Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2006, Article ID 61769, Pages 1–12
DOI 10.1155/WCN/2006/61769

Key Management for Secure Multicast over IPv6 Wireless Networks

Win Aye[1] and Mohammad Umar Siddiqi[2]

[1] *Faculty of Information Technology, Multimedia University, Jalan Multimedia, 63100 Cyberjaya, Selangor, Malaysia*
[2] *Faculty of Engineering, International Islamic University Malaysia, Jalan Gombak, 53100 Kuala Lumpur, Malaysia*

Received 26 September 2005; Revised 21 April 2006; Accepted 17 May 2006

Multicasting is an efficient method for transmission and routing of packets to multiple destinations using fewer network resources. Along with widespread deployment of wireless networks, secure multicast over wireless networks is an important and challenging goal. In this paper, we extend the scope of a recent new key distribution scheme to a security framework that offers a novel solution for secure multicast over IPv6 wireless networks. Our key management framework includes *two scenarios* for securely distributing the group key and rekey messages for joining and leaving a mobile host in secure multicast group. In addition, we perform the security analysis and provide performance comparisons between our approach and two recently published scenarios. The benefits of our proposed techniques are that they minimize the number of transmissions required to rekey the multicast group and impose minimal storage requirements on the multicast group. In addition, our proposed schemes are also very desirable from the viewpoint of transmission bandwidth savings since an efficient rekeying mechanism is provided for membership changes and they significantly reduce the required bandwidth due to key updating in mobile networks. Moreover, they achieve the security and scalability requirements in wireless networks.

1. INTRODUCTION

Multicast communication has been at the center of interest in the area of Internet activities for commercial, military, distributed, and group-based applications. A multicast address is designed to enable the delivery of datagrams to a set of hosts configured as members of a multicast group in various scattered subnetworks [1]. A local multicast router periodically sends the membership query messages using MLDv2 [2] for IPv6 in a multicast group. Any host that wishes to join the group replies with a membership report message. A multicast router periodically gathers and manages the membership report messages and then sends a join message to the upstream-multicast routers. A multicast branch is constructed between two adjacent multicast routers based on multicast membership information. The link of multicast branches forms the multicast delivery tree. This tree can be built using different techniques between source and receivers. Most of current researches concentrate on providing multicast for real-time applications in wired networks [3, 4].

Along with widespread deployment of wireless networks, it is believed that a large number of services requested by mobile users will be multicasted to them from various service providers. Content and service providers are increasingly interested in supporting multicast communications over wireless networks. Businesses can use wireless multicast to distribute software, news updates, and stock quotes to branch offices. Wireless multicast becomes a challenging task and a topic of great interest to Internet service providers. However, many important issues must be addressed before multicast can be widely deployed, including new business models for charging wireless customers and for revenue distribution among providers [5].

The security aspects are as important as performance and low energy consumption in many wireless applications. For secure wireless multicasting, we need cryptography and key management schemes in which cryptographic keys must be used to encrypt and decrypt messages. The cryptographic keys must also be recalculated and redistributed upon certain events such as a member joining and leaving the group. It must ensure that only authorized participants to the group may access the distributed keys and group data [6]. For secure multicasting in a wireless environment, we must consider other factors: battery power, bandwidth constraints, host mobility, loss of packets, and wireless security issues [7].

The new services on future wireless networks are the lack of thorough and well-defined security solutions that meet the challenges posed by wireless networks. We believe that an integrated approach to security development, which considers both network and application-specific issues, is critical to facilitating the ultimate deployment of a secure, pervasive computing infrastructure. In particular, security algorithms and protocols for wireless computing must be designed to consider the resource limitations of network nodes, the mobility of network nodes, and the underlying interworking of wireless networks.

Most researchers focus on two main kinds of wireless multicasts: multicast for infrastructure-based wireless network and multicast for ad hoc networks. Infrastructure-based wireless networks involve base stations and switches in a fixed topology. On the other hand, ad hoc wireless networks contain no fixed structure; all network components are subject to move without any constraints. In this paper, our proposed key management framework focused on infrastructure-based wireless network.

This paper contains three main contributions. First, we present our proposed schemes for securely distributing the group key and rekey messages for joining and leaving a mobile host in secure multicast group over IPv6 wireless network. Our proposed scheme includes (1) group creation, (2) initial key distribution, (3) new member join, (4) member leave, (5) handover process, and (6) multicast data distribution. Second, we perform the security analysis regarding group key security and group data secrecy. Third, we provide performance comparisons between our approach and the corresponding scenario in [8].

The rest of the paper is organized as follows. Section 2 outlines the issues of security requirements included in our approach. The detail explanations of our proposed schemes and security analysis on them are described in Section 3. The performance comparisons between our approach and scenarios in [8] are provided in Section 4. Concluding remarks are provided in Section 5.

2. SECURITY AND SCALABILITY REQUIREMENTS IN WIRELESS NETWORKS

Backward secrecy and forward secrecy are two important security properties encountered in group key distribution. To achieve forward and backward secrecy, the group key is updated after each member join and departure event, and the new key information is distributed to the legitimate group members. It is important to update and distribute the keys in a secure, scalable, and reliable way. In this section, we outline the issues of security and scalability requirements in wireless multicast. The fundamental services of secure multicast for wireless networks [6, 9] are as follows.

Authentication

This provides access control to the network by denying access to client stations that cannot authenticate properly. This service addresses the question, "Are only authorized persons allowed to gain access to my network?"

Confidentiality

It was developed to provide "privacy achieved by a wired network." The intent was to prevent information compromise from casual eavesdropping (passive attack). This service, in general, addresses the question, "Are only authorized persons allowed to view my data?"

Integrity

This service ensures that messages are not modified in transit between the wireless clients and the access point in an active attack. This service addresses the question, "Is the data coming into or exiting the network trustworthy—has it been tampered with?"

Group key secrecy

This property guarantees that it is computationally infeasible for an adversary to discover any group key.

Backward secrecy

The join user cannot decrypt the content that was sent before his join.

Forward secrecy

The departure/revoked user cannot decrypt the content that is sent after his deletion from the group.

1 affects n

This failure occurs when a group member affects all the other members.

1 does not equal n

This failure occurs when a protocol has to deal with each member separately.

3. OUR APPROACH

Our key management framework includes two scenarios for secure multicast over wireless network. One is key distribution on decentralized architecture for mobile multicast (DAMM) and another is key distribution on centralized architecture for mobile multicast (CAMM).

