http://dx.doi.org/10.5392/IJoC.2011.7.4.035

Security Improvement of Authentication Method Using Transfer Agent in USN

Do-EunCho
Innovation Center for Engineering Education
Mokwon University, Do-An-dong, Seo-gu, Daejeon 302-729, Korea

ABSTRACT

USN is a technology to detect human external environment. It is an important factor in buildinga ubiquitous computing environment. In this thesis, an authentication method was proposed to allow the sensor nodes, which have weak computing operation capability, to safely communicate with each other in USN and guarantee the anonymity of users for their privacy. In the proposed authentication method that takes into account the characteristics of sensor network, sensor nodes based on a symmetric key algorithm do not transfer keys directly, instead, they mix the random numbers received from AS to generate keys necessary for communications, having a master key and a pseudo-random number generator.In addition, in this thesis, TA was adopted to minimize the leakage of users' information, and a scheme through which virtual IDs received from AS are delivered to sensor nodes was applied to improve anonymity.

Keywords*: USN, Authentication method, Security, Sensor node, Anonymity*

1. INTRODUCTION

With the rapid growth of IT environment, ubiquitous computing has been emerged. It is an intelligent environment where our daily lives are connected with computing, allowing anyone to create a network at any time and at any place. These days, wired and wireless networks have evolved into broadband convergence network(BcN) that has a type of a subscriber network through IP core network. Along with that, newly studied Ubiquitous Sensor Network(USN), which is a technology to detect human external environment is a key to comprise ubiquitous computing environment[1].

USN, as a base network to implement ubiquitous computing, is a wireless network, consisting of many sensors with ultralight weight and low-power. Numerous sensors connected in a single network detect geographical and environmental changes, and then send a base station the detected information which will be delivered to users by a ubiquitous sensor network server[2]. But, since the USN is a broadcast-based communications network, it is easily exposed to external attack:data forgery and alteration attack through the tapping of sensor information, distribution of abnormal packets, message reuse, and a denial-of-service attack paralyzing the entire network. For the reason, it is important to encrypt and authenticate the messages that will be transmitted between nodes in order to implement a safe USN environment[3][4].

Therefore, in this thesis, an authentication method using Transfer Agent is proposed to improve security in USN.As for the proposed authentication method, the USN comprises sensor nodes, Transfer Agent(TA) that has great operation capability and large storage space, and Authentication Server(AS). Also, a sensor node via TA acquires a session key, communicates, and updates a key. Since each node uses its own pseudo-random number generator and a random-number received from AS to generate a key, no keys are exchanged, and thus the proposed method is more efficient in safety and key management aspects than the existing method. In addition, sensor nodes use virtual IDs at the time of communications and transmit messages through TA, so MIX channels are formed. Such channels enhance security and guarantee anonymity without any additional operation of sensor nodes. Moreover, in this study, an analysis on security was conductedto make sure that the proposed authentication method satisfies security requirements of sensor network. This thesis is made of for the following chapters: in chapter 2 is described the concept of USN, the authentication and key management of the existing USN, and anonymity technique; in chapter 3 is proposed an authentication method using Transfer Agent; in chapter 4is described the results of security evaluation of the proposed authentication method; and in chapter 5 is drawn conclusions and is suggested future study direction.

2. RELATED WORK

2.1 Authentication Method

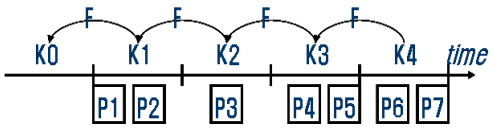
The representative security authentication mechanism proposed early for USN security is SPINS(Security Protocols for Sensor Networks)[5],[6].

SPINS has two secure building blocks: SNEP which is a protocol to guarantee data confidentiality, data authentication,

*Corresponding author. E-mail :decho@mokwon.ac.kr
Manuscript received Oct 24, 2011 ; accepted Nov.21, 2011

data integrity, and data freshness, and μTESLA which is a protocol to authenticate broadcasting data. The SPINS mechanism is a method to safely communicate in resource restricted USN environment. As for SNEP, each node shares a base station and a master keyK_j which will be used to induce all other keys. Regarding μTESLA, through time delay mechanism, a technology to generate key chain, a set of symmetric keys used to create MAC, is applied to achieve safe authentication.

In μTESLA protocol, a base station broadcasts authenticated information to each node. The base station uses a secret key to authorize a packet, and then calculates MAC for the packet. When receiving a packet, a sensor node saves the packet in a buffer, and then, at the time of key opening, the base station broadcasts a certification key to all nodes.The sensor node that receives the public key uses the key to authenticate the packet saved in the buffer. Fig. 1 presents the method to generate a key in SPINS. In the figure,$F_K(x)$is a function to create a new key which is calculated when key value$K$ and x are entered in MAC function. The master key$K_i$is regularly updated by a base station, and with the master key, an encryption key and an authentication key are newly created through$F_K(x)$[7],[8].



$$K_i = F(K_{i+1}),\quad i = 1,2,3,4$$

$$K \rightarrow \begin{cases} K_{encr} = F_k(1) \\ K_{mac} = F_k(2) \\ K_{rand} = F_k(3) \end{cases} \quad Where \quad F_k(x) = MAC(K, x)$$

Fig.1. Key Generation Method of SPINS

The SPINS has the following problems:

① The more the number of nodes for authentication increases, the longer the delay time it takes.

