International Journal of Control and Automation
Vol. 8, No. 6 (2015), pp. 411-420
http://dx.doi.org/10.14257/ijca.2015.8.6.39

Freshness Preserving Secure Data Gathering Protocol over Wireless Sensor Networks

Hyunsung Kim[1] and Sung Woon Lee[2]

[1]Dept. of Cyber Security, Kyungil University
Kyungsan, Kyungbuk 712-701, Korea
[2](Corresponding Author) Dept. of Information Security, Tongmyong University
Busan 608-711, Korea
kim@kiu.ac.kr

Abstract

Wireless sensor networks (WSNs) are vulnerable to various forms of security attacks because they are deployed in potentially adverse or even hostile environment. Research into security and routing mechanism designs specifically focused on WSNs has been challenging issues to researchers. Recently, Choi et al. proposed a secure data gathering protocol over WSNs based on an extended Sakai et al.'s non-interactive identity-based key agreement scheme. However, their protocol could provide attacker information including traffic flow identification, traffic flow tracking, or disclosing application-level information due to lack of freshness. This paper proposes a freshness preserving secure data gathering protocol over WSNs to solve the problem in Choi et al.'s protocol. Thereby, the proposed protocol could efficiently cope from the information leakage problem from adversary and could provide secure multipath over WSNs.

Keywords: *Security, Wireless sensor network, Non-interactive key agreement, Freshness, Multipath routing*

1. Introduction

Wireless sensor networks (WSNs) have recently emerged as a promising computing model for various applications such as military target tracking and surveillance, natural disaster relief, biomedical health monitoring and hazardous environment sensing. WSN usually consists of a large number of low-cost, battery-powered sensor nodes that are of limited computation and communication capacity [1-2]. While these nodes are left unattended after deployment, they can adaptively form a routing graph and continuously collect data for events of interests and deliver the data to a designated destination. In a hierarchical WSN, a sensory data is periodically gathered in cluster head and then forwarded to the sink. This method to collect data makes WSNs very vulnerable to adversary's malicious attacks [1-4].

Research into security and routing mechanism designs specifically focused on WSNs has been challenging issues to researchers. Especially, packet encoding and key agreement issues in WSNs have been intensively researched to improve security in data collection [5-7]. Shamir in [5] proposed an algorithm to break a data packet into a few shares by using the (t, n)-threshold secret sharing scheme and then deliver shares via various routing paths. However, the algorithm has security problem if attacker could collect t data shares. The secret sharing and routing parameters in [6] are optimized to minimize the energy cost for a given packet delivery probability constraint. Yuxin *et al.*, in [7] proposed a feedback-based secure path approach based on Shamir's algorithm to establish multiple paths. The paths in Yuxin et al.'s approach are not always secure and furthermore, the approach shares the security problems in Shamir's algorithm.

For secure routing in WSNs, Shamir's algorithm was applied to various ad hoc on-demand multipath routing [8-9]. A non-interactive hierarchical key agreement protocol is proposed based on Bilinear Pairing by Sakai *et al.*, [10]. Choi *et al.*, proposed a secure data gathering protocol over WSNs based on an extended Sakai *et al.*'s non-interactive identity-based key agreement scheme, which is for hierarchical [11]. In Sakai *et al.*,'s scheme and Choi *et al.*,'s scheme, they do not provide key freshness. It means that the established session keys in different sessions are always the same, which could provide some means or useful information to attacker [12]. Thereby, attacker could get information including traffic flow identification, traffic flow tracking, or disclosing application-level information.

In order to solve problems in Sakai *et al.*,'s scheme and Choi *et al.*,'s scheme, this paper proposes a freshness preserving secure data gathering protocol over WSNs. The proposed protocol uses a new hierarchical non-interactive identity-based authenticated key agreement by enhancing freshness in each session. Thereby, the proposed protocol could efficiently solve the information leakage problems efficiently, which are traffic flow identification leakage, traffic flow tracking, and disclosing application-level information leakage.

2. Security Operations

This section introduces the security operation backgrounds used in this paper. We give basic definition and properties of bilinear pairings and Sakai *et al.*,'s non-interactive identity-based key agreement protocol in [10-11, 13].