During the group initialization, the approach DAMM is more efficient than CAMM. Moreover, it requires a storage space less significant than others. On the other hand, CAMM is more efficient for dynamic groups, because it distributes the computational cost of rekeying among the whole group. The CAMM resolves the failure *1 affects n* by dividing the multicast group into subgroups. Each subgroup, managed by

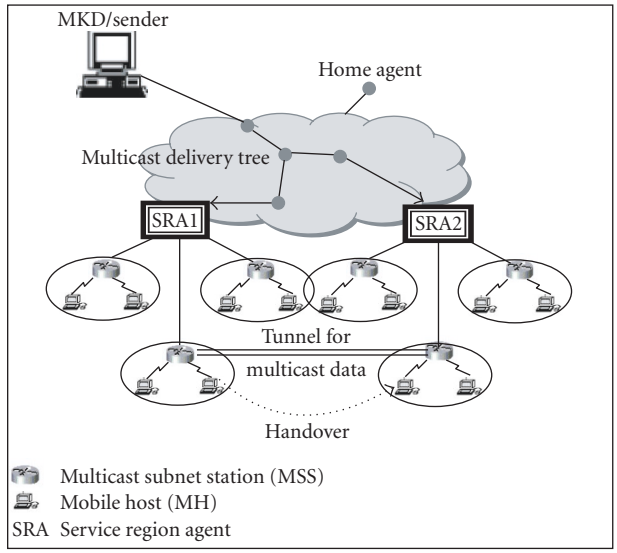

Figure 1: Multicast enabled delivery path over IPv6 wireless network.

a local controller, has its own key. The subgroups are linked by intermediate agents for building a virtual group. The intermediate agent role is to translate the multicast data diffused by a member within its subgroup to all members of the virtual group. Consequently, CAMM fits better dynamic groups. However, it is less efficient for diffusion of group data which undergoes encryption and decryption operations by the intermediate agents. On the other hand, DAMM is more efficient for data diffusion because it uses only one key shared among group members. DAMM is also a solution for scalability problems, in particularly for the revocation problem, *1 does not equal n*.

Both scenarios include (1) group creation, (2) initial key distribution, (3) new member join, (4) member leave, (5) handover process, and (6) multicast data distribution. We also perform the security analysis regarding group key security and group data secrecy. In addition, we provide performance comparisons between our approach and the corresponding scenarios in [8].

The multicast enabled delivery path is shown in Figure 1. The components included in our approach referred to Figure 1 are multicast key distributor (MKD), service region agent (SRA), multicast subnet station (MSS), and mobile hosts (MH).

Multicast key distributor

MKD manages all the access control, accounting, logging, and key distribution and data traffic distribution to a set of multicast support stations (MSS_i). It also distributes the data encryption key to group members when they subscribe. The effects of group dynamics and host mobility are confined to each subnet, thus MKD is free from the rekeying operations upon join and leave operations.

Service region agent

There is only one SRA in which several subnets form a service region. SRA is a multicast router and will act as the core on the multicast delivery tree.

Multicast subnet station

MSS acts as a proxy for the mobile hosts by honestly relaying the data traffic to the mobile hosts and correctly managing the control traffic. There is only one MSS in each subnet that provides multicast service to all mobile hosts in that subnet. SRA and MSS are correctly managing the control traffic and they are the multicast listener delivery (MLD) capable IPv6 routers to discover the presence of interested receivers of a given multicast group. SRA and MSS use the multicast listener discovery version 2 (MLDv2) (Vida and Costa, 2004) protocol that allows a host to inform its neighboring routers of its desire to receive IPv6 multicast transmissions.

Mobile host

MH_i are mobile hosts in each subnet. The group dynamics and host mobility are confined to the subnet level. MH_i are connected with MSS_i via broadcast, transmission channel such as air. MH_i logically belong to one cell only at any given instance.

Our approach exploits the physical separation between the wired and wireless portions of the network. It is divided into two scoped areas. MKD, SRA, and MSS comprise the wired portion of the network, and MSS and MH_i comprise the wireless portion of the network shown in Figure 1. DAMM and CAMM use the region-based hierarchical multicast routing protocol (RHMoM) [10] on IPv6. In RHMoM,

a tunnel is built between previous multicast subnet station (MSS_p) and current multicast subnet station (MSS′). This makes the multicast service interruption time very short because the tunnel is much shorter than that between the mobile host and its home agent, especially when the mobile host is far away from its home network. The subnets are also clustered into different regions and the multicast delivery tree will be reconstructed at most one time when mobile host moves into a new service region, and when a mobile host moves around all subnets within the same MSS's region, the multicast delivery tree will not be reconstructed.

One-to-many multicast applications such as stock quote exchange systems, scheduled audio/video (a/v) distribution, and push media have a single sender and multiple simultaneous receivers, and transmission is unidirectional from one sender to many receivers. In this type of application, a single sender transmits secret information to a large number of patrons. Secret information would need to be encrypted and only paying users should have the decryption keys. One of the issues that must be addressed in secure sessions is key distribution, that is, how to securely distribute the keys to all members of a group. Multicast-based applications such as video conferencing, Internet broadcasting, and real-time finance data distribution will play an important role in the future of the Internet as continued multicast encourages their use and deployment. In this paper, we consider a stock exchange system as an example of one-to-many large group communication in which a single sender distributes its stock quotes to its customers.

3.1. Assumptions on proposed schemes

For both scenarios, we assume that multicast key distributor (MKD) is colocated with the sender only for the simplification purpose. MKD may be a group organizer and has the right to create the secure groups on Internet.

In our approach, we assume that all members must have a capability certificate (CC) from the designated certification authority (CA) to enforce the group access control and distribute their public keys securely and keep them initially through an off-line method. CA is a trusted third party that issues certificates for each entity. We assume that all public keys of responsible entities involved in our approach had been registered in the CA. We also assume that MKD and MSS keep CA's public key to verify the authenticity of each mobile node's certificate.

Our proposed schemes use RSA [11] encryption algorithm for securely distributing the signed TEK and other keys. RSA is a public key scheme based on security due to the difficulty of factoring large numbers. They also use ECDSA digital signature [12] scheme whose efficiency is superior to existing signature schemes for signing the broadcast access key (BAK). For symmetric key encryption, we use IDEA and MD5 [13] for message integrity. Prior to initial key distribution, each mobile host generates a public and private key pair using RSA encryption algorithm and publishes the public key (n, e) (i.e., it registers its public key in CA) shown in Algorithm 1. MKD and MSS also generate ECDSA key pair and publish its public key. The key generation procedures of ECDSA key pair generated by BAKD are shown in Algorithm 2.

(1) Each mobile node generates two large random primes, p and q [11], of approximately equal size such that their product $n = pq$ is of the required bit length.
(2) Compute $n = pq$ and (φ) phi $= (p-1)(q-1)$.
(3) Choose an integer $e, 1 < e < \varphi$, such that $\gcd(e, \varphi) = 1$.
(4) Compute the secret exponent $d, 1 < d < \varphi$, such that $ed \equiv 1 (\mathrm{mod}\, \varphi)$.
(5) The public key is (n, e) and the private key is (n, d). The values of p, q, and φ should also be kept secret.
    (i) n is known as the modulus.
    (ii) e is known as the public exponent or encryption exponent.
    (iii) d is known as the secret exponent or decryption exponent.

