International Journal of Control and Automation
Vol.8, No.11 (2015), pp.279-288
http://dx.doi.org/10.14257/ijca.2015.8.11.27

Authenticated Key Agreement Scheme with Forward Secrecy for Wireless Sensor Networks

Hyunsung Kim* and Sung Woon Lee**

*Dept. of Cyber Security, Kyungil University
kim@kiu.ac.kr
Dept. of Information Security, Tongmyong University
secueye@gmail.com

Abstract

To establish secure communication, authenticated key agreement, which combines user authentication and key agreement, is the basic services for many security and privacy services over wireless sensor networks (WSNs). Recently, Jiang et al. proposed an efficient authenticated key agreement scheme with unlinkability for WSNs. Unfortunately, this paper shows two weaknesses in Jiang et al.'s scheme, which are the problem of global time synchronization requirement and the lack of forward secrecy. After that, this paper proposes an enhanced authenticated key agreement scheme with forward secrecy to remedy Jiang et al.'s scheme. The proposed scheme does not use timestamp that requires the global time synchronization and provides forward secrecy. It provides user anonymity and un-traceability by adopting dynamic identifier depending on each session dependent random number.

Keywords: *Wireless sensor network, authentication, key agreement, authenticated key agreement, forward secrecy*

1. Introduction

Wireless sensor networks (WSNs) composing of a large number of sensor nodes can be deployed in any unattended environment such as military target tracking and surveillance, natural disaster relief, biomedical health monitoring and hazardous environment sensing. The sensor nodes are small in size and capable to sense and process data. A WSN is designed to detect events, collect and process data and transmit sensed information to interested users. Basic features of WSNs have limitations on energy, transmission power, memory and computing power. They make WSNs different from the other wireless ad hoc or mesh networks [1-5]. Many security solutions for wireless networks can be applied to WSNs directly. However, several unique characteristics, which include hostile environment, limited resources, in-network processing and application-specific architectures, of WSNs require new security mechanisms [6].

Security and privacy are very critical for the success of WSNs. WSN is subject to various attacks due to the unique characteristics, such as eavesdropping, modification, interception, insertion and deletion. Therefore, basic security mechanisms like authentication, confidentiality and integrity are essential services for WSNs. This paper is focused on authentication and key agreement for confidentiality, which could combined into authenticated key agreement. The network environment we consider is that users want to log into a WSN via gateway node (GWN). However, it is not easy to access real time data from the sensor nodes via GWN only. Thereby, user needs to take direct access to the sensor nodes to acquire data whenever he (or she) requires.

ISSN: 2005-4297 IJCA

To provide security and privacy in WSNs, There are many research efforts until now [7-]. Wong et al. firstly proposed a hash based user authentication scheme over WSNs, which is less complex, light weight and dynamic [7]. But some works showed that it is vulnerable to stolen-verifier, replay, and forgery attacks. Das proposed a two factor method of user authentication, which implements password based authentication with the aid of GWN and is suitable for resource-constrained WSNs [8]. Unfortunately, the scheme has some security flaws and does not provide mutual authentication and key agreement. After that, series of security schemes are proposed to improve the scheme [9-13]. Recently, Xue *et al.* proposed a temporal credential based mutual authentication and key agreement scheme for WSNs, which only involves hash and XOR operations [12]. However, Jiang et al. showed that Xue et al.'s scheme is weak against identity guessing attack, tracking attack, privileged insider attack and stolen smart card attack. Furthermore, Jiang et al. proposed an efficient two factor user authentication scheme with unlinkability and argued that their scheme is secure against various security attacks [13].

First of all, this paper shows security weaknesses in Jiang *et al.'s* user authentication scheme focused on the requirement of global time synchronization and the lack of forward secrecy in the session key. Furthermore, this paper proposes an authenticated key agreement scheme with forward secrecy to solve the weaknesses in Jiang et al.'s scheme. It provides user anonymity and un-traceability by adopting dynamic identifier depending on each session's random number.

The rest of this paper is organized as follows. In Section 2, network configuration on WSNs is reviewed to understand the network environment. Section 3 reviews Jiang et al.'s user authentication scheme and Section 4 shows weakness analyses on it. An enhanced authenticated key agreement scheme is proposed to solve the weakness problems in Jiang *et al.'s* scheme and to provide the forward secrecy in Section 5. In Section 6, we provide security analysis for the proposed authenticated key agreement scheme. Section 7 concludes the paper.

