JOURNAL OF KOREA MULTIMEDIA SOCIETY, VOL. 9, NO. 12, DECEMBER 2006(pp. 1649-1656)

An Efficient Renewal Mechanism of Group Key Employing the Fiat-Shamir Method on Mobile Communications

Dong-Gil Tak[†], Yeo-Jin Lee[††], Jae-Hoon Lee[†††], Il-Yong Chung[††††]

ABSTRACT

Renewal of the group key on the mobile communication needs it can be not re-shared by all members of the group with the exception of excluded members but also prevented from making a fraudulent use of group key due to leakage of security information for terminal. In this paper, we propose an efficient renewal mechanism of group key in order for all members of the group to be able to get digital information and to perform the renewal of group key employing the Fiat-Shamir method. It can guarantee the security of a group key since a terminal renews a group key by using security information of an excluded terminal and the previous group key.

Keywords: Group Key Renewal, Fiat-Shamir Method

1. INTRODUCTION

Demand for group communication to provide identical service to many users is increasing as application area for mobile communication has expanded to diverse fields. Therefore, security requirements have to be satisfied for information transmitted to group users to ensure safe group communications[1]. Technology that will prevent fraudulent calls by illegal subscribers while minimizing losses for the mobile communications provider by providing a validation procedure for subscribers is being developed[2]. Mobile communication standards like CDMA and GSM already provided security services including validation[3,4]. Security service including validation and encryption is also a standard in IMT-2000. In general, a mobile communication system is a star type network that is organized as a center for controlling communication of all terminals belonging to the group. If encryption function is provided, all information can be encrypted using the group key that will be distributed secretly between the center and the terminals. The encrypted information can be broadcasted to all devices simultaneously so that within a specific group, wireless encrypted communication is carried out[2]. However, wireless communication is vulnerable to threats like counterfeiting or illegal changes as well as eavesdropping[5].

In this paper, we propose an efficient renewal mechanism of group key in order for all members of the group to be able to get digital information and to perform the renewal of group key employing the Fiat-Shamir method. It is an efficient key renewal mechanism for dealing with users who leave and with those who become new members. In order to exclude specific terminals or illegal terminals within a group, the center must detect eavesdropping or fraudulent use of communication as quickly

※ Corresponding Author : Il-Yong Chung, Address : (501-759) 375 Seoseog-dong, Dong-gu, Gwangju, 501-759, Korea, TEL : +82-62-230-7712, FAX : +82-62-233-6896, E-mail : iyc@chosun.ac.kr

Receipt date : July 26, 2006, Approval date : Nov. 20, 2006

[†] Dept. of Computer Engineering, Chosun University (E-mail : jasmine99@korea.com)
[††] Dept. of Computer Engineering, Chosun University (E-mail : mailto:smile96@naver.com)
[†††] Dept. of Computer Engineering, Chosun University (E-mail : mailto:nuridepo@chosun.ac.kr)
[††††] Dept. of Computer Engineering, Chosun University

as possible and promptly renew group key for all terminals excluding those lost or those which have leaked secret information illegally. Such renewals must be carried out quickly without affecting general communications. In addition, lost terminals or terminals that have leaked secret information must be prevented from finding out the group key after the renewal. In this research, an efficient group key renewal method that satisfies these conditions and also solves problems contained in existing methods is proposed.

This paper consists of five sections. Section 2 examines existing group secret key distribution and renewal methods. Section 3 is a core part and proposes an efficient renewal mechanism of group key. A procedure for authenticating illegal terminals is also discussed. Security analysis for the proposed method and existing methods is presented in Section 4. Section 5 concludes with remarks.

2. RELATED RESEARCH

There are a few techniques for sharing a new group key through a public communication network[6-8]. The first method is to redistribute the key. A method uses symmetrical key encryption[9] or asymmetrical encryption[10]. However, the method requires the center to distribute the keys many times and since key transmission takes a lot of time, they may hinder normal communication[1,2]. It may also not be appropriate for a digital mobile communication system in which encrypted broadcast transmission is carried out.

In another method, renewal information of group key is encrypted and is broadcasted to all terminals. Matsuzaki-Anzai(MA) method[11], Sm- Park-Won (SPW) method[2] and Park-Lee (PL) method[5] are some of the examples. SPW method and PL method use smart cards to conceal and to distribute a large amount of group key information to each terminal. However, making terminals lightly weighted may be difficult with this method and renewal processes carried out can be limited by the smart card capacity. SPW method cannot prevent the leaking of group key through collusion between users. Because modular information is provided in advance, if more than two terminals are lost simultaneously, these terminals can generate group keys. Two terminals may also collude to share a group key[2]. On the other hand, PL method transmits modular information each time renewal is carried out instead of distributing them with a smart card to prevent group secret key generation through collusion. By transmitting renewal information for terminals to be excluded and by using it to generate group keys, the problem of excluding such terminals was also solved[5]. However, making terminals lightly weighted and the number of renewals being limited by the smart card capacity are two problems that remain to be solved. They are appropriate for mobile communication systems because few communication exchanges are needed and the terminals generate group keys themselves.