② It is required to synchronize the time between nodes.

③ Given the characteristic of USN, splitting a time period causes high power consumption of the entire USN.

Localized Encryption and Authentication Protocol(LEAP) was proposed to minimize the exposure risk of the nodes adjacent to some exposed nodes, by using an initial key value to make different keys depending on each communications area [9]. The LEAP uses Pairwise Key setting method in which a key is not shared in the entire network, but, instead, only the nodes over the path of data transmission share a key. An attack node does not know a private key, and cluster and Pairwise keys are used only to authenticate neighboring nodes, and a group key is used only to decrypt broadcast messages. Therefore, the LEAP mechanism has an advantage in maximizing the existence of USN with a threat node.

In building USN, the security matter to be considered first is how to set a cryptographic key. The key is used for authentication between sensor nodes and for protection of information exchanged between them.

Recently, more attention has been paid on the guarantee of node anonymity in USN[10],[11]. .If an actual ID is use for message transmission, then an attacker intercepts network traffic, and easily analyzes the traffic and recognizes a node's location. Accordingly, to design an effective and safe authentication method in USN, with the consideration of the characteristic of USN, it is necessary to make keys through minimum communicationsand generate the keys in a safe way. In addition, it is necessary to make the IDs of message sender and receiver anonymous, and thus an attacker won't be able to recognize their actual IDs.

2.2 Anonymity method

Chaum's MIX Channel plays a role as a router between a sender and a receiver. Chaum's MIX-type anonymous communications path using k number of MIX centers is presented as follows[12],[13]. N number of receivers is described as $A_1, A_2, \ldots, A_n$, and each receiver A_i keeps the corresponding relation between A_i and M_i in secret when it transmits message M_i. The public key of receiverB_i is named as $E_{B_i}$and, the public key of sender S_i named asE_i. Here, the role of sender$S_i$is to decrypt a cryptograph of each sender, and remove random number, and then put the result in alphabetical order.

[Step 1] Each receiver$A_i$generates k number of random numbers$R_1, R_2, \ldots, R_K$, and calculates the following cryptograph before transmitting it to public board.

$$E_1\left(R_1, E_2\left(R_2, \ldots, E_K\left(R_K, B_i, E_{B_i}(m_i)\right)\right)\right)$$

[Step 2] The first MIX $S_i$decrypts a received cryptograph, and removes random number R_i from the decrypted message, and then puts the result in alphabetical order before transmitting it to public board.

$$E_2\left(R_2, \ldots, E_K\left(R_K, B_i, E_{B_i}(m_i)\right)\right)$$

[Step 3] The [Step 2] operation is repeatedly applied to MIX $S_2, \ldots, S_{K-1}$ except for the last MIX S_K.

[Step 4] Lastly, S_K puts$B_i, E_{B_i}(m_i)$in alphabetical order, and then transmit the result to public board.

MIX-type anonymous communications path method can maintain message security if at least one MIX is honest. But, it causes a lot of loads in sending and receiving messages, and leads to the failure of the entire function when some MIXs stop functioning. Despite such disadvantages, it is possible to use the method in order to improve security only if a path is short.

3. AUTHENTICATION METHOD USING TRANSFERAGENTINUSN

3.1 Configuration of USN

The proposed USN consists of Sensor Node, Transfer Agent (TA), Authentication Server(AS)[Fig. 2]. Each sensor node is made up for Micro Controller Unit(MCU), sensor interface and RF module, and has the minimum capability for calculation and memorization with low power. Sensor nodes communicate with each other wirelessly. TA located in between Sensor Node and AS relays messages through data encryption. In particular, it serves as an intermediate medium between Sensor Node and AS accessed by the Sensor Node for registration and authentication, and receives from AS a random number necessary for key generation to send the number to the Sensor Node. AS, as a server, authenticates Sensor Node and an object for TA, and generates a random number necessary for the registration of each object and for key generation. In addition, when asession key is created, the AS generates a Virtual Identifier (VID) to send it to users.

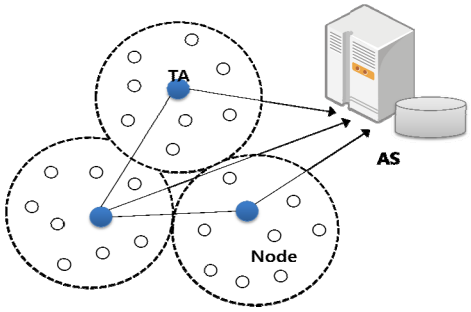


Fig. 2.Configuration of the proposed sensor network

In case of all communications such as between TA and AS, and between a node and AS, a symmetric key which leads to fast encryption/decryption speedis used. Each subnet has one TA, and a sensor node in each subnet executes initial registration into AS and an authentication process through AS. Each object participating in USN communications generate all keys necessary for communications by mixing a master key, a pseudo-random number created by its generator, and a random number. And each symbol is described in the Table 1.

