논문 2012-49TC-1-13

이동 애드혹 네트워크에서의 익명성을 제공하는 아이디 기반의 안전한 키 교환 프로토콜

(Secure ID-Based Key Agreement Protocol with Anonymity for Mobile Ad Hoc Networks)

박 요 한*, 박 영 호**, 문 상 재***

(YoHan Park, YoungHo Park, and SangJae Moon)

요 약

애드혹 네트워크에서 보안을 제공하는 것은 매우 중요한 요소이다. 특히 역동적인 구조에서는 시스템의 안전을 위해서 개인키를 업데이트해 주는 키 교환 프로토콜이 필수적이다. 그리고 개인의 사생활 보호 문제를 방지하기 위해 각각의 노드의 아이디를 보호하는 것도 필요하다. 하지만 기존의 많은 애드혹 네트워크의 키 교환 프로토콜들은 이러한 보안 문제들을 동시에 고려하지 않았다. 본 논문에서는 익명성을 제공하는 키 교환 프로토콜과 개인키 업데이트 프로토콜을 제안하다. 또한 서로 다른 서비스 영역에서의 키 갱신 프로토콜을 제안한다. 제안한 프로토콜들은 여러 공격에 안전하고 서비스를 제공하는 이동 애드혹 네트워크에 적합하다.

Abstract

Security support is a significant factor in ad hoc networks. Especially in dynamic topologies, key agreement with private key updating is essential in providing a secure system. And it is also necessary to protect the identities of individual nodes in wireless environments to avoid personal privacy problems. However, many of the existing key agreement schemes for ad hoc networks do not consider these issues concurrently. This paper proposes an anonymous ID-based private key update scheme and a key agreement scheme for mobile ad hoc networks. We also suggest a method of rekeying between different domains using service-coordinators. These schemes are secure against various attacks and are suitable for service-oriented mobile ad hoc networks.

Keywords : mobile ad hoc networks, ID-based cryptography, service-coordinator, private key update, anonymity

Ⅰ. Introduction

Mobile ad hoc networks (MANETs) are infrastructureless, autonomous, and stand-alone wireless networks with dynamic topologies. Unlike conventional wireless networks, such as wireless cellular networks and wireless LAN, MANETs are rapidly deployable with self-organizing and self-maintaining capabilities. Because of the advantages of these features, MANETs have naturally been deployed in emergency rescue, disaster relief, and military operations, where fixed infrastructures are often destroyed, unavailable, or unreliable, and fast network establishment and self-maintenance are required[1]. Recently, MANETs have been extended to intelligent transport systems, often called vehicular ad hoc networks (VANETs)[2].

* 정회원, *** 평생회원, 경북대학교 전자공학과
(Kyungpook National University)
** 정회원-교신저자, 경북대학교 산업전자전기공학부
(Kyungpook National University)
접수일자: 2011년11월1일, 수정완료일: 2012년1월17일

Although MANETs offer many advantages, they also pose many design challenges. Wireless channel condition is usually very poor and time-varying due to mobility, power depletion, and unpredictable interference, those lead to constant transmission failures. Moreover, the channel environment is open, so that attacks, such as eavesdropping of communication channels, modification of m-commerce transactions, denial of service, and impersonation by malicious insiders, cause security concerns.

Regarding the security requirements of MANETs, secure key agreement and update schemes are required to build a secure network[3]. Many of the existing key agreement and update schemes[4~5] assume that on-line certificate servers support public key infrastructure (PKI) service. Even though it is feasible to support on-line PKI services, the cost to implement is very high. It can limits the applicability of ad hoc networks especially when the dynamic topology is considered. As a powerful alternative to certificate-based public key cryptography, ID-based cryptography (IBC)[6] proposed by Shamir has been gaining momentum in recent years. It allows public keys to be derived from entities' known identity information, thus eliminating the need for public key distribution and certificates. Fortunately, most ad hoc applications meet this requirement such as e-mail addresses, IP addresses or MAC. This feature has inspired a few IBC-based public-key certification management schemes for MANETs, such as [7~8].

