SECURE IP MULTICASTING WITH ENCRYPTION KEY MANAGEMENT

Authors: Nadim Maharjan and Daryl Moten
Advisor: Dr. Richard Dean
Department of Electrical and Computer Engineering
Morgan State University
namah1@mymail.morgan.edu, damot2@morgan.edu

ABSTRACT

This paper presents the design for secure IP multicasting in an iNet environment using public key cryptography. Morgan State University has been conducting research to improve the telemetry network by improving network performance, implementing IP (Internet Protocol) multicasting and providing a stronger security system for the iNet environment. The present study describes how IP multicasting could be implemented to provide more secure communication in the iNet environment by reducing traffic and optimizing network performance. The multicast of data is closely tied to the key management center for secure applications. This paper develops a means of delivering keys between two or more parties showing a relationship between the multicast network and the Key Management Center (KMC). The KMC is an element of the system which distributes and manages session keys among multicast members. A public key encryption method is used to address the distribution of session keys in the multicast network. The paper will present a system level design of multicast and key management with dual encryption session keys for the iNet system.

KEYWORDS

IP Multicasting, Public-key Cryptosystem, Key Management Center, Security, Public Certificates, iNet

1. INTRODUCTION

IP multicasting is one of the most fundamental communication modes in a network service. IP Multicasting plays an important role on improving the telemetry network by reducing the traffic in the network, increasing the bandwidth of the network and optimizing the performance of the network. Multicast is essentially multipoint communication where a host (Test Article) sends packets to other hosts (Ground Station) that have expressed an interest in receiving the packets. These hosts sending or receiving multicast packets within a network are called multicast group members. All the multicast groups are segmented based on the security clearance classification. The applications which are sent out within multicast group members are called multicast applications. Encryption keys are distributed to applications based on a predefined set of policies. Users would be assigned certificates based on security level. The certificates would be used to provide electronic signatures and data integrity. While sending secure multicast applications, public-key cryptography offers security by providing confidentiality, integrity and authentication. Public-key algorithms use two keys (private key and public key) for encryption and decryption. Only a particular user will know the private key whereas public keys are distributed to the rest of all the multicast members in the multicast group in a network. KMC plays the role of distributing the keys to the multicast members focusing on delivery and maintenance of encryption keys in the network. Thus, this paper provides a system level design of multicasting and key management securing the data for the iNet system.

2. MULTICASTING

IP Multicasting has become a necessity in the network service because it is an efficient communication method that can transmit data from sender to receiver(s). Multicasting is one-to-many communication which is used in many real-life applications like teleconferencing, video-conferencing, news or weatherbroadcasting, as well as database updating.

There are three fundamental communication modes in networks: unicast, broadcast and multicast. Unicast is a one-to-one or point-to-point communication system where data is sent from a single host to another single host. With unicast, a source would send a packet to each host in the network. If the network is really small, unicast communication is good, but when the network is large, transmitting the same data again and again will increase the congestion in the network. Broadcast is a one-to-many communication system where data is sent from a single host to all other hosts. However, multicast is a mix of unicast and multicast systems. In multicast, data is sent from a single host to selected hosts which have indicated interest in receiving packages of data [1]. In broadcast, a source has to send packet to all hosts in the network. Some hosts will drop the packets if they are not multicast group members. In multicast, hosts will send the packets only to multicast group once so that there is minimum traffic flow, which makes it efficient in the network [1].
Below are some requirements for multicasting [2]:

i. Multicast addresses should be identified so that in IPv4, class D address is reserved for this purpose.
ii. Each host or node should translate the IP multicast address within the multicast group.
iii. A router must translate between an IP multicast address and a sub-network multicast address in order to deliver a multicast IP datagram on the destination network.
iv. Multicast address lists are generated dynamically so that any host can join or leave the multicast network.
v. Routers must exchange information. Firstly, routers should know which subnet include the members of multicast group and secondly, routers need sufficient information in order to calculate the shortest distance between other multicast group members.
vi. A routing algorithm is needed to calculate shortest paths to all group members.

vii. Each router determines the shortest path on the base of source host and destination host.

While classes A, B and C IP addresses are reserved for unicast group, multicast group members use class D (224.0.0.0 – 239.255.255.255). The format of CLASS D IP address is shown as in figure 1 with the header 1110 [1, 3].

1110xxxx| -------|--------|--------

Fig.1: Format of a class D IP address.

In Ethernet with MAC addresses, a multicast address is identified by setting the lowest bit of the “most left byte” as shown in the figure 2.