Algorithm 1: RSA key generation procedures.

(1) Select an elliptic curve E defined over Zp. The number of points in $E(Zp)$ should be divisible by a large prime n.
(2) Select a point $P \in E(Zp)$ of order n.
(3) Select a statistically unique and unpredictable integer d in the interval $[1, n-1]$.
(4) Compute $Q = dP$.
(5) MSS's public key is (E, P, n, Q) and private key is d.

Algorithm 2: ECDSA key generation procedures.

The capability certificate contains entity's identity, entity's ECDSA signature public key, or entity's RSA public key plus CA's signature over these. For example, the capability certificate of mobile host is $CC_{MH} = \{$MH's Identity, KU_{MH}, $S_{CA}[$MH's Identity, $KU_{MH}]\}$. To achieve the requirements of secure key distribution, the best solution is to combine the public and secret key systems in order to optimize the speed of symmetric key encryption while maintaining the security of public key encryption.

3.2. DAMM: key distribution algorithms

In this section, we propose the key distribution algorithms on decentralized architecture for mobile multicast (DAMM) on IPv6. The physical architecture and components are described in Figure 1.

In DAMM, a single group key (TEK) is used at any time to encrypt the *group traffic*. SRA and MSS_i are fully trusted and delegated by MKD so that they receive the group key (TEK) and distribute it to mobile hosts in their own sub-network. Whenever the membership changes within the

subnets, MSS can play the role of MKD and can create a new group key (TEK_{new}). It also accepts or refuses a new member within the subnet and notifies the other multicast subnet stations of any change in the subnet. We assume that SRA1 and SRA2 are adjacent, wired, and they are already preauthenticated with each other via the secure channel. The notation used in this section is described in Table 1.

3.2.1. Group creation

Group creation is managed by the MKD. MKD is configured with group and access control information. MKD may be a group organizer and has the right to create the secure groups on Internet. Before holding a group session, multicast key distributor (MKD) has to prepare the members who are willing to join the group by other means (e-mail, fax, phone, post, etc.). MKD holds the group control list (GCL). MKD sends the updated GCL to all multicast subnet stations (MSS_i).

Whenever a mobile host joins or leaves the multicast group, GCL is updated. After preparing the member list, MKD sends the invitation message to all the initial members and then waits for them to join. Upon receipt of the reply messages from members, MKD starts the initial key distribution.

The group controller MKD starts the process of the group initialization by creating the group key TEK. For simplification purposes, we assume that every MSS can securely generate the cryptographic keys. Whenever the membership changes within the subnets, MSS is delegated by MKD. MSS can play the role of MKD and can create a new group key (TEK_{new}). The MSS also accepts or refuses a new member within the subnet and notifies the other multicast subnet stations of any change in the subnet. Then, the group controller MKD communicates the key TEK to group members via local controllers MSS.

(1) Initial key distribution

The multicast key distributor (MKD) starts the process of the group initialization by creating the traffic encryption key (TEK). For simplification purposes, we assume that every controller (MSS) can securely generate cryptographic keys. Then, the MKD communicates the key TEK to group members via local controllers (MSS). The decentralized nature of DAMM uses a single group key (TEK) at any time to encrypt or decrypt the group traffic.

In Step 1, MKD distributes the encrypted message that includes its signed group key (TEK), its public key, and priority number of MSS to all multicast subnet stations. In Step 2, MSS sends the encrypted message that includes its signed secret key and its public key to mobile hosts. Eventually, the group key (TEK) is forwarded to the legitimate mobile hosts within the subnets.

Step 1.

$$\mathrm{MKD} \Rightarrow \mathrm{MSS_i} : \mathrm{EP}_{\mathrm{KU}_{\mathrm{MSSi}}}[\mathrm{S}_{\mathrm{KR}_{\mathrm{MKD}}}[\mathrm{TEK}],\ \mathrm{KU}_{\mathrm{MKD}}, \mathrm{MSS}_{\mathrm{pri}}]. \tag{1}$$

Table 1: Notation used in Section 3.

CC_{MH}	Capability certificate of mobile host
$EP_{KR_{MKD}}$	Public key encryption with the private key of MKD
$EP_{KU_{MKD}}$	Public key encryption with the public key of MKD
ES_{SKi}	Symmetric key encryption with the secret key SK_i
f	One-way hash function
Id	Identifier (IP address)
KC-Msg	Key change message
$S_{KR}[M]$	Message M is signed by private key
SEK_i	Subnet encryption key for multicast subnet station i
SM	Secret key from sender to multicast subnet station
SK_i	Secret key of mobile host i
TEK	Traffic encryption key

Step 2.

$$\begin{aligned} &\mathrm{MSS_i} \Rightarrow \mathrm{MH_i} : \mathrm{EP}_{\mathrm{KU}_{\mathrm{MHi}}}[\mathrm{S}_{\mathrm{KR}_{\mathrm{MSSi}}}[\mathrm{SK_i}], \mathrm{KU}_{\mathrm{MSSi}}], \\ &\mathrm{MSS_i} \Rightarrow \mathrm{MH_i} : \mathrm{EP}_{\mathrm{KR}_{\mathrm{MSSi}}}(\mathrm{ES}_{\mathrm{SK_1}}[\mathrm{TEK},\ \mathrm{MSS}_{\mathrm{pri}}], \ldots, \\ &\qquad\qquad \mathrm{ES}_{\mathrm{SK_i}}[\mathrm{TEK},\ \mathrm{MSS}_{\mathrm{pri}}]). \end{aligned} \tag{2}$$

3.2.2. New member join

In join procedure, a local multicast router, MSS periodically sends membership query messages using multicast listener discovery (MLDv2) [2] for IPv6. Any host that wishes to join the group replies with a membership report message. A multicast router periodically gathers and manages the membership report messages, and then sends a join message to the upstream-multicast routers. There are two steps: source level subscription and subnet-level subscription. There are two steps for join operation.

Step 1 is concerned with a mobile host wishing to become a member of a multicast group. If the new mobile host wants to join the multicast group, it sends a join request that includes its capability certificate with MLD membership report to a multicast subnet station (MSS). A mobile host capability certificate contains MH's identity and public key.

In Step 2, MSS authenticates the new host's join request. If authentication is successful, it generates the new TEK and shared secret key SK. Then MSS encrypts the TEK_{new}, the new shared secret key SK_{new}, and MSS's priority with new mobile host public key, and sends it to a new mobile host. MSS also encrypts TEK_{new} with old TEK and multicasts it to the other multicast subnet stations and to its existing mobile receivers.

