Key Management for Overlay-based IPTV Content Delivery

Jabeom Gu, Jaehoon Nah
Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea

Summary
An overlay-based IPTV content delivery is a relatively new type of content delivery in which user devices such as set-top boxes are connected with one another to form a dynamic, virtual delivery path. In the network, each overlay node forwards data, which one has received from another overlay node. To ensure security of the IPTV content delivered through the overlay, we propose a new key management scheme.

Key words:
Overlay-based content delivery, IPTV security, group key management.

1. Introduction

Internet Protocol Television (IPTV) is a system designed for live broadcast TV, video-on-demand (VoD), and additional value-added services through QoS guaranteed IP networks. The protection of TV program is critical for the success of the IPTV.

In traditional TV systems, a key management function, called *conditional access* [13], is employed to permit authorized access to only legitimate users (i.e., subscribers who have paid for specific TV programs). The conditional access is designed to be used in a broadcasting system that has no return path (for key management). The basic idea of the conditional access system is to share a common key between legitimate subscribers. To limit the possibility that the key is exposed to non-legitimate users, the key is refreshed frequently (e.g., 5 to 20 seconds). To support millions of users in the TV systems, efficient key management was a major issue. Several mechanisms are proposed to reduce the key management load [14-16]. In these schemes, the users are divided into several subgroups and use hierarchical key management. In this scheme, the lowest level key is updated in every 5 to 20 seconds, while the higher level keys are updated less frequently (e.g., once in a month).

In the IPTV systems, however, the TV programs are delivered through the IP networks, in which a return path is available for key management. Therefore, the conditional access is not guaranteed to be optimal because it is designed for a system without the return path. Furthermore, recent activities in ITU-T IPTV GSI include several content delivery schemes, including the overlay-based content delivery. In this relatively new type of content delivery, a user may receive his/her TV program from other user(s) at any moment if it is more efficient that the traditional delivery (i.e., receiving TV programs from the broadcast station). However it becomes much easier to expose TV programs to non-legitimate users. The frequent key update employed in the conditional access can hardly protect the content delivered through the overlay network.

In this paper, we propose a new key management scheme suitable for the protection of the overlay-based content delivery.

The proposed scheme is realized using the two cryptographic techniques, *one-way accumulator* and *identifier-based cryptography*. One-way accumulator, introduced by Benaloh and de Mare [9], is designed to accumulate large number of values into one value, regardless of the accumulation order [10, pp. 95-96]. In our scheme, the one-way accumulator is used for constructing a group key from member specific secrets. To allow access to a broadcasted TV program, our scheme uses modified version of a key distribution system based on the identifier-based cryptography, proposed by Okamoto and Tanaka [11].

Our scheme has the following distinct properties.

(1) **Many small subgroups**: The users who have paid for a same TV program are treated as a group. The proposed scheme supports dynamic membership for upper bounded, sufficiently large users with size |U|, while the size of each group is small.
(2) **Dynamic access grant**: Members are granted to access to TV programs broadcasted and shared between multiple overlay users.
(3) **Minimized computation overhead**: The computation that is proportional to the group size |U| is performed only once by the media source during 'off-line' setup period.

The rest of the paper is organized as follows. Section 2 provides background information and related works about the security of overlay-based content delivery. Section 3 presents our security mechanism. Section 4 provides a brief discussion about security and computation overhead. Section 5 concludes the paper.

Manuscript received December 5, 2008
Manuscript revised December 20, 2008

2. Backgrounds

2.1 Overlay-based content delivery

In the overlay-based content delivery scheme, end user devices such as set-top boxes are connected with one another to form a dynamic, *virtual delivery path*. In the network, each overlay node forwards data, which one has received from another overlay node. As a result, the virtual network will form a tree-like structure in which each overlay node acts as a router. It is an intuitive method to distribute large amounts of video data widely without incurring system and network bandwidth bottleneck at the media source (e.g., the Head-End system in the IPTV architecture).