2. Network Configuration

This section briefly reviews Xue *et al.'s* network configuration for the better understanding Jiang et al.'s scheme and the proposed scheme for WSNs [12]. Xue et al.'s network configuration provides five basic models but this paper only will consider a specific model that user only could access data on the sensor nodes via GWN but not directly from them. The model is consisted with three main parties as shown in Fig. 1, which are user, GWN, and sensor nodes over a WSN.

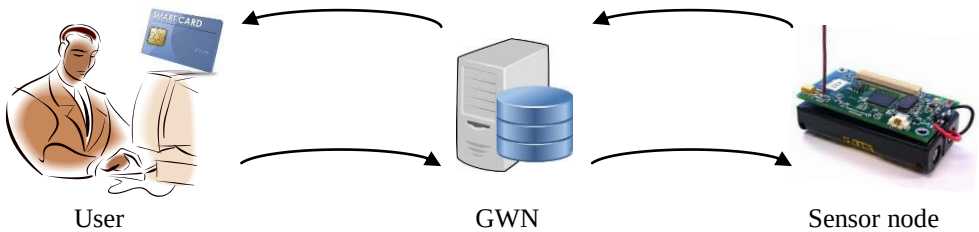

Figure 1. WSN Network Configuration

GWN plays an important role in the network. In order to further reach the specific sensor node, remote user is required to reach GWN through Internet at first. Contrary, sensing data from the sensor nodes firstly gets to GWN and further reaches the end user. If the data in the WSN is made available to the remote user on demand, mutual authentication between them must be ensured before allowing the remote user to access.

With the aid of GWN, impenetrability of lightweight mutual authentication is going to be possible. Since the sensor nodes are deployed in harsh environments, authentication of the GWN is necessary for the user and the sensor node. Three parties have the following functionalities

User: To read data on the sensor nodes over the WSN, user needs to have rights to access them via GWN, which requires to be registered on the GWN.

GWN: GWN works as an authentication server over the WSN and intervenes between user and the sensor nodes.

Sensor node: To provide sensed data, it only communicates with the authenticated GWN not with the user.

3. Jiang User Authentication Scheme

This section reviews Jiang et al.'s efficient two-factor user authentication scheme with unlinkability for WSNs [13]. Jiang *et al.'s* user authentication scheme is consisted with three phases: registration phase, login and authentication phase, and password update phase

3.1. Registration Phase

User registers with GWN. A new user U_i proceeds with the following steps through a secure channel.

Step 1: U_i selects a unique identity ID_i and a password PW_i, and generates a random value r. Then he (or she) computes $RPW_i=H(r||PW_i)$ and submits the registration request message $R=(ID_i, RPW_i)$ to GWN.

Step 2: Upon receiving R, GWN verifies the validity of ID_i and rejects the registration request if ID_i is invalid. Then GWN continues to compute $TC_i=H(K_{GWN-U}||ID_i||TE_i)$ and $PTC_i=TC_i \oplus RPW_i$. GWN initializes the temporary identity TID_i and stores (TID_i, ID_i, TE_i) in the verification table. Finally, GWN issues the smart card containing { $H(\cdot)$, TID_i, TE_i, PTC_i } to U_i.

Step 3: After receiving the smart card, U_i stores r into the card.

The registration phase for SNs is described as follows.

Step 1: S_j submits it's identifier SID_j to GWN through a secure channel.

Step 2: Upon receiving the message, GWN computes $TC_j=H(K_{GWN-S}||SID_j)$, where K_{GWN-S} is the GWN's private key and TC_j is the temporal credential for S_j. Finally, GWN sends TC_j to S_j.

Step 3: After receiving the message, S_j stores TC_j as its temporal credential.

3.2. Login and Authentication Phase

Step 1: U_i inserts his/her smart card to a terminal and enters ID_i and PW_i. The terminal generates a timestamp TS_4 and randomly chooses a key K_i and computes $TC_i=PTC_i \oplus H(r||PW_i)$, $PKS_i=K_i \oplus H(TC_i||TS_4)$, and $C_i=H(ID_i||K_i||TC_i||TS_4)$. Finally, U_i sends TID_i, C_i, PKS_i, and TS_4 to GWN.