However, there are still many remaining unresolved issues. One such issue is the updating of private key. This must be dealt with in a dynamic topology which considers self-organized and decentralized networks to protect against compromised nodes. Another security requirement that has recently become an issue is personal privacy against eavesdropping and user tracking. These problems can be resolved by supporting key update considering entity anonymity. Adversaries or malicious parties who are not in communication cannot know which parties are communicating and cannot eavesdrop. Recently anonymous key agreement schemes[9~10] and key update schemes[5,8,11] have been proposed, but they didn't consider both of them concurrently.

In this paper, we address all these concerns by devising an ID-based private key update, key agreement and rekeying scheme for MANETs aided by service-coordinators (SCs)[12~13]. An SC-based approach results in a more scalable architecture that tends to separate the network into various service areas. Therefore it is suitable for service-oriented MANETs and wireless cells for operating differentiated tasks. This type of application has been recognized as a major application category for wireless ad hoc networking techniques, and it will continue to be an important area of application into the future. Typical examples are those deployed in mobile marketplace, military battlefield operations, and VANETs. The major contributions of this study may be summarized as follows:

- **Secure private key update scheme and key agreement scheme.** We propose a secure private key update scheme and a key agreement scheme with anonymity within each domain. Private key updating ensures that the compromise of an arbitrary number of nodes does not jeopardize the secrecy of non-compromised nodes. Key agreement also ensures secure communication between nodes.

- **Protection of personal privacy.** Our schemes support entity anonymity. The types of anonymity are classified by [14]. Our private key update scheme and rekeying scheme support type 3. That is, identity protection is required for the client but not for the server. The key agreement scheme supports type 4. That is, identity protection is required for both the client and the server, and only the entities of the matched session can know the identity of others with whom they are in communication.

- **Consideration of rekeying for multi-domain.** Our rekeying scheme considers movement between domains. By updating a node's private key, it can communicate flexibly when moving to other domains.

The rest of the paper is organized as follows. In Section Ⅱ, we survey the related works, network model and outline a bilinear pairing. Next we present secure ID-based private key update with anonymity in Section Ⅲ, followed by a analysis in Section Ⅳ. The paper is finally concluded in Section Ⅴ.

Ⅱ. Preliminaries

In this section, we first survey related works. We then introduce scenarios using the SC and define bilinear pairing on which our design is based.

1. Related Works

Many previous work have proposed key agreement schemes and key management schemes for ad hoc networks. In ID-based schemes, the identity of a node is used to derive its public key, while the private key is generally provided by an external entity[15].

The key management schemes proposed in [11] combine an ID-based cryptosystem with a threshold technique. However, the scheme assumes that identities are recorded in hardware and cannot be altered, so an attacker who creates false identities or alters its own identity can be a threat to network security. In [16], another ID-based key management scheme combined with a threshold technique was proposed. It has three phases: key redistribution, key revocation, and key update. In this scheme, nodes must update their public/private keys at periodic intervals or when the number of revoked nodes reaches a predefined value. Revoked nodes cannot update their keys, thus becoming isolated from the network. Unfortunately, these schemes cannot protect the privacy of nodes because they do not provide entity anonymity. A nodes could disclose its location to malicious adversaries who are continuously tracking that specific node.

The key agreement scheme proposed by Bohio *et. al*[17] uses pair-wise symmetric keys computed noninteractively by nodes. However, [18] finds several weaknesses in Bohio's scheme. The signature scheme is vulnerable to the universal forgery attack in which an adversary can forge signatures on any message chosen. Moreover, the key escrow-free version violates the certificate-less property of ID-based schemes and requires on-line server support, which violates the properties of ad hoc networks. H. Y. Chien also proposed an ID-based key agreement scheme[9]. Although it provides anonymous key agreement, it does not mention any key update process. Thus, these schemes are vulnerable to attacks of compromised nodes.