There already exist some overlay-based Video-on-Demand (VoD) services including PPLive [1], PPStream [2], and Cool-Stream [3]. This area is examined in several researches [4] with a similar focus on performance and scalability of the global-scale video streaming. In general, the media source (i.e., the broadcast station) divides its video stream is into small chunks, and distributes the chunks to the clients who are interested in the steam. Instead of serving all clients, the media source supply data to a subset of recipients. The recipients who have acquired the VoD stream also supply data to other recipients.

A generic server-based configuration for content delivery is shown in Figure 1. In the Figure, the media source S is serving all users A, B, C, and D. On the other hand, the overlay-based content delivery is shown in Figure 2, in which the first two users A and C are served from the media source S, while other uses B and D are served from their parents, namely users A and C, respectively. In the following figures, the server-based content delivery is marked by the solid arrow line, and the overlay-based content delivery is marked by the dashed arrow line.
The benefits of the overlay-based content delivery over the generic server-based approach are:

- The network does not require network-level multicast support from multicast-aware routers.
- Bandwidth and resource requirement at the media source is reduced.

For the success of the overlay-based IPTV content delivery, however, it should be guaranteed that the delivered content is available only to legitimate users, namely, who have paid for the content. In general server-based content delivery, this was achieved by the conditional access system (CAS) (Figure 1). Because the overlay-based approach introduces virtual delivery path – from one overlay node to another – a new protection mechanism is required.

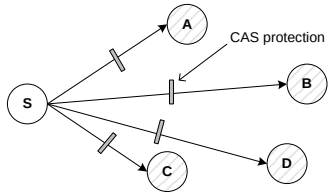

Fig. 1 Generic 'server-based' IPTV content delivery scheme. The content delivered from the media source S is protected using CAS.

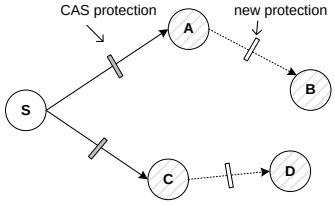

Fig. 2 Overlay-based IPTV content delivery scheme. Beside the CAS protection, a new protection mechanism is required for the new delivery paths from one overlay node to another.

2.1.1 Many small groups

In this paper, the users who have paid for a same TV program are treated as a group. In general, a group-oriented communication (such as the multicast delivery) is beneficial when large portion of members are interested in the same content.

However, the efficiency of the group-oriented communication is weaker in the TV programs, because users |S| in the TV programs tend to be very small compared to the total number of users |U|. In [12], it is shown that users' TV program selection follow a *power law distribution* such that only a few users select several most popular channels, while most users select non-popular channels. Therefore, it is common for any TV program that |S| is much smaller than |U|.

2.1.2 Dynamic access grant

The connection status of the overlay node changes frequently not only because a user turns switches the set-top box on and off, but also because the user moves into another TV channel. If the connection status changes, it is natural to reconstruct the overlay delivery path. This is illustrated in Figures 2 and 3.

If the node C is on-line as in Figure 2, the node D may receive the content from the node C. If the node C becomes off-line, however, the node D should reconfigure to change the delivery path from the node C to, for example, the node A (or even to the media source). To

support this, members needs to access broadcasted (and shared between multiple overlay nodes) TV programs.

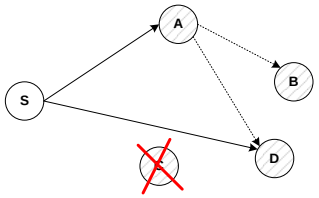

Fig. 3 Reconfiguration of the overlay-content delivery path when the node C becomes "off-line."

2.2 Protection of overlay-delivered content

Conditional access [13] is a key management function to permit authorized access to legitimate subscribers (who have paid for specific TV programs). The basic idea of the conditional access system is to share a common key between legitimate subscribers and update the key frequently (e.g., 5 to 20 seconds) to minimize the effect of the unauthorized access. In traditional TV broadcasting systems, there are tens or hundreds of TV channels and millions of subscribers. Therefore, efficient key management was a major issue.

Because those users who paid for a specific program form a group, a group-oriented cryptographic mechanism is required to protect the service from the illegal use. In general, the media source (or a TV broadcast station) encrypts a TV program with a group key, and broadcasts the encrypted data. Only the group members who have paid for the program and have access right to the group key should be able to decrypt the TV program. Then the group security is reduced to the problem of distributing the group key only to legitimate, pre-paid group members.