Table 1.Key symbols used for communications

Symbol	Description
AS	Authentication Server
TA_i	Transfer Agent of Subnet i
Node A	Sensor Node A
ID_A,ID_B	ID s of Sensor Node A and B
K_M	Master Key of entire sensor nodes
K_{MT}	Master key of entire TAs in the network
K_{M_A}	Separate Master Key of Sensor Node A
K_A	Separate Encryption Key of Sensor Node A
K_{MAC_A}	MAC Key of Sensor Node A
K_{TA_i}	Separate Encryption Key ofTA_i
R_S	Random Number Generated by AS
$K_{A,B}$	Share Key of A and B
$\{K_{M_i}\}$	A Set of separate master keys of Sensor Nodei
$E(K, M)$	Encryption of message M by Using Symmetric keyK
$MAC(K, M)$	CBC-MAC operation of message M with key K
A||B	Combination of A and B

All keys necessary for communications are created by a pseudo-random number generator$F_K(R)$.

$$F_{K_M}(ID_i) = K_{M_i}(1)$$
$$F_{K_M}(R_i) = K_{MAC_i}(2)$$

AS generates two random numbers$R_S$andR_{ST}. $R_S$is used for a separate random number of a sensor node, andR_{ST} used for TA's separate random number. Both each sensor node and TAuse their own master key and random number to create a key which will be used for various types of communications. In addition, through the simple addition of operation to a parameter, a key, which is to be used when MAC is generated for a cryptography, can be generated.

3.2 Initial authentication and registration

Each sensor node and TA, prior to their installation, receive from AS the entire master key $K_M$andK_{MT}, and temporary random numbers$R_X$andR_{XT}, respectively, and save them. At this time, they generate a separate master key and a temporary MAC key based on their own ID. AS also generates each node's separate master key and temporary MAC key based on each node's ID, and saves them into a database. Accordingly, each node, prior to its installation, holds the following keys, and then is installed at a certain place. Table 2 displays the list of initial keys which objects generate and hold according to formula (1) and formula (2).

Table 2.List of initial keys held by objects

Object	Node i	TA_i	AS
Holding key	K_M, K_{M_i}, K_{MAC_X}	K_{MT},$K_{M_{TA_i}}$ $K_{MAC_{XT}}$	K_M, K_{M_i},$\{K_{M_i}\}$ $\{K_{MT_{TA_i}}\}$, K_{MAC_X} $K_{MAC_{XT}}$
Holding random number	R_X	R_{XT}	R_X, R_{XT}

Each node is installed at a certain place, and then executes initial authentication and registration process. For example, each step of Node A is performed as follows.

① Right after Node A is installed, it selects its own ID and a random number(R_A) with the separate master key(K_{M_A}) generated through its own ID(ID_A), and encrypts them. In addition, for authentication, it creates MAC with a temporary MAC key(K_{MAC_X}), and sends it toTA_i.

Node A $\rightarrow TA_i$:$E(K_{M_A}, ID||R_A)||MAC(K_{MAC_X}, ID_A||R_A)$

②TA_iencrypts its own ID(ID_{TA_i}) and the message from the node with its own separate master key($K_{M_{TA_i}}$), and then sends them to AS.

$TA_i \rightarrow AS$:

$$E\left(K_{M_{TA_i}}, ID_{TA_i}||R_{TA_i}||(ID_A||R_A)\right)$$
$$||MAC\left(K_{MAC_{XT}}, ID_{TA_i}||R_{TA_i}||(ID_A||R_A)\right)$$

③ Prior to the installation of initial nodes, AS generates and hold each node information(ID and separate master key) as a temporary random number. Based on the information, it checks if the sensor node's ID received from $TA_i$is proper. In this way, a malicious node's interference can be blocked at an initial step.

④ After each node's ID is identified, AS generates random numbers(R_S, R_{ST}). All keys to be used for actual communications are generated through each node's pseudo-random number generator, the entire master key, separate master key, and random numbers(R_S, R_{ST}) sent by As. R_S is a random number to be sent to each sensor node, and R_{ST} is a random number to be transferred to each TA.

⑤ AS encrypts the generated random numbers R_S, R_{ST} with sensor node A's separate master key and withTA_i's separate master key, and then transmits them. And for authentication, MAC is to be added.

AS $\rightarrow$TA :

$$E\left(K_{M_{TA_i}}, R_{ST}||R_{TA_i}||\left(K_{M_A}, R_S||R_A\right)\right)$$
$$||MAC\left(K_{MAC_{XT}}, R_{ST}||R_{TA_i}||(R_A)\right)$$

⑥TA_iuses a random number(R_{ST}), which is drawn from the decryption of the message received from AS, to create the encryption and MAC keys necessary for communications.

$$F_{K_{M_{TA_i}}}(R_{ST}) = K_{TA_i}, F_{K_{M_{TA_i}}}(R_{ST}+1) = K_{MAC_{TA_i}}$$

⑦TA_isends the sensor node the message received from.