Step 1.

$$\mathrm{MH}_{\mathrm{new}} \Rightarrow \mathrm{MSS} : \mathrm{CC}_{\mathrm{MHnew}}. \tag{3}$$

Step 2.

$$\begin{aligned} &\text{MSS} \Rightarrow \text{MH}_{\text{new}} : \text{EP}_{\text{KU}_{\text{MHnew}}}[\text{TEK}_{\text{new}},\ \text{SK}_{\text{new}},\ \text{MSS}_{\text{pri}}], \\ &\text{MSS} \Rightarrow \text{MH}_{\text{i}},\ \text{MSS}_{i} : \text{ES}_{\text{TEK}_{\text{old}}}[\text{TEK}_{\text{new}}]. \end{aligned} \tag{4}$$

3.2.3. Member leave operation

It is possible that a mobile receiver (MH_{i}) may want to leave from the multicast group either compulsorily or voluntarily. For both cases, the group key must be rekeyed. In Step 1, MSS encrypts the created TEK_{new} and its priority number with the old TEK. Next, MSS multicasts this encrypted message only to the multicast subnet stations and service region agents, upstream, which are capable to decrypt. To guarantee the forward secrecy, MSS must not forward this message to its mobile receivers (MH_{i}) within its subnetwork. MSS unicasts the new key TEK_{new} to them under their respective unique secret keys (SK_{i}), but not the evicted one shown in Step 2. The priority number of the local controller (MSS) must be included in these messages.

An evicted member cannot any more obtain the new group key because its MSS, which proceed to change the key (TEK), multicasts the new TEK, downstream, to members under their respective unique secret keys, but not to the evicted one. We assume that the evicted member is only linked to one subnetwork. Thus, evicted members cannot retrieve the new traffic encryption key-TEK_{new}.

Step 1.

$$\text{MSS} \Rightarrow \text{MSS}_{\text{i}} : \text{ES}_{\text{TEK}_{\text{old}}}[\text{TEK}_{\text{new}},\ \text{MSS}_{\text{pri}}]. \tag{5}$$

Step 2.

$$\begin{aligned} \text{MSS} \Rightarrow \text{MH}_{\text{i}} : &\ \text{ES}_{\text{SK}_1}[\text{TEK}_{\text{new}}, \text{MSS}_{\text{pri}}], \ldots, \\ &\ \text{ES}_{\text{SK}_{\text{i}}}[\text{TEK}_{\text{new}}, \text{MSS}_{\text{pri}}]. \end{aligned} \tag{6}$$

In order to maintain the synchronization of the use of data encryption key TEK, all group members use the same TEK at the same time, join and leave operations can be buffered at a break point. During the membership changes, all multicast group members may receive many traffic encryption keys (TEKs) sent by different multicast support stations (MSS_{i}) at a break point. In order to use the same group key (TEK) at the same time, group members may choose one of the group keys coming from the multicast subnet stations with the highest priority number (the smallest priority number).

3.2.4. Handover process

Handover process is concerned with a mobile host moves from one IP network to another shown in Figure 2. In this case, we combine the protocol RHMoM [10] with our join procedure (Section 3.2.2) described as follows.

(1) If the mobile host is the first member of desired multicast group in the new subnet, the current MSS′ builds a tunnel between the mobile host and the previous multicast subnet station (MSS_{p}) on the previous network and gets the packets from MSS_{p}. At the same time, the current MSS′ sends an MLD report message to its service region agent SRA.

(2) If there are hosts in the subnet that have already been in the group, the mobile host can get multicast packets from the current MSS′ without any additional operations and it is not needed to build a tunnel between the current MSS′ and previous subnet MSS_{p}. The mobile host receives the multicast packets by the tunnel and it sends an MLD group report messages to the MSS′ on the current network to start to rejoin the procedure (using the same member join procedure referred to Section 3.2.2).

(3) After receiving the multicast packets directly from the MSS′, the tunnel will be removed.

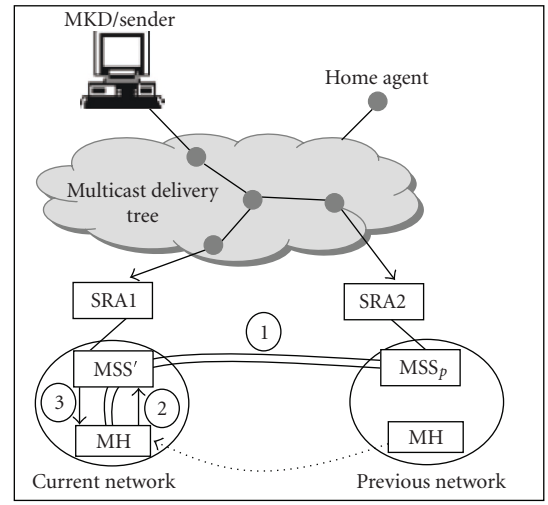

Figure 2: Handover process.

3.2.5. Multicast data distribution

Message plus concatenated hash code is encrypted using $\text{TEK-ES}_{\text{TEK}}[\text{M} \parallel \text{H(M)}]$ by the sender. The sender sends this encrypted message to multicast support stations and MSS_{i} then forward it to their mobile hosts. All mobile receivers of the multicast group with TEK can decrypt the multicast data. In this case, the hash code provides the structure required to achieve authentication. Because encryption is applied to the entire message plus hash code and confidentiality is also provided since the sender and mobile hosts share the secret key, the message must have come from sender.

DAMM's keys assigned to MKD, MSS, and MH are shown in Table 2.

3.2.6. Security analysis on DAMM

In this section, we discuss group key security and group data secrecy on decentralized architecture for mobile multicast (DAMM).

Table 2: DAMM assigned keys.

Keys	Owner	Shared user
TEK, KU_{MKD}	MKD	MSS
TEK, KU_{MKD}	MKD	MH_i
KU_{MSS}	MSS	MKD
SK_i	MSS	MH

(1) Group key security

During the traffic data encryption key (TEK) distribution phase in Section 3.2.1(1), an opponent may substitute the encrypted message—$EP_{KU_{MSSi}}[S_{KR_{MKD}}[TEK], KU_{MKD}, MSS_{pri}]$. However, the opponent would be extremely difficult to alter the message without knowing the MSS's private key and only MKD could create the signed TEK-$S_{KR_{MKD}}[TEK]$. In addition, traffic data encryption key (TEK) is providing both the authentication function and confidentiality by a double use of the public key scheme. Thus, this attack fails.

