Security Improvement of ID-based Multiple Key Management Scheme for Scalable Ad Hoc Networks[†]

YoHan Park*, YoungHo Park**, and SangJae Moon***

Abstract Security supports are a significant factor in mobile ad hoc networks. Especially in dynamic topologies, considering cluster, key management is essential to provide a secure system. Recently, Li-Liu proposed ID-based multiple key management scheme for cluster-based ad hoc networks. However, we found the security weakness of their scheme. In this paper, we analyze the security of Li-Liu's scheme and show that master secret key and fragment of the master secret key can be revealed to compromised CHs and nodes. Furthermore, we propose a solution to improve the scheme against disclosure of the share key and the master secret key even though system parameters are opened to compromised nodes and modify the Li-Liu's scheme fitted for a scalable networks. The improved IMKM scheme could be usefully applied in dynamic cluster-based MANETs such as the military battlefields, mobile marketplace and VANETs.

Key Words : Ad hoc networks, Cluster, Key management, Scalability

1. Introduction

Key management schemes allow a mobile ad hoc networks (MANETs) to securely run when registered nodes are changing. The researches for key management for MANETs have been in progress widely[1][2]. And ID-based cryptosystem[3] is considered powerful alternative to CA-based systems in MANETs when considering the infrastructure-less environment because ID-based cryptosystem enable any pair of users to

communicate securely without exchanging public key certificates. However, the private key generator (PKG), which issues a user's private key corresponding to each user's identity information, represents a single point of failure and key escrow problem. To encounter this problem, Boneh and Franklin[4] suggested distributed PKGs (D-PKGs) using threshold cryptography. And cluster-based networks are considered as a suitable model when considering distributed authorities, such as D-PKG. Recently, Li-Liu proposed an ID-based multiple key management (IMKM) scheme[5] for cluster-based MANETs. They assigned the role of D-PKGs to CHs of the network. The private key of the PKG is distributed over the CHs, i.e., every CH holds a fragment of the master secret key and the set of CHs can construct master secret key using Lagrange interpolation. In this paper, we analyze the

[†] This work was supported by the Korea Research Foundation Grant funded by the Korean Government (KRF-2008-521-D00449)

* Kyungpook National Univ. School of Electrical Engineering and Computer Science

** Kyungpook National Univ. School of Electronic Engineering

*** Kyungpook National Univ. School of Electrical Engineering, Corresponding Author

security of Li-Liu's IMKM scheme and show that master secret key and fragment of the master secret key can be revealed to compromised CHs. Furthermore, we propose a solution to improve the scheme against disclosure of the share key and the master secret key even though system parameters are opened to compromised nodes and modify the key management scheme.

2. Preliminaries

Li-Liu proposed the key management scheme based on bilinear pairings[5]. In this section, we briefly describe the basic notations and properties of the bilinear pairing.

2.1 Notations

Table 1 specifies some important notations that IMKM employ. The specific notations were mentioned in [5].

<Table 1> Notations

p, q	Two large prime
g	Generator of subgroup of order q
$\hat{e}$	Bilinear pairing
U	Maximum update phase index
P_m	Generator of G_1 ($0 \leq m \leq U$)
s/P_{pub}	private key/public key of PKG
G_1, G_2	Cyclic groups of order q
CH_i	Clusterhead i
ID_i	Network ID of CH_i
S_i, Q_i	private/public key of CH_i
H_1, H_2, H_3	Mapping $\{0, 1^*\} \rightarrow Z_p^*, G_1 \rightarrow G_q, G_2 \rightarrow G_q$
$K_{i,j}$	Pair-wise key of CH_i and CH_j
$f(x), g(x)$	$(t-1)$ degree polynomials
$\lambda_v(x)$	Lagrange coefficient
D/D_{pub}	Master secret key/Public key of share
$d_i/d_{i_{pub}}$	share key of CH_i /public key of share key

2.2 Bilinear Pairings

Let G_1 be a cyclic additive group generated by p , and let G_2 be a cyclic multiplicative group of the same order, q . We assume that the discrete logarithm problems (DLP) in G_1 and G_2 are difficult to compute. The bilinear pairing, $\hat{e}: G_1 \times G_1 \rightarrow G_2$, satisfies the following conditions:

- ① *Bilinear*: If $P, Q, R, S \in G_1$ and $a, b \in Z_q^*$, $\hat{e}(P+Q, R+S) = \hat{e}(P, R)\hat{e}(P, S)\hat{e}(Q, R)\hat{e}(Q, S)$ and $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$
- ② *Non-degenerate*: There exists $P, Q \in G_1$ such that $\hat{e}(P, Q) \neq 1$.
- ③ *Computable*: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in G_1$.

