An Enhanced Light-weight Anonymous Authentication and Encryption Protocol in Wireless Sensor Network

Jeong-Hyo Park[1,*], Yong-Hoon Jung[2], Kwang-Hyung Lee[2], Keun-Wang Lee[3] and Moon-Seog Jun[1]

[1]*Department of Computer Science, Soongsil University, Korea*
{helios914, mjun}@ssu.ac.kr

[2]*Department of Internet Information, Seoil University, Korea*
{jyh0178, dreamace}@seoil.ac.kr

[3]*Department of Multimedia Science, Chungwoon University, Korea*
{kwlee}@chungwoon.ac.kr

Abstract

Until now, the interests of the research about sensor network security have been focused on the security services that provide authentication, confidentiality, integrity, and availability. However, the interest in the issue of actual identifier's exposure of sensor node is rapidly increasing. Also, the interest in the efficiency of creating encryption key that is used for the sensor network is increasing. Many schemes for providing node's anonymity in the existing Ad-Hoc network were suggested, but these schemes are not appropriate for sensor network that is energy-limited, so a scheme for providing anonymity that is suitable for sensor network's characteristics is required. Also, Sensor network maintains high limitation of resource because it performs many communications in order to create encryption keys. To solve these problems, this research suggests LA^{2}EP Protocol. LA^{2}EP Protocol can minimize resource and provide a new scheme for authentication and encryption that can provide anonymity of node for safe communication. To analyze the performance of the suggested protocols, a degree of anonymity that is provided by the scheme suggested by using an Entropy-based modeling was measured. As a result, when the suggested scheme was used, the degree of anonymity of sensor node was high. It showed that an important element to increase the degree of anonymity was to let the sensor's ID not known correctly. Also, as a result of calculating spaces for operation, communication, and storage while considering the characteristic of sensor network, which is limited in resource, it showed suitability for sensor network environment.

Keywords: *Sensor Network; high limitation of resource; LA^{2}EP Protocol; Anonymous Authentication; Optimized Encryption; Entropy-based Modeling*

1. Introduction

Since the sensor network technology fundamentally has a wireless communication infra and high limitation of resource (e.g. low computing capability, limited capability for electric power supply, and realization of low cost), security vulnerability is considerably higher than the capability of the general existing network. Also, the facts that sensor can get exposed to the outside environment and receive physical attacks and that a man with bad purpose can plant a malicious code to make it malfunction; that it

has a problem of exposure of transmission signal that wireless communication has; that sensor network to which popularization of sensor-related equipment and environmental particularity of getting installed outside are sometimes added has to use limited energy due to the limited computing capability; and that the organization of network is atypical and sensors can easily join, leave and reorganize the network can be problems.

Therefore, a method of security that is specialized for sensor network, not the one that is used in the perspective of the existing network, is studied. However, the research on the existing sensor network security has been focused on the security services that provide authentication, confidentiality, integrity, and availability. Recently, the interest in the problem of guaranteeing the anonymity of node in wireless sensor network is rising. In case when sensor node uses real ID, instead of a false name for message in the middle of communication, attacker can snatch the network traffic and easily analyze the traffic or easily learn not only the identifier of the sending sensor node that communicates with the base station, but also the move of the sensor's location. Therefore, it is very important to make the moving sensor node not to let the transmitter that exchanges data and the third party besides the receiver to easily distinguish the identifier of the sender receiver in the middle of communication in the environment of doing the daily surveillance or tracking certain object. Also, in case when monitoring some important asset, since the information acquired through sensor's monitoring should not be exposed to the third party, a security device such as encryption will be used to protect the information. However, one point to pay attention here is that though information about the environment or asset itself that senor monitor is important, the source that transmitted the information can be also important. Therefore, an additional device for preventing exposure of source that is right for the characteristics of sensor network is required besides protecting information through encryption.

This thesis is organized like the following. In Chapter Two, it explains the problems of authentication and key distribution in the existing sensor network, and in Chapter Three, it proposes LA^{2}EP Protocol that provides authentication and encryption to provide safe communication in the next generation sensor network environment. In Chapter Four, it analyzes LA^{2}EP Protocol qualitatively and quantitatively, and at last, in Chapter Five, it gives conclusion of this thesis.

2. Related Works

2.1. The Research Related to the Existing Anonymity Authentication Scheme

A privacy problem in wireless sensor network is the naming of nodes and base stations. In particular, we have in mind the problem of identity hiding in the local single-hop communication. Previously described schemes do not address this problem in its full scope. Although some of them have the need to somehow identify the sender or the receiver, no satisfactory solution providing anonymity is proposed. Using the node real ID in this context may be considered as a vulnerable, because an adversary is able to identify individual nodes. A naive solution is to use a key shared with the recipient and hide the IDs by encryption. Nevertheless, in the worst case, the recipient has to perform decryption with the keys shared with each other neighbor, in order to find out whether the message is addressed to her or not. This approach may be computationally expensive and may introduce significant delays. So a better solution is to use some kind of pseudonyms that are transmitted in a plaintext header of the message and help to identify the sender and/or the receiver. However, fixed

pseudonyms provide as little anonymity as the real IDs. Therefore dynamically changing pseudonyms should be adopted to provide the node anonymity.

Table 1. An Example of Simple Anonymity Scheme

Index	U's range	Neighbor's range	Neighbor's Beacon Range	Neighbor's Index	Shared Key
$Index_u$	$ID_{uv1} - ID_{uv2}$	$ID_{vu1} - ID_{vu2}$	$ID_{bv1} - ID_{bv2}$	$Index_v$	K_{uv}
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.

The problem of hiding the identity of nodes and the base station in wireless sensor network was first addressed by Misra and Xue. As shown in the above Table 1, they have proposed the Simple Anonymity Scheme (SAS) that utilizes a contiguous range of pseudonyms to conceal the real node identity. Each node is pre-assigned with a certain number of non-overlapping pseudonym ranges. After the deployment, in the set-up phase, the node associates each pseudonym range with one of its neighbors. Each two neighboring nodes then exchange information on mutually assigned pseudonym ranges. Afterwards, if the node wants to send a message to its neighbor, it uses random pseudonyms from the appropriate pseudonym ranges in place of the sender and the receiver ID.