A new join member cannot obtain the old TEK key because its MSS_i updates the traffic data encryption key (TEK). MSS_i then encrypts TEK_{new}, secret key (SK_{new}) and MSS's priority number with the new mobile host's public key—$EP_{KU_{MHnew}}[TEK_{new}, SK_{new}, MSS_{pri}]$ and sends it to the new mobile host. Then MSS_i multicasts the encrypted key change message—$ES_{TEK_{old}}[TEK_{new}]$ to its existing mobile receivers under its old local traffic encryption key. Hence, the new member cannot retrieve the old traffic encryption key.

Similarly, an evicted mobile host cannot obtain any new group key because its MSS_i updates the subnet encryption key-SEK. MSS_i then multicasts the encrypted new traffic encryption key and MSS's priority number—$ES_{SK_1}[TEK_{new}, MSS_{pri}], \ldots, ES_{SK_i}[TEK_{new}, MSS_{pri}]$ to its only remaining mobile receivers. Thus, the evicted member cannot retrieve the new traffic encryption key and he cannot know the new traffic encryption key.

(2) Group data secrecy

Only group members *owning the traffic encryption key (TEK)* can decrypt the group data. *Multicast subnet stations cannot get the group data* and group data confidentiality is assured.

During the membership changes, all group members can choose the same TEK from different rekeying message and start to use it at the next break point. Hence, the new members and evicted members cannot access old and new group data because they cannot retrieve the old and new group keys.

3.3. CAMM: key distribution algorithms

In this section, we propose the key distribution algorithms on centralized architecture for mobile multicast (CAMM) on IPv6. In this scenario, multicast subnet stations (MSS_i) are not trusted and used to assist in enforcing the secure multicast group without having any access to the multicast data. We propose key distribution algorithms regarding four operations: group creation, member join, member leave, and multicast data distribution. The physical architecture and components are similar to the one described in Section 3, for DAMM refer to Figure 1.

3.3.1. Group creation

Group creation is similar to the one described in Section 3.2.1.

(1) Initial key distribution

In Step 1, MKD generates a random number as a traffic encryption key (TEK). It then encrypts its signed TEK, public key, and secret key (SM) with MSS_i's public key. Then MKD sends this encrypted message to the multicast subnet stations.

In Step 2, the corresponding MSS decrypts it with its private key and stores the MKD's public key and secret key (SM). Then MSS reencrypts the message that includes sender's signed TEK, public key, local subnet encryption key, and unique secret key (SK) under the public keys of each mobile receiver and sends it to each mobile receiver within their subnets. Then MKD updates the group control list (GCL).

Step 1.

$$\text{MKD} \Rightarrow \text{MSS}_i : EP_{KU_{MSSi}}[S_{KR_{MKD}}[\text{TEK}], KU_{MKD}, \text{SM}]. \tag{7}$$

Step 2.

$$\text{MSS}_i \Rightarrow \text{MH}_i : EP_{KU_{MHi}}[S_{KR_{MKD}}[\text{TEK}], KU_{MKD}, SEK_i, SK_i]. \tag{8}$$

Each mobile receiver decrypts the TEK, MKD's public key, subnet encryption key-SEK, and unique secret key (SK) with their corresponding private keys and MKD's public key.

3.3.2. New member join

This operation is concerned with a mobile host wishing to become a member of a multicast group. It includes two steps: source-level subscription and subnet-level subscription.

(1) Source-level subscription

In Step 1, when a new mobile host wants to join the multicast group, it sends the join request message that includes its capability certificate to multicast subnet station (MSS). Next, MSS forwards MH's capability certificate to multicast key distributor MKD.

In Step 2, MKD verifies MH's capability certificate. If the member is legitimate, MKD generates a random number as a traffic encryption key (TEK) and encrypts its signed TEK, its public key, and f(SM) with new MH's public key. Then, MKD sends this encrypted message to MSS. Next, MSS only forwards it to the new mobile host. MKD updates the group control list (GCL).

Step 1.

$$\begin{aligned} &MH_{new} \Rightarrow MSS : CC_{MHnew}, \\ &MSS \Rightarrow MKD : CC_{MHnew}. \end{aligned} \tag{9}$$

Step 2.

$$\begin{aligned} &MKD \Rightarrow MSS : EP_{KU_{MHnew}}[S_{KR_{MKD}}[TEK],\ KU_{MKD},\ f(SM)], \\ &MSS \Rightarrow MH_{new} : EP_{KU_{MHnew}}[S_{KRMKD}[TEK],\ KU_{MKD},\ f(SM)]. \end{aligned} \tag{10}$$

(2) Subnet-level subscription

In Step 1, the new mobile host requests the subnet encryption key (SEK) from its corresponding MSS by sending its capability certificate and encrypted f(SM) after receiving the traffic encryption key (TEK). Encrypted hash code f(SM) lets MSS_i know that the new mobile host has received the traffic encryption key (TEK) from MKD. Then, MSS_i authenticates the new MH's certificate and computes its own f(SM).

In Step 2, if authentication is successful and the computed f(SM) equals MH's presented f(SM), MSS encrypts its signed new subnet key (SEK_{new}) and secret key (SK_i) with new MH's public key and sends it to new mobile host. Verification of f(SM) shows that the new joining mobile node has received the traffic encryption key (TEK) from MKD. To guarantee the backward secrecy, MSS then multicasts the encrypted key change message—$ES_{SEK_{old}}$[KC-Msg] to its existing members. Each mobile receiver decrypts the KC-Msg and updates the subnet encryption key (SEK) by passing the key data through a randomly generated function in the key change message (Table 4).

Step 1.

$$MH_{new} \Rightarrow MSS : CC_{MH},\ EP_{KR_{MHnew}}[f(SM)]. \tag{11}$$

Step 2.

$$\begin{aligned} &MSS \Rightarrow MH_{new} : EP_{KU_{MHnew}}[S_{KR_{MSS}}[SEK_{new},\ SK_i]], \\ &MSS \Rightarrow MH_i : ES_{SEK_{old}}[KC\text{-}Msg]. \end{aligned} \tag{12}$$

The format of key change message used in mobile join and leave operations are shown in Table 4. The function type field in the key change message comprises four randomly generated functions based on SEK: *00 for hash function,* 01 for *4 bits left shift*, 10 *for no operation*, and 11 for *4 bits right shift*. The key version included in a key change message is increased whenever MSS wants to update its subnet encryption key (SEK) on join and leave operations.

3.3.3. Member leave operation

It is also possible that some mobile members may want to leave from the multicast group either voluntarily or compulsorily. For the first case, a mobile host sends a member leave request to the corresponding MSS. To guarantee the forward secrecy for both cases, MSS updates its local subnet encryption key (SEK) and sends the encrypted key change message to its remaining mobile receivers. Each of the mobile receivers decrypts the key change message with its respective shared secret keys (SK_i) and updates the local subnet key (SEK) by passing the key data through the randomly generated key change functions. Group control list (GCL) is updated on both MKD and MSS whenever a mobile host joins and/or leaves the multicast group.