2.1. Bilinear Map and Security Assumption

The admissible bilinear map $\hat{e}$ is defined over two groups of the same prime order p denoted by G and G_T in which the computational Diffie-Hellman (CDH) problem is hard. The following definition 1 gives a more formal definition [13].

Definition 1: Let G is an additive group of prime order q and G_T a multiplicative group of the same order. Let P denote a generator of G. An admissible pairing is a bilinear map $\hat{e} : G \times G \rightarrow G_T$ which has the following properties:

- Bilinearity: given $Q, R \in G$ and $a, b \in Z_q^*$, we have $\hat{e}(aQ, bR) = \hat{e}(Q, R)^{ab}$
- Non-degeneration: $\hat{e}(P, P) \neq 1_{G_T}$
- Computability: $\hat{e}$ is efficiently computable

G is a subgroup of the group of points on an elliptic curve over a finite field. G_{T} is a subgroup of a multiplicative group of a related finite field. Throughout this paper, we will simply use the term "bilinear map" to refer to the admissible bilinear map.

2.2. Non-interactive Identity-based Key Agreement

Sakai *et al.*, proposed a non-interactive (but not hierarchical) identity-based key agreement scheme [10]. In Sakai *et al.*,'s scheme, the central authority firstly chooses two cyclic groups G and G_T and the bilinear map $\hat{e} : G \times G \rightarrow G_T$ to setup the parameters for an identity-based public key system. Moreover, it chooses a cryptographic hash function $H : \{0,1\}^* \rightarrow G$. It then chooses a secret key $s \in Z_q$ and generates the secret key $S_{ID}=sH(ID) \in G$ for a node with identity ID.

Suppose two nodes with identities ID_1 and ID_2 want to establish a shared secret key. The shared key between them is $K=\hat{e}(H(ID_1), H(ID_2))^s \in G_T$, which party ID_1 computes as $K=\hat{e}(S_{ID_1},H(ID_2))$ and ID_2 computes as $K=\hat{e}(H(ID_1), S_{ID_2})$. The security of this scheme can be reduced to the decisional bilinear Diffie-Hellman (DBDH) assumption in the random-oracle model.

Choi *et al.*, proposed a secure data gathering protocol over WSNs based on an extended Sakai *et al.*,'s non-interactive identity-based key agreement scheme, which is for hierarchical [11]. It means that Choi *et al.*,'s key agreement scheme is a hierarchical version on Sakai *et al.*,'s scheme.

In both of Sakai *et al.*,'s scheme and Choi *et al.*,'s scheme, each party computes a session key, *sk* between any two entities in a WSN, which depends on both of their own private key and identity tuples but not on the session dependent random value. Thereby, they do not provide key freshness. No freshness support means that the established session keys in different sessions are always the same, which could provide some means or useful information to attacker [12]. One of serious effects is traffic analysis attack, which is focused on traffic flow identification, traffic flow tracking, or disclosing application-level information.

3. Freshness Preserving Secure Data Gathering Protocol

This section proposes a freshness preserving secure data gathering protocol over WSNs based on non-interactive hierarchical key agreement scheme, symmetric key encryption scheme and (t, n) threshold scheme. The proposed protocol is composed of three phases including hierarchical key settlement, secure path construction and data gathering. We will more focused on the secure path construction and the data gathering because the hierarchical key settlement is the same as Choi *et al.*,'s protocol in [11] but needs to be recalled for better understanding of the protocol. For the simplicity of the protocol description, we assume the data aggregation scenario, which requires communications only from cluster head to sink or the other cluster heads. Notations used in this paper are listed in Table 1.

Table 1. Notations

Symbol	Description
ID_i	Identities of entity i
$\{S_1, S_2, S_3\}$	Set of private key for sink node, $S_i \in Z_q^*$
$h(.)$	One way hash function $h : \{0, 1\}^* \rightarrow Z_q$
$\cdot$	Multiplication operation
G	Additive group of prime order q
G_T	Multiplicative group of prime order q
$\hat{e}$	Bilinear map $\hat{e} : G \times G \rightarrow G_T$
P_i	Amplified identities by applying $h(ID_i)$
r	Random number for a session
sk	Session key established between two entities
L_R	Path's set of identities
C	Path's credential level
α	Permitted transmission delay

3.1. Hierarchical Key Settlement

This phase is to settle hierarchical secret keys as shown in Figure. 1 used to establish credential between entities, which uses the pre-established secret key method. This phase is a very important for the non-interactive key agreement, which will use the same as Choi et al.'s scheme in [11].

