Journal of Korea Multimedia Society Vol. 18, No. 4, April 2015(pp. 499-505)
http://dx.doi.org/10.9717/kmms.2015.18.4.499

Secure Private Key Revocation Scheme in Anonymous Cluster-Based MANETs

YoHan Park[†], YoungHo Park[††]

ABSTRACT

Security supports are a significant factor in the design of mobile ad hoc networks. In the dynamic topology where the node changes frequently, private key generation and revocation for newly joining and leaving nodes must be considered. In addition, the identities of individual nodes must be protected as well in mobile networks to avoid personal privacy concerns. This paper proposes ID-based private key revocation scheme and non-interactive key agreement scheme in anonymous MANETs. The proposed scheme provides the user privacy using pseudonyms and private key generation and revocation schemes with consideration of dynamic user changes. Therefore, our schemes can be applied in dynamic and privacy-preserving MANETs which are helpful to share multimedia data.

Key words: Private Key Revocation, Anonymous Cluster-based MANETs, Threshold Cryptography, ID-based Cryptography, Key Agreement

1. INTRODUCTION

Mobile ad hoc networks (MANETs) are infrastructure-less, autonomous, and stand-alone wireless networks with dynamic topologies. Unlike conventional wireless networks, such as wireless cellular networks and wireless LANs, MANETs are rapidly deployable with self-organizing and self-maintaining capabilities. Because of the advantages of these features, MANETs usually refer to networks created for a special purpose. Recently, MANETs have been extended to cluster-based architectures to enhance the efficiency and security of MANETs. And this structure helps users in MANETs to share multimedia data efficiently [1,2].

However, MANETs are subject to various types of attacks because of the wireless and infrastructure-less environment. Moreover, these network structures make it difficult to apply conventional security mechanisms in MANETs directly. In traditional certificate-based cryptography (CBC), a user's public key is certified with a certificate, which is issued by a certification authority (CA). Even though it is feasible to support on-line public key infrastructure (PKI) services, the cost is very high, and this limits their application when the dynamic property and the poor connectivity are considered. As a powerful alternative to CBC, ID-based cryptography (IBC) [3,4], which was proposed by Shamir, has been gaining momentum in recent years. This is enabled by a trusted private key generator (PKG), which issues a private key corresponding to each user's identity before users first join the networks. Recently, Boneh and Franklin [5] suggested spreading the PKG using threshold cryptography to counter key escrow problem. Research on distributed PKGs (D-PKGs) is applied to ad hoc networks, called cluster-based

※ Corresponding Author : YoungHo Park, Address: (702-701) 80 Daehakro, Bukgu, Daegu, Korea, TEL : +82-53-950-7842, FAX : +82-53-950-5505, E-mail : parkyh@knu.ac.kr
Receipt date : Nov. 27, 2014, Revision date : Feb. 6, 2015
Approval date : Mar. 13, 2015

[†] Department of Electronics Enginerring, Kyungpook National University,
(E-mail : hanny12@ee.knu.ac.kr)
[††] School of Electronics Engineering, Kyungpook National University, parkyh@knu.ac.kr

ad hoc networks [1,6]. Most studies about cluster-based MANETs have been based on hierarchy topology structures which classify nodes into two types, representative nodes, which perform the role of D-PKGs, called clusterheads (CHs), and common nodes.

This paper proposes an ID-based private key generation and revocation schemes for newly joining and leaving nodes. And we also proposes non-interactive key agreement scheme using key pairs of pseudonyms. Our schemes are compatible with anonymous cluster-based MANETs [7] and suitable for dynamic and practical MANETs.

The rest of the paper is organized as follows. In Section 2, we present preliminaries and review the anonymous cluster-based MANETs. In Section 3, we describe ID-based private key generation and revocation schemes for newly joining and leaving nodes. Finally, we analyze the security of the proposed scheme in Section 4 and have conclusions in Section 5.

2. PRELIMINARIES

In this section, we present cryptographic techniques and notations used as building blocks. Then we review the anonymous cluser-based MANET [7].

2.1 ID-Based Cryptosystem

Recently IBC has its rapid development taken place due to the application of the pairing technique outlined below.