Table 3: CAMM assigned keys.

Keys	Owner	Shared user
SM, KU_{KD}	MKD	MSS
TEK, KU_{KD}	MKD	MH_i
KU_{MSS}	MSS	MKD
SEK_i, SK_i	MSS	MH_i
KU_{MH}	MH	MKD

Table 4: Key change message.

	2 bits	16 bits
Node identifier	Function type	Key version

Step 1.

$$MH_{leave} \Rightarrow MSS : ES_{SK_i}[LEAVE]. \tag{13}$$

Step 2.

$$MSS \Rightarrow MH_i : ES_{SK_1}[KC\text{-}Msg], \ldots, ES_{SK_i}[KC\text{-}Msg]. \tag{14}$$

3.3.4. Handover process

Handover process in DAMM is similar to the one described in Section 3.2.4

3.3.5. Multicast data distribution

When a sender multicasts the group data (M) encrypted with a traffic encryption key-TEK first and then reencrypted with the corresponding subnet encryption key (SEK)-$ES_{SEK}[ES_{TEK}[M]]$. All mobile receivers of the multicast group with TEK and the corresponding local subnet key (SEK) can decrypt the multicast data.

CAMM's keys assigned to MKD, MSS, and MH are shown in Table 3.

3.3.6. Security analysis on CAMM

In this section, we discuss group key security and group data secrecy on CAMM.

(1) Group key security

During the traffic encryption key distribution phase in Section 3.2.1(1), an opponent may substitute the encrypted

message—$EP_{KU_{MHi}}$ [$S_{KR_{MKD}}$[TEK], KU_{MKD}, SEK_i, SK_i]. However, the opponent would be extremely difficult to alter the message without knowing the mobile host's private key and only MKD could create the signed TEK-$S_{KR_{MKD}}$[TEK]. In addition, traffic data encryption key (TEK) is providing both the authentication function and confidentiality by a double use of the public key scheme. Thus, this attack fails.

A new join member cannot obtain the old subgroup key because its MSS_i updates the local subnet encryption key (SEK). MSS_i then encrypts its signed new subnet encryption key (SEK_{new}) and secret key (SK_i) with the new mobile host's public key—$EP_{KU_{MHnew}}$ [$S_{KR_{MSS}}$[SEK_{new}, SK_i]] and sends it to the new mobile host. Then MSS_i multicasts the encrypted key change message—$ES_{SEK_{old}}$[KC-Msg] to its existing members under its old local subgroup key. Hence, the new member cannot retrieve the old local subgroup key.

Similarly, an evicted mobile host cannot obtain any new group key because its MSS_i updates the subnet encryption key-SEK. MSS_i then multicasts the encrypted key change message—ES_{SK_1}[KC-Msg], . . ., ES_{SK_i}[KC-Msg] to its only remaining mobile receivers. Thus, the evicted member cannot retrieve the key change message and he cannot know the new local subgroup key.

(2) Group data secrecy

Only group members (receivers) *owning the corresponding local subnet key (SEK) and the traffic encryption key (TEK)* can decrypt the group data. *Multicast subnet stations cannot get the group data* because they have *no traffic encryption key (TEK)*. When a new mobile host joins the group, the corresponding MSS updates its local subnet key. MSS_i then sends $(SEK_i)_{new}$ to the new mobile host and distributes the encrypted key change message to its existing mobile receivers. Thus the new joining member cannot get the previous (old) group data because the old group data is encrypted as $ES_{SEK_{old}}$[ES_{TEK}[M]]. He cannot know $(SEK)_{old}$. This achieves backward secrecy.

Similarly, when a mobile host leaves the group, the corresponding MSS_i distributes the encrypted key change message to its remaining members. The leaving member cannot retrieve the future group data because it is encrypted-[$ES_{(SEK)_{new}}$[ES_{TEK}(M)]]. He knows only TEK and $(SEK)_{old}$ keys. This achieves forward secrecy.

4. PERFORMANCE COMPARISON

4.1. Comparative analysis of DAMM with FT-MSS

In this section, we provide a comparative analysis of proposed scheme (DAMM) with *fully trusted mobile support stations* (FT-MSS) in [8]. Both schemes use the public and secret key systems to achieve scalable and secure key distribution. We compare the performance evaluation of these two scenarios based on storage requirements, new member join, member leave, and rekeying operations.

DAMM

(i) As we presented the initial key distribution in Section 3.2.1(1), the number of keys stored at an MSS depends on the number of mobile hosts within a subnet. However, the total keys stored at a mobile host are constant rather than increasing in logarithmic growth in the number of mobile hosts within the subnet.

(ii) In the case of a new member join in Section 3.2.2, MSS sends only one transmission to a new mobile host. The steps used in the member join operation are described as follows:

(1) $MH_{new} \Rightarrow MSS : CC_{MHnew}$,
(2) $MSS \Rightarrow MH_{new} : EP_{KU_{MHnew}}[TEK_{new}, SK_{new}, MSS_{pri}]$,
(3) $MSS \Rightarrow MH_i, MSS_i : ES_{TEK_{old}}[TEK_{new}]$.

(iii) In DAMM, MSS incurs less key decryption costs than FT-MSS. Each mobile receiver also incurs less key decryption costs than ST-MSS. MSS needs only one time to encrypt and decrypt the traffic encryption key (TEK) and subnet encryption key (SEK) during the group data transmission. Each mobile host incurs only one key decryption cost which is significantly reduced to retrieve the traffic encryption key (TEK) and unique secret key (SK). In this case, only three transmissions are required to receive all the node keys.

(iv) In the case of member leave (Section 3.2.3), the corresponding MSS changes the traffic encryption key (TEK) and encrypts TEK_{new} with the unique secret keys (SK_i) of remaining mobile receivers and multicasts that information to them. At the receiver side, each mobile host needs to decrypt only one time to get the new TEK. The number of transmissions required to rekey the mobile hosts within the subnet is significantly reduced from 2(log M) to 2.

FT-MSS

In initial key distribution on *fully trusted multicast support stations* (FT-MSS) in [8], the total keys stored at a mobile host are increasing in logarithmic growth in the number of mobile hosts within the subnet. The steps used in the member join operation on fully trusted multicast support stations are described as follows:

(1) $MKD \Rightarrow MSS : ES_{SK}[KEK_i, TEK_{new}]$, $S_{KR_{MKD}}[EP_{KU_{MSS}}[SK]]$,
(2) $MSS \Rightarrow MH_{new} : S_{KR_{MSS}}[EP_{KU_{MHnew}}[CEK]]$.