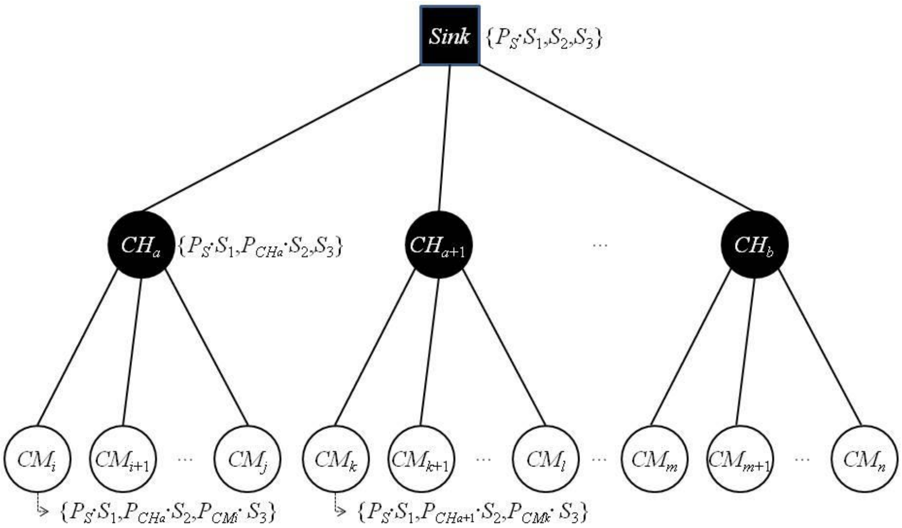

Figure 1. Hierarchical Key Settlement [11]

This phase uses an identity of each node ID_i for the public key, which is based on the identity-based cryptosystem. Sink is responsible for distributing a secret key to each participant of the WSN. As Choi et al.'s protocol in [11], this paper has the same assumption that each entity plays a different role in a network; sink has more abilities, cluster heads have neutral abilities and sensor nodes have least abilities. The privilege of each entity is determined with the degree of how many elements does the entity have from the private key set of the sink. To set up keys, the following operations are necessary.

Step 1. The sink with identity ID_S creates a private key set, $\{S_1, S_2, S_3\} \in Z_q^*$, for a WSN and computes $P_S=h(ID_S)$ and $P_S \cdot S_1$, where $h(\cdot)$ is a secure one-way hash function. After that, sink stores the information in memory and sends $\{\{P_S \cdot S_1, S_2, S_3\}, P_S\}$ to cluster heads.

Step 2. When a cluster head with identities ID_{CH} receives the message, it computes $P_{CH}=h(ID_{CH})$ and $P_{CH} \cdot S_2$. After that, it stores the information in memory and sends $\{\{P_S \cdot S_1, P_{CH} \cdot S_2, S_3\}, P_S, P_{CH}\}$ to member nodes in the cluster.

Step 3. When a member node with identities ID_{CM} receives the message, it computes $P_{CM}=h(ID_{CM})$ and $P_{CM} \cdot S_3$ and then stores the computed results in memory.

3.2. Secure Path Construction

The goal of this phase is to establish multiple secure paths between source nodes and sink by establishing a fresh session key using the settled keys from the hierarchical key settlement, which uses fresh random number, encryption/decryption, MAC and (t, n) threshold mechanism. It operates to as follows:

Step 1. When a cluster head CH_j intends to send a data share by using the (t, n) threshold mechanism to the sink, CH_j sends an encrypted data packet with it's identity set $\{P_S', P_{CHj}'\}$, a session dependent value R_1 and the message authentication code MAC_1 to the sink. The data is encrypted by using a fresh session key sk_1, which is computed as $sk_1=\hat{e}(P_S \cdot S_1, P_S') \cdot \hat{e}(P_{CHj} \cdot S_2, P_S') \cdot \hat{e}(R_1, P_S')^{S_3}$ with it's own identity set $\{P_S', P_{CHj}', P_{CMk}'\}$ after selecting a session fresh random number r_1 and computing

R_1=r_1·P_{CHj}. CH_j breaks the data into n shares according to the (t, n)-threshold algorithm, computes MAC_1=h(sk_1||the data share) for each share, and forwards them to the neighbor cluster heads after it adds its identity CH_j to L_R, where L_R keeps an identity set of routing path initialized with an empty.