$TA_i \rightarrow$ Node A :$E(K_{M_A}, R_S||R_A)||MAC(K_{MAC_X}, R_S||R_A)$

⑧ Node A uses a random number(R_S), which is drawn from the decryption of the message received fromTA_i, to generate the encryption and MAC keys necessary for communications.

$$F_{K_{M_A}}(R_S) = K_A, F_{K_{M_A}}(R_S+1) = K_{MAC_A}$$

⑨ By removing the random numbers and temporary MAC keys used for key generation, each sensor node and TA delete the information that is to be used to create keys necessary for communications. Therefore, even though a node is in a physical danger by an attacker, the attacker can't generate keys used for other nodes only with the node's information.

3.3 Setting-up of Session Key

The node which completes its registration needs a session key for node authentication and communications when it communicates with other nodes. Each node receives from AS a session key and a VID which is used on behalf of its ID. The VID and the session key are received prior to the beginning of communications. A node which wants to communicate with other nodes receives a session key in the following process.

① Let's assume that Node A wants to communicate with Node B. For authentication, Node A sends its ID and Node B's ID to TA_iwhich is located in Node A's subnet.

Node A $\rightarrow TA_i$:

$$E(K_A, ID_A||ID_B||R_A)||MAC(K_{MAC_A}, ID_A||ID_B||R_A)$$

②TA_i receives the information, and encrypts the message received from Node A with its own encryption key, and then sends it to AS.

$TA_i \rightarrow AS$:

$$E\left(K_{TA_i}, R_{TA_i}||(K_A, ID_A||ID_B||R_A)\right)$$
$$||MAC\left(K_{MAC_{TA_i}}, R_{TA_i}(K_A, ID_A||ID_B||R_A)\right)$$

③ AS identifies the sensor node's ID received from TA_i, and then generates random numbers R_E and VID, which will be used to create a session key.

$$VID_A = H(ID_A, R_E)$$
$$VID_B = H(ID_B, R_E)$$

④ AS encrypts the generated random numbersR_E,VID_A, $VID_B$and sends them to $TA_i$and TA_j which are located in each sensor node's subnet.

AS $\rightarrow TA_i$:

$$E\left(K_{TA_i}, R_{TA_i}||(K_A, VID_A||VID_B||R_E||ID_A||ID_B)\right)||$$
$$MAC\left(K_{MAC_{TA_i}}, (K_{MAC_A}, VID_A||VID_B||R_E||ID_A||ID_B)\right)$$

AS $\rightarrow TA_j$:

$$E\left(K_{TA_j}, R_{TA_j}||(K_B, VID_A||VID_B||R_E||ID_A||ID_B)\right)||$$
$$MAC\left(K_{MAC_{TA_j}}, (K_{MAC_B}, VID_A||VID_B||R_E||ID_A||ID_B)\right)$$

Since the transmitted message is encrypted with each TA's separate encryption key, other TAs that received the message can't understand it. And, since the transmitted message is encrypted with a receiver's separate encryption key, a MIX channel ends up being established between AS and the node.

⑤$TA_i$and TA_jreceives the message, and decrypts it with their own separate encryption key, and then sends the decrypted message to a relevant node.

$TA_i \rightarrow$ Node A :

$$E(K_A, VID_A||VID_B||R_E||ID_A||ID_B)||$$
$$MAC(K_{MAC_A}, VID_A||VID_B||R_E||ID_A||ID_B)$$

$TA_j \rightarrow$ Node B :

$$E(K_B, VID_A||VID_B||R_E||ID_A||ID_B)||$$
$$MAC(K_{MAC_B}, VID_A||VID_B||R_E||ID_A||ID_B)$$

At this time, the decrypted message is also encrypted with each node's separate encryption key. So, other TAs neither know which node will receive the message nor understand the message.

⑥ The relevant node receives the message, and decrypts it. And then, it generates a session key($K_{A,B}$) and a MAC key ($K_{MAC_{A,B}}$) by using a random number R_E. In addition, since the node removes R_E, it is impossible to know the information used for key generation.

In the process of setting up a session key, each node receives a virtual ID and a random number R_E used to generate a session key from AS by using a TA which is located in each node's subnet. This communications method by way of Transfer Agent seems to increase more calculation in the entire process of setting up a session key than the existing authentication method. But in fact, without increase in calculation from a sensor node's perspective, and only with increase in calculation from the perspective of TA an AS, it is possible to step up security and provide anonymity.

3.4 Addition of Sensor node

When a sensor node does not live any longer due to its energy consumption, or when it should be replaced by a new sensor node due to leakage, the new node should get a key in USN. In the step of initial authentication and registration, the newly added sensor node receives from AS the entire master keyK_M, and a random number R_X, and save them. After that, it creates its separate master key(K_{M_C}) and a temporary MAC key(K_{MAC_X}) based on its own ID. Through the new sensor node's ID, AS also saves the sensor node's separate master key into a database. After the new sensor node is installed, it sets up keys necessary for communications through the following steps. This is fundamentally equal to initial authentication and registration process.