Let p,q be the large primes and E/F_p indicate an elliptic curve $y^2 = x^3 + ax + b$ over the finite field F_p. We denote by G_1 a q-order subgroup of the multiplicative group of the finite field $F_{p^2}^*$. The discrete logarithm problem (DLP) is required to be hard in both G_1 and G_2. For us, a pairing a map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ with the following properties:

- Bilinear: $\forall P,Q,R,S \in G_1$, $\hat{e}(P+Q,R+S) = \hat{e}(P,R)\hat{e}(P,S)\hat{e}(Q,R)\hat{e}(Q,S)$.

  Consequently, for $\forall a,b \in Z_q^*$, we have $\hat{e}(aP,bQ) = \hat{e}(aP,Q)^b = \hat{e}(P,bQ)^a = \hat{e}(P,Q)^{ab}$ etc.
- Non-degenerate: If P is a generator of G_1, then $\hat{e}(P,P) \in F_{q^2}^*$ is a generator of G_2.
- Computable: There is an efficient algorithm to compute $\hat{e}(P,Q)$ for all $P,Q \in G_1$.

Note that $\hat{e}$ is also symmetric, i. e., $\hat{e}(P,Q) = \hat{e}(Q,P)$, for all $P,Q \in G_1$, which follows immediately from the bilinearity and the fact that G_1 is a cyclic group. Modified Weil [4] and Tate [8] pairing are examples of such bilinear maps for which the bilinear diffie-hellman problem (BDHP) is believed to be hard.

2.2 Threshold Scheme

Secret sharing schemes were independently introduced by the Blakley [9] and the Shamir [10] in 1979. They introduced a way to split a secret K into n shares. And only t or more than t shares among n can reconstruct a secret K. It is called (t,n)-secret sharing, denoted as (t,n)-SS.

Shamir's (t,n)-SS. Shamir's $(t,n)-SS$ is based on polynomial interpolation. The scheme consists of two algorithms:

① Secret Sharing Generation. A trusted party T distributes shares of a secret K to n users as follow:
- T chooses a prime $p > \max(K,n)$, and defines $a_0 = K$.
- T picks a polynomial $f(x)$ of degree $(t-1)$ randomly: $f(x) = a_0 + a_1 x + \cdots a_{t-1} x^{t-1}$, in which the secret $K = a_0 = f(0)$ and all coefficients $(a_0,\ldots,a_{t-1})$ are in a finite field $F_p = GF(p)$ with p elements.
- T computes $K_i = f(s_i)$ (mod p) for i=1,...,n. and securely transfer the shares K_i to each user.

② Secret Reconstruction. Any group of size t or more than t can reconstruct the polynomial $f(x)$

as

$$f(x) = \Sigma_{i \in A} \lambda_i(x) K_i \pmod{q} \quad (1)$$

where $A = \{1,...,t\} \subseteq \{1,...,n\}$, $\lambda_i(x) = \Pi_{j \in A \setminus i} \frac{s_j - x}{s_j - s_i}$ is called a Lagrange coefficient. The secret is recovered by $f(0) = K$.

For more information on this scheme, readers can refer to the original paper [10].

2.3 Notations

Table 1 lists some important notations. whose concrete meanings will be further explained.

2.4 Anonymous Cluster-Based MANETs

In this section, we review the anonymous cluster-based MANETs [7]. The network architecture of the anonymous cluster-based MANETs is illustrated on Fig. 1. Each cluster is composed of a clusterheader (CH) and common nodes (users in Fig. 1).

Table 1. Notations

G_1, G_2	cyclic groups of order q
$\hat{e}$	pairing s. t. $\hat{e}: G_1 \times G_1 \rightarrow G_2$
P	generator of G_1
CH_j / ID_A	network ID of clusterhead j and common node A
PS_A	pseudonym of ID_A
S_j / Q_j	private/public key pair of clustehead j
S_A / Q_A	private/public key pair of common node A
S_{PS_A} / Q_{PS_A}	private/public key pair of pseudonym PS_A
U	maximum update phase index
K_m	cluster key at m-th update phase
$g_m(x)$	polynomial for cluster key K_m
$f_m^{CH_j}(x)$	polynomial of CH_j
(t, n)	secret sharing parameters for $g_m(x)$
(t_1, n_1)	secret sharing parameters for $f_m^{CH_j}(x)$
S_G	group secret key
H_0	mapping $(0,1)^* \rightarrow Z_p^*$
H_1	mapping $(0,1)^* \rightarrow G_1$
H_2	mapping $Z_p^* \rightarrow (0,1)^*$
H_3	mapping $G_1 \rightarrow Z_p^*$