2. Scenarios

There are various MANET scenarios. These scenarios are classified according to the existence of a trusted third party (TTP). This depends on the implemented environment or application area. In the ideal scenario for ad hoc networks, each node performs a role similar to that of the TTP during network initialization and in the running network. However, this scenario may be more restrictive than the actual environment of most MANET applications; thus, it can put an unnecessary burden on the protocol design. Many researchers have studied practical models, such as a distributed model[19], in which only nodes that were present at the time of network formation are initialized by an external TTP, but nodes which need to be initialized to join established networks are initialized by other initialized nodes.

In this study, we consider a distributed ad hoc network model regarding SCs. SCs are special nodes acting as brokers on behalf of clients or as helpers to update node's private key[12]. They differ from TTPs. The TTP is fixed and expensive. It initializes

networks and can operate in several networks concurrently. An SC, however, is mobile and inexpensive and helps networks to operate efficiently. For example, RSUs in VANET or tanks in a military battlefield could be members of a participating node, and though they are somewhat more powerful than normal nodes, they are kinds of SCs. SCs make the private key update process easily. We assume that SCs are secure and parties in networks have already been initialized. Figure 1 shows the communication between an SC (i. e. *zeus*) and other nodes (i. e. *ares, hydra, artemis et al.*). In this phase, nodes can update their private keys using the SC by establishing a secure channel.

Figure 2 shows communication between nodes.

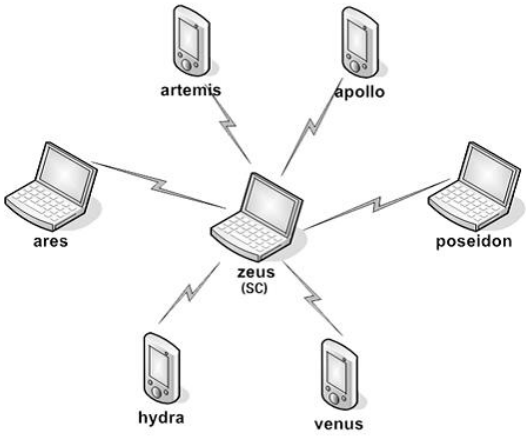

그림 1. 비밀키 업데이트 시나리오
Fig. 1. Private key update scenario.

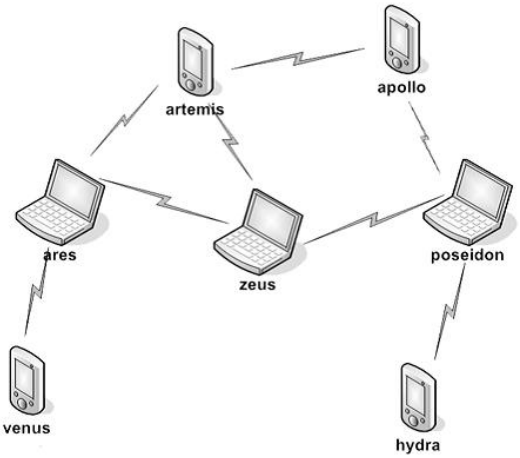

그림 2. 키 교환 시나리오
Fig. 2. Key agreement scenario.

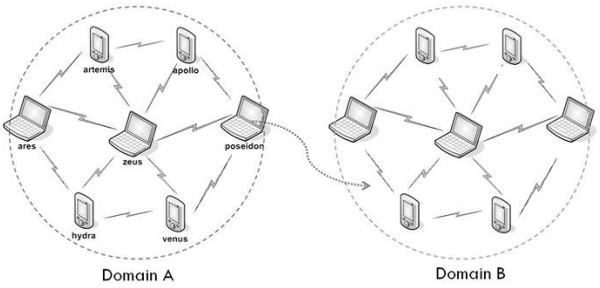

그림 3. 다른 도메인 이동시 키 갱신 시나리오
Fig. 3. Rekeying scenario when moving other domain.

Here, *zeus* is a general node which communicates with other nodes.