① New Node C is installed additionally. And then, it uses the separate master key(K_{M_C}) created with its own ID(ID_C) to select ID and a random number(R_C), and then encrypts them. In addition, for authentication, it creates MAC with a temporary MAC key(K_{MAC_X}), and then sends it to TA_i.

Node C $\rightarrow TA_i$:$E(K_{M_C}, ID_c, R_C)||MAC(K_{MAC_X}, ID_C||R_C)$

②TA_iencrypts its own ID(ID_{TA_i}) and the message received from the Node C with its own encryption key(K_{TA_i}), and sends them to AS.

$TA_i \rightarrow$AS :

$$E\left(K_{TA_i}, ID_{TA_i}||R_{TA_i}||(ID_C||R_C)\right)||$$
$$MAC\left(K_{MAC_{TA_i}}, ID_{TA_i}||R_{TA_i}||(ID_C||R_C)\right)$$

③ Based on each node's information (each object's ID, separate master key), AS checks out if the sensor node's ID received from TA_i is proper.

④ When the ID is identified, AS transmits a random number(R_S). Keys used for actual communications are generated through each node's pseudo-random number generator, the entire master key, separate master key, and the random number(R_S) sent by AS. $R_S$is a common random number which is delivered to sensor nodes in the entire network.

⑤ AS encrypts the random number R_S with the Node C's separate master key, and then encrypts it again with TA_i's separate encryption key before sending it. In addition, MAC is added for authentication.

AS $\rightarrow TA_i$:

$$E\left(K_{TA_i}, R_{TA_i}||\left(K_{M_C}, R_S||R_C\right)\right)||$$
$$MAC\left(K_{MAC_{TA_i}}, R_{TA_i}||\left(K_{MAC_X}, R_S||R_C\right)\right)$$

⑥TA_idecrypts the message received from AS, and then sends it to the Node C.

$TA_i \rightarrow$ Node C :$E(K_{M_C}, R_S||R_C)||MAC(K_{MAC_X}, R_S||R_C)$

⑦ The Node C uses the random number (R_S) which is drawn after the message received fromTA_i is decrypted in order to create the encryption MAC keys necessary for communications.

$$F_{K_{M_C}}(R_S) = K_C\,, F_{K_{M_C}}(R_S + 1) = K_{MAC_C}$$

⑧ By removing the random number(R_S) used for key generation, the Node C deletes the information which will be used to generate the keys for communications.

3.5 Disposal of Sensor node

When a sensor node is in a physical danger by an attacker or fails to do its work, the sensor node should be scrapped. At this time, if the sensor node's key information is leaked, the entire network can be damaged. Accordingly, such keys should be newly updated. Regarding the key update process, when only the sensor nodes in a relevant subnet are updated, unnecessary operation of the entire network and energy consumption can reduce. First, AS removes the ID and the keys of the node which will be scrapped from a database. After that, keys are updated in the following process.

① AS removes the relevant Node'sID_i and separate master key (K_{M_i}) from a database, and generates a new random

number (R'_S).

② The generated random number (R'_S) is encrypted with TA_i's separate encryption key, and MAC is added before transmission.

$$AS \rightarrow TA_i : E\left(K_{TA_i}, (K_M, R'_S)\right) || MAC\left(K_{MAC_{TA}}, (K_M, R'_S)\right)$$

③TA_ibroadcasts the message to all nodes in the relevant subject to deliver the new random number R'_S.

$$TA_i \rightarrow Node : E(K_M, R'_S) || MAC\left(K_{MAC_X}, R'_S\right)$$

④ Each node decrypts the message, and then uses the new random number R'_S to update the keys which could be exposed to a danger caused by the scrapped sensor node.

$$F_{K_{M_i}}(R'_S) = K_i, F_{K_{M_i}}(R'_S + 1) = K_{MAC_i}$$

⑤ By removing the random number (R'_S), each node deletes all the information used for key update.

3.6 Key Update

If the same key is used for a long time, it is possible for the key to be leaked.Accordingly, keys used in USN should be updated at a certain period of time. Keys are updated in the way that AS creates new random numbers (R''_S, R''_{ST}) and deliver them to the entire network, and thus each node updates the entire master key(K_M) and TA's entire master key(K_{MT}). With the updated master keysK''_MandK''_{MT}, each object updates its separate master key, and mixes the updated master keys with newly delivered random numbers to update all keys used for communications.

① AS generates new random numbers R''_S, R''_{ST}.