Former studies of key management that are closely related to the conditional access can be categorized into two groups: *secure multicasting* and *secure broadcasting*. In the secure multicasting, a common key (also known as a group key) is shared between group members. The media source needs to update and redistribute the group key to legitimate group members efficiently to support large group size with dynamic membership change [5, 6]. However, this approach is not as efficient as it appears. To be applicable for TV programs, the media source must be able to divide the group into small subgroups according to the access privilege for a specific TV program and the channel change. This means the group should manage many, frequently changing group keys, which will result in increased key management cost. Moreover, such re-keying approach is not suitable for our purpose. In overlay-based IPTV content delivery, the media source cannot update and redistribute the group key according to the membership change because the encrypted TV program is already stored in one or more overlay nodes.

The secure broadcasting (also known as broadcast encryption) was introduced by Fiat and Naor [7] to send an encrypted message to a legitimate group of receivers through a broadcast channel. Formally, the broadcast station prepares and assigns each user $u \in U$ a unique key K_u. The broadcast station wants to broadcast message to $S \subset U$ non-revoked members. A member $u \in S$ can decrypt the message using his/her own key K_u, while another member $v \notin S$ (a revoked member) should not be able to do so. Until now many variants of the secure broadcasting scheme are proposed [8]. However these schemes basically assume that the targeted receiver set S is known before the transmission so that broadcast station can prepare appropriate encryption key. For example, Y. Mu et al. [8] proposed a broadcast encryption mechanism that uses identifier of a group as an input to the encryption mechanism so that only members of that group can decrypt the message.

One shortcoming of this mechanism is that it is not applicable if the membership is decided *after* the broadcasting. In overlay-based content delivery, user's TV program selection may occur after the broadcast. Therefore, the secure broadcasting approaches are not suitable for overlay-based content delivery.

3. Proposed Scheme

3.1 Problem setting

We are considering an environment that is managed by a broadcast station (BS), which is also an original source of data streams (for example, TV programs). It is 'original' because (parts of) the outgoing data streams can be stored in overlay nodes and shared between multiple overlay nodes to realize the overlay-based content delivery. It is assumed that the BS generates data streams for a TV channel out of one or more TV programs (including commercials). Furthermore, each TV program can be sub-divided into multiple chunks. The BS is also controlling access to the group so that only legitimate users can see the content of the data stream received directly from the BS or indirectly from other users.

To realize such access control, we consider a cryptographic mechanism to encrypt chunk-sized data streams using *channel-chunk keys* (CCKs) and revealing the keys only to legitimate users who are paid for those

chunks. Because the access control is channel-chunk based, the BS can manage the channel independently from the programs. This approach relaxes management issue not only when each program is provided by more than one content provider, but also when there are many small groups (as discussed in the Section 2.1.1).

In our scheme, the BS is encrypting its outgoing packets using CCK_ℓ, where ℓ denote the index number of ℓ-th chunk in a channel and $CCK_\alpha \neq CCK_\beta$ for $\alpha \neq \beta$. This is illustrated in Figure 4.

In the figure, the overlay nodes *w*, *x*, *y*, and *z* are served directly from the BS. Let an overlay node *i* wants to see program 2, which comprises chunks #3, #4, #5, and so on. Thus node *i* can receive chunks #3 and #4 from node *w*, chunk #5 from node *x*, chunks #6, #7, and #8 from node *y*, and so on.

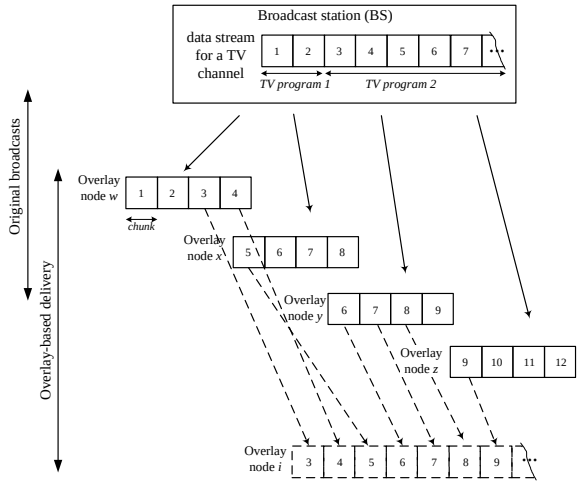

Fig. 4 Overlay-based IPTV content delivery example using overlay nodes that can buffer four chunks.