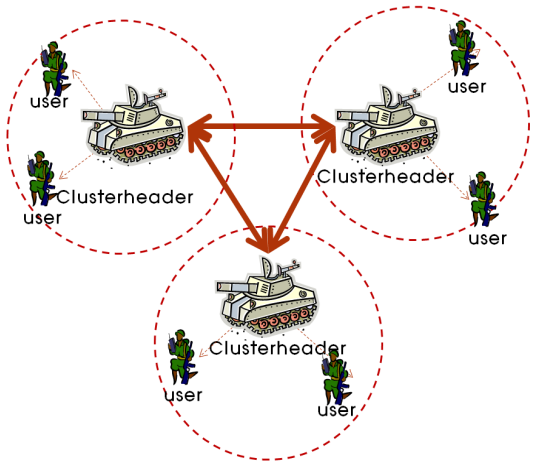

Fig. 1. Cluster Configuration and Pseudonym Generation.

2.4.1 Configuration of clusters

Before the network is established, each CH has received secret sharings $g_m(ch_j)$, where $0 \le m \le U, 1 \le j \le n$ from the PKG. To recover a cluster key, CHs, at least t, gather their secret sharing at the same update phase m. Using these secret sharings, CHs can compute cluster key K_m. And the initial secure channel between a CH and a user is established using their private/public key pairs. In here, the system cannot support user's anonymity, that is, adversaries can guess and find users what they want to attack.

2.4.2 Generation of pseudonyms

To generate pseudonyms for users within a cluster, each CH initially generates it's polynomial, called respective polynomial with a cluster key K_m. And they generate pseudonyms for common nodes using their respective polynomials. Common nodes receive private/public key pairs of pseudonyms using channel previously established. By using these pseudonym key pairs, a CH and a user or between users can establish secure channels without exposing their real identities. The pseudonyms are generated as follows,

① Generate respective polynomial. CHs have a same cluster key K_m by reconstructing polynomial $g_m(x)$. Each CH generates a respective polynomial $f_m^{CH_j}(x)$ by setting the cluster key K_m as a secret, This means that respective polynomials have same a secret $f_m^{CH_j}(0) = K_m$.

② Generate pseudonym key pairs. The CH generates pseudonyms for common nodes within it's cluster using common nodes identities. For instance, the pseudonym of ID_A within the cluster CH_j is constructed as $PS_A = f_m^{CH_j}(id_A)$. And the public and private key pair is made as $Q_{PS_A} = PS_A K_m P$ and $S_{PS_A} = PS_A$.

③ Record pseudonyms. CHs record identities and corresponding pseudonyms at pseudonym lookup table (PLT)

④ Share pseudonym key pairs. CHs then forward pseudonym key pairs to corresponding users using a secure channel established by initial private/public key pairs.

For more information on anonymous cluster-based MANETs, readers can refer to the original paper [7].

3. PRIVATE KEY GENERATION/REVOCATION SCHEME AND KEY AGREEMENT SCHEME

In practical MANETs, new nodes which are not member of networks join networks and registered nodes at networks could leave networks frequently. Furthermore, some registered nodes could be compromised by adversaries. Therefore, the security system must provide private key generation for joining nodes and private key revocation for leaving or corrupted nodes. In this section, we propose private key generation and revocation schemes for newly joining and leaving nodes.

3.1 Private Key Generation for Newly Joining Nodes

Private key generations for newly joining nodes are same as [7]. Because of the property of threshold scheme, pseudonyms are generated by respective polynomials, the added private keys do not affect the security of system as long as newly joining nodes are uncorrupted ones and the networks can accept unbounded nodes academically. Thus we do not describe private key generation for newly joining nodes in detail in this paper.

3.2 Private Key Revocation for Leaving or Misbehaving nodes

In the anonymous security system using pseudonyms, each node can verify the validity of a pseudonym with a pair-wise key because only registered nodes who have received pseudonyms from CHs can have a group secret key S_G. However, these registered nodes have the possibility of being subject to attacks and consequently could compromise the security of networks; therefore, the system should provide a priavate key revocation process to protect lasting attacks against those nodes. Y. Zhang et al. [11] proposed a key revocation using secret sharings. To provide node revocation, we modified their scheme to adopt to our system. Node revocation is carried out when more than $\Gamma = \{1,...,\gamma\}$ misbehavior revocations are reported to a CH to protect innocent nodes against false accusations. The pseudonym revocation scheme is carried out as follows;

1) Misbehavior Notification. To report a suspicious node whose public key is Q_{PS_X} to a CH_j, nodes perform the following:

① Compute misbehavior notification. Node A detecting misbehavior of a suspicious node generates a misbehavior notification: $\{Q_{ps_A}, Q_{PS_i}, T_i\}$ where T_i is the timestamp.