② The generated random numbers are encrypted with TA's master key, and are transmitted after the addition of MAC.

$$AS \rightarrow TA_i : E\left(K_{MT}, R''_{ST} || (K_M, R''_S)\right) || MAC\left(K_{MAC_{XT}}, R''_{ST} || K_{MAC_X}, R''_S\right)$$

③ TA uses the random number (R''_{ST}) which is drawn after the message received from AS is encrypted in order to update all keys necessary for communications.

$$F_{M_{MT}}(R''_{ST}) = K''_{MT},\ F_{K''_{MT}}(ID_i) = K''_{MT_i}$$
$$F_{K''_{MT}}(R''_{ST} + 1) = K''_{TA_i},\ F_{K''_{MT}}(R''_{ST} + 2) = K''_{MAC_{TA_i}}$$

④ The new random number R''_S is transferred to each node. Each node uses the number to update all keys necessary for communications.

$$TA_i \rightarrow Node : E(K_M, R''_S) || MAC\left(K_{MAC_X}, R''_S\right)$$

$$F_{K_M}(R''_S) = K''_M,\ F_{K''_M}(ID_i) = K''_{M_i}$$
$$F_{K''_{M_i}}(R''_S + 1) = K''_i,\ F_{K''_{M_i}}(R''_S + 2) = K''_{MAC_i}$$

⑤ BY removing the transmitted random numbers (R''_S, R''_{ST}), TA and each node deletes the information used for key update.

4. PERFORMANCE EVALUATION

4.1 Security Analysis

For the analysis on the proposed authentication method's safety and security, the comparison of the proposed method and the existing ones is presented in the Table 3 as follows.

Table 3.Comparison of the proposed authentication method and the existing ones

Type	Proposed Authentication Method	SPINS	LEAP
Key generation position	Sensor Node, TA, AS	Sensor Node BS	Sensor Node, BS
Key generation way	Downward	Downward	Upward
Direct transfer of Key	-	O	O
Key Management	Dependent on AS	Dependent on BS	Dependent on Sensor Node
Cluster concept	O	-	O
Authentication provider	AS	BS	Sensor Node
Number of communications for the setting-up of a session key	4	2	m(Number of neighboring nodes)+1
Security	O	O	O
Support of various communications methods	O	-	O
Anonymity	O	-	-

The security requirements in USN are confidentiality, mutual authentication, integrity, anonymity and freshness[14]. On the basis of the setting-up of a session key necessary for authentication between sensor nodes, which is proposed in this thesis, the security requirements in USN are analyzed as follows.

(1) Guarantee of Confidentiality

Some important messages like a key exchange message should be guaranteed in terms of their confidentiality. Since sensor nodes communicate with each other wirelessly, they are exposed to trapping. In the case of the authentication method proposed in this thesis, keys are not transferred directly, for each node generates keys by using its own pseudo-random

number generator. Also, as for the method, the messages are encrypted with encryption keys based on symmetric key algorithm, and then are transmitted. Therefore, even though an attacker achieves successful tapping, it is impossible to recognize secret keys between TS and AS, and between a sensor node and AS. As a result, the proposed method guarantees confidentiality.

(2) Guarantee of Mutual Authentication

Data authentication is the most significant security requirements in USN.As for the authentication method proposed in this thesis, a sensor node creates MAC with a one-to-one key to communicate with a target node in every step of setting up a session-key. Therefore, through this method, it is possible to authenticate data as to whether the data are altered by an attacker.In addition, since AS holds the IDs of TA and sensor nodes, it is possible to achieve ID-based object authentication hierarchically and block malicious nodes at the very onset.

(3) Guarantee of Integrity

As for the authentication method proposed in this thesis, messages are encrypted with a MAC key used for a one-to-one communications so that the message integrity is guaranteed. Also, as for the method, since the random numbers used for key generation at the initial step of setting up keys are removed, it is impossible for any attackers to generate keys.

(4) Guarantee of Freshness

Data freshness means the protection of data reuse. Generally, it is divided into weak freshness and strong freshness. In order to compare request message and reply message, the weak freshness only uses count value, and the strong freshness uses random numbers. As for the authentication method proposed in this thesis, each node generates random numbers in every communications step so that it provides strong freshness.

(5) Lightweight

The hardware performance of a sensor node is extremely limited. Therefore, as for the proposed authentication method, messages are encrypted/decrypted through RC5 and CBC modes.As a symmetric encryption algorithm, RC5has a fast speed and uses a small memory so that it is proper to apply it to a sensor node. And, to create MAC used for authentication, CBC-MAC is used in the method. As a result, the storage space of a sensor node can reduce.

(6) Guarantee of Anonymity

Since sensor nodes engaging in communications use virtual IDs, they can be protected against impersonation attack caused by the exposure of a node identifier. As for the proposed authentication method, after registering the transfer details and IDs of internal nodes, nodes can communicate through their virtual IDs. Also, since a MIX channel between nodes is formed through TA, each node's information is not exposed to TA, an intermediate agent. Therefore, in this way, the proposed method guarantees anonymity.

The authentication method proposed in this thesis was analyzed from the security perspective. Table 4 presents various types of attacks and the security evaluation of the proposed method about the attacks.