Matsuzaki-Anzai(MA) method which was first introduced to use group key sharing method in a digital mobile communication system is described below.

2.1 Matsuzaki-Anzai(MA) Method

Matsuzaki-Anzai introduced an efficient and novel group key re-sharing method for the first time that was appropriate for digital mobile communication[4]. This method does not depend on the number of users when renewing the group key. This method refers to the case in which encrypted broadcast transmission is carried out using a shared secret key within the group for a star type mobile communication system in which a base station maintains multiple terminals. It allows exclusion of specific terminals from the group and allows generation of new group secret keys as quickly as possible. MA method system co-

efficients are shown in <Table 1>.

Table 1. Notation of the MA Method

$T_i (1 \le i \le n)$: the i^{th} Terminal
S_i: Secret information of the i^{th} Terminal needed for group key renewal
p, q: Large prime numbers generated by the center
k: Group secret key

1) Preparation step

① The center generates and stores secret information S_i until $GCD(S_i, S_j) = 1 (i \neq j)$ is satisfied and secretly transmits to each terminal.

② The center randomly generates a group secret key K that will be renewed and stores it.

③ After the center generates large decimals p, q it calculates $N = p \times q$ and secretly stores the result.

④ After the center calculates $X_i = K^{S_i} (mod\ N), GCD(X_i, N) = 1$ using secret information from each terminal, the result is stored and transmitted to each terminal securely.

⑤ Each terminal T_i secretly stores S_i, X_i received from the center.

2) Group key renewal step

① If the center wants to exclude terminal, T_i it broadcasts information (S_i, X_i, N) related to terminal T_i to all terminals.

② Terminal T_j searches for a, b that satisfies $a \cdot S_i + b \cdot S_j = 1$ using the received information. Integers a, b can be calculated in polynomial time by employing the Euclidean algorithm.

③ Terminal renews the group key as follows.

If , $a < 0$ $K = (X_i^{-1})^{-a} \cdot X_j^{b} \bmod N$

If , $b < 0$ $K = X_i^{a} \cdot (X_j^{-1})^{-b} \bmod N$

In MA method, terminal T_i cannot generate an accurate a, b because the received information is it's secret key. Therefore, new group key K cannot be generated in case a lost terminal is illegally obtained. This method cannot prevent collusion by terminals in case each terminal finds out N. In other words, specific terminals T_i, T_j can exchange secret information S_i, X_i and S_j, X_j and generate a separate group secret key without the help of the center and use it to exclude all other terminals[2,5]. Let's suppose an illegal terminal T_k has obtained secret information S_i, X_i from a legitimate terminal T_i and is eavesdropping illegally and that the center has found out. In this case, the center can prevent illegal eavesdropping by T_k by transmitting secret information S_i, X_i of terminal T_i to all terminals. However, if the center broadcasts secret information S_j, X_j of terminal T_j to all terminals in order to exclude another terminal T_j T_k can generate a new group secret key using the secret information from T_j. MA method uses RSA open key encryption to deal with this type of danger. In other words, the difficulty of calculating a new group secret key using illegally obtained information is dependent on security of RSA[11].

In MA method, group shared secret key may be renewed only once. Renewing group secret key more than once requires starting again from the preparation step[2,5]. In addition, since calculation for an inverse number is carried out by a terminal, it is inefficient in terms of time complexity[5].

3. THE DESIGN OF A NEW GROUP KEY RENEWAL METHOD

In this paper, a method to share the group secret key, required to obtain secure communication between terminals maintained by the center, is proposed. It is targeted for small group meetings in specific spaces in a mobile communication system. For group key sharing and distribution, sufficient consideration was given to small and light mobile terminals and key centers with large calculation capabilities that reflect the general characteristic of mobile communication. We selected the star-type network, which can carry out broadcasting. In order to perform secure communications within a group with a key center in the

middle, the first thing to consider is the group secret key. However, if a terminal is lost, the shared group secret key or secret information in the terminal can be used to easily eavesdrops communications within the group or distribute false information. Problems that can be caused by using the shared group secret key can be prevented by group secret key renewal. However, eavesdropping or false information distribution using secret information is difficult to prevent by simple group key renewal. The problem is more critical when broadcast transmission is used.