Step 2. When a cluster head CH_m receives a share, it adds its identity CH_m to L_R. The share of data is forwarded by a collection of relay heads until it reaches sink.

Step 3. On the arrival of the share, sink decrypts the share by establishing $sk_1=\hat{e}(P_S, P_S')^{S_1}\cdot\hat{e}(P_S, P_{CHj}')^{S_2}\cdot\hat{e}(P_S, R_1)^{S_3}$ with the source node using it's private key set and the received identity set $\{P_S', P_{CHj}'\}$. When sink successfully finishes the check of MAC_1, it extracts L_R={ CH_j, CH_m, …, CH_z } from the share and stores it in its local database. Here, L_R is called a secure path.

Step 4. Sink adds the secure path L_R to a notification packet and sends the packet, R_2 and MAC_2 with the trust value C to the source node by using the route in L_R. R_2 and MAC_2 are computed as $R_2=r_2\cdot P_{CHj}'$ with a session fresh random number r_2 and $MAC_2=h(sk_2||L_R||C)$ where sk_2 is computed as $sk_2=\hat{e}(P_S, P_S')^{S_1}\cdot\hat{e}(P_S, P_{CHj}')^{S_2}\cdot\hat{e}(P_S, R_2)^{S_3}$. C is used as a counter with an initial value t (t>0), which represents credibility level of the route. The notification packet contains the secure path for data collection and the credibility of the path, C.

Step 5. When a cluster head CH_o receives the packet, it extracts a sub-path P_o={ CH_{o+1}, CH_{o+2}, …, CH_n } from L_R and stores it into its local cache only if it's identity is within L_R. CH_o extracts its next-hop cluster head CH_{o-1} from L_R and forwards the packet to the cluster head.

Step 6. When the cluster head CH_j receives the packet, it extracts L_R from the packet, and verifies MAC_2 by establishing the session key $sk_2=\hat{e}(P_S\cdot S_1, P_S')\cdot\hat{e}(P_{CHj}\cdot S_2, P_S')\cdot\hat{e}(R_2, P_S')^{S_3}$. It stores L_R and C in its local cache only if the verification of MAC_2 is successful.

The proposed secure path construction uses a freshness preserving session key for the confidentiality, which does not need any additional communication for the session key set up with the counterpart node. It is very important aspect in WSNs due to their limitations.

3.3. Data Gathering

This phase is for data gathering based on the multi-path L_R with C established from the secure path construction. Each cluster head keeps the secure paths information in their local database and selects a path with the highest value from C among multiple secure paths. When a cluster head wants to send a packet to a destination node, it first breaks the packet into m shares according to the (t, n) threshold mechanism. Each share is then encrypted and transmitted to the neighbor from the multi-path. The overall steps for setting up the data gathering are as follows.

Step 1. When a cluster head CH_j intends to send a data share by using the (t, n) threshold mechanism to the sink, CH_j needs to generate a new freshness preserving session key sk_3 with r_3, encrypts the aggregated data with the session key, attaches MAC_3 of the encrypted data with the session key, and sends the encrypted data, R_3 and MAC_3 with the identity set related information to the sink. To perform this, they perform the following sequences. CH_j generates a session key $sk_3=\hat{e}(P_S\cdot S_1, P_S')\cdot\hat{e}(P_{CHj}\cdot S_2,$

$P_S')\cdot\hat{e}(R_3, P_S')^{S_3}$, where $\{P_S, P_{CHj}\}$ is it's own identity set after selecting a session fresh random number r_3 and computing R_3=r_3·P_{CHj} and computes MAC_3=h(sk_3||the data share) for each share.

Step 2. When CH_j intends to send the message to the sink, it first checks its local cache. If there are secure paths, it selects a secure path P=<CH_j, L_R, C> with the largest value C from its local data repository. CH_j attaches L_R={CH_m, CH_{m+1}, …, CH_z} to the head of the data share. If there are no secure paths in the local cache of the relay nodes, it just performs the secure path construction.