Table 4.Security Evaluation of Proposed Authentication Method

Type	Description
Replay Attack	Since a random number selected by a relevant node is attached to the messages to be sent, a sensor node is safe from replay attack, and guarantees strong freshness.
Impersonation Attack	At the time of setting up a session key, as shown in the function$\mathrm{VID_A} = \mathrm{H}(\mathrm{ID_A}, \mathrm{R_E})$, a VID is created, and then a random number used for key generation is removed. Therefore, it is impossible for an attacker to predict a random number.
Conspiracy Attack	When n number of TAs conspires to know VID, they need a sensor node's separate encryption key. In the proposed method, it is impossible for the separate encryption key to be exposed. So, each sensor node is safe from the conspiracy attack.
Non-repudiation	In the case that a TA engaging in communications repudiates the receipt of messages, the messages can be transmitted only after they are encrypted and decrypted with the secret key of TA which is located in a relevant subnet.

4.2 Efficiency Analysis

For analysis on efficiency of the authentication method proposed in this thesis, the execution time of algorithm was calculated. In addition, the proposed method was compared with KARL method[15] both in the same subnet and different subnet. As for the algorithm execution time, execution time of the algorithm running in a single node($\mathrm{SN_{alg}}$) was calculated, and the total algorithm execution time($\mathrm{Tot_{alg}}$) was calculated by multiplying $\mathrm{SN_{alg}}$by the number of passing nodes(PN).

The symbols necessary to calculate algorithm execution time are presented in Table 5.

$$\mathrm{SN_{alg}} = \mathrm{IQ} + \mathrm{KG} + \mathrm{KA} + \mathrm{EC} + \mathrm{DC} + \mathrm{AC} \quad (3)$$

$$\mathrm{Tot_{alg}} = \mathrm{SN_{alg}} \times \mathrm{PN} \quad (4)$$

Table 5. Symbols for the calculation of algorithm execution time

Symbol	Description
IQ	Inquiry execution time
KG	Key Generation execution time
KA	Key Agreement execution time
EC	Encryption execution time
DC	Decryption execution time
AC	Authentication execution time

A single subnet comprising 50 sensors is built in the form of square, and thus a total of 450 sensors make up a network. A sensor node is deployed at fixed intervals of 10m×10m.

As for the route length between nodes to communicate from Node A to Node B(Node A → Node B), the shortest route node is set as node 5, and the longest route node is set as node 13 if the two nodes are in the same subnet.

TA and AS feature 2.4GHz, 250kbps, and 915Mhz so that they have better operation ability than general sensor nodes, and sensor nodes have operation ability of a node defined in Smart Dust.To shorten the algorithm execution time of a sensor node, the processes of key generation and authentication are designed to be performed on TA which has better performance than general sensor nodes.

The communications method of to calculate the execution time is presented as follows.

■ In the case of KARL method

In the same subnet:Node A → Node B

In different subnets:

$$\text{Node A} \rightarrow \text{Node}_i \rightarrow \text{Node}_j \rightarrow \text{Node B}$$

■ In the case of proposed method

In the same subnet:

$$\text{Node A} \rightarrow \text{TA}_i \rightarrow \text{AS} \rightarrow \text{TA}_i \rightarrow \text{Node B}$$

In different subnets:

$$\text{Node A} \rightarrow \text{TA}_i \rightarrow \text{AS} \rightarrow \text{TA}_j \rightarrow \text{Node B}$$

Fig. 3 and Fig.4 illustrate the graphs of the total algorithm execution time both in the case that the two nodes are in the same subject and in the case that the two nodes are in different subnets.

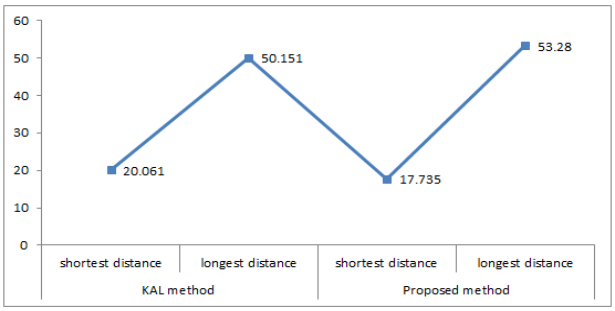


Fig. 3.Algorithm execution time in the same subject

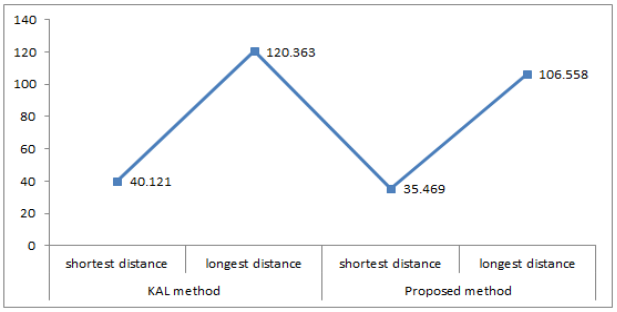


Fig. 4.Algorithm execution time in different subnets

The proposed method has larger number of nodes than the KAL method, since the communications require the passing of TA and AS. Nevertheless, in the case of the shortest length in the same subnet, the proposed method has a large number of operations in the TA and AS aspects and has a small number of node operations so that the proposed method shows remarkably less execution time than the KARL method. But, in the case of the longest distance environment where there are relatively larger node operations, the algorithm execution time in the proposed method increases by 3.128/byte. On the other hand, in the case of the communications in different subnets, as the number of nodes increase, the proposed method shows faster algorithm execution time by 13.804/byte than the KARL method which requires a lot of operations in the aspect of a sensor node.