Step 2: Upon receiving the message, GWN checks whether the transmission delay is within the allowed time interval ΔT. T_{GWN}* is the current time. If T_{GWN}*- TS_4 > ΔT, GWN terminates the current session and sends REJ message back to U_i; Otherwise, GWN continues to obtain ID_i from the verification table according to TID_i and computes $TC_i=H(K_{GWN-U}||ID_i||TE_i)$ and C_i*$=H(ID_i||K_i||TC_i||TS_4)$. If C_i*$\neq C_i$, GWN rejects it and sends REJ message to U_i. Otherwise, GWN authenticates U_i successfully and computes $K_i=PKS_i \oplus H(TC_i||TS_4)$.

Then GWN computes the accessed sensor node S_j's temporal credential

$TC_j=H(K_{GWN-S}||SID_j)$, $C_{GWN}=H(TID_i||TC_j||TS_5)$ and $PKS_{GWN}=K_i\oplus H(TC_j||TS_5)$, where TS_5 is the timestamp. Finally, GWN sends TS_5, TID_i, C_{GWN}, and PKS_{GWN} to S_j.

Step 3: Upon receiving the message, S_j checks whether the transmission delay is within the allowed time interval ΔT. If $T_j^*- TS_5 > \Delta T$, where T_j^* is the current time, S_j terminates the current session. Otherwise, S_j confirms that the sender of the received message is a legitimate GWN, and computes $K_i=PKS_{GWN}\oplus H(TC_j||TS_5)$. Then S_j generates a timestamp TS_6 and a random key K_j and computes $C_j=H(K_j||TID_i||SID_j||TS_6)$ and $PKS_j=K_j\oplus H(K_i||TS_6)$. Finally, S_j sends SID_j, TS_6, C_j, and PKS_j to GWN.

Step 4: After verifying the timeliness of TS_6, GWN computes $C_j^*=H(K_j||TID_i||SID_j||TS_6)$. If $C_i^*=C_i$, it can confirm that S_j is a legitimate sensor node. GWN generates a new temporary identity TID_i', and computes $D_{GWN}=TID_i'\oplus H(K_i||TS_7)$. After that, GWN replaces TID_i with TID_i' in the verification table and computes $E_{GWN}=H(ID_i||SID_j||TC_i||D_{GWN}||K_j||TS_7)$. Finally, GWN sends SID_j, TS_7, PKS_j, D_{GWN}, and E_{GWN} to U_i.

Step 5: After verifying the timeliness of TS_7, U_i computes $TID_i'=D_{GWN}\oplus H(K_i||TS_7)$, $K_j=PKS_j \oplus H(K_i||TS_6)$ and $E_{GWN}^*=H(ID_i||SID_j||TC_i||D_{GWN}||K_j||TS_7)$. If $E_{GWN}^*=E_{GWN}$, he (or she) can confirm that both S_j and GWN are legitimate. U_i replaces TID_i with TID_i' in the smart card and computes the shared session key $KEY_{ij}=H(K_i\oplus K_j)$. Finally, U_i and S_j can use KEY_{ij} to secure the communications between them.

3.3. Password Update Phase

If a legal user U_i wants to change his password, U_i enters his password PW_i, selects a new password PW_i', computes $PTC_i' = TC_i\oplus RPW_i\oplus H(r||PW_i')$, and replaces PTC_i with PTC_i'.

4. Weakness Analysis On Jiang *Et al.'s* Scheme

This section provides weakness analyses on Jiang et al.'s user authentication scheme. The scheme has bad effect due to the usage of global time synchronization and furthermore, does not provide forward secrecy against the established session key.

4.1. Global Time Synchronization

Due to the collaborative nature of sensor nodes over WSNs, many applications require global time synchronization. Several time synchronization algorithms have been proposed for WSNs [14-17]. However, many of the schemes were not designed with security in mind. Song *et al.* provided vulnerabilities in most existing time synchronization schemes as follows [18]

Masquerade attack: Suppose that a node *A* sends a reference beacon to its two neighboring nodes *B* and *C*. An attacker *E* can pretend to be *B* and exchange wrong time information with node *C*, disrupting the time synchronization process between nodes *B* and *C*.

Replay attack: Using the same scenario in the masquerade attack, attacker *E* can replay node *B*'s old timing packets, misleading node *C* to be synchronized to a wrong time.

Message manipulation attack: In this attack, an attacker may drop, modify, or even forge the exchanged timing messages to interrupt the time synchronization process.

Delay attack: The attacker deliberately delays some of the time messages, *e.g.*, the beacon message in the reference broadcast synchronization scheme in [14], to fail the

time synchronization process. Note that this attack cannot be defended by cryptographic techniques.