② Forward the notification. Each node generating the misbehavior notification unicasts the notification to CH_j using a secure channel.

2) Pseudonym Revocation. To revoke a reported

node, CH_j performs the following:

① Performs pseudonym revocation. When more than γ notifications are collected on a CH, CH_j performs a secret reconstruction algorithm:

$$f_m^{CH_j'}(x) = \Sigma_{i \in B} \lambda_i(x) PS_i \pmod{q} \quad (2)$$

where $\Gamma = \{1,...,\gamma\} \subset B = \{1,...t_1\} \subseteq \{1,...,n_1\}$, $\lambda_i(x) = \Pi_{j \in B \setminus i} \frac{id_j - x}{id_j - id_i}$ are called a Lagrange coefficient. Although the number of notifications is not as high as the number of t_1, it works properly because CH_k can generate arbitrary pseudonyms, $PS_r = f_m^{CH_j}(r)$, where $r \in Z_q^*$.

② Checks the validity of accusers. A CH can verify all accusers as legitimate nodes by comparing $f_m^{CH_j'}(0) = K_m$. If it does not hold, a CH knows that at least one of the accusers is incorrect and stops the pseudonym revocation.

③ Revokes the identity of unlawful node. A CH records ID_X to its credential revocation list (CRL) [12] and notifies to other CHs ID_X as an unlawful node. Then a CH erases ID_X from PLT and stops updating it to isolate it from the networks.

④ Publishes the pseudonym revocation. A CH publishes the pseudonym revocation to the networks: $< PS_X, Q_{PS_X} >$.

3) Revocation Verification. To verify the pseudonym revocation, every node in the networks performs the following:

① Computes the revocation. Every node computes $\hat{e}(Q_{PS_X}, S_G) = \hat{e}(P,P)^{PS_X}$. If it holds, the nodes revoke the public key Q_{PS_X} and record it as unlawful. Then, all CHs change the update phase into $m+1$ and nodes update pseudonyms.

The revocation of a CH is similar to the process described above. If CHs (assume that nodes report a misbehaving CH to its CH) find a misbehaving CH, they report it to the revocation leader, one of the most powerful CHs, with their secret sharings. If the misbehavior notifications are more than γ, the revocation leader starts the revocation generation and computes $g_m(x)$. If $g_m(0) = K_m$, the revocation leader publishes the accused CH as a compromised CH, and then other CHs update the cluster key except the accused CH. Finally, the accused CH is isolated from the networks.

3.3 Non-interactive Key Agreement Scheme Using Pseudonyms

Key agreement is an essential process to exchange messages securely. The non-interactive key agreement scheme which happens under different clusters is the same as the scheme which happens under the same cluster, as long as the clusters are in the same update phase. We slightly modify the key agreement scheme in [7]. Our key agreement scheme with pseudonym between nodes is carried out as follows;

$$D_{AB} = \hat{e}(S_{PS_A}, Q_{PS_B}) = \hat{e}(Q_{PS_A}, S_{PS_B}) = D_{BA} \quad (3)$$
$$k_{AB} = H_2(D_{AB} \| H_3(S_G))$$

4. SECURITY ANALYSIS

In this section, we describe an analysis of our system with respect to security.

- **Non-manipulation.** Our proposed security system ensure non-manipulation in case of at most (t-1 or t_1-1) compromised nodes. Only the CH who has a respective polynomial can generate valid pseudonyms in a cluster, and no other nodes and CHs can do it. Adversaries should know the cluster key K_m to generate the pseudonym working correctly in networks and the respective polynomial $f_m^{CH_j}(x)$ to generate the pseudonym working correctly in a cluster. Thus, as long as (t or t_1) or more than (t or t_1) nodes and CHs are not colluding, non-manipulation is guaranteed.