5. CONCLUSIONS

All sensor nodes in USN, which participate in communications, have only limited battery power. Sensor nodes in the USN environment consume a lot of their power due to the overheads caused by key generation, encryption/decryption, and operation for authentication.

Since the authentication method proposed in this thesis uses RC5 encryption algorithm and CBC-MAC function, it is appropriate for the method to be applied to the ubiquitous sensor network that has weak capability for computing operation. Moreover, because the proposed method took into account the limitation of operation and low-power caused by the smallness and lightweight of a sensor node, it was possible to minimize the operation and communications traffic of a node. In addition, since the method uses a virtual ID assigned to each session, even though an illegal user taps communications and receipt messages, privacy is guaranteed, and the personal information of users in USN is protected in the registration and authentication step.In particular, by inducing TA, the proposed method increased the calculation only in TA and AS aspects, without imposing any burden on sensor nodes. In doing so, the method realized anonymity.

In the future, it is necessary to study a method through which, according to a circumstance, users can be authenticated and session keys can be shared, while anonymity is being guaranteed.

REFERENCES

[1] Jae-yoon Kim, "Ubiquitous Computing: Business Model and Evolution Outlook, “Samsung Economic Research Institute Report, Dec. 2003.

[2] TaeshikShon, KyusukHan,“Efficient Mobile Node Authentication in WSN,"Journal of the Korea Information and Communication Society,vol.35, no.5, 2010, pp.833-839.

[3] Do-Won Hong, Goo-Young Jang, Tae-JoonPark, Gyo-IlJeong, "Encryption Technology Trend for Ubiquitous Environment," Electronic Telecommunications Trend

Analysis, Electronics and Telecommunications Research Institute, vol.20, no.5, 2005, pp. 63-72.

[4] A. Wood, and J. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, vol. 35, Oct. 2002, pp.54-62.

[5] A. Perrig, R. Szewczyk. V. Wen, D. Cullar and J.D. Tygar, "SPINS:Security Protocols for Sensor Networks," Journal of Wireless Networks(WINET), vol.8, no.5, 2002, pp.521-534.

[6] Boseung Kim, Huibin Lim, Jongseok Choi, and Yongtae Shin,"A Study on Node Authentication Mechanism using Sensor Node'sEnergy Value in WSN,"Journal of the Institute of Electronics of Engineers of Korea, vol.48, no.2, 2011, pp.86-95.

[7] R. Rivest, "The RC5 encryption algorithm," in Proc. of the 1994 Leuven Workshop on Fast Software Encryption. Springer-Verlag, 1995, pp.86-96.
[Online] http://citeseer.nj.nec.com/rivest95rc.html.

[8] A. Perrig, R. Canetti, B. Briscoe, D. Tyger, and D. Song, "TESLA: Multicast Source Authentication Transform," Internet Draft, IETF, Nov. 2000.

[9] S. Zhu, S. Setia and S. Jajodia. "LEAP:Efficent Security Mechanisms for Large-Scale Distributed sensor Networks," The 10th ACM Conference on Computer and Communications Security(CCS '03) Washington D.C., Oct. 2003.

[10] K. Mehta, D. liu, and M. Wright "Location Privacy In Sensor Networks Against A Global Eavesdropper," in Proc. on IEEE Conference on Network Protocols (ICNP 2007), 2007.

[11] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, and K. Jones, "On Anonymity in Wireless Sensor Networks," in Proc. on Tenth International Conference of Parallel and Distributed Systems, 2004.

[12] D. Chaum, "Security WithoutIdentification: Transaction Systems to Make Big Brother Obsolete," Communications of the ACM, vol.28, pp.1030-1044, Oct, 1985.

[13] Didier Samfat, RefikMolva, N. Asokan, "Untraceablity in Mobile Networks," ACM Wireless Network Journal, special issue on Security in Mobile Communications Systems, 1996.

[14] Gang Kim, Jin-Seop Park, Bong-Hee Kim,"Risk Analysis Model for Information System Security,"Journal of the Korean Society of Computer and Information, vol.7, no.3, 2002, pp.60-67.

[15] Karl E Persoon and D. Manivannan, "Secure Connection in Bluetooth Scatternets,"System Sciences. 2003. In Proc. of the 36th Annual Hawaii International Conference on 6-9, Jan. 2003, pp.10-19.

Do-Eun Cho

She received Ph.D. degree in Computer Engineering from Chungbuk National University, Korea in 2007. She was a researcher for BK21 in Chungbuk National University. She currently lectures at the Innovation Center for Engineering Education, Mokwon University, Korea. Dr. Cho's research interests include Security, Ubiquitous Computing and Ubiquitous Sensor Network.