--------1|--------|--------|--------|-------|--------|--------|--------

Fig.2: Multicast Address Translation.

Not all Ethernet cards can filter multicast addresses in hardware, so filtering is done in software by a device driver [3]. Multicast addresses can be mapped as shown in figure 3. In Ethernet with MAC addresses 01:00:5e are reserved for IP Multicasting in the first 3 bytes. The five bits after the multicast header 1110 are ignored in order to map with an Ethernet address. The mapping in figure 3 places the low-order 23 bits of the IP multicast group ID into the low order 23 bits of the Ethernet address [3, 4].

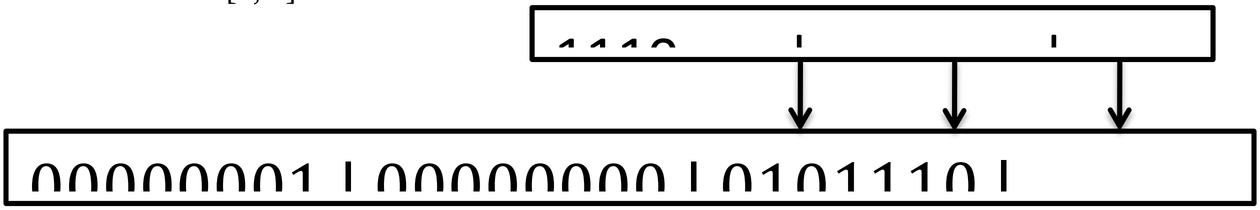

Fig 3: Mapping of a class D IP address into Ethernet multicast address.

2.1 Internet Group Management Protocol (IGMP)

IGMP stands between the hosts and the routers. The main mechanism of the protocol is to send the information from a host to the routers when joining the multicast network. The router sends the IGMP query LAN if they are still connected to the multicast group, and hosts send the IGMP report to the router. Hosts communicate with the nearest routers sending join or leave messages [5].

2.2 Multicast Routing Algorithms

IGMP works as a postman. That is, it only provides the service of multicast packet delivery notification regardless of the traffic flow from the host to the routers in the multicast network. However, it is necessary to have a vehicle for a postman to carry the packets to be delivered in the destinations. In other words, it is necessary to define multicast routing algorithms in order to deliver internet multicast service.

2.2.1 Source-based and Core-based trees

The Source-based tree and Core-based tree both have different ways of building a spanning tree joining all the members of the multicast group which can be observed in the Figure 4.

There is only one source and three destinations on both sides. On the left part of the Figure 4, the Source-based tree uses a shortest path tree that minimizes the path cost from the source to each receiver. In the right part of figure 4, it uses a shared distribution tree where there are more than one sender and many more receivers. The packets circulate through a core point which is even called rendezvous point. Both Source based tree and Core-based tree use reverse path forwarding algorithm in order to get the shortest path tree.

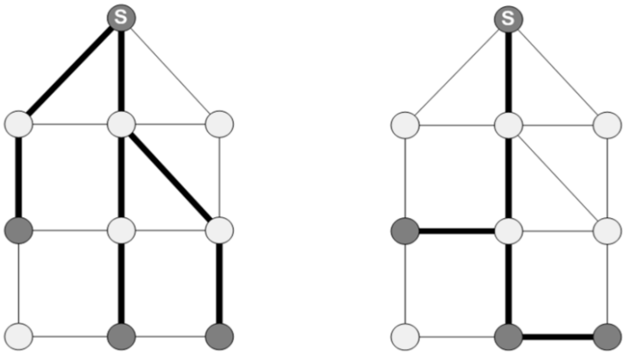

Fig 4: Multicast network tree structure using source-based tree and core-based tree.

2.3 Protocol Independent Multicast in Sparse Mode (PIM-SM)

Protocol Independent Multicast in Sparse Mode (PIM-SM) was chosen to be an appropriate protocol for the iNet system. PIM-SM uses both source-based and core-based trees using explicit joins. PIM-SM is designed in such a way that all the group members of multicast are sparsely distributed. PIM-SM does not use the flood and prune method. In PIM-SM protocol, all the routers send the join message to the main source and the source sends the packets to the near routers when the message arrives at the interface. PIM messages can be sent as unicast or multicast packets in the network. When packets are sent in the multicast network, PIM uses the multicast IP address 224.0.0.13, which is reserved as the ALL-PIM-Routers group [7]. From a bandwidth point of view, it is not necessary to transmit all the packets to all the group members of the multicast network. There is a reason PIM-SM was chosen instead of PIM-DM (Protocol Independent Multicast in Dense Mode). PIM-DM uses the flood and prune method which is waste of bandwidth in the network whereas PIM-SM is bandwidth efficient in the multicast network. PIM-SM initially builds a core-based tree routing protocol for a multicast group, which is shared by all sources in the network. When the traffic from a source exceeds the threshold, PIM constructs a source-based tree for that source.