(i) In the case of a new member join, MSS incurs only two key encryption costs compared to (N + 3) for DAMM. Each mobile receiver incurs the same decryption costs as with DAMM.

(ii) MSS needs more encryption and decryption costs for traffic encryption key (TEK) and cell encryption key (CEK) during the group data transmission.

(iii) Each mobile receiver incurs more decryption costs to retrieve the traffic encryption key (TEK) and cell encryption key (CEK). In this case, the number of transmissions depends

on two times logarithmic growth in the number of multicast support stations.

(iv) In the case of member leave, MSS changes its cell encryption key (CEK) and key encryption keys (KEK_i) that is shared with other MSS_i according to the centralized tree VersaKey [14] to prevent MH from accessing the data traffic and guarantee the traffic forward secrecy at cell level. The number of transmissions required to rekey the mobile receivers depends on two times logarithmic growth in the number of multicast support stations.

4.2. Comparative analysis of CAMM with ST-MSS

In this section, we provide a comparative analysis of proposed scheme (CAMM) with *semi-trusted mobile support stations* (ST-MSS) in [8]. Both schemes use the public and secret key systems to achieve scalable and secure key distribution. We compare the performance evaluation of these two scenarios regarding storage requirements, new member join, member leave, and rekeying operations.

CAMM

(i) As we presented initial key distribution in Section 3.3.1(1), the total keys stored at a mobile host are constant rather than increasing in logarithmic growth in the number of mobile hosts within the subnet. The number of keys stored at an MSS is also constant.

(ii) In the case of a new member join described in Section 3.3.2, MKD sends only one transmission to a mobile host. The steps used in the member join operation are described as follows:

(1) $MH_{new} \Rightarrow MKD : CC_{MHnew}$,
(2) $MKD \Rightarrow MH_{new} : EP_{KU_{MHnew}}[S_{KR_{MKD}}[TEK], KU_{MKD}, f(SM)]$,
(3) $MH_{new} \Rightarrow MSS : CC_{MHnew}, EP_{KR_{MHnew}}[f(SM)]$,
(4) $MSS \Rightarrow MH_{new} : EP_{KU_{MHnew}}[S_{KR_{MSS}}[SEK_{new}, SK_i]]$,
(5) $MSS \Rightarrow MH_i : ES_{SEK_{old}}[KC\text{-}Msg]$.

(iii) In CAMM, MSS incurs less key encryption costs than ST-MSS. Each mobile receiver incurs less key decryption costs than ST-MSS. The new mobile receiver has to decrypt four times to get the traffic encryption key (TEK) and subnet encryption key (SEK). From the security viewpoint, both TEK and SEK are providing both the authentication function and confidentiality by a double use of the public key scheme [15]. The number of transmissions is reduced from 2(log M) to 5.

(iv) In the case of member leave (Section 3.3.3), the corresponding MSS changes its local subnet key and encrypts the key change message—$ES_{SK_1}[KC\text{-}Msg], \ldots, ES_{SK_i}[KC\text{-}Msg]$ with the shared secret keys of all mobile receivers and multicasts that information to them. At the receiver side, each mobile host needs only one symmetric key decryption time. The number of transmissions required to rekey the mobile hosts within the subnet is significantly reduced from 2(log M) to 1.

ST-MSS

(i) In initial key distribution on *semi-trusted mobile support stations* (ST-MSS) in [8], the total keys stored at a mobile host are increasing in logarithmic growth. The number of keys stored at an MSS depends on the number of mobile hosts under an MSS control.

(ii) The steps used in the member join operation on semi-trusted multicast support stations are described as follows:

(1) $MH_{new} \Rightarrow MSS : S_{KR_{MHnew}}[JOIN]$,
(2) $MSS \Rightarrow MKD : S_{KR_{MHnew}}[JOIN]$,
(3) $MKD \Rightarrow MSS : S_{KR_{MKD}}[EP_{KU_{MHnew}}[TEK]]$,
(4) $MSS \Rightarrow MH_{new} : S_{KR_{MKD}}[EP_{KU_{MHnew}}[TEK]]$,
(5) $MSS \Rightarrow MH_{new} : S_{KR_{MSS}}[EP_{KU_{MHnew}}[SM]], ES_{SM}[CEK]$,
(6) $MSS \Rightarrow MH_i : S_{KR_{MSS}}[EP_{KU_{MHi}}[SM]], ES_{SM}[$new keys from leaf to root$]$.

(iii) In the case of a new member join, MSS incurs more key encryption costs than CAMM. Each mobile receiver incurs more key decryption costs than CAMM. In member join, the number of transmissions depends on two times logarithmic growth in the number of multicast support stations.

(iv) In the case of member leave, MSS changes its *cell encryption key* (CEK) to prevent MH from accessing the data traffic and guarantee the traffic forward secrecy at cell level. In this case, multicast cell stations apply the centralized tree VersaKey [14]. The number of transmissions required to rekey the mobile receivers depends also on two times logarithmic growth in the number of multicast support stations.

4.3. Tabular comparison

In this section, we summarize the merits and shortcomings of a comparative analysis between DAMM and FT-MSS, as well as CAMM and ST-MSS shown in Table 5. A value written in *bold* is the best value for a certain row. All scenarios use both public and secret key systems to achieve scalable and secure key distribution scheme. The scalability problem of group key management for a large group with frequent joins and leaves in wireless network was previously addressed by [8] which applies centralized versa key (CVK) scheme [14]. In all these schemes, the session key is modified each time a mobile host joins and leaves. In comparing the two approaches, there are several issues to consider: performance, trust, and reliability. The main difference between CVK and our approach is in how the 1-affects-*n*-type problem [16] is addressed. In CVK, every time a client joins/leaves the secure group, a rekeying operation is required, which affects the entire group and the server cost is O(log(N)). In CAMM, there is no globally shared group key with the apparent advantage that whenever a client joins/leaves a subnet, only the subnet needs to be rekeyed.

Although our scenarios DAMM and CAMM incur more key storage at the sender, they have less key storage at MSS and mobile receivers. In our approach, DAMM incurs only one encryption and decryption operation on each mobile

Table 5: Comparison of secure one-to-many multicast protocols (N: no. of participating mobile receivers, M: no. of multicast subnet stations, M′: no. of mobile hosts under MSS control).