Table 2. An example of Cryptographic Anonymity Scheme

Index	Mutual Exchange		Neighbor's Cluster Exchange			Neighbor's Cluster Key	Neighbor's Hash Key	Shared Key	Shared Hash Key	Neighbor's Index
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
$Index_u$	a_{uv}	seq_{uv}	a_{cv}	b_{cv}	seq_{cv}	$k`_{cv}$	k_{cv}	$K`_{uv}$	k_{uv}	$Index_v$
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.

As shown in the above Table 2, Misra and Xue have proposed also another anonymity scheme called the Cryptographic Anonymity Scheme (CAS). In this scheme, the pseudonyms are generated on per-message basis using keyed hash function H_K and are computed as Pseudonym = $H_{Kuv}(x_{uv} \oplus seq_{uv})$ where H_{Kuv} is the key shared between communicating nodes u and v, x_{uv} is a random seed shared between u and v, seq_{uv} is a message sequence number and $\oplus$ denotes exclusive-or operation. When compared to the SAS, the CAS is more computationally expensive in exchange for the memory efficiency.

Table 3. Hashing-based ID Randomization

Hash times (HT)	Hash values (HV)	Link
1	$H_{K\ AB}(ID_A)$	down
2	$H_{K\ AC}(ID_A)$	down
4	$H_{K\ AD}(ID_A)$	down
2	$H_{K\ AE}(ID_E)$	down

As shown in the above Table 3, Ouyang et al. have proposed the Hashing based ID Randomization (HIR) scheme to replace the real node ID. Similarly to the CAS, it utilizes the keyed hash function. However, unlike the CAS where the sequence number is used to change the resulting pseudonym message by message, in the HIR, a new pseudonym is obtained by hashing the previous one, creating a keyed hash chain. The advantage over the 12 CAS arises when the node is compromised. If the HIR is used, it is more difficult for the adversary to reveal the old pseudonyms used. The HIR can be also modified to limit the possibility of an attacker to impersonate the node when the keys are compromised. In this case, the hash chain is pre-generated and used in the reverse order. Nonetheless, when the reverse hash chain is used, each node has only limited number of pseudonyms available.

2.2. The Research Related to the Existing Key Distribution Scheme

As shown in the above table3, Ouyang et al. have proposed the Hashing based ID Randomization (HIR) scheme to replace the real node ID. Similarly to the CAS, it utilizes the keyed hash function. However, unlike the CAS where the sequence number is used to change the resulting pseudonym message by message, in the HIR, a new pseudonym is obtained by hashing the previous one, creating a keyed hash chain. The advantage over the 12 CAS arises when the node is compromised. If the HIR is used, it is more difficult for the adversary to reveal the old pseudonyms used. The HIR can be also modified to limit the possibility of an attacker to impersonate the node when the keys are compromised. In this case, the hash chain is pre-generated and used in the reverse order. Nonetheless, when the reverse hash chain is used, each node has only limited number of pseudonyms available. Due to the limited resource capability of sensor node, it is difficult to apply the scheme of key management such as PKI. That is why currently, SPINS Protocol is used, and there are the researches in progress on schemes of key management that are suitable for sensor network such as Key infection, Network-wide shared Key, Base station-node pairwise key, Random key distribution, and Random Pairwise key.

Local encryption and authentication protocol LEAP, suggested by Sencun Zhu, Sanjeev Setia, and Sushil Jajodia in 2003, is a key protocol for sensor network that provides processing. LEAP is in the master key-based method, and it is suggested to decrease the damage of exposing the neighboring sensor node when information of some sensor node is exposed for the same period of time. This scheme creates shared key with the neighboring sensor node by using node identifier and then removes the master key. Then even if the information of node is exposed, the shared key with the

neighboring sensor node can be not exposed to the attacker. However, the LEAP scheme loads private key and group key before sensor node is placed. That is why a malicious attacker can obtain the information of sensor node. If here the sensor node is seized before the process of initialization is completed, then this malicious attacker will acquire all the saved information in the sensor node within one minute. Then the attacker can create all the keys that are used in the sensor network.

Security Protocols for Sensor Networks SPINS is an authentication mechanism that is initially suggested by A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar for sensor network security. It is the method of exchanging keys with the neighboring sensor node that can communicate through a trustable base station. SPINS, which is an assembly of security protocol for sensor network environment, is consisted of SNEP and µTESLA. SNEP is a symmetric key encryption protocol for providing data confidentiality in communication between nodes. And it provides not only data confidentiality, but also integrity and data authentication by using nonce value and MAC. And it provides security and freshness for end-to-end communication and guarantees semantic secureness. The µTESLA is a light-weighted version of EMSS and TESLA Protocol, which are the previous research results of Professor A. Perrig, and it provides authentication for data that gests broadcasted. In other words, it is a message authentication protocol using symmetric key. µTESLA uses one-way key chain scheme that is created by one-way function. So it creates asymmetric key like public key with secret key encryption through delayed exposure of authentication key based on synchronized clock. Each node communicates with the base station for key exchange. That is why rapid energy consumption of nodes around the base station occurs. Consequently, it can become an inefficient method in the environment of large-scale sensor network. SPINS does not provide a way to restore from a threat when information leaks out or receives physical threats; in other words, it does not provide node's termination, addition and key renewal. This scheme's key creation is simple, so when the master key leaks out, the other keys used for communication can be easily exposed. The µTESLA needs all the sensor nodes to be synchronized timely. Also, since delay in transmission to network can occur, it needs time to delay key exposure and space for storage for packet.

3. Assumptions and Design Goals

LA^2EP Protocol is the one that provides authentication and encryption to provide safe communication in the next generation sensor network environment. Also, it was designed while considering the point that security vulnerability is weak because of the reasons such as high limitation of resource of sensor network, low computing capability, limited capability for electric power supply, and realization of low cost. LA^2EP Protocol has assumption details and purpose like the following.