The bilinear pairing, $\hat{e}$, is symmetric, therefore, it satisfies $\hat{e}(P, Q) = \hat{e}(Q, P)$ for all $P, Q \in G_1$. The Weil pairing[4] and the Tate pairing[6] satisfy this property and are example of such bilinear maps for which the Bilinear Diffie-Hellman Problem(BDHP) is believed to solve hard.

3. Review of Li-Liu's IMKM scheme

We first review Li-Liu's IMKM schemes in brief using the same notation as [5]. In this section, we only explain of the network initialization and the key revocation schemes of IMKM because other schemes are not affected by the security weakness.

3.1 Network Initialization

It is reasonable to assume a trusted PKG to bootstrap the network, which itself is not part of the resulting network. The basic operations consist of generating of the pairing parameters, the private

keys, and the share keys.

1) Generation of pairing parameters

To bootstrap the network, the PKG does the following:

- (1) Selects an arbitrary generation $s \in Z_q^*$, as the its private key. $P_{pub} = sP_0$ is the PKG's public key.
- (2) Predefines the number of the key update phase index, U , and selects a set of generators, $P_m (1 \leq m \leq U)$, of G_1 , for the periodic key updates.

The system parameters of PKG are as follows:

$$\langle p, q, g, G_1, G_2, \hat{e}, P_0, P_{pub}, P_m, H_1, H_2, H_3 \rangle$$

2) Generation of private keys of CH

- (1) A CH submits its identity, ID_i , to the PKG, which then computes $I_i = H_1(ID_i)$ and the user's public-private key pair:
 $Q_i = (I_i + s)P_0, S_i = (I_i + s)^{-1}P_0$.

The PKG then preloads the key pair and system parameters onto $CH_i (1 \leq i \leq n)$, securely.

3) Generation of the share key (secret sharing)

- (1) Generation of the secret sharing. All CHs participate in the construction of the master secret key, and that the role of D-PKG is assigned to the CHs of the network. Let the set of unrevoked CHs be ϕ , and $\epsilon \subset \phi$ be any subsets of size t CHs. Each CH_j computes its share key, $d_j = JP_0$, where $J = \sum_{i=1}^n f_i(I_j)$, and where $f_i(x) = \sum_{l=0}^{t-1} a_{i,l}x^l \pmod{q}$. Let $a_{i,l} \in Z_q^* (1 \leq i \leq n, 0 \leq l \leq t-1)$ be random coefficients and g be the generator. After the above distributed key generation steps, each CH holds a share key, d_j , and broadcasts public key

$$d_{j_{pub}} = H_2(P_{pub})d_j.$$

- (2) Generation of the master secret key. Master secret key, D , can be constructed by share key, d_j . Based on Lagrange interpolation, any subset, $\epsilon \subset \phi$, of size t CHs, can determine the master secret key

$$D = \sum_{j \in \epsilon} \lambda_j(0) d_j = (a_{1,0} + a_{2,0} + \dots + a_{n,0}) P_0,$$

$$\text{where } \lambda_j(0) = \prod_{i \in \epsilon, i \neq j} \frac{-I_i}{I_j - I_i} \pmod{q}, \text{ and } \epsilon$$

is the set of t unrevoked CHs participating in IMKM operations. The public key, D_{pub} , of the master secret key, can be generated from any t CHs' public keys:

$$D_{pub} = \sum_{j \in \epsilon} \lambda_j(0) d_{j_{pub}} = H_2(P_{pub})D. \quad \text{Detailed}$$

derivations of the share key and master secret key are presented in [5].

3.2 Key revocation

The key revocation scheme consists of three phases; misbehavior notification, revocation generation and revocation verification. <Figure 1> illustrates the key revocation scenario. If CH's misbehavior are detected, other unrevoked CHs send misbehavior

<Figure 1> Key revocation scenario

notification to revocation leader. Then misbehavior CHs are revoked when partial revocations have been correctly accumulated from all other $t-1$ CHs.

3.2.1 Misbehavior notification.

Upon detection of CH_i 's misbehavior, CH_j generates an accusation, $\{ID_i, T_j\}_{K_{j,v}}$, against CH_i and securely transmits it to clusterheader, CH_v , where T_j is a time stamp and $K_{j,v}$ is the pair-wise key of CH_j and CH_v ($1 \leq v \leq n, v \neq i, j$).