Figure 3 illustrates a scenario of rekeying between different domains. When a node A (i. e. *poseidon*) in domain A is out of coverage of the SC (i. e. *zeus*), poseidon cannot update its private key using *zeus* anymore. Another SC in domain B which covers poseidon can help *poseidon* update its private key. After updating, *poseidon* can communicate with nodes within domain B.

3 Bilinear Pairing

Although the idea of IBC dates back to 1984[6], only recently 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[20] and Tate[21] pairing are examples of such bilinear maps for which the *bilinear diffie-hellman problem* (BDHP) is believed to be hard.

Ⅲ. D-Based Key Agreement Scheme with Anonymity

This section presents three schemes, namely, the private key update scheme, key agreement scheme, and rekeying scheme. Table 1 lists some important notations whose concrete meanings will be further explained where they appear for the first time.

We first describe the key redistribution phase in Section Ⅲ.1. Next, we discuss the method to achieve private key updating in Section Ⅲ.2. In Section Ⅲ.3, key agreement between nodes is explained. Finally, rekeying between different domains is discussed in Section Ⅲ.4.

표 1. 기호들
Table 1. Notations.

x_1, x_2, y	random integers $\in Z_1^*$
p, q	two large primes
$\hat{e}$	pairing s. t. $\hat{e}: G_1 \times G_1 \rightarrow G_2$
p_i	i-th key update period
$salt_i$	unique binary string associated with p_i
$E_k(m)$	encryption of m with symmetric key k
$Sig_A(m)$	signature of m with private key A
D_{AB}	pair-wise secret of node A and node B
H_1	$\{0,1\}^* \rightarrow G_1$, *MaptoPoint* function
H_2	$G_2 \rightarrow \{0,1\}^t$, where t is bit length of key
ID_A	network ID of node A
W	generator of G_1
K_{ms_1}	master secret for ID; only the TTP knows
$K_{ms_{2(A)}}$	master secret for the update element (in domain A); the TTP and a SC know
K_A^{-1}	private ID of node A
$K_{p_i}^{-1}$	private update element in phase p_i

1. Network Initialization

For a single-authority MANET under consideration, it is reasonable to assume a trusted PKG to bootstrap the network, which itself is not part of the resulting network. We adopted some notations and frameworks for network initialization from [8].

(1) *Generation of pairing parameters*: To bootstrap the network, the PKG does the following:

(a) Generate the pairing parameters $(p, q, \hat{e})$. Select an arbitrary generator W of G_1.

(b) Choose a hash function H_1 that maps arbitrary binary strings to non-zero elements in G_1. The specific *MapToPoint* operation, H_1 is described by [17].

(c) Pick two distinct random numbers $K_{ms_1}, K_{ms_2} \in Z_q^*$ as network master secrets.

Parameters $(p, q, \hat{e}, H_1, W)$ are public knowledge preloaded to each node, while K_{ms_1} should never be disclosed to any single node. But $K_{ms_{2A}}$ is known to the SC in domain A only. In other words, only SCs can know the master secret for the update element.

(2) *Generation of ID-based private key*: In our schemes, the private key is both *node-specific* and *phase-specific*. For instance, node A's private key which is valid only during phase p_i is denoted by K_{A,p_i}^{-1}, in particular, $K_{A,p_i}^{-1} := (K_A^{-1}, K_{p_i}^{-1}) = (K_{ms_1} H_1(ID_A), K_{ms_2} H_1(salt_i))$. Initially, the PKG issues K_{A,p_1}^{-1} to node A, then which can acquire $K_{A,p_i}^{-1} (1 < i \leq M)$ from the SCs in running network, as will be shown later. Such p_i'-s may not be of the same duration and thus do

not require nodes to be time-synchronized for them either. Each p_i is associated with a unique binary string, called a *phase salt* and denoted by $salt_i$.

Due to the difficulty of solving the DLP in G_1, it is computationally infeasible to derive the network master secrets K_{ms_1} and K_{ms_2} from an arbitrary number of private key[20]. It means that, no matter how many key pairs adversaries acquire from compromised nodes, they cannot deduce the private key of any non-compromised node.