To support the dynamic change of the connection status in the overlay-based content delivery, members needs to access broadcasted (and shared between multiple overlay nodes) TV programs. As shown in Figure 5, when a user *i* is allowed to see the TV program 2 only, the server should be able to enforce this regardless from whom and where the user *i* receives the chunks. As illustrated in the figure, the encryption key CCK_5 should be known only to user *j*. The encryption key CCK_6 should be known to both users *i* and *j*. To allow chunk #6 to both users in generic group key management scheme, the BS should change its encryption key to CCK_6 right after the membership change and redistribute the key only to *i* and *j*. However, this approach is not feasible for overlay-based content delivery because the membership is determined after the broadcasting.

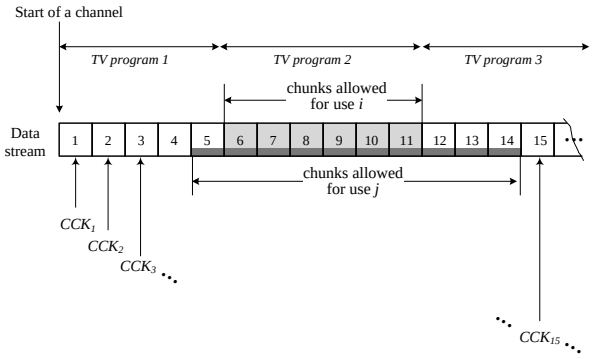

Fig. 5 Channel-chunk keys (CCKs). First chunk of the channel is encrypted using CCK_1, second chunk using CCK_2, and so on.

3.2 Our approach

3.2.1 Assumptions

We denote $c \in \mathcal{C}$ as the specific TV channel of interest. For the overlay-based content delivery, the BS prepares a secret space $\mathcal{S}_c$. The secrets $s_u \in \mathcal{S}_c$ are random numbers generated by the server only once before it starts a specific channel. Let $|U_c|$ be the upper bound of the number of users of the channel *c*. Then the size of $\mathcal{S}_c$ is set to $|U_c|$. Before starting the transmission, the BS shall have $\mathcal{S}_c$.

When a user *i* decides to see a program in the channel, the BS let him know the *i*-th secret through a dedicated secure channel (e.g., SSL protected). To support all possible number of users in the group, the size of secret space should be large enough. We assume that computing sufficiently large amount of secrets before the service (i.e., off-line) can be performed by a single server in reasonable time.

Note that the BS should authenticate a user before it can allocate a secret to the user. But because the scheme relies on the operation of the BS, we can simply use the BS for Internet-style ID/Password based authentication. (For simplicity, the proposed scheme just focuses on group security, not the authentication of individuals.)

Let *m* denote the size of the secret space, that is, $m = |U_c|$. The BS computes accumulated hash z_c for channel $c \in \mathcal{C}$ using binary hash of all $s_u \in \mathcal{S}_c$ as follows:

$$z_c = \overset{\circ}{h}(\overset{\circ}{h}(\overset{\circ}{h}(\cdots \overset{\circ}{h}(\overset{\circ}{h}(\overset{\circ}{h}(x_0, s_1), s_2), s_3), \cdots, s_{m-2}), s_{m-1}), s_m) \quad (1)$$

where x_0 must be agreed upon between multiple users. In the equation (1), the z_c is the accumulation of all secrets. The full set of secrets s_k are only known to the BS. We also define $\overline{z}_{ic}$ as the accumulation of all secrets except the s_i. The BS distributing the $\overline{z}_{ic}$ and s_i to user *i*. Notations used in this paper are summarized in Table 1. In the following notations, we will omit the subscript *c* for simplicity.