3.1. Network and Assumptions

In order to prevent things like loss and theft of sensor network device and unauthenticated access point, authentication is necessary. Authentication is the most basic way to act against the means of attack from outside that tries to participate in the network without permission. Since the connection of sensor network is temporary and not continuous, unlike the existing network, a case when legitimate node authenticates illegitimate node due to uncertainty of the connection can occur. Therefore, a research

on authentication scheme to prevent this is necessary. Also, the very first thing to consider for composing key in sensor network is the problem of setting encrypted key. This key is used to exchange information between sensor nodes or to protect the exchanged information. For authentication and key management, the following assumption is made. It is not limited only to LA2EP in this thesis, but it is used in many general encryption protocols.

- Attacker can wiretap all the messages that are exchanged through key.
- Attacker can interrupt the process of key. Especially, he can change, insert, and block messages, and he can also convey them to other destination.
- Attacker can be a user who normally participates in key, or the third party.
- Old session key can be exposed to attackers.

3.2. Design Goals

Sensor must have encryption algorithm in order to perform security functions of sensor network. Here, since sensor nodes have highly limited resource such as memory, communication, operation, and power, memory should be used as small as possible so that it fits the limitation of resource of sensor network, and encryption algorithm with small amount of calculation should be applied. The most important resource in sensor node is energy; therefore, power consumption should be decreased as much as possible to increase the life of sensor node. Power consumption is determined by the amount of operation and that of communication, so it is one of the details to be considered primarily when selecting encryption algorithm. Therefore, encryption algorithm is necessary that can let it stay in the sleep mode for the most of the time and that can decrease the amount of operation or that of communication as much as possible even in the execution mode. Also, anonymity authentication of sensor node should not let the moving sensor node to allow the sending node that exchanges data and the third party besides the receiving node to easily distinguish the identifier of the sender-receiver in the middle of communication in the environment of doing the daily surveillance or tracking certain object.

4. Proposed Protocol

Unlike the existing network, where several ten thousands of computers are connected to each other, sensor network is a vulnerable side in security due to the reasons such as the environment exposed to dangers, dynamic network topology, weakness in wireless communication, risk of node's capture, and limited resource. Therefore, in the wireless sensor network environment, there is difficulty in applying the security policies that were applied to the existing network as they were. Thus, in this passage, this paper proposes an enhanced LA^2EP Protocol that is designed based on the required details in information protection of sensor network.

4.1. Overview and Notation

An enhanced LA^2EP Protocol provides light-weight anonymity authentication and optimized encryption key distribution in order to provide safe communication in the next generation sensor network environment.

Figure 1. Sensor Network Configuration in a Cluster Environment

The node's anonymity authentication scheme makes the moving sensor node not to allow the sending node that exchanges data and the third party besides the receiving node to easily distinguish the identifier of the sender-receiver in the middle of communication in the environment of doing the daily surveillance or tracking certain object. An enhanced LA^2EP Protocol's optimized encryption key distribution scheme was designed while considering the point that security vulnerability is weak because of the reasons such as high limitation of resource, low computing capability, limited capability for electric power supply, and realization of low cost.

Notation This follow Table 4 shows a notation and description.

Table 4. Notation used in an Enhanced LA2EP Protocol

Notation	Description
$H(ID_A)$	the index value that is agreed with the base station not to expose the actual sensor node A's identifier
N_A	the material to create anonymous identifier, which is created by sensor node A
$N_{A`}$	the material for key for creation of optimized encryption key, which is created by sensor node A
$H(ID_{BS})$	the index value, provided not to expose the identifier of the actual base station
N_{BS}	the material to create anonymous identifier, which is created by the base station
$N_{BS`}$	the material for key for creation of light-weighted encryption key, which is created by the base station
K_M	the master key that is used in the same cluster sensor network
K_A	the node A's secret key that has been saved when sensor node was distributed
PID	the anonymous identifier used in same cluster sensor network

4.2. Light-weighted Anonymous Authentication Protocol

In case when using the sensor's actual ID instead of using a false name for message that is in the middle of communication in the sensor network, a malicious attacker can snatch the network traffic and easily analyze the traffic or easily learn not only the identifier of the transmission sensor that communicates with the base station, but also the move of the sensor's location. Therefore, this research suggests an enhanced LA^2EP Protocol that makes the moving sensor node not to allow the sending node that exchanges data and the third party besides the receiving node to easily distinguish the identifier of the sender-receiver in the middle of communication in the environment of doing the daily surveillance or tracking certain object. To guarantee the authentication in sensor network environment, the required details like the two-way authentication between nodes, regular change of key, key exchange scheme between wireless sections, and node authentication that can be used regardless of device are applied. Also, when performing safe mutual authentication in a way of encryption, simultaneously with authentication, a scheme that can create safe key for the security of link level is applied. LA^2EP Protocol's light-weight anonymity authentication scheme is created by communication between sensor node A and the base station. Here, even if a malicious attacker snatches the content of the message in the middle of communication and then attempts traffic analysis, he cannot conjecture the actual identifier of sensor node A. To create a phantom ID that used in same sensor network temporarily, sensor node A performs the process like the following picture Figure 2.