3.2.2 Revocation generation.

The generation of revocation requires the joint effort of t CHs. Each of t unrevoked CH_j generate a partial revocation $REV_j = H_1(ID_i)d_j$, and send it to the revocation leader securely using the pair-wise key. The revocation leader checks whether the equation $H_2(P_{pub})REV_j = d_j H_1(ID_i)$ holds. If the partial revocation is valid, revocation leader construct a complete revocation from these partials using Lagrange interpolation. A complete revocation is derived as follows:

$$ID_i' = \sum_{j \in \epsilon} \lambda_j(0) REV_j = H_1(ID_i)D. \quad \text{Then}$$

revocation leader broadcasts $\langle ID_i, ID_i' \rangle$ to inform other CHs that CH_i has been revoked.

3.2.3 Revocation verification

Upon receipt of ID_i' , each CH verifies where the equation $H_2(P_{pub})ID_i' = H_1(ID_i)D_{pub}$ holds. If it is correct, CH records ID_i in its key revocation list and declines to interact with it.

4. Security Weakness of the IMKM scheme

In this section, we show that any nodes which

know system parameters can recover CH's share key and master secret. System parameters, such as generator, hash functions, and so on, are generally opened to all nodes in ID-based cryptosystem for MANETs[7][8]. While, the IMKM assumes that system parameters are hidden to others except for CHs. It is strong assumption compared to other ID-based schemes in MANETs. This assumption restricts the scalability of networks because common nodes except CHs cannot learn system parameters easily. If system parameters are disclose to other common nodes, they can threaten the network security. Any compromised nodes who know only P_0, H_2 concurrently can recover the secret sharing, d_j from $d_{j_{pub}}$, and the master secret key, D , from D_{pub} .

$$Q_i = (I_i + s)P_0 = I_iP_0 + P_{pub} \quad \dots\dots\dots (1)$$

$$P_{pub} = Q_i - I_iP_0 \quad \dots\dots\dots (2)$$

$$d_{j_{pub}} = H_2(P_{pub})d_j \quad \dots\dots\dots (3)$$

$$D_{pub} = H_2(P_{pub})D \quad \dots\dots\dots (4)$$

From the equation (1) and (2), common nodes who know only P_0 can learn P_{pub} because Q_i and I_i are known values, public key and identity of CH_i . And from the equation (3) and (4), common nodes can recover the share key, d_j , and the master key, D because $d_{j_{pub}}$ and D_{pub} are also public values. The disclosure of these informations ignores the property of threshold technique, thus the advantage of distributed authority disappear. And networks become vulnerable to the compromised nodes, which can be CHs or common nodes who know P_0 and H_2 . Therefore, Li-Liu's IMKM scheme is inappropriate to extent MANETs and insecure in real environment.

5. Improvement

To apply IMKM to various environment, where no strong assumption is needed, we modify the IMKM. We use same notations as [5].

The weakness of the IMKM scheme is on generation of $d_{j_{pub}}$ and D_{pub} , therefore, we change the generation of them. First, CHs generate it's share key as (5). Then public key of master key, D_{pub} , can be generated from any t CHs' public keys as (6). And then, CHs broadcast public key of the share key and the master key.

$$d_{j_{pub}} = JP_{pub} = s d_j \dots\dots\dots (5)$$

$$D_{pub} = \sum_{j \in \epsilon} \lambda_j(0) d_{j_{pub}} = s D \dots\dots\dots (6)$$

D_{pub} is only updated when CHs are vary. Although CHs know $d_{j_{pub}}$ and D_{pub} , it is hard to compute d_j and D because of the private key, s , of PKG and the difficulty of BDH.

The key revocation scheme must be changed properly for modification of d_{pub} . Misbehavior notification is same as original scheme. At revocation generation, when the revocation leader checks whether the REV_j is from a valid node or not, the equation, $H_2(P_{pub})REV_j = d_{j_{pub}} H_1(ID_i)$ is changed as (7).

$$\hat{e}(REV_j, P_{pub}) = \hat{e}(d_{j_{pub}}, H_1(ID_i)P_0) \dots\dots\dots (7)$$

If this message is holds, revocation leader authenticates the sender of REV_j and constructs a complete revocation from these partials using Lagrange interpolation. At revocation verification, to check the correctness of ID_i' , each CH verifies the equation (8) is holds.

$$\hat{e}(ID_i', P_{pub}) = \hat{e}(D_{pub}, H_1(ID_i)P_0) \dots\dots\dots (8)$$

6. Conclusions

Security supports are a significant factor in mobile ad hoc networks[9][10]. Especially the key management schemes for cluster-based MANETs are very important and useful to provide security to networks.