2. Private Key Update Scheme

To withstand cryptanalysis and limit any potential damage from compromised keys, it is a common practice to employ relatively frequent private key updating. Figure 1 shows the private key updating scenario. A new key update phase p_{i+1} starts when the registered nodes whose update element is in p_i are compromised or who have left the networks. These nodes could be powerful adversaries because they can still communicate in networks pretending to be rightful users.

In our anonymous private key update scheme, SCs can update the private keys of nodes using a network master secret. To update a private key, SCs and nodes establish a secure channel first. This channel has to be protected against various attacks. Even insider adversaries are powerful attackers in MANETs because of the importance of private keys. Revoked nodes, which cannot update their keys, are isolated from the networks. Let us assume that the node which performs a private key update is node A, and the SC is node B for easy explanation. As we previously mentioned, the identity of the SC is open and only the SC knows the network master secret. Here, we suggest the use of Hess's ID-based signature[22] because it is efficient and has been proven secure in the random oracle model. The anonymous private key update scheme is carried out as follow:

① B → A

B chooses a random integer $y \in Z_q^*$, computes $Y = yH_1(ID_B)$, and sends $ID_B, Y, Sig_B(ID_B \| Y)$ to A.

② A → B

A checks the validity of signature first. If it is correct, A chooses random integer $x \in Z_q^*$, and computers $X = xH_1(ID_A)$. Then A computes pair-wise secret key $D_{AB} = \hat{e}(K_A^{-1}, Y)^x \cdot \hat{e}(K_{p_i}^{-1}, W)$, $k_1 = H_2(D_{AB})$ and sends $p_i, X_1, E_{k_1}(ID_A, Sig_A(p_i \| X \| ID_A))$ to B.

③ B → A

B computes pair-wise secret key $D_{BA} = \hat{e}(K_B^{-1}, X)^y \cdot \hat{e}(K_{p_i}^{-1}, W)$, $k_1' = H_2(D_{BA})$ first, and checks the validity of A's signature. If it is correct, B sends $p_i, ID_B, E_{k_1'}(K_{p_{i+1}}^{-1}, Sig_B(p_i \| ID_B \| K_{p_{i+1}}^{-1}))$ to A.

A checks the validity of B's signature. If it is correct, A update its private key as $(K_A^{-1}, K_{p_{i+1}}^{-1}) = (K_{ms_1}H_1(ID_A), K_{ms_2}H_1(salt_{i+1}))$.

3. Key Agreement Scheme

Key agreement is an essential process to exchange messages securely. Figure 2 shows the key agreement scenario. Personal information, such as location or movement of nodes, are of great value in wireless environments; therefore, it need to be protected.

In our anonymous key agreement scheme, SCs can be considered general nodes like others, and they are secure against passive insider adversaries. The anonymous key agreement scheme is carried out as follows:

① A → B

A chooses a random integer $x \in Z_q^*$, computes $X = xH_1(ID_A)$, and sends it to B.

② B → A

B chooses a random integer $y \in Z_q^*$, and computers $Y = yH_1(ID_B)$. Then B computes pair-wise secret key $D_{BA} = \hat{e}(K_B^{-1}, X)^y \cdot \hat{e}(K_{p_i}^{-1}, W)$, $k_1 = H_2(D_{BA})$ and sends $p_i, Y, E_{k_1}(ID_B, Sig_B(p_i \| Y \| ID_B))$ to A.

③ A → B

A computes pair-wise secret key $D_{AB} = \hat{e}(K_A^{-1}, Y)^x \cdot \hat{e}(K_{p_i}^{-1}, W)$, $k_1' = H_2(D_{AB})$ first, and checks the validity of B's signature. If it is correct, A sends $p_i, E_{k_1'}(ID_A, Sig_A(p_i \| ID_A))$ to B and sets session key as $k_{sess} = H_2(p_i \| k_1' \| ID_A \| ID_B)$.