Existing methods can renew group key only one time. However, they can not do more than two times. In this research, we propose a method, which solves this problem without using an additional device like a smart card to enable use of small and light mobile terminals. It is an efficient method which can be used to renew securely secret keys within a group when a subscriber within a group has lost a secret key or secret information, has lost a terminal or the key center wants to exclude a specific terminal which is suspected of being used illegally from group communications. The ability to exclude forever illegal eavesdropping terminals based on illegal information is the greatest advantage. In addition, digital signature method based on ID was implemented to screen illegitimate users and group secret key renewal requests from an illegitimate center [12, 13]. System coefficients for the new group key renewal method are shown in <Table 2>.

Table 2. Notation of the Proposed Group Key Renewal Mechanism

C: Key distribution center(KDC)
T_i: the i^{th} Terminal $(1 \le i \le n)$
GK: Group key
Uk : Next group key
US_i: Secret information of the i^{th} Terminal for group key renewal
UX_i: Public information of the i^{th} Terminal for group key renewal
ID_i: Identification information for user i
f, h: One-way function
Un: Prime number for group key renewal
Dn: Prime number for digital signature
X_c, Y_c : Signature information.

3.1 Preparation Step

1) Key distribution center

① The Key distribution center(C) registers identification information ID_i from T_i, and then randomly generates the first group secret key GK. It is stored secretly and then securely distributed to each terminal.

② The KDC generates secret information $US_i(1 \le i \le n)$ for the i^{th} Terminal, store it secretly and distribute it securely to each terminal.

$GCD(US_i, US_j) = 1, \quad (i \ne j)$

③ After calculating $DSc_j(1 \le j \le k)$, store it securely. It does not have to be concealed.

$DIc_j = f(ID_c, j)$, $\mathrm{DSc}_j = \sqrt{DIc_j^{-1}} \bmod Dn$, where DIc_j is a quadratic residue (mod Dn) and compute the smallest square root DSc_j of $\sqrt{DIc_j^{-1}}$.

④ Calculate public information UX_i for terminals for group key renewal. In this step, UX_i does not have to be concealed.

$$UX_i = GK^{US_i} (\bmod Un)$$

⑤ Broadcast the following information to all terminals.

$(Un, Dn, f, h, ID_c, ID_1 \| UX_1, \cdots, ID_n \| UX_n, X_c, Y_c)$

2) Each terminal

① Store securely US_i, UX_i and $Dn, ID_c, ID_i, \cdots ID_n$, received from the center.

② After calculating $DSi_j(1 \le j \le k)$ store securely. This need not be concealed.

$DIi_j = f(ID_i, j), DSi_j = \sqrt{DIi_j^{-1}} (\bmod\ Dn)$

3.2 Renewal Step of Group Key

1) Key distribution center

① Key distribution center wants to exclude terminal T_i.

② Find a, b that satisfies $a \cdot US_i + b \cdot US_j = 1$.

$(a<0),\ UK=(UX_i^{-1})^{-a} \cdot UX_j^{b} (\text{mod} Un)$

$(b<0),\ UK=UX_j^{a} \cdot (UX_j^{-1})^{-b} (\text{mod} Un)$

③ Compute information UX_j on terminal $T_j (j \neq i)$ and generate a new group key.

$$UX_{j_t} = UK^{US_j} (\text{mod} Un)$$

$$GK = GK * UK (\text{mod} Un)$$

④ Generate signature information X_c, Y_c.

A. Generate a random number $R_c \in Z_{Dn}$

B. $X_c = R_c^2 \bmod Dn$

C. $(e_{c_1}, \cdots, e_{c_k}) = h(GK, ID_c \| ID_1 \| \cdots \| ID_n, X_c)$

D. $Y_c = R_c \cdot \prod_{e_{c_j}=1} DSc_j (mod)\ Dn$

⑤ Broadcast the following information to all terminals.

$$(US_i, UX_i, ID_c, ID_1 \| UX_1, \cdots, ID_n \| UX_n, X_c, Y_c)$$

2) Each terminal

① After receiving the information shown below from the center, terminal T_j verifies whether it came from a legitimate center.