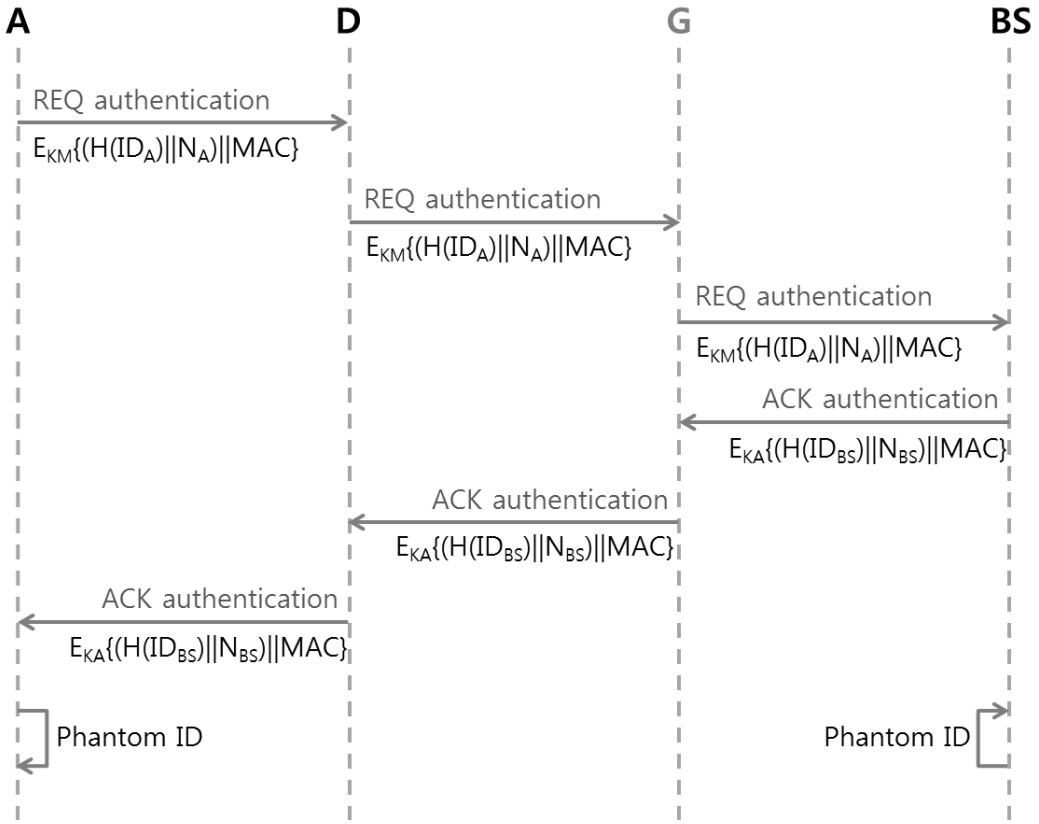

Figure 2. The Phantom Identification Agreement between Node A and the Base Station

Step 1 (A)

Node A utilizes a part of information among what it possesses and attempts authentication with BS. Here the information that is used prevents replay attack, $H(ID_A)$, its identifier through the hash operation, and creates random number N_A, which is to help create Phantom ID, and the value of MAC to guarantee the integrity of message that is in the middle of message.

$$(\mathrm{H}(ID_A)||N_A)||MAC$$

Step 2 (A → BS)

To guarantee the confidentiality within the same sensor network, message is encrypted by the master key K_M and sent to BS. During this process, there is a risk of wiretapping, but since message is a part of the information that is used to make identifier, the actual identifier of node cannot be induced, even if it is exposed.

$$E_{KM}\{(\mathrm{H}(ID_A)||N_A)||MAC\}$$

Step 3 (BS)

The contents of the encrypted message are decrypted by the master key K_M that is imposed in the same sensor network. The base station that has received the message from node A examines MAC to first check integrity. If there is a problem in the integrity, it ignores the message, and if there is none, it continues proceeding. First, among the contents of the message, it examine the table, utilizing $H(ID_A)$ as index, and save the N_A value in the searched column. And it creates arbitrary random number N_{BS} that participates in the creation of node A and $H(ID_{BS})$, which is its identifying information that is matched and hashed, and identifier. And it creates MAC to guarantee the integrity of the message that is in the middle of communication.

$$(\mathrm{H}(ID_{BS})||N_{BS})||MAC$$

Step 4 (BS → A)

In order to prevent a malicious attacker's wiretapping or message fabrication in the same sensor network, it is encrypted with the secret key of node A, which has been defined previously at node distribution, and sent.

$$E_{KA}\{(\mathrm{H}(ID_{BS})||N_{BS})||MAC\}$$

Step 5 (A)

Sensor node A decrypts the received encrypted contents of the message by using the secret key K_A, which is already saved. To verify the integrity of the message that is received from BS, sensor node A checks MAC. If there is a problem in the integrity, it ignores the message, and if there is none, it continues proceeding. It saves $H(ID_{BS})$, which is the necessary information in the received message, and the arbitrary random number N_{BS}, which is created at the base station.

$$D_{KA}\{(\mathrm{H}(ID_{BS})||N_{BS})||MAC\}$$

Step 6 (A/BS)

This process is the process of making anonymous identifier that has different location by sensor node A and the base station together. Anonymous identifier is created based on the information that has been sent and received previously in communication. The information that A and BS each possesses is X(BS, A), Y(N_A, N_{BS}), Z($H(ID_{BS})$, $H(ID_A)$). Each X, Y, Z show on the plane coordination, and they can be expressed in the matrix of 2 columns and 3 rows like the following. To create anonymous identifier, operation like the following is performed.

$$T_A, T_B = (BS \oplus N_A \oplus H(ID_{BS}) / 3, A \oplus N_{BS} \oplus H(ID_A) / 3)$$

T_A and T_B are the temporary values to create sensor node A's phantom ID. Later, PID is created by the following operation.