3. MULTICAST CRYPTOSYSTEM

A Public-key Cryptosystem is chosen for the multicast cryptosystem for the iNet network which rely on one key for encryption and another key for decryption. Public-key cryptography addresses two main issues in the system: Key Management to secure the communication and Digital Signatures to verify the message. A public-key system also provides the flexibility to create multicast groups and to add and subract users dynamically. In public-key cryptography, a public-key, which may be known by anybody, can be used to encrypt session key, and verify signatures and a related private-key, known only to the recipient, is used to decrypt messages, and sign (create) signatures[6]. It is impossible to determine a private key from any public multicast members. However, any multicast member who knows the public keys can encrypt messages or verify signatures but cannot decrypt messages or create signatures.

3.1 Public-Key Cryptosystem: Authentication and Confidentiality

Public-Key Cryptosystems: Public-key encryption is a security scheme that provides the highest level of security of authentication and confidentiality. In this scheme, the session key is encrypted twice using a key pair source and decrypted twice using related key pair source in order to achieve the original message in the destination. Figure 5 illustrates a public-key encryption scheme using authentication and confidentiality [6]. *A* is indicated as KMC which is the local root to distribute keys to multicast members. *A* has a pair of authentication keys: PR_a, a private key known only to *A* and PU_a, a public key known to all the multicast groups whereas *B*, a multicast user, has a related pair of secrecy keys: a public key, PU_b, and a private key, PR_b. PR_b is only known to *B* and PU_b is known to selected multicast group so that it is accessible by *A*.

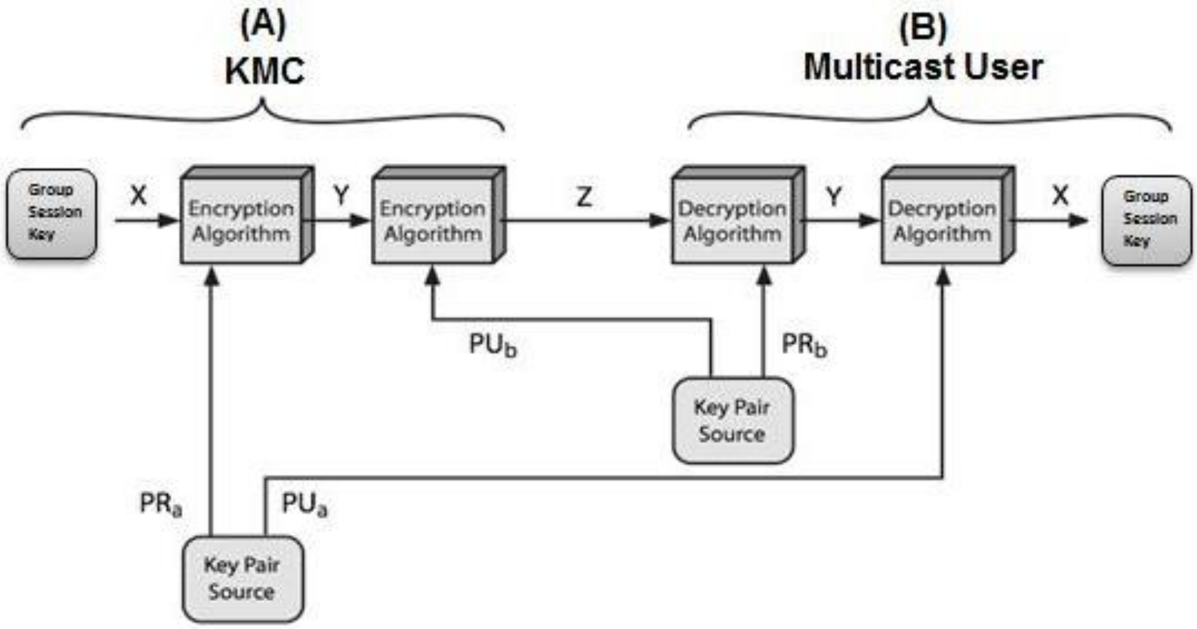

Fig 5: Public-Key Cryptosystem: Authentication and Confidentiality from [6].