Table 1: Notations

ID	Identifier of the Broadcast Station (BS)
ID_i	Identifier of a user *i*, $ID_i = (\mathbb{S}_i \mid \mathbb{P}_i)$
$\mathbb{P}_i$	Personal description of a user *i*
$\mathbb{S}_i$	Selected program description in which a user *i* is interested
z	Accumulated hash for a channel
d	BS's master secret
g	BS's private key derived from ID and *d*
Y_i	Request message of a user *i*
gi	Private key of a use *i*
ℓ	Chunk number of a channel
$\|$	Concatenation operator
n	Multiplication of two large prime numbers *p* and *q*
h	Unary one-way function
$\mathring{h}$	Binary one-way function

3.2.2 Preparation of the scheme

The purpose of our scheme is to make a user to have the CCK_ℓ when it is required (through the dynamic access grant), in the environment when there are many small groups, while the major computation occurs at the BS before the start of the content delivery (i.e., off-line).

The encryption key CCK_ℓ is constructed as follows

$$CCK_\ell = h(z \,\|\, D_\ell) \pmod{n} \qquad (2)$$

where *h* is a cryptographic unary one-way function, *z* is the total accumulated hash from equation (1), and the value D_ℓ is the unique description of the ℓ-th chunk.

In the above, the D_ℓ is introduced to enable per-chunk key generation. That is, $CCK_\alpha \neq CCK_\beta$ for $\alpha \neq \beta$. In the first part, we will use a fixed value for the D_ℓ to simplify the description. Later, we will extend the scheme to enable per-chunk based access control (See Section 3.2.5).

To prepare the system, the BS selects two prime numbers *p* and *q* and computes $n = pq$. Because the *p* and *q* are kept secret, the factorization $n = pq$ is known only to the BS. Further the BS computes a co-prime *e*, a large prime that is relatively prime to $\varphi(n)$, where $\varphi(n)$ is an Euler's totient function. All users participating in the operation have the same *n* and *e*. A value *d* corresponding to the coprime *e* is determined to be $ed = 1 \pmod{\varphi(n)}$. The BS also selects an integer *t*, which is a primitive element in GF(*p*) and GF(*q*).

We assume that the BS uses a fixed value ID for its own identifier and generate its own *master key* as follows

$$g = \mathrm{ID}^{-d} \qquad (3)$$

The values *d* and *g* are kept secret to the BS while ID is made public. The mechanism that is used for the BS to let the secret s_i be known only to the user *i* will be discussed below. Although the server simply sends $\overline{z}_{ic}$ to user *i* through the secure channel, it is not allowed to send s_i directly to the user *i* because we let the server enforce who can see the packet.

3.2.3 Access request

A user notifies his/her interest in a specific program (i.e., collection of chunks) of a channel to the BS as follows.

We assume that a well-formed string $\mathbb{P}_i$ describes information about the user *i*, and another string $\mathbb{S}_i$ describes selected program information for which the user *i* is interested. For example, $\mathbb{P}_i$ and $\mathbb{S}_i$ can be constructed as follows:

$\mathbb{P}_i$ = bob || E34AC8 || 2008.06.01 || 100.0.0.2

$\mathbb{S}_i$ = TheTestMovie.avi || *from* 350 *to* 1500

Note that the description may be implemented in various ways. In the above example, $\mathbb{P}_i$ comprises the user's name (Bob) and the hash of password followed by a time stamp and the IP address. $\mathbb{S}_i$ comprises the channel name (VOD title or program name) and the description of the specific chunk interval(S) that Bob is interested. Note that various modifications may be made for such description and that the scheme may be implemented in various forms.

A user *i* presents his/her interest through $\mathbb{P}_i$ and $\mathbb{S}_i$ as follows:

$$ID_i = (\mathbb{P}_i \,\|\, \mathbb{S}_i) \qquad (4)$$

The user *i* generates a request description as

$$Y_i = t^{e \cdot ID_i \cdot r_i} \pmod{n} \quad (5)$$

where *t* and *e* are system parameters known to all users. Because the parameter r_i is randomly selected by *i* and kept secret, anyone else cannot construct Y_i. The user *i* can freely send Y_i to the BS through an open channel.