In this paper, We analyzed the security problem of IMKM scheme and proposed solutions for it. We showed that the secret sharing and master secret key can be revealed to any compromised CHs who know some public parameters. Furthermore, we proposed a solution to improve the scheme against disclosure of the share key and the master secret key even though public parameters are opened to others and modify IMKM scheme.

We believe that the improved IMKM scheme could be usefully applied in dynamic cluster-based MANETs such as the military battlefields, mobile marketplace and VANETs.

References

- [1] E. D. Silva, A. L. D. Santos, and L. C. P. Albini, "Identity-based key management in mobile ad hoc networks: techniques and applications," IEEE Wireless Communications, vol. 15, pp. 46-52, Oct. 2008.
- [2] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," IEEE Transactions on Dependable and Secure Computing, vol. 3, pp. 386-399, 2006.
- [3] A. Shamir, "Identity-based cryptosystems and signature schemes," CRYPTO84, LNCS 196, pp. 47-53, Springer-Verlag, 1984.
- [4] D. Boneh, and M. Franklin, "Identity-based encryption from the weil pairing," CRYPTO01, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

- [5] L. C. Li, and R. S. Liu, "Securing cluster-based ad Hoc networks with distributed authorities," IEEE Transactions on Wireless Communications, vol. 9, pp. 3072-3081, 2010.
- [6] P. Barreto, H. Kim, B. Byn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," CRYPTO 02, LNCS 2442, pp. 354-368, Springer-Verlag, 2002.
- [7] Z. Zhu, Y. Zhang and F. Wang, "An efficient and provable secure identity based ring signcryption scheme," Computer Standards & Interfaces 31, pp. 1092-1097, 2009.
- [8] H. Y. Chien, "ID-based key agreement with anonymity for ad hoc networks," EUC 2007, LNCS 4808, pp. 333-345, Springer- Verlag, 2007.
- [9] I. G. Han, K. W. Rim, and J. H. Lee, "The directional partial dominant pruning algorithm for efficient message forwarding in an wireless ad-hoc network," Journal of the Korea Industrial Information System Society, vol. 14, no. 2, pp. 1-22, June, 2006.
- [10] Y. H. Park, "Vehicle registration protocol for secure communication in VANET environment," Journal of the Korea Industrial Information System Society, vol. 15, no. 4, pp. 1-5, Dec. 2010.

박 요 한 (YoHan Park)

- 2006년 2월: 경북대학교 전자전기 컴퓨터 학부 학사
- 2008년 2월: 경북대학교 전자공학과 석사
- 2008년 3월~현재: 경북대학교 전자공학과 박사과정
- 관심분야: 정보보호, 무선통신보안, 네트워크보안

박 영 호 (YoungHo Park)

- 1989년 2월: 경북대학교 전자공학과 학사
- 1991년 2월: 경북대학교 전자공학과 석사
- 1995년 8월: 경북대학교 전자공학과 박사
- 1996년~2008년: 상주대학교 전자전기공학부 교수
- 2003년~2004년: Oregon State Univ. 방문교수
- 2008년~현재: 경북대학교 산업전자전기공학부 교수
- 관심분야: 무선통신, 네트워크보안, 모바일 컴퓨팅

문 상 재 (SangJae Moon)

- 1972년 2월: 서울대학교 공업교육(전자전공)과 학사
- 1974년 2월: 서울대학교 전자공학과 석사
- 1984년 6월: 미국 UCLA 전지공학과 박사
- 1984년 7월~1985년 6월: UCLA Postdoctor 근무
- 1984년 7월~1985년 6월: 미국 OMNET 컨설턴트
- 1997년 9월~1998년 8월: 경북대학교 전자전기공학부 학부장
- 1974년 12월~현재: 경북대학교 IT대학 전자공학과 교수
- 2008년 8월~현재: 경북대학교 이동네트워크 정보보호기술 연구센터장
- 2002년 2월~현재: 한국정보보호학회 명예회장
- 관심분야: 정보보호, 디지털 통신, 이동 네트워크

논문접수일: 2011년 05월 25일
 1차수정완료일: 2011년 06월 08일
 게재확정일: 2011년 06월 23일