B checks the validity of A's signature. If it is correct, B sets session key as $k_{sess} = H_2(p_i \| k_1 \| ID_A \| ID_B)$.

4. Rekeying Scheme

It is necessary to provide a rekeying scheme between different domains when considering ad hoc networks regarding SCs. If we consider a conventional MANET environment, the network operator should employ several SCs to cover the whole service area because of the SC's limited coverage ability. If we consider a service-oriented MANET environment, such as the mobile marketplace or a battlefield, independent SCs are needed to support different services. In these environments, a rekeying problem occurs when nodes move from the coverage domain of one SC to another SC's coverage. Figure 3 shows the scenario for entity authentication between domains.

In our anonymous rekeying scheme, an SC assists in the private key updating of joining nodes which come into its coverage by using the master key of the update element. Each domain can be protected against compromised SCs by setting a different master key of the update element for each SC. Let a node which moves from domain A to domain B be node A, and let the SC in domain B be node B. The master secret for the update element, $K_{ms_{2B}}$, can only be possessed by the SC in domain B. The private key of node A before moving to domain B is $(K_A^{-1}, K_{p_i}^{-1}) = (K_{ms_1} H_1(ID_A), K_{ms_{2A}} H_1(salt_i))$. The anonymous rekeying scheme between different domains is carried out as follows:

① B → A

B chooses a random integer $y \in Z_q^*$, computes $Y = yH_1(ID_B)$, and sends $ID_B, Y, Sig_B(ID_B \| Y)$ to A.

② A → B

A checks the validity of signature first. If it is correct, A chooses random integers $x \in Z_q^*$, and computers $X = xH_1(ID_A)$. Then A computes pair-wise secret key $D_{AB} = \hat{e}(K_A^{-1}, Y)^x$, $k_1 = H_2(D_{AB})$ and sends $p_i, X, E_{k_1}(ID_A, Sig_A(p_i \| X \| ID_A))$ to B.

③ B → A

B computes pair-wise secret key $D_{BA} = \hat{e}(K_B^{-1}, X_1)^y$, $k_1' = H_2(D_{BA})$ first, and checks the validity of A's signature. If it is correct, B sends $p_i, ID_B, E_{k_1'}(K_{p_{i+1}}^{-1}, Sig_B(p_i \| ID_B \| K_{p_i}^{-1}))$ to A.

A checks the validity of B's signature. If it is correct, A update its private key as $(K_A^{-1}, K_{p_i'}^{-1}) = (K_{ms_1} H_1(ID_A), K_{ms_{2B}} H_1(salt_i'))$

Ⅳ. Analysis

This section presents security and efficiency analysis. We describe the security against insider adversaries, eavesdropping, impersonation, known-key security, and perfect forward secrecy. Our security analysis focuses on the private key update scheme because key agreement scheme and rekeying scheme are branches of it.

- **Inside Adversaries:** Insider adversaries are malicious authorized nodes performing unauthorized actions. They can have access to

additional information and may be trusted by other network nodes. The private key update scheme is secure against active insider adversaries because they cannot decrypt messages although they already possess the network information. Messages are also protected against modification by signature and ephemeral pair-wise key. If adversaries modify (Sig, X, Y) at a time, the parties who are communicating recognize the modification. The key agreement scheme is secure against passive insider adversaries and active/passive outsider adversaries. Outsider adversaries are malicious unauthorized nodes. Active insider adversaries are the most powerful attackers.