$(US_i, UX_i, Un, ID_c, ID_1 \| X_1, \cdots \| ID_n \| X_n, X_c, Y_c)$

A. $(e_{c_1}, \cdots, e_{c_k}) = h(GK, ID_c \| ID_1 \| \cdots \| ID_n, X_c)$

B. $DIc_j = f(IDc, j)$

C. $Z_c = Y_c^2 \cdot \prod_{e_{c_j}=1} DIc_j (mod)\ Dn$

D. If $(Z_c = X_c)$, then the message is validated.

② Find a, b that satisfies $a \cdot US_i + b \cdot US_j = 1$

$(a<0),\ UK=(UX_i^{-1})^{-a} \cdot UX_j^{b} (\text{mod} Un)$

$(b<0),\ UK=UX_j^{a} \cdot (UX_j^{-1})^{-b} \cdot (\text{mod} Un)$

③ Compute public information WX_j of the terminal for group key renewal.

$$WX_j = UK^{US_j} (\text{mod} Un)$$

④ Verify the correctness of the renewal information.

If $(WX_j = UX_j)$ then the renewal information is corrected.

⑤ Generate a new group key

$$GK = GK * UK (\text{mod}\ Un)$$

In this method, a terminal T_i cannot generate an accurate a, b because the received information is its own secret key. In other words, even if a lost terminal has obtained it, a new group key GK cannot be generated. A terminal T_i that did not generate a legitimate group key cannot generate WX_i correctly. Hence it is excluded forever from future group key renewal processes. Therefore, an illegal user who has obtained the secret information of a terminal T_i is excluded forever. In addition, for excluded terminals, it is not possible for two terminals to exchange secret information US_i and US_j with each other and to calculate the group key.

3.3 Authentication Step of the terminal

By using digital signatures, the proposed method can verify and validate illegal use at regular intervals to exclude them arbitrarily.

① After generating the signature information X_c, Y_c the key distribution center broadcasts these information to all terminals.

② Random number $R_c \in Z_{Dn}$ is generated.

$$X_c = R_c^2 (\text{mod}\ Dn)$$
$$(e_{c1}, \cdots, e_{ck}) = h(GK, ID_c \| ID_1 \| \cdots \| ID_n, X_c)$$
$$Y_c = R_c \cdot \prod_{e_{cj}=1} DSc_j (\text{mod}\ Dn)$$

③ T_i will generate its signature information, and transmit to the center.

④ Random number $R_c \in Z_{Dn}$ is generated.

$$X_i = R_i^2 (\text{mod}\ Dn)$$
$$(e_{i_1}, \cdots, e_{i_k}) = h(GK, US_i \| ID_c \| ID_1 \| \cdots \| ID_n, X_i)$$
$$Y_i = Y_c \cdot R_c \cdot \prod_{e_{ij}=1} DSi_j (\text{mod}\ Dn)$$

⑤ Examine whether a terminal is legitimate using signature information for each terminal from the key distribution center.

A. $DIc_j = f(IDc, j)$

B. $DIi_j = f(IDi, j)$

C. $Z_i = Y_i^2 \cdot \prod_{e_{c_j}=1} DIc_j \cdot \prod_{e_{i_j}=1} DIi_j\ (mod)\ Dn$

D. After verifying whether

$(e_{i_1}, \cdots, e_{i_k}) == h(GK, US_i, ID_c \| ID_1 \| \cdots \| ID_n, Z_i)$ is sat-

isfied, validate it.

4. SECURITY ANALYSIS OF THE PROPOSED METHOD

Comparing with other methods previously presented, our method is better in terms of forward secrecy, backward secrecy, solution of conspiracy problem and authentication. Forward Secrecy guarantees that a passive adversary who knows a contiguous subset of old group keys cannot discover subsequent group keys. And Backward Secrecy guarantees that a passive adversary who knows a contiguous subset of group keys cannot discover preceding group keys. <Table 3> shows these comparisons.

Table 3. comparisons of Group key renewal Mechanisms

Method / factor	MA[11]	SPW[2]	PL[5]	the proposed method
Forward Secrecy	×	×	×	○
Backward Secrecy	×	×	×	○
solution of conspiracy problem	×	×	○	○
Authentication	×	×	×	○

4.1. Security of Preparation Step

In the proposed method, the counterpart cannot find out the group secret key and secret information for each terminal because the KDC distributes these information securely. Later, even though ^{UX_i} is revealed, he/she cannot know what these information are. This is more difficult than to solve discrete logarithm problem.

4.2. Security of Renewal Step

In the proposed method, information transmitted from the center during the key renewal step consists of secret information ^{US_i} needed for exclusion of terminal ^{T_i}, public information ^{UX_i}, divisor for modular calculation Dn. It is impossible for an excluded terminal to carry out calculations of the new group key because it does not knows any secret information except its own secret information. Later, even though it receives other secret information during renewal process, it cannot generate an accurate group key because it does not have a group key for the previous step.