$$PID = T_A \oplus T_B$$

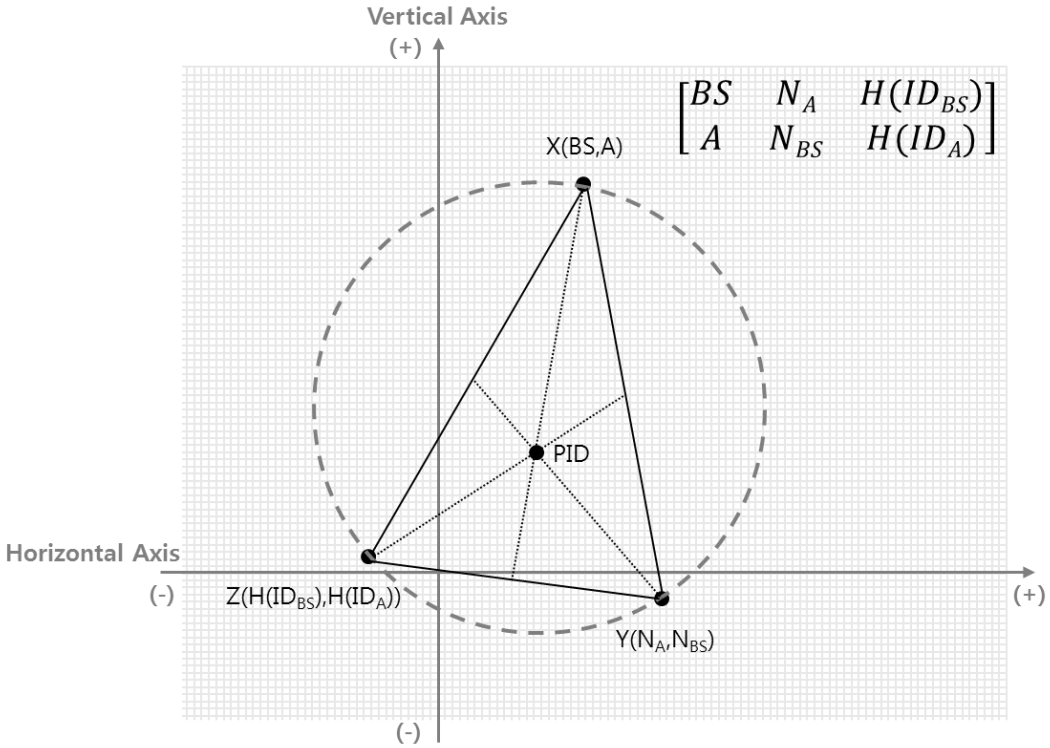

Figure 3. The Matrix to Create Anonymous Identifier in Same Cluster Sensor Network

4.3. Optimized Encryption Key Management Protocol

The key management technology can be said to be the hardest part in the security of sensor network due to the reason such as the limitation of resource. Key management protocol should construct safe communication structure, forming trust relation between sensor nodes that are randomly set in the state of having no institution. Also, it sometimes create secret key in later various security protocols. For key distribution, each sensor must have secret information in any kinds of forms, and after the installation, by using this information, relative location between sensor nodes is figured out. After that, the setting for key distribution and communication is made. The previous process of key distribution is a communication process of sending symmetric key from the base station to sensor node to simply have the key distributed. However, in an enhanced LA^2EP Protocol, optimized key management scheme is proposed that has been designed to suit the limitation of resources of sensor network, which has highly limited resource such as sensor nodes memory, communication, operation and power. The following picture Figure 4 shows the process of key distribution of LA^2EP Protocol.

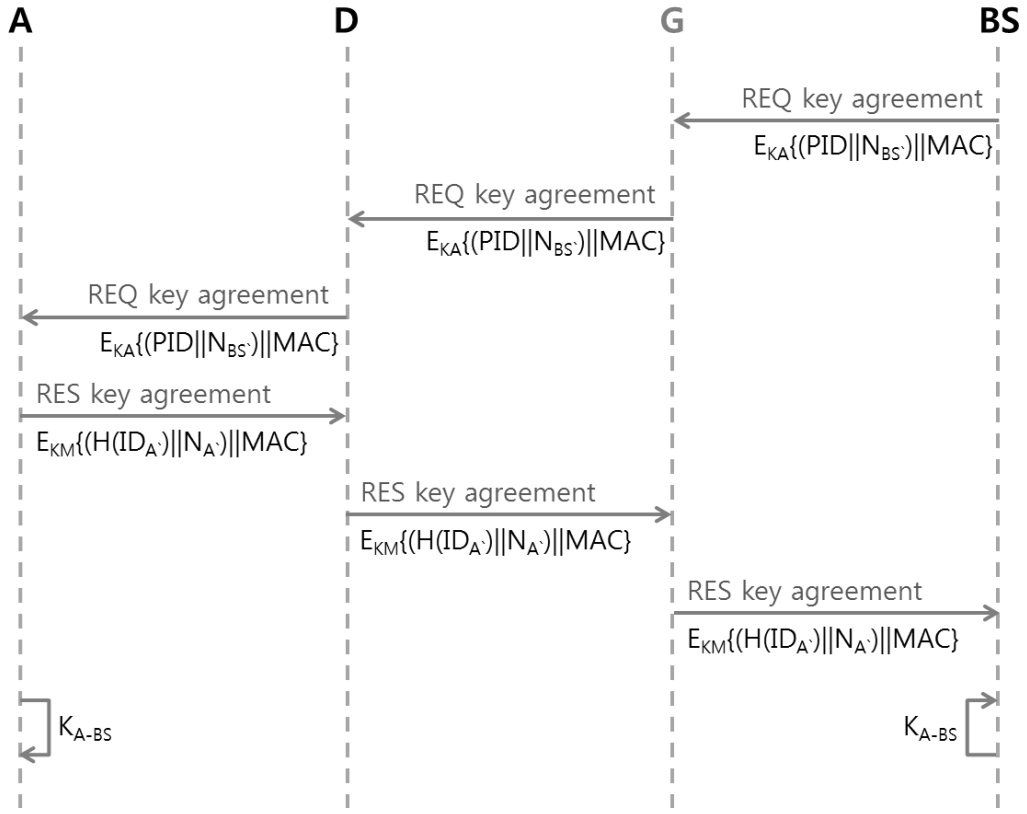

Figure 4. The Optimized Key Agreement between the Sensor Node A and the Base Station

Step 1 (BS)

During the initial process of key distribution, the base station creates the arbitrary random number value, $N_{BS`}$, which will be used as the material for key, and creates MAC to guarantee the integrity upon the communication. When the period of using sensor node key expires, it redistributes automatically.

$$(\mathrm{PID}||N_{BS`})||MAC$$

Step 2 (BS → A)

In order to prevent the exposure of the encryption key in the same sensor network, it is encrypted as the secret key K_A of sensor node A and sent.

$$E_{KA}\{(\mathrm{H}(ID_A)||N_A)||MAC\}$$

Step 3 (A)

The sensor node that received the message decrypts the encrypted message with its secret key. Also, it confirms MAC in order to verify the integrity of the message. When there is a problem in the messages integrity, it terminates the message, and if there is no

problem, it performs the next procedure. It creates random value $N_{A'}$ as the material for the key that will be used in creation of the encryption key, and after going through the operation of $BS'=BS+N_A$ and $A'=A+N_{BS}$, it creates MAC to guarantee the integrity of the message.

$$(\mathrm{H}(ID_{A`})||N_{A`})||MAC$$

Step 4 (A → BS)