- **Eavesdropping:** In eavesdropping, passive adversaries listen in communication. The proposed scheme is secure against eavesdropping because public values in communication are ephemeral and important values, such as user's ID, are protected by encryption.
- **Impersonation:** In impersonation, insider or outsider adversaries masquerade as an authorized user and attempt to access network services. This problem becomes even more difficult to solve in fully self-organized MANETs, because it is hard to make a pair-wise secret key, which is used to hide network information and entities identities. Moreover, it is impossible to use a signature scheme before knowing the identity of another node. However by setting SCs and opening the identity of SCs, we can make pair-wise keys anonymously and authenticate nodes using signature securely. As a result, our scheme is secure against impersonation attacks.
- **Known-Key Security:** A compromised past session key or a subset of past session keys allows a passive adversary to compromise future session keys and allows an active adversary to impersonate other protocol participants. Our scheme is secure by using p_i because private keys are changed periodically. In addition, by using random values (x,y), each session has a unique session key, so it does not affect other session keys.
- **Perfect Forward Secrecy:** A compromise of long-term keys cannot result in compromise of past session keys. Our scheme is secure against perfect forward secrecy by using p_i, and random values (x,y) to update private keys periodically.

Table 2 compares our proposed schemes with other schemes. The proposed scheme and H. Y. Chien' s scheme support anonymity which makes it secure

표 2. 다른 아이디 기반 키 교환 프로토콜과 비교
Table 2. Comparisons among other schemes for ad hoc networks.

	Y. Zhang[16]	H .Y. Chien[9]	Chien-Lin[18]	Proposed Scheme
Private key update	○	X	X	○
Entity Anonymity	X	○	X	○
No. of flows in dynamic two party key agreement	○	3 runs	2 runs	3 runs
Cost of dynamic two party key agreement	X	$2T_P + T_M + T_S + 2T_{ENC}$ for one entity	$2T_P + T_M + T_S$ for one entity	$3T_P + T_M + T_S + 2T_{ENC}$ for one entity

(○ denotes the scheme consider the property; X denotes the scheme does not consider the property; T_E denotes the cost of one modular exponentiation; T_{ENC} denotes the cost of one symmetric encryption; T_P denotes that of one pairing operation; T_M denotes that of one modular multiplications; T_S denotes that of one scalar multiplication in G_1)

against disclosure of privacy information. Y. Zhang's scheme and our scheme provide private key updating; thus, these schemes limit any potential damage from compromised nodes. The main difference between Y. Zhang's scheme and the proposed scheme as regard private key updating is that Y. Zhang's scheme uses threshold technique so that each D-PKG (general nodes that work like PKG) has some load. We adapt SCs to reduce the computational burden on each node as much as possible.

V. Conclusions

The concerns for security in wireless environments are increasing rapidly as mobile devices are becoming more popular. Service-oriented MANETs are being quickly considered to pioneer new markets; however, there are urgent unresolved security problems. Private key updating is a challenging issue for secure MANETs, especially in dynamic topologies. It is important to hide participants' identities; therefore the design of a secure key update scheme and key agreement scheme with anonymity in service-oriented MANETs is required.

This paper proposed an ID-based private key update scheme and a key agreement scheme within domain with anonymity for SC-based MANETs. We also presented a method for rekeying between different domains. It could be usefully applied in dynamic MANETs such as the mobile marketplace, military battlefields and VANETs.

References

[1] Y. Fang, X. Zhu, and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," *IEEE Wireless Communications*, vol. 16, pp. 24-30, April 2007.

[2] M. Raya, and J. P. Hubaux, "The security of vehicular ad hoc networks", Proc. of the 3rd ACM workshop on Security of Ad Hoc and Sensor Networks, pp. 11-21, Nov. 2005.

[3] V. Varadharajan, R. Shankaran, and M. Hitchens, "Security for cluster based ad hoc networks," *Computer Communications*, vol. 27, pp. 488-501, 2004.

[4] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," Proc. of the 19th IEEE International Parallel Distributed Processing Symposium, Denver, 2005.

[5] B. Zhu, F. Bao, R. H. Deng, M. S. Kankanhalli, and G. Wang, "Efficient and robust key management for large mobile ad hoc networks," *Computer Networks*, vol. 48, pp. 657-682, 2005.

[6] A. Shamir, "Identity-based cryptosystems and signature schemes," CRYPTO 84, LNCS 196, pp. 47-53, Springer-Verlag, 1984.