3.2.3 Access grant

When the user *i* presents its request description, the BS returns some parameters (namely, *hints*) that allow the user to access the program.

The parameters are computed as follows. Firstly, the BS selects a random value *r* for the user's request and computes x_i as

$$x_i = g \cdot t^r \quad (6)$$

The BS also computes

$$\hat{s}_i = Y_i^r \pmod{n} \quad (7)$$

The BS sends x_i, $\overline{z}_i$ and $\varsigma_i = s_i \oplus \hat{s}_i$ to the user *i* as a response. Here the $\oplus$ is a bit-wise XOR operation.

3.2.4 Recovery of the key

On receiving these values, user *i* can construct s_i as follows:

$$\hat{s}_i = (x_i^e \cdot ID)^{ID_i \cdot r_i} \longrightarrow s_i = \varsigma_i \oplus \hat{s}_i \quad (8)$$

Therefore, the user can also construct the accumulated hash *z* as

$$z = \overset{\circ}{h}(\overline{z}_i, s_i) \quad (9)$$

Consequently the user can construct *z* that is required to construct CCK_ℓ in equation (2).

As discussed before, the construction of the equation (8) does not allow per-chunk access grant. Therefore, the scheme needs to be extended as described in the next Subsection.

3.2.5 Extension for per-chunk access

If the D_ℓ is a fixed value (or simply a sequence number), however, user *i* can successively construct CCK_ℓ once it find s_i in Equation (8). This is not what is intended. Therefore, the BS also hides D_ℓ and applies key management similarly to s_i.

To enable per-chunk access control, the scheme is extended as follows.

In addition to the original request message in Equation (5), the user *i* also sends request message(s) for one or more chunks.

$$Y_{i\ell} = t^{e \cdot ID_i \cdot r_i \cdot \ell} \pmod{n} \quad (10)$$

In addition to the original hint for encryption key in Equation (7), the BS also sends chunk key hint(s). That is,

$$\hat{s}_{i\ell} = Y_{i\ell}^r \pmod{n} \quad (11)$$

and

$$\delta_{i\ell} = D_{i\ell} \oplus \hat{s}_{i\ell} \quad (12)$$

The per-chunk information D_ℓ is integrated into the request message. Then the user shall receive a x_i, a $\overline{z}_i$, and multiple $\delta_{i\ell}$'s as response. At last, the user *i* computes D_ℓ as

$$\hat{s}_{i\ell} = (x_i^e \cdot ID)^{ID_i \cdot r_i \cdot \ell} \longrightarrow D_\ell = \delta_{i\ell} \oplus \hat{s}_{i\ell} \quad (13)$$

As a result, the user can construct CCK_ℓ for the chunk ℓ using the equation (2).

4 Discussions

4.1 Security of the scheme

Security of the scheme is similar to that of the RSA. That is, it depends on two mathematically difficult problems: 1) the problem of factoring large numbers; and 2) finding *e*-th root modulo *n* when *n* is a composite number whose factors are not known. In addition, the difficulty is also related to the hash function. That is, it is recommended to use cryptographically strong hash function for *h* and $\overset{\circ}{h}$.

4.2 Computation overhead

In our approach, the BS prepares a secret space $\boldsymbol{\mathcal{S}}_c$ for a channel *c* before the start of the service. The secrets $s_u \in \boldsymbol{\mathcal{S}}_c$ are random numbers generated by the server only once regardless of the subscriber. To support actual number of

subscribers U of the channel *c*, the size of secret space should be large enough.

Therefore, the proposed scheme is designed in such a way that the overhead of initial setup stage at the broadcast station (BS) is proportional to the expected number of users in the channel. More precisely, encryption at the BS takes $|U|^2$ power-modulo operations for each TV channel.

After the initial setup stage, however, the computation at the BS and subscribers is very efficient. When a user *i* decides to see a program in the channel, the BS let him know the *i*-th secret through a SSL-like secure channel.