Step 3. When a cluster head CH_i receives the share, it first checks if the cluster head CH_{i+1} in L_R is in its neighbor list. If the cluster head is not in the list, it just performs random multipath routing and path construction. Otherwise, it sends the share to the cluster head CH_{i+1} in L_R.

Step 4. On the arrival of the share to the sink successfully, the sink generates a session key sk_3 with CH_j using the included identity set in the message. It generates $sk_3=\hat{e}(P_S, P_S')^{S_1}\cdot\hat{e}(P_S, P_{CHj}')^{S_2}\cdot\hat{e}(P_S, R_3)^{S_3}$ by using the identity set {P_S', P_{CHj}'} from CH_j. After that, the sink validates MAC_3 of each share, decrypts the message and extracts L_R={CH_j , CH_m, CH_{m+1}, …, CH_z} only if the validation is successful. If there is a secure path in the share, it means every relay cluster heads have used the path and the sink just sends back an empty notification to CH_j. Otherwise, the sink extracts the identity set as a new secure path from the share, updates its local database, and sends back a notification with the newly-constructed secure path to CH_j. The relay cluster heads on the path update their local cache with the sub-paths. On the arrival of the notification, CH_j extracts a new secure path from the packet, and stores it in its local cache. If the share is dropped or does not reach to the sink within the allowed time span, CH_j does not receive a notification from the sink, and then it just decreases the credential counter C by 1 of the path. If the counter of a secure path is cleared, each node will remove it from its local cache.

The data gathering phase performs differently based on the application whether it requires data aggregation or not. If the application does not require data aggregation, CM_k establishes a session key sk with the sink and use the key to support confidentiality and integrity of data. Otherwise, CH_j needs to establish secure channel with the sink using a new session key sk.

4. Analysis

This section provides security analysis and performance analysis by comparing properties between Choi et al.'s protocol and the proposed protocol.

4.1. Security Analysis

Our security analysis is focused on verifying the overall security requirements for the proposed protocol including passive and active attacks as follows.

If we consider *the confidentiality of the private key set*, the key set is combinations of the amplified identity and secret value. This indicates that the attacker has to know both of them to know the private key set. However, there are no ways that the attacker can derive the secret value or the amplified identity from the private key set even if the attacker is registered to the sink. Also, in order to obtain the session key sk, the attacker must try to derive sk from any intercepted messages { R_i, MAC_i } and {an encrypted data packet, identity set, MAC_i}. However, there are no ways that the attacker can derive the shared key due to the DBDH problem even if the attacker is registered entity.

The fresh nonce used in the session key agreement and secure communication phase guarantees *the freshness of the session keys*. To achieve freshness, session initiator uses a nonce r_i along with MAC_i to generate session key sk_i. There are no ways that the attacker can generate session key due to the DBDH problem even if the attacker is registered entity. Furthermore, the proposed protocol is strong against the replay attack due to the session key freshness.

An adversary *cannot impersonate* the sink to cheat CH_i. As described before, only the legal sink can form the legal messages by including the proper integrity code, which needs to be properly matched with the information from CH_i in the protocol steps. Even if the attacker could pass the verifications at the protocol steps, the attacker still cannot get any useful information from the encrypted messages due to the difficulty of the underlying DBDH problem and cannot generate the consequent valid messages.

Table 2 provides security comparisons between the proposed protocol and Choi *et al.*,'s in [11].

Table 2. Security Comparisons

Properties	Choi et al. [11]	Proposed
Confidentiality	Support	Support
Integrity	Support	Support
Privacy	Partially support	Partially support
Colluding attack	Secure	Secure
Freshness	Not support	Support

4.2. Performance Analysis

For the simplicity of performance analysis and comparison, we follow notations from [11].

- TG_e : the time of executing a bilinear map operation
- TG_{mul} : the time of executing a scalar multiplication operation of point
- T_{hash} : the time of executing a hash function
- $TS_{e/d}$: the time of executing a symmetric encryption or decryption
- T_{th} : the time of executing a (t, n) threshold mechanism

Table 3 demonstrates the security comparisons between the proposed protocol and Choi *et al.*,'s in [11] in terms of security operation requirements. We can conclude the proposed protocol supports better security than Choi *et al.*,'s protocol but requires similar operation overheads due to the security reasons.

