services for group multicasting which improves data security and privacy just by little costs in the side of hosts, routers, and servers.

Corresponding Author:
Masomeh Adhami,
Kerman University of Medical Sciences, Kerman,
Iran
adhamimasomeh@yahoo.com

References

[1] Austerberry, D., *The Technology of Video and Audio Streaming*, Second Edition, Focal Press publication, USA, 2005.

[2] Deering, S., *Host extensions for IP multicasting*, RFC 1112, August 1989.

[3] Waitzman, D., Partridge, C., Deering, S., *Distance vector multicast routing protocol (DVMRP),* RFC 1075, November 1988.

[4] Estrin, D., Wei, L., Farinacci, D., Helmy, A., Thaler, D., Deering, S., Handley, V., Sharma, P., *Protocol independent multicast sparse mode (PIM-SM): Protocol specification*, RFC 2362, June 1998.

[5] Ballardie, A., *Core-based tree (CBT version 2) multicast routing*, RFC 2189, September 1997.

[6] *Multicast routing: PIM sparse mode and other protocols*, White Paper, Spirent Communications, USA, November 2003.

[7] Islam, S., William Atwood, J., "Sender access control in IP multicast", *Proceedings of the 32nd IEEE Conference on Local Computer Networks*, Dublin, Ireland, pp. 79-86, Oct. 2007.

[8] Metz, C., "AAA Protocols: authentication, authorization, and accounting for the internet", IEEE Internet Computing, vol. 3, n. 6, pp. 75-79, 1999.

[9] Zou, X., Shun Dai, Y., Bertino, E., "A Practical and Flexible Key Management Mechanism For Trusted Collaborative Computing", *IEEE INFOCOM*, Phoenix, AZ, pp. 538 - 546, April 2008.

[10] Steer, D. G., Strawczynski, L., Diffie, W., Wiener, M., "A Secure Audio Teleconference System", *Lecture Notes in Computer Science*, vol. 403, pp. 520-528, USA, 1990.

[11] Ng, W. H. D., Howarth, M., Sun, Z., Cruickshank, H., "Dynamic Balanced Key Tree Management for Secure Multicast Communications", *IEEE Transactions on Computers*, vol. 56, no. 5, pp. 590-605, 2007.

[12] Adusumilli, P., Xukai, Z., Ramamurthy, B., "Distributed group key distribution with authentication capability", *Proceedings of the IEEE Workshop on Information Assurance and Security*, pp. 286-293, June 2005.

[13] Mittra, S., "Iolus: A framework for scalable secure multicasting", *J. of Computer Communication Reviews*, vol. 27, no. 4, pp. 277-288, 1997.

[14] Amir, Y., Kim, Y., Nita-Rotaru, C., Schultz, J. L., Stanton, J., Tsudik, G., "Secure Group Communication Using Robust Contributory Key Agreement", *IEEE Transactions on Parallel Distrib. Syst.*, vol. 15, No. 5, pp. 468-480, 2004.

[15] Chan, H., Gligor, V. D., Perrig, A., Muralidharan, G., "On the distribution and revocation of cryptographic keys in sensor networks", *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 3, pp. 233 - 247, 2005.

[16] Kim, Y., Perrig, A., Tsudik, G., "Tree-based group key agreement", *ACM Transactions on Information and Systems Security*, vol. 7, no. 1, pp. 60-96, 2004.

[17] Moy, J., *OSPF Version 2*, RFC 2328, April 1998.

[18] Hilt, S., Pansiot, J., "Using IGMPv3 to manage multicast access", *Proceedings of the Fourth Conference on Security and Network Architectures*, Batz sur Mer, France, June 2005.

2/17/2013