[7] W. K. Koo, J. Y. Hwang, H. J. Kim, and D. H. Lee, "ID-Based proxy re-encryption scheme with chosen-ciphertext security," *Journal of IEEK*, vol. 46, no. 1, 2009.

[8] Y. Zhang, W. Liu, W. Lou, Y. Fang, and Y. Kwon, "AC-PKI: anonymous and certificateless public-key infrastructure for mobile ad hoc networks," Proc. IEEE International Conference on Communication, pp. 3515-3519, May 2005.

[9] H. Y. Chien, "ID-based key agreement with anonymity for ad hoc networks," EUC 2007, LNCS 4808, pp. 333-345, Springer-Verlag, 2007.

[10] Z. Wan, K. Ren, W. Lou, and B. Preneel, "Anonymous ID-based group key agreement for wireless networks," Wireless Communications and Networking Conference, pp. 2615-2620, 2008.

[11] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," Proc. of the 2003 Symposium on Applications and the Internet Workshop, pp. 342-346, Jan. 2003.

[12] C. K. Toh, G. Guichal, D. K. Kim, and Victor O. K. Li, "Service location protocols for mobile wireless ad hoc networks," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 2, pp. 250-262, 2006.

[13] Y. H. Park, Y. H. Park, and S. J. Moon, "ID-based private key update protocol with anonymity for mobile ad-hoc networks," Proc. of the 10th International Conference on Computational Science and Its Applications, pp. 323-326, March 2010.

[14] H. Y. Chien, "Practical anonymous user authentication scheme with security proof," Computers and Security, vol.27, pp. 216-223, 2008.

[15] 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.
[16] 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.
[17] M. Bohio and A. Miri, "Efficient identity-based security schemes for ad hoc network routing protocols," *Ad Hoc Networks*, vol. 2, pp. 309-317, 2004.
[18] H. Y. Chien, and R. Y. Lin, "Improved ID-based security framework for ad hoc network," *Ad Hoc Networks*, vol. 6, pp. 47-60. 2008.
[19] M. Omar, Y. Challal, and A. Bouabdallah, "Reliable and fully distributed trust model for mobile ad hoc networks," *Computers and Security*, vol. 28, pp. 199-214, 2009.
[20] D. Boneh, and M. Franklin, "Identity-based encryption from the weil pairing," CRYPTO 01, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.
[21] P. Barreto, H. Kim, B. Bynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," CRYPTO 02, LNCS 2442, pp. 354-368, Springer-Verlag, 2002.
[22] F. Hess, "Efficient identity based signature schemes based on pairings," SAC 2002, LNCS 2595, pp. 310-324, Springer-Verlag, 2003.

저 자 소 개

박 요 한(정회원)
2006년 경북대학교 전자전기 컴퓨터학부 학사
2008년 경북대학교 전자공학과 석사
2008년～현재 경북대학교 전자공학과 박사과정
<주관심분야 : 무선통신, 네트워크 보안, 모바일 컴퓨팅>

문 상 재(평생회원)
1972년 서울대학교 공업교육 (전자전공)과 학사
1974년 서울대학교 전자공학과 석사
1984년 미국 UCLA 전기공학과 박사
1984년～1985년 UCLA Postdoctor 근무
1984년～1985년 미국 OMNET 컨설턴트
1997년～1998년 경북대학교 전자전기공학부 학부장
1974년～현재 경북대학교 IT대학 전자공학과 교수
2000년～현재 경북대학교 이동네트워크 정보보호 기술 연구센터장
2002년～현재 한국정보보호학회 명예회장
<주관심분야 : 정보보호 디지털 통신, 이동 네트워크>

박 영 호(정회원)-교신저자
1989년 경북대학교 전자공학과 학사
1991년 경북대학교 전자공학과 석사
1995년 경북대학교 전자공학과 박사
1996년～2008년 상주대학교 전자전기공학부 교수
2003년～2004년 Oregon State University 방문 교수
2008년～현재 경북대학교 산업전자전기공학부 교수
<주관심분야 : 무선통신, 네트워크 보안, 모바일 컴퓨팅>