A encrypts a session-key *X* using its private key PR_a which can be expressed as follows:

$$Y= E(PR_a, X) \tag{1}$$

A encrypts the session key using RSA algorithm [6] which signs the session key *X* with its private key which is termed as “Digital Signature”. This provides that authentication that, since only A has PR_a, *A* is the only user who could send this message.

A then encrypts *Y* using public key PU_b as:

$$Z= E(PU_b,Y) \tag{2}$$

The ciphertext represented by *Z* is then transmitted to B which provides confidentiality as only *B* can decrypt this message with PR_b . *B* first decrypts the ciphertext *Z* using private key PR_b as:

$$Y=D(PR_b,Z) \tag{3}$$

Then, *B* receives the original message decrypting the ciphertext *Y* and private key PU_a as:

$$X=D(PU_a,Y) \tag{4}$$

To recapitulate, the ciphertext Z is generated as:

$$Z = E(PU_b, E(PR_a, X)) \tag{5}$$

The receiver recovers the session key *X* as:

$$X = D(PU_a, D(PR_b, Z)) \tag{6}$$

With this method, public-key cryptosystem helps to encrypt and decrypt the session key passing from KMC to multicast members, exchanging the keys (private keys or public keys) and provide authentication and confidentiality. For this to work, a KMC is needed to distribute these keys which are discussed later in this paper.

3.2 The RSA Algorithm

RSA is one of the best-known public key encryption algorithms that use properties of the prime number theory. RSA encryption uses the following elements [6]:

Key Generation	
Select p,q	p and q both prime
Calculate $n=p$ xq	
Calculate $\phi(n) = (p-1)\ (q-1)$	
Select integer e	$\gcd(\phi(n),e)=1; 1< e < \phi(n)$
Calculate d	$D=e^{-1} mod\ \phi(n)$
Public-key	$KU =\{e,n\}$
Private-key	$KR= \{d,n\}$
Encryption	
Plaintext	$M < n$
Ciphertext	$C=M^e(mod\ n)$
Decryption	
Plaintext	C
Ciphertext	$M=C^d(mod\ n)$

RSA algorithm supports encryption/decryption, digital signature and key exchange. The security of this algorithm is tied to the difficulty in factoring the n, the product of two prime numbers. Good security is achieved with prime numbers on the order of 500-2000 bits.

4. Multicast Key Management Center

Key management is a significant challenge. Key Management is used to achieve reliable and secure communication using secure multicasting in iNet environment. The main issue with key management is determining how to securely distribute the keys among multicast members and secure the data. The Multicast Key Management can be accomplished with a Symetric Key Management Center (KMC), with a Public Key Authority, or with a combination of the two. In order to secure multicast iNet data, these data should be segmented based on security levels. Table 1 indicates segmentation of multicast groups and test data based on security level. In this example, security group or domain designation includes clearance classification and "need to know" access level. Multicast users located in the ground station network, would have access to certain data based on security clearance.Test Data (Fuel Data, Wing Data, Fuselage Data and Radar Data) are encrypted based on the security levels (V, W and Y). The encryption solution includes the deployment of KMC based on public key infrastructure (PKI). The set of computer systems, organizations and policies that issue and manage certificates is known as PKI.The KMC manages the creation and distribution of encryption keys and user certificates.

Table 1: Test Data and Multicast Group segmented based on Security Level

Example Test Data	Security Group	Multicast Group
Fuel Data	V	1
Wing Data	W	2
Fuselage Data	W	2
Radar Data	Y	3

The security clearance of users is used to determine which multicast groups they can join. Based on the security level of the users, the KMC distributes a session key to a particular multicast group. A Public-key method is used to distribute the session key and the session key is then used to encrypt the data. This session key is used to encrypt and decrypt segmented test article data.There is a hierarchy of keys in KMC. Typically, there are session keys, private keys and public keys. Session key is a temporary key used for encryption of data between users and logical connections. Before distributing the session keys to all the multicast members, it is necessary to distribute public certificates.

4.1 Public Certificates

Since private keys are used to authenticate users and organizations, there must be a method of validating the identity of multicast member or group before a key pair is issued. Proof of an identity is documented in electronic certificates issued by certificate authorities. In this paper, a certificate authority refers to KMC hat validates the identity of a multicast member or group that has a public key. KMC assigns the public/private key pair and generates the certificate. A certificate contains information about the holder's the private key component of the public key. It also contains information about the KMC as well as the digital signature of the KMC, which authenticates the certificate. The certificate of the certificate authority is called the root certificate. PKI depends on public trust of each of the established certificate authorities. Figure 6 shows the main components of a certification.