In order to prevent the exposure of the key materials that will create the encryption key in the same sensor network, it is encrypted using the master key K_M and then sent.

$$E_{KM}\{(\mathrm{H}(ID_{A`})||N_{A`})||MAC\}$$

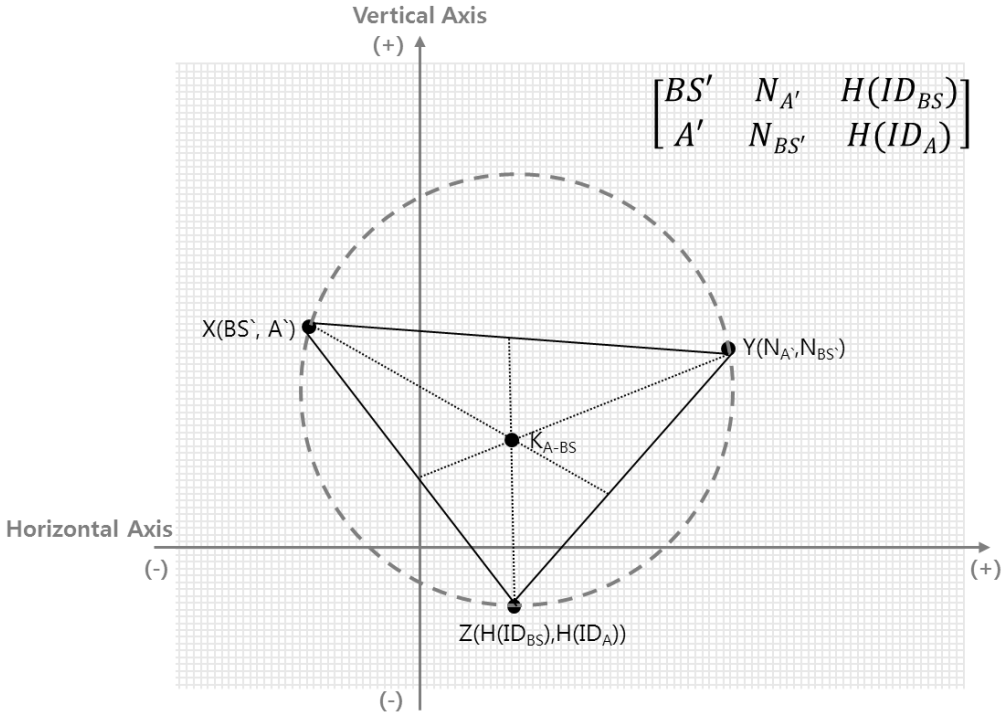

Figure 5. The Matrix to Create Pairwise Key between the Sensor Node A and the Base Station

Step 5 (BS)

The encrypted message is decrypted using the master key. If there is a problem in the messages integrity, it terminates the message, and if there is no problem, it follows the next procedure. The calculations $BS'=BS+N_A$ and $A'=A+N_{BS}$ are performed. And it saves the acquired resulting values of BS' and A' and also saves $N_{A'}$ and $N_{BS.}$

$$D_{KM}\{(\mathrm{H}(ID_{A`})||N_{A`})||MAC\}$$

Step 6 (A/BS)

It creates symmetric key with X(BS', A'), Y($N_{A'}$, $N_{BS'}$), Z(H(ID_{BS}), H(ID_A)), which are the values that were acquired through communicating between the sensor node and the base station. The operation is conducted after composing the matrix of two columns and three rows. $T_{A'}$ and $T_{B'}$, which were acquired through the formula, $T_{A'}$,$T_{B'}$=(BS' $\oplus$ $N_{A'}$ $\oplus$ H(ID_{BS}) / 3, A' $\oplus$ $N_{BS'}$ $\oplus$ H(ID_A) / 3), create the symmetric key K_{A_BS} through $T_{A'}$ $\oplus$ $T_{B'}$ operation.

5. Performance Evaluation

In this passage, it was distinguished between the security aspect and efficiency aspect and was analyzed qualitatively and quantitatively in order to measure the performance of LA^2EP. First, in security aspect, it was analyzed based on the entropy formula in order to get the mathematically quantified numerical value of the degree of anonymity of the anonymity authentication scheme. In the efficiency aspect, it was evaluated about spaces for operation, communication, and storage, which must be considered the most among the factors that suit the characteristics of sensor network.

5.1. Security Analysis

In the part that was considered in the security aspect, the range that a malicious attacker could conjecture in the anonymity authentication scheme was quantified mathematically and then analyzed.

5.1.1. Degree of Anonymity: To quantify the degree of anonymity, a relational expression of entropy was used (see Expression (7)).

$$H(X) = -\sum_{i=1}^{N} P_i \times \log_2 P_i$$

P_i is the likelihood that, when an event of source transmitting data occurs, i-th sensor is the source, as judge by the eavesdropper. If the total number of nodes is N, each node can be defined as 1/N. When this is applied to the all sources, $\sum_{i=1}^{N} P_i = 1$ results. H_M is the max value of entropy (see Expression (8)).

$$H_M = -\sum_{i=1}^{N} \frac{1}{N} \cdot \log_2 \frac{1}{N}$$

The degree of anonymity is defined as follows, from the definition of entropy.

$$d = 1 - \frac{H_M - H(X)}{H_M}$$

It can be seen that the degree of anonymity is $0 \leq d \leq 1$ according to the above definition. If a local eavesdropper is completely unable to know which among the sensors the source is, entropy gets the max value, which denotes the highest degree of anonymity.