- **Fundamental Security Services.** Authentication of nodes and the confidentiality and integrity of messages are guaranteed by the non-interactive key agreement schemes. Each CH authenticates the nodes within a cluster by non-interactive key agreement using the initial key pair. For the proof, see e.g., [13]. Authentication of the pseudonym and confidentiality and integrity of messages are guaranteed by non-interactive key agreement using pseudonyms. The pair-wise key is in the form of $H_2(D_{AB} \| H_3(S_G))$, where $D_{AB} = \hat{e}(P,P)^{PS_A PS_B}$. Active outside/passive inside adversaries cannot generate a legitimate pseudonym of a specific node even though they have unspecific pseudonyms and identities. Furthermore, active outside adversaries do not know and compute the group secret key, S_G. As a result, the non-interactive key agreement scheme using pseudonym is secure against active outside/passive insider adversaries.

5. CONCLUSIONS

Concerns for personal privacy and security in wireless environments are increasing rapidly as mobile devices are becoming more popular. Cluster-based MANETs are being considered to pioneer new markets; however, there are urgent unresolved security problems. Fundamental security services, such as authentication and key agreement, are challenging for secure security systems. Especially, private key update for newly joining and leaving or corrupted nodes should be supported considering dynamic topologies of MANETs. In addition, the protection of the user privacy becomes more important with wider use of wireless networks; therefore, the design of secure private key generation and revocation in privacy-preserving MANETs are required.

We presented private key generation and revocation schemes for privacy-preserving MANETs under practical assumptions. According to our protocol analysis, our proposed method provides most security requirements for dynamic MANETs by using the anonymity. Our schemes can be effectively applied in the dynamic environments with relatively better efficiency by using secret sharing schemes. Our proposed schemes improve security and widens the possible application area compared to previously proposed security systems. It could be usefully applied to preserve privacy in dynamic MANETs, where a trusted entity is not available. Such examples include military battlefields, emergency areas, mobile marketplaces, and VANETs.

REFERENCE

[1] L. Li and R. Liu, "Securing Cluster-Based Ad Hoc Networks with Distributed Authorities," *IEEE Transactions on Wireless Communications*, Vol. 9, No. 10, pp. 3072-3081, 2010.

[2] M. Bechler, H.J. Hof, D. Kraft, F. Pahlke, and L. Wolf, "A Cluster-Based Security Architecture for Ad Hoc Networks," *Proceeding of IEEE Infocom.,* pp. 2393-2403, 2004.

[3] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Proceeding of CRYPTO 84*. LNCS 196, pp. 47-53, 1984.

[4] S.I. Kang, N.H. Lee, and I.Y. Lee, "A Study on Group Key Management based on Mobile Device ID in Ad-hoc network," *Journal of Korea Multimedia Society*, Vol. 12, No.4, pp. 540-549, 2009.

[5] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Proceeding of CRYPTO 01*. LNCS, Vol. 2139, pp. 213-229, 2001.

[6] 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, No. 4, pp. 386-399, 2006.

[7] Y.H. Park, Y.H. Park, and S.J. Moon, "Anonymous Cluster-Based MANETs with Threshold Signature," *International Journal of Distributed Sensor Networks,* pp. 1-9, 2013.

[8] P. Barreto, H. Kim, B. Bynn, and M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," *Proceeding of CRYPTO 02.* LNCS 2442, pp. 354-369, 2002.

[9] G.R. Blakley, "Safeguarding Cryptographic Keys," *American Federation of Information Processing Societies 79,* pp. 313-317, 1979.

[10] A. Shamir, "How to Share a Secret," *Communication*, Vol. 22, No. 11, pp. 612-613, 1979.

[11] Y. Fang, X. Zhu, and Y. Zhang, "Securing Resource-Constrained Wireless Ad Hoc Networks," *IEEE Wireless Communications 16*, Vol. 16, No. 2, pp. 24-30, 2007.

[12] M. Raya and J. Hubaux, "Securing Vehicular Ad Hoc Networks," *Journal of Computer Security*, Vol. 15 No. 1, pp. 39-68, 2007.

[13] R. Dupont and A. Enge, "Provably Secure Non-Interactive Key Distribution based on Pairings," *Discrete Applied Mathematic,* Vol. 154, No. 2, pp. 270-276, 2006.

YoHan Park

received B.S, M.S. and Ph.D. degrees from Kyungpook National University in 2006, 2008, and 2013 respectively. Currently, he is a lecturer in Kyungpook National University. His research interests are information security, mobile communication and network security.

YoungHo Park

received B.S, M.S. and Ph.D degrees from Kyungpook National Univeristy in 1989, 1991, and 1995 respectively. Currently, he is a professor in the School of Electronics Engineering at Kyungpook National University. His research interests are information security, network security, and mobile communication.