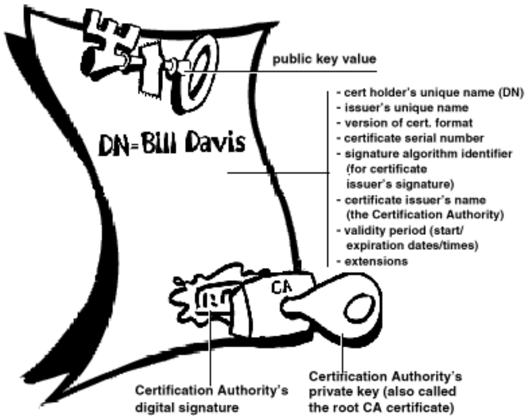
DN=Bill Davis
public key value
- cert holder's unique name (DN)
- issuer's unique name
- version of cert. format
- certificate serial number
- signature algorithm identifier (for certificate issuer's signature)
- certificate issuer's name (the Certification Authority)
- validity period (start/ expiration dates/times)
- extensions
CA
Certification Authority's digital signature
Certification Authority's private key (also called the root CA certificate)

Fig6: Information contained in a Certificate from [8].

4.2 Multicast Group Session Key Management Scenario

When multicast members need to communicate between each other, KMC distributes the session keys using public-key cryptosystem. Figure 6 represents the multicast key management scenario [6] where each user acquires a domain session key for the group. This assumes that certificates are in place for all users. This step can be accomplished before the test or dynamically as part of a test.

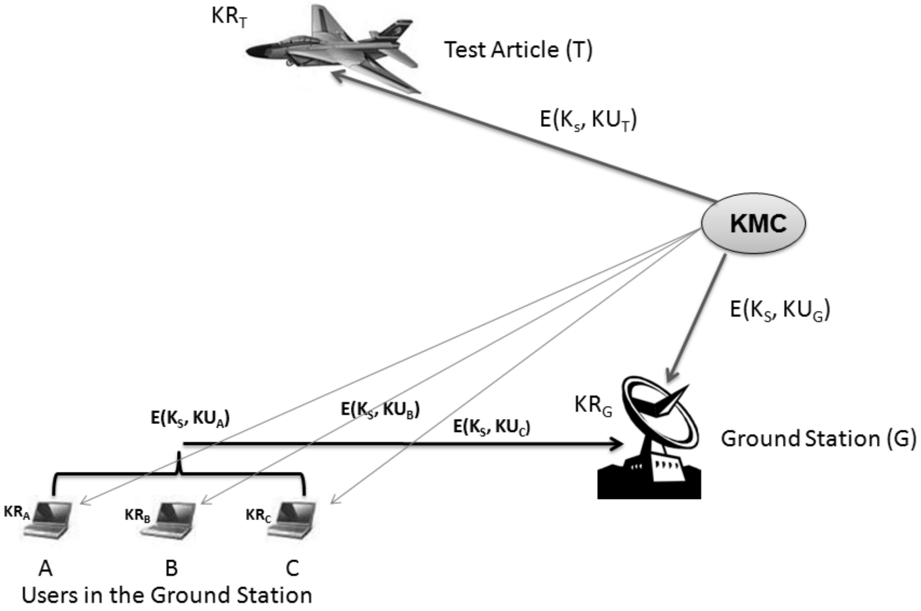

Fig 7: KMC distributingGroup Session Keys using Public-key Cryptosystem.

When a member joins a multicast group, the KMC distributes a public certificate that includes private and public keys. To start a logical connection between multicast groups, KMC needs to distribute session keys to them. Let's take a scenario where a test article T needs to sends a message to some multicast members in the ground station network. The following steps should be taken into consideration as shown in figure 7.

i. Each test article (T) requests a session key to KMC.