5. CONCLUSION

The proposed method can prevent an illegal user from transmitting key renewal information to terminals by applying the Fiat-Shamir method. Illegal terminals can be excluded by validating the users with this method. Only authorized users may receive digital information. In addition, because secret information needed for group key renewal is also renewed simultaneously each time the group key is renewed, terminal security can be guaranteed and illegal terminals can be prevented from renewing accurate group secret key. So, it can guarantee that an illegal terminal cannot renew an accurate group key since it does not contain the previous group key.

Comparing to the methods previously published, even though the MA method, the SPW method and the PL method did not assure the forward secrecy and the backward secrecy requisite for mechanism of group key, our method can solve these problems. It also handles the conspiracy problem and authentication service by applying the Fiat-Shamir method. Therefore, it can strengthen security for design of group key.

6. REFERENCES

[1] Young-Ho Park and Kyung-Hyun Lee, "A Group Key Management Architecture in Mobile Network Environments," *The Journal of The Korea Institute of Information Security and Cryptology*, Vol. 12, No. 2, pp. 89-91, 2002.

[2] Joo-Goel Sim, Choon-Sik Park, and Dong-Ho

Won, "Secret Group Key Re-sharing Method Suitable for Digital Mobile Communication," *The Journal of the Korean Institute of Communication Sciences*, Vol. 10, No. 3, pp. 69-76, 2000.

[3] TIA/EIA Telecommunications Systems Bulletin, Cellular Radio telecommunications Intersystem Operations: Authentication, Signaling Message Encryption and Voice Privacy, TSB 51, 1995.

[4] ETSI-RES, European Telecommunication Standard, ETS 300 175-7, DECT, Common Interface, part 7: Security features, 1992.

[5] Hee-Un Park and Im-Yeong Lee, "An Efficient Mobile Communication Group Key Reforming Method," *The Journal of the korean Information Science Society(KISS) : Information Networking*, Vol. 8, No. 1, pp. 367-370, 2001.

[6] Jung-Hyun Nam and Jin-woo Lee, "Provably Secure and Communication Efficient Protocol for Dynamic Group Key Exchange," *The Journal of The Korea Institute of Information Security and Cryptology*, Vol. 14, No. 4, pp. 163-165, 2004.

[7] Deok-Gyu Lee and Im-Yeong Lee, "A Study on Efficient Key Renewal for Broadcast Encryption," *Proceedings of the Korea Institutes of Information Security and Cryptology Conference*, Vol. 13, No. 1, pp. 263-267, 2003.

[8] I. Chung, "Erratum : The Design of Conference Key Distribution System Employing a symmetric Balanced Incomplete Block Design," Information Processing Letters, Vol. 91, No. 6, pp. 299-300, 2004.

[9] T. Hwang, "Scheme for Secure Digital Mobile Communications Based on Symmetric Key Cryptography," *Information Processing Letters*, Vol. 48, pp. 35-37, 1993.

[10] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Inform. Theory*, Vol. 22, pp. 644-654, 1976.

[11] N. Matsuzaki and J. Anzai, "A Group Key Renewal Method Suitable for Mobile Telecommunications," *Proceedings of SCIS*, 5.2.E. 1998.

[12] R. L. Rivest and A. Shamir, "How to expose an eavesdropper," *Communications of the ACM*, Vol. 27, No. 4, pp. 393-395, 1984.

[13] A. Fiat and A. Shamir, "How to prove yourself : Practical Solutions to identification and signature problems." *Proc. Crypto*, pp. 186-194, 1986.

Dong-Gil Tak

She received the M.S. and Ph.D. degrees in Computer Science from Chosun University in 1998 and 2006, respectively. From 2005, she is a researcher at Doul Information Technology Co., LTD. Her research interests are in areas of network and information security, PKI and PMI.

Yeo-jin Lee

She received the B.E. and M.S. degrees in Computer Science from Chosun University in 2000 and 2003, respectively. Since 2004, she is working towards the Ph.D. degree in Computer Science at Chosun University. Her research interests are in areas of network and information security, sensor networks

Jae-Hoon Lee

He received the B.E. and M.S. degrees in Computer Science from Chosun University in 2000 and 2002, respectively. Since 2002, he is working towards the Ph.D. degree in Computer Science at Chosun University. His research interests are in areas of software engineering, programming language, object-oriented software, genetic algorithm, eCRM

Il-Yong Chung

He received the B.E. degree from Hanyang University in 1983 and the M.S. and Ph.D. degrees in Computer Science from City University of New York in 1987 and 1991, respectively. From 1991 to 1994, he was a senior researcher at Electronics and Telecommunications Research Institute(ETRI). Since 1994, he has been a faculty member at Department of Computer Science, Chosun University. His research interests are in areas of network and information security, parallel and distributed systems, computer algorithms.