5.1.2. Measuring Degree of Anonymity: In this passage, LA2EP's degree of anonymity is analyzed by using the entropy formula that was defined above. It can be known that the degree of the defined anonymity has the range of $0 \leq d \leq 1$ through the following equation.

$$d = \frac{H(X)}{H_M}$$

Here, when the value of entropy is the largest (the value that d is proximate to 1), the degree of anonymity could be said to be high; when it is the smallest (the value that d is proximate to 0), the degree of anonymity could be said to be low. In other words, the fact that the value of d is close to the maximum value means that it satisfies $H_M \approx H(X)$

$$H_M = -\sum_{i=1}^{N} \frac{1}{N} \cdot \log_2 \frac{1}{N} = \log_2 N$$

H_M is the value of entropy in the case when the probability that all the nodes will be distinguished by attacker is identical. H(X) is the value of entropy after the event happened and the value that can be measured after the signal was occurred by the node.

$$H(X) = -\sum_{i=1}^{N} P_i \times \log_2 P_i = \log_2 P_i$$

To compare H(X) and H_M when determining d, it can be known that the most important factor is P_i. It is the probability that attacker will catch the source of sensor when the event of sending the data happens. If $P_i = 1/N$, then the same value comes out for both H(X) and H_M, so the degree of anonymity, d, can be said as the maximum value.

$$P_i = P_r(X = i)$$

For the probability to catch the source where the event happened correctly in the network with N numbers of sensors, attacker must be able to correctly identify the sensor that works in certain time and presume the location. In other words, since the attacker knows all the value of ID and information for all the sensors in the network that the anonymous scheme is not applied, the equation is $P_i = 1$ like the following. However, the range of key-pool that N numbers of nodes can have in LA^2EP is like the following picture. The range of key-pool can be determined by the random number, which was exchanged between sensor node A and BS, the value acquired from the hash operation, and the individual key of each. We used matrix to draw the acquired value on the plane coordination. When the matrix of two columns and three rows was expressed in three points, the area of circle that wraps around the surroundings is the area of total creation key-pool. In other words, the probability pi of malicious attacker finding random ID with brute-force is the same as $1/ \pi r^2$. Like so, when the value of P_i of LA^2EP scheme is applied to H(X) is like the following equation.

$$H(X) = -\sum_{i=1}^{N} \frac{1}{\pi r^2} \times \log_2 \frac{1}{\pi r^2} = \log_2 \pi r^2$$

As a result, since it is defined the same as H(X) and H_M above, the degree of anonymity, d, is like the following.

$$d = \frac{H(X)}{H_M} = \frac{\log_2 \pi r^2}{\log_2 N}$$

Just like what has been verified in d, the degree of anonymity, the larger the number of N of sensor node becomes, the wider the radius of πr^2, the range of key-pool, expands. It can be correctly known through the entropy formula that it is hard for the malicious attacker to conjecture the identifier regarding the random sensor node when the range of key-pool increases.

5.2. Cost Analysis

The most important consideration detail in sensor network environment is how well it can fulfill high limitation of resources. Therefore, the protocol that this thesis suggested is described as it is divided into the aspects of operation, communication, and storage.

5.2.1. Computational Cost: When renewing the key in the same sensor network, the encryption operation is performed to send the new key. The key that is used at this time is pairwise key of sender-receiver node. Therefore, how many encryption operations will be performed is decided by the number of sender-receiver nodes. When the sender sensor node is do, each legitimate receiver nodes can be defined as d_i, i=1, 2,…, N. In other words, the number of performance of encryption operation using pairwise keys is $\sum_{i=1}^{N} d_i$. The number of performing decryption operation by the node that received the encrypted message, using pairwise key, is also the same as the number of performance of encryption operation. Therefore, when the total amount of consumption of operation is calculated, the total sum of encryption and decryption operations can be defined as 2S, and when the network size is N, it could be analyzed as 2S/N in average.

5.2.2. Communication Cost: It could be said that when creating, renewing, and consuming secret key of sensor node, the average of communication consumption is similar to the operation consumption that was calculated above. What the number of encryption/decryption operation means is exchanging the communication with base station and neighboring nodes. For example, in the sensor network environment where the network size is N and the degree is d, the average amount of sender-receiver communication can be analyzed as $(d - 1)^2 / (N-1)$.

5.2.3. Storage Cost: When it is supposed that there are d numbers of neighboring nodes in the random sensor node to calculate the storage consumption, each sensor node stores d number of pairwise keys, d number of cluster keys, and one group key. Also, authentication and encryption key can be renewed with random numbers at update stage, not at the bootstrap stage, where the key is issued. Therefore, the storage is separately needed to create the key, besides the key storage. When the storage is defined as T, the storage that each sensor node needs can be analyzed as 2d+2+T.

6. Conclusion

Collected through the wireless sensor network, the data are sent to the base station, which is safe and trustable center node, for the wireless communication and provide useful information to humans. Whatever the information is, the provided data in creating the information must be precise and trusted. Likewise, the wireless sensor network must collect the data correctly and send it to the base station safely. The leak, forge, and falsification of the data that are sent by an attacker with malice may cause serious problems. Because of this reason, the wireless sensor network requires the encryption and authentication of communication for the security. In this thesis, it suggested LA^2EP Protocol, which is the scheme of authentication and encryption that considered the characteristics of the sensor network.

LA^2EP Protocol is consisted of two big components. In the anonymity authentication scheme, the moving sensor node does not allow the sending node that exchanges data and the third party besides the receiving node to easily distinguish the identifier of the sender-receiver in the middle of communication in the environment of doing the daily surveillance or tracking certain object. In the key management scheme, it suggested encryption algorithm that uses memory as minimal as possible and has less amount of calculation so that it would suit the sensor networks limitation of resources.

By analyzing the performance of LA^2EP protocol qualitatively and quantitatively, the security and efficiency have been verified. The entropy formula was applied to the aspect of security and was analyzed quantitatively. For the degree of anonymity, d, the larger the number of sensor node N becomes, the wider the radius of πr^2, which is the range of key-pool, expands. Through the entropy formula, it can be correctly known that when the range of key-pool increases, it is hard for the malicious attacker to conjecture the identifier of the random sensor node. In the aspect of efficiency, it was quantitatively analyzed in spaces for operation, communication, and storage. In the aspects of operation consumption and communication consumption, the differences in result value were large, based on the network composition, but viewing it in average, it showed suitability for the sensor network, and largely increased efficiency was confirmed in storage consumption.

As a result, it showed that it was efficient to the network and hypothesis that this thesis suggested. Afterwards, it will review the performance analysis, using a realistic topology, and the problems that occur during realization.

Acknowledgements

This paper is a revised and expanded version of a paper entitled “An Enhanced Data Privacy Mechanism Suitable for Ubiquitous Sensor Network” presented Jeju Grand Hotel by Jeong-Hyo Park, December 8 2011, GDC2011 conference.