ii. Since all the multicast members have public certificates, KMC will forward encrypted session key K_S and related public keys KU_T, KU_A, KU_B and KU_C as shown in the following equation:

$$KMC \xrightarrow{E_{KU_T}(K_S)} T \tag{6}$$

Equation 6 only represents encrypted session key and public key assigned only to a test article. Similarly, same kind of message is sent out to all the multicast members in the ground station network (Users A, B, and C) as listed in the following equations:

$$KMC \xrightarrow{E_{KU_A}(K_S)} A \tag{7}$$

$$KMC \xrightarrow{E_{KU_B}(K_S)} B \tag{8}$$

$$KMC \xrightarrow{E_{KU_C}(K_S)} C \tag{9}$$

iii. It is a time for multicast group members to decrypt that encrypted session key using their particular related private keys KR_T, KR_A, KR_B and KR_C as shown below:

$$KMC \xrightarrow{E_{KR_T}[E_{KU_T}(K_S)]} T \tag{10}$$

In equation 10, test article decrypts the encrypted session key using its own private key, KR_T. In the same way, the users in the ground station network also decrypt the encrypted session key using their related private keys as shown below:

$$KMC \xrightarrow{E_{KR_A}[E_{KU_A}(K_S)]} A \tag{11}$$

$$KMC \xrightarrow{E_{KR_B}[E_{KU_B}(K_S)]} B \tag{12}$$

$$KMC \xrightarrow{E_{KR_C}[E_{KU_C}(K_S)]} C \tag{13}$$

In this way, KMC distributes session keys to all the multicast group members using public-key cryptosystem. Now, session keys are used on encrypting all the messages in one communication session. When a multicast member joins or leaves the multicast group, the group session keys can be updated and sent to all the multicast members. The group session keys are encrypted and distributed using public-private keys pairs of each multicast user. When a test packet is created and sent via multicast, routers on the network copy that packet to hosts who have subscribed to that domain.

5. RESULT

The paper summarized multicast routing algorithms incorporating public-key cryptography and KMC, securing the data transmitting from one multicast member to other multicast member based on the security clearance classification. Based on the security clearance, multicast members are classified into different groups/domains in order to distribute session key. A new session key should be issued for each session or exchange of data so that an opponent has less time to attack the key. Double encryption protocol of public-key scheme was used to provide both authentication and confidentiality to provide stronger security in iNet environment. In this way, a secure multicast architecture is shown to be feasible.

6. CONCLUSION AND FUTURE WORK

To recapitulate, it is evident that IP multicasting is important for theiNet system. IP multicasting enables many applications that require sending packets from one host to many hosts in a network. PIM-SM can be the foundation for communications in a network service and will help to unleash the full bandwidth of the network, allowing an enhanced flow of traffic and optimizing the performance of the network. This paper has attempted to present the relationship between IP multicasting, KMC and public-key cryptosystem. The present study suggests that KMC allows multicast members to communicate with each other in a secure and effective way. The double encryption of the public-key cryptosystem seems is an appealing and innovative scheme to secure iNet data. Beyond the encryption and digital signature, PKI is a good algorithm to effectively manage and use keys and certificates. These public keys can then be used to dynamically distribute multicast session keys. In the future work, traffic analysis can be investigated for multicast operation using OPNET (Optimized Network Engineering Tools) modeler. Moreover, studying a simple symmetric key management schemes can be for a simpler, but less dynamic approach.

7. ACKNOWDLEDGEMENTS

The authors would like to express appreciation to TRMC, SRC and CSC for their support for this effort and heartfelt gratitude to my advisor, Dr. Dean, and my senior, Dr. Maozzami for providing such fruitful discussions, comments and support.

8. REFERENCES

[1] Liebeherr, Jorg and Zarki, Magda, Mastering Networks: An Internet Lab Manual, Addison-Wesley, 2003.
[2] Stallings, Williams, Data and Computer Communications, Seventh Edition, Upper Saddle River, NJ: Pearson Prentice Hall, 2004.
[3] Gosh, Sujoy, Indian Institute of Technology, [Video], Kharagpur, India. : Center for Educational Technology, 2005. Available: http://www.youtube.com/watch?v=TApIo_BiX6U
[4] Stevens, William, TCP/IP Illustrated, First Edition, Addison-Wesley, 1994.
[5] Deering, Steve, "Host Extensions for IP Multicasting, (RFC 1112)," The Internet Engineering Task Force, 1989, Available: http://www.ietf.org/rfc/rfc1112.txt
[6] Stallings, Williams, Cryptography and Network Security, Second Edition, Upper Saddle River, NJ: Pearson Prentice Hall, 1999.
[7] Estri, Farinacci, Helmy, Thaler, Deering, Handley, Jacobson, Liu, Sharma and Wei, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, (RFC 2117)," 1997. Available: http://www.ietf.org/rfc/rfc2117.txt.
[8] Adler, Mark and Gailly, Jean-Loup, An Introduction to Cryptography, PGP Corporation, 2004.