Criteria	FT-MSS [8]	DAMM	ST-MSS [8]	CAMM
No. of keys managed by the sender	**O(log M)**	M+1	**M+1**	M+2
No. of keys stored at the sender	**M+1**	M+2	**N+M+1**	N+M+2
No. of keys stored at an MSS	**M′**	M′ +1	M′	**4**
No. of keys stored at a member	O(log M′)	**3**	O(log M′)	**5**
Total key encryptions at the sender	3	**2**	2	2
Total key encryptions at the MSS	**2**	N+3	6	**3**
Total key decryptions at the MSS	3	**2**	**0**	1
Total key decryptions at a member	2	2	5	**4**
Total session key encryptions at sender	3	**0**	2	2
Total session key encryptions at an MSS	2	**1**	0	0
Total session key decryptions at an MSS	3	**1**	0	0
Total session key decryptions at a member	2	1	2	2
No. of messages at join	O(log M′+log M)	O(1)	O(1)	O(1)
No. of messages at leave	O(log M′+log M)	O(1)	O(1)	O(1)
Total messages on member join	**2(log M)**	3	**2(log M)**	5
Total messages on member leave	**2(log M)**	1	**2(log M)**	1
One affects *n* scalability	**Yes**	**Yes**	**Yes**	Yes
Intermediate nodes (trusted?)	Yes	Yes	No	No
Forward secrecy	Yes	Yes	Yes	Yes
Backward secrecy	Yes	Yes	Yes	Yes
Public key/ secret key	**Both**	**Both**	**Both**	**Both**

receiver that must be performed in order to access the group key used to encrypt the data traffic.

Both DAMM and CAMM reduce the total number of messages transmitted during the membership changes from 2(log M) to two transmissions. Our approach is very desirable from the viewpoint of transmission savings since an efficient rekeying mechanism is provided for membership changes. In addition, proposed protocols ensure the forward secrecy and backward secrecy and provide for transmission efficiency. In particular, they achieve better performance than ST-MSS and FT-MSS.

5. CONCLUSION

The main focus of the key management approach and techniques proposed in this paper is to make better provision for securely distributing the group key and rekey messages for joining and leaving a mobile host in a secure multicast group. We provided the security analysis and performance comparisons between our approach and the scenarios in [8]. All scenarios apply both public and secret key cryptosystems in order to achieve the security advantages of public key cryptosystem and speed advantages of secret key cryptosystems. They all ensure the forward secrecy and backward secrecy, confidentiality, authentication, and message integrity. The benefits of our proposed technique are that it minimizes the number of transmissions required to rekey the multicast group and it imposes minimal storage requirements on the multicast group. In our approach, dynamic architecture for mobile multicast (DAMM) is very desirable from the viewpoint of transmission overhead since an efficient rekeying mechanism is provided for membership changes. In addition, it ensures the forward secrecy, backward secrecy and provides transmission efficiency. Centralized architecture for mobile multicast (CAMM) also achieves robust against collusion of excluded users with generating fresh keys, and sending them to members securely. Our proposed protocols significantly reduce the communication burden associated with key updating.

REFERENCES

[1] M. Goncalves and K. Niles, "Multicasting overview," in *IP Multicasting: Concepts and Application*, pp. 91–117, McGraw-Hill, New York, NY, USA, 1999.

[2] R. Vida and L. Costa, Eds., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6," 2004, (Requests For Comments—3810), IETF Network Working Group.

[3] X. Jia, "A distributed algorithm of delay-bounded multicast routing for multimedia applications in wide area networks," *IEEE/ACM Transactions on Networking*, vol. 6, no. 6, pp. 828–837, 1998.

[4] S. Banerjee, C. Kommareddy, K. Kar, B. Bhattacharjee, and S. Khuller, "Construction of an efficient overlay multicast infrastructure for real-time applications," in *Proceedings of 22nd Annual Joint Conference on the IEEE Computer and Communications Societies (INFOCOM '03)*, vol. 2, pp. 1521–1531, San Francisco, Calif, USA, March-April 2003.

[5] U. Varshney, "Multicast over wireless networks," *Communications of the ACM*, vol. 45, no. 12, pp. 31–37, 2002.

[6] M. Baugher, R. Canetti, L. Dondeti, and F. Lindholm, "Multicast Security (MSEC) Group Key Management Architecture," Requests For Comments—4046, 2005.

[7] C. Perkins, "IP Mobility Support," (Request for Comments—2002), IETF Network working group, 1996.

[8] D. Bruschi and E. Rosti, "Secure multicast in wireless networks of mobile hosts: protocols and issues," *Mobile Networks and Applications*, vol. 7, no. 6, pp. 503–511, 2002, special issue on multipoint communication in wireless mobile networks.

[9] T. Karygiannis and L. Owens, "Wireless network security, 802.11, Bluetooth and Handheld Devices," NIST Special Publication 800-48, 2002, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf.

[10] L. Sun, Y. Liao, J. Zheng, W. Yichuan, and J. Ma, "An efficient multicast protocol in mobile IPv6 networks," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC '04)*, vol. 1, pp. 155–159, Atlanta, Ga, USA, March 2004.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *ACM Communication*, vol. 21, no. 2, pp. 120–126, 1978.

[12] D. Johnson and A. Menezes, "The elliptic curve digital signature algorithm (ECDSA)," Tech. Rep. 99-34, University of Waterloo, Canada, 1999, http://www.cacr.math.uwaterloo.ca.

[13] R. Rivest, "The MD5 Message-Digest Algorithm," 1992, (Request For Comments—1321), IETF Network working group.

[14] R. Vida and E. Costa, "Multicast Listener Discovery Version 2 (MLD) for IPv6," 2004, (Requests For Comments—3810), IETF Network Working Group.

[15] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The versakey framework: versatile group key management," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 9, pp. 1614–1631, 1999.

[16] W. Stallings, *Cryptography and Network Security, Principles and Practice*, Prentice Hall, Englewood Cliffs, NJ, USA, 2nd edition, 1999.

Win Aye received the B.C. Tech. (Bachelor of Computer Technology) and M.C. Tech. (Master's of Computer Technology) degrees from the University of Computer Studies, Yangon (UCSY, Myanmar), in 1995 and 1999, respectively, and the Ph.D. degree from Multimedia University, Malaysia, in 2005. She has been teaching at UCSY since 1995. Currently, she is an Associate Professor in the Department of Computer Hardware Technology at UCSY. Her research interests include control engineering, multicast transmission, multicast security, and network security.

Mohammad Umar Siddiqi received the B.S. Eng. and M.S. Eng. degrees from Aligarh Muslim University (AMU Aligarh) in 1966 and 1971, respectively, and the Ph.D. degree from Indian Institute of Technology Kanpur (IIT Kanpur) in 1976, all in electrical engineering. He has been in the teaching profession throughout, first at AMU Aligarh, then at IIT Kanpur. In 1998, he joined Multimedia University, Malaysia. Currently, he is a Professor in the Faculty of Engineering at the International Islamic University Malaysia. He has published more than 90 papers in international journals and conferences. His research interests are in error control coding and cryptography.