References

[1] Li N, Zhang N, Das SK, Thuraisingham B, “Privacy preservation in wireless sensor networks: A state-of-the-art survey”, Ad Hoc Networks, vol. 7, **(2009)** November , pp. 1501-1514.

[2] Liu D, Ning P, Liu A, Wang C, Du WK, “Attack-resistant location estimation in wireless sensor networks”, ACM Trans. Inf. Syst. Secur., vol. 11, no. 4, **(2008)**, pp. 1-39.

[3] Pietro RD, Mancini LV, Mei A, “Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks", Wirel. Netw., vol. 12, no. 6, **(2006)**, pp. 709-721.

[4] Misra S, Xue G, "Efficient anonymity schemes for clustered wireless sensor networks", IJSNet, **(2006)**, pp. 50-63.

[5] Akkaya K, Younis M, "A survey on routing protocols for wireless sensor networks", Ad Hoc Networks, vol. 3, **(2005)** May, pp. 325-349.

[6] Schuler M, Donnes P, Nastke M, Kohlbacher O, Rammensee H, Stevanovic S, "Snep: Snp-derived epitope prediction program for minor h antigens", Immunogenetics, vol. 57, no. 11, **(2005)**, pp. 816-820.

[7] Liu D, Ning P, Li R, "Establishing pairwise keys in distributed sensor net-works", ACM Transactions on Information and System Security (TISSEC), vol. 8, no. 1, **(2005)**, pp. 41-77.

[8] Du W, Deng J, Han Y, Varshney P, Katz J, Khalili A, "A pairwise key predistribution scheme for wireless sensor networks", ACM Transactions on Infor-mation and System Security (TISSEC), vol. 8, no. 2, **(2005)**, pp. 228-258.

[9] Zhu S, Setia S, Jajodia S, "Leap: efficient security mechanisms for large-scale distributed sensor networks", in Proceedings of the 10th ACM conference on Computer and communications security, **(2003)**, pp. 62-72, ACM.

[10] Karlof C, Wagner D, "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks, **(2003)**, pp. 293-315.

[11] Sweeney L, "Achieving k-anonymity privacy protection using generalization and suppression", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, **(2002)**, pp. 571-588.

[12] Perrig A, Szewczyk R, Tygar J, Wen V, Culler D, "Spins: Security protocols for sensor networks", Wireless networks, vol. 8, no. 5, **(2002)**, pp. 521-534.

[13] Samarati P, "Protecting respondents' identities in microdata release", IEEE Trans. Knowl. Data Eng., **(2001)**, pp. 1010-1027.

[14] Ouyang Y, Le Z, Xu Y, Triandopoulos N, Zhang S, Ford J, Makedon F, "Providing anonymity in wireless sensor networks", International Conference on Pervasive Services, vol. 0, **(2007)**, pp. 145-148.

[15] Nezhad AA, Makrakis D, Miri A, "Anonymous topology discovery for multihop wireless sensor networks", in Procs. of the 3rd workshop on QoS and security for wireless and mobile networks, **(2007)** October, pp. 78-85, ACM.

[16] Mehta K, Liu D, Wright M, "Location privacy in sensor networks against a global eavesdropper", in ICNP'07, **(2007)**, pp. 314-323.

[17] Xi Y, Schwiebert L, Shi W, "Preserving source location privacy in monitoring-based wireless sensor networks", in Procs. of the 20th Int. Parallel and Distributed Processing Symposium, IEEE Computer Society, **(2006)** April.

[18] Cheng Y, Agrawal D, "Efficient pairwise key establishment and management in static wireless sensor networks", in Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on, **(2005)**, pp. 7-10, IEEE.

[19] Ozturk C, Zhang Y, Trappe W, "Source-location privacy in energy-constrained sensor network routing", in Procs. of the 2nd ACM workshop on Se-curity of ad hoc and sensor networks, **(2004)**, pp. 88-93, ACM.

[20] Wadaa A, Olariu S, Wilson L, Eltoweissy M, Jones K, "On providing anonymity in wireless sensor networks", in ICPADS'04, **(2004)**, pp. 411-418.

[21] Gruteser M, Grunwald D, "Anonymous usage of location-based services through spatial and temporal cloaking", in Procs. of the 1st int. conf. on Mobile systems, applications and services, **(2003)** May, pp. 31-42, ACM.

Authors

Jeong-Hyo Park was born in South Korea in 1982. He received the Bachelor degree in Computer Science from Soong-sil University, Seoul, Korea in 2009, and the Master degree for the study of The Design and Implementation of Anonymous Authentication Method based on Smart-Card in 2010. He was the recipient of the Best Student Paper Award of the Korea Academia-industrial cooperation Society in 2007. He have taught computer Network at Soong-sil University. His research interests include Network Security, Cryptography and Network Protocol.

Yong-Hoon Jung received his M.S. and Ph.D degrees in Computer engineering from University of Soongsil, Korea, in 2006. His research interests are in the network security, RFID, information hiding, and DRM System. He researched Computer Communication Lab.

Kwang-Hyoung Lee received the B.S. degree in Computer engineering from Kwang-Ju Univ., Korea, in 1998, the M.S. and the Ph.D. degrees in Computer engineering from Soongsil Univ., Korea, in 2002 and 2004, respectively Korea. He is research interests art in the multimedia data search , RFID Application.

Keunwang Lee received his BS degree in computer science from Hanbat National University, Daejeon, Korea, in 1993, and MS and PhD degrees in computer science from Soongsil University, Seoul, Korea, in 1996 and 2000, respectively. Currently he is an Associate Professor in Chungwoon University, Chungnam, Korea. His research interests include multimedia communications, multimedia applications, mobile communications and multimedia security.

Moon-Seog Jun received his B.S. at Soongsil Univ, M.S. and Ph.D degrees in computer science from University of Maryland, USA, in 1985, 1988. He taught computer Network at Morgan State University and researched Physical Science Lab. New Mexico, USA. He has been taught and researched as a full professor at Soongsil University. His research interests include Network Security, Cryptography, Computer Algorithms, and Network Protocol.