Table 3. Performance Comparisons

Properties	Choi et al. [11]	Proposed
Security computational cost (head)	$6TG_e+5TG_{mul}+mTS_{e/d}+(m+2)T_{hash}$	$6TG_e+6TG_{mul}+mTS_{e/d}+(m+3)T_{hash}$
Security computational cost (sink)	$6TG_e+5TG_{mul}+mTS_{e/d}+(m+2)T_{hash}+T_{th}$	$6TG_e+6TG_{mul}+mTS_{e/d}+(m+3)T_{hash}+T_{th}$

5. Conclusion

The focus on this paper was for the research focused on security and multipath ad hoc routing mechanism on WSNs. Recently, Choi *et al.*, proposed a secure data gathering protocol over WSNs based on an extended Sakai et al.'s non-interactive identity-based key agreement scheme. However, their protocol was weak against information leakage attack including traffic flow identification, traffic flow tracking, or disclosing application-level information due to lack of freshness. Thereby, this paper has been proposed a freshness preserving secure data gathering protocol over

WSNs to solve the problem in Choi *et al.*,'s protocol. The proposed protocol could efficiently cope from the information leakage problem from adversary and could provide secure multipath over WSNs.

Acknowledgements

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2010-0021575) and also was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2011-0008890).

References

[1] G. Mao, B. Fidan, B. Anderson, Wireless sensor network location techniques Computer Networks, The International Journal of Computer and Telecommunications Networking, 29 **(2007)**, pp.2529-2553.

[2] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Computer Networks, 52 **(2008)**, pp. 2292–2330.

[3] A. Hadjidg, M. Souil, A. Bouabdallah, Y. Challal, H. Owen, Wireless sensor networks for rehabilitation applications: Challenges and opportunities, Journal of Network and Computer Applications, 36 **(2013)**, pp. 1-15.

[4] S. M. Zin, N. B. Anuar, M. L. M. Kiah, A. K. Pathan, Routing protocol design for secure WSN: review and open research issues, Journal of Network and Computer Applications, 41 **(2014)**, pp. 517-530.

[5] A. Shamir, How to share a secret, Comm. ACM, 22 **(1979)**, pp. 612-613.

[6] T. Shu, S. Liu, M. KrunzSecure, Data collection in wireless sensor networks using randomized dispersive routes, Proc. of IEEE INFOCOM 2009, **(2009)**, pp. 2846-2850.

[7] M. Yuxin, W. Guiyi, A Feedback-based Multipath Approach for Secure Data Collection in Wireless Sensor Networks, Sensors, 10,10 **(2010)**, pp. 9529-9540.

[8] K. M. Mahesh, R. D. Samir, Ad hoc on-demand multipath distance vector routing, ACM SIGMOBILE Mobile Comput. Commun. Rev, 6, 3 **(2002)**, pp. 92-93.

[9] S. J. Lee, M. Gerla, Split multipath routing with maximally disjoint paths in Ad hoc networks, Proc. of ICC 2001, **(2001)**, pp. 3201-3205.

[10] R. Sakai, K. Ohgishi, M. Kasahara, Cryptosystems based on pairings, Proc. of Symposium on Cryptography and Information Security 2000, (**2000**).

[11] H. W. Choi, M. C. Ryoo, C. S. Lee, H. Kim, Secure data gathering protocol over wireless sensor network, The Journal of Digital Policy & Management, 11, 12 **(2013)**, pp. 367-280.

[12] H. Kim, Privacy Preserving Security Framework for Cognitive Radio Networks, IETE Technical Review, 30, 2 **(2013)**, pp. 17-24.

[13] D. Boneh, M. Franklin, Identity based encryption from the Weil pairing, Lecture Notes in Computer Science, 2139 **(2001)**, pp. 213-229

Authors

Hyunsung Kim is a full professor at the Department of Cyber Security, Kyungil University, Korea from 2012. He received the M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.

Sung Woon Lee is a professor at the Department of Information Security, Tongmyong University, Korea. He received the B.S. and M.S. degrees in Computer Science from Chonnam National University, Korea in 1994 and 1996, respectively, and the Ph.D. degree in Computer Engineering from Kyungpook National University, Korea, in 2005. He was with the Korea Information System as a researcher, Korea, from 1996 to 2000. His research interests include cryptography, network security, and security protocol.