5. Conclusion

In this work, we proposed a new group key management scheme for overlay-based content delivery, where the broadcast station (BS) can easily enforce access grant for broadcasted TV programs. The overlay-based content delivery is unique in its security requirement that the access control for a TV program occurs after the TV program is already broadcasted.

The approach we took is a group key management scheme, which is designed to make a user to have the per-chunk key CCK when it is required (through the dynamic access grant), in the environment when the members are divided into many small groups, while the major computation occurs at the broadcast station before the start of the content delivery.

Acknowledgments

This work was supported by the IT R&D program of MKE/IITA [2008-S-006-01, Development of Open-IPTV(IPTV2.0) Technologies for Wired and Wireless Networks].

References

[1] PPLive, available: www.pplive.com
[2] PPStream, available: www.ppstream.com
[3] CoolStreaming, available: www.coolstreaming.us
[4] X. Hei, C. Liang, J. Liang, Y. Liu, and K. W. Ross, A measurement study of a large-scale p2p IPTV system, in Proc. Workshop on Internet Protocol TV (IPTV) services over World Wide Web, Edinburgh, Scotland, 2006.
[5] C. K. Wong, M. G. Gouda, and S. S. Lam, " Secure group communications using key graphs, IEEE/ACM Trans. Netw., vol. 8, no. 1, pp. 16-30, 2000.
[6] S. Mittra, Iolus: A framework for scalable secure multi-casting, in Proceedings of the ACM SIGCOMM, vol. 27, New York, 1997, pp. 277-288.
[7] A. Fiat and M. Naor, Broadcast encryption, in Advances in Cryptology (Crypto 93). New York: Springer-Verlag, 1994, LNCS 773, pp. 480-491.
[8] Y. Mu, W. Susilo, and Y.-X. Lin, Identity-based broad-casting, in INDOCRYPT 2003, T. Johansson and S. Maitra, Eds. Springer, 2003, vol. 2904, pp. 177-190.
[9] J. C. Benaloh and M. d. Mare, One-way accumulators: A decentralized alternative to digital signatures (extended abstract), in EUROCRYPTO93, T. Helleseth, Ed. Springer-Verlag, 1993, pp. 274-285.
[10] B. Schneier, Applied cryptography: protocols, algorithms, and source code in C, 2nd ed., Wiley, 1996.
[11] E. Okamoto and K. Tanaka, Key distribution system based on identification information, Selected Areas in Comm., IEEE Journal on, vol. 7, no. 4, pp. 481-485, 1989.
[12] N. Sinha and R. Oz, .The statistics of switched broadcast, in Proc. of SCTE Conference on Emerging Technologies, Huntington Beach, CA, 2005.
[13] D. J. Cutts, DVB Conditional Access, Electronics & Communication Engineering Journal, vol. 9, no.1, 1997, pp. 21-27.
[14] J. W. Lee, Key distribution and management for conditional access system on DBS, in Proc. Int. Conf. Cryptology and Information Security, 1996, pp. 82-86.
[15] F. K. Tu, C. S. Laih, and S. H. Toung, On key distribution management for conditional access system on Pay-TV system, in IEEE int. Symp. Consumer Electronics (ISCE'98), vol. 45, pp. 151-159, 1998.
[16] Y. Huang, S. Shieh, F. Ho, J. Wang, Efficient Key Distribution Schemes for Secure Media Delivery in Pay-TV Systems, IEEE Trans. Multimedia, vol. 6, no. 5, 2004, pp. 760–769.

Jabeom Gu received the M.S. and Ph.D. degrees in Electrical Engineering from Chung-Ang University in 2002 and 2006, respectively. He is with Electronics and Telecommunications Research Institute, Korea. His research interest includes distributed network security, peer-to-peer network, overlay multicasting, wireless network security, and IPTV security.

Jaehoon Nah received the M.S. degree in Computer Engineering from Chung-Ang University in 1987. He received the Ph.D. degree in Electronic and Information Engineering from Hankuk University of Foreign Studies in 2005. He is a principal research engineer and a team leader in Division of Information Security in Electronics and Telecommunications Research Institute, Korea. His research interest includes distributed network security, peer-to-peer network, overlay multicasting, and IPTV security.