Thereby, it is not easy to establish a synchronized time over a WSN and thereby, it is better to not use timestamp based technique in the security schemes. However, the freshness of the message in Juang et al.'s scheme is based on the timestamp, TS_i.

4.2. Forward Secrecy

Jiang et al. argued that their scheme is secure against various attacks and provides good properties. However, this section shows that Jiang et al.'s scheme does not provide forward secrecy, which is necessary property to be supported in the key agreement scheme. We need to have an assumption that attacker could get the system's long term secret keys K_{GWN-U} and K_{GWN-S} as the normal assumption to the forward secrecy. Also, we need another assumption that attacker also could steal and read the verification table stored in the GWN [19].

For the attack, first of all, an attacker could get { TID_i, ID_i, TE_i } from the verification table. After that, the attacker could compute $TC_i'=H(K_{GWN-U}||ID_i||TE_i)$ by using the long term secret key K_{GWN-U} and ID_i and TE_i on the verification table and could derive $K_i'=PKS_i \oplus H(TC_i'||TS_4)$, where PKS_i and TS_4 are from the intercepted message in advance between U_i and GWN. Note that K_i' works as a very important factor for the confidentiality of communication messages. The attacker could derive $K_j'=PKS_j \oplus H(K_i'||TS_6)$, where PKS_j and TS_6 are from the intercepted message in advance between GWN and U_i. Then, the attacker could derive the session key $KEY_{ij}'=H(K_i' \oplus K_j')$ properly. Thereby, Jiang et al.'s scheme does not provide forward secrecy.

5. Proposed Authenticated Key Agreement Scheme

This section proposes an authenticated key agreement scheme with forward secrecy over WSNs to solve the weakness problems in Jiang et al.'s scheme. The aim of the proposed scheme is to remove the usage of the global time synchronization over WSN and is to provide forward secrecy. The proposed scheme is composed of three phases, registration, login and authenticated key agreement, and password update.

5.1. Registration Phase

Let K_{GWN-U} and $PU_{GWN-U}=g^{K_{GWN-U}}$ denote GWN's private key and its corresponding public key, where s is kept secret by GWN and PU_{GWN-U} is stored inside each user's smart card. When a user, U_i wants to be registered to the GWN, U_i proceeds with the following steps through a secure channel.

Step 1: U_i selects a unique identity ID_i and a password PW_i, and generates a random number r. Then he (or she) computes $RPW_i=H(r||PW_i)$ and submits the registration request $\{ID_i, RPW_i\}$ to GWN.

Step 2: Upon receiving the message, GWN rejects the request if ID_i is invalid. Otherwise, GWN computes $TC_i=H(K_{GWN-U}||ID_i)$ and $PTC_i=TC_i \oplus RPW_i$, where K_{GWN-U} is the long term secret key of GWN. Finally, GWN issues a smart card containing { $H(\cdot)$, g, PTC_i, PU_{GWN-U} } to U_i.

Step 3: After receiving the smart card, U_i computes $R=r \oplus ID_i \oplus PW_i$ and stores R into the card.

The registration phase for sensor nodes is described as follows.

Step 1: S_j submits it's identifier SID_j to GWN through a secure channel.

Step 2: Upon receiving the message, GWN computes $TC_j=H(K_{GWN-S}||SID_j)$ and $PU_{GWN-S}=g^{K_{GWN-S}}$, where K_{GWN-S} is the GWN's private key, PU_{GWN-S} is another public key of the GWN for sensor nodes, and TC_j is the temporal credential

for S_j. Finally, GWN sends { TC_j, g, PU_{GWN-S} } to S_j.

Step 3: After receiving the message, S_j stores { TC_j, g, PU_{GWN-S} } as its temporal credential.

5.2 Login and Authenticated Key Agreement Phase

When U_i wants to access services from the GWN, U_i with the smart card proceeds with the following steps

Step 1: U_i inserts his/her smart card into a terminal and enters ID_i and PW_i. The terminal generates chooses a random number K_i and computes $r^*=R\oplus ID_i\oplus PW_i$, $TC_i^*=PTC_i\oplus H(r^*||PW_i)$, $PU_i=g^{K_i}$, $DID_i=PU_{GWN-U}{}^{K_i}\oplus ID_i$ and $C_i=H(ID_i||PU_{GWN-U}{}^{K_i}||TC_i^*)$. Finally, U_i sends { PU_i, DID_i, C_i} to GWN.

Step 2: Upon receiving the message, GWN obtains ID_i^* by computing $ID_i^*=DID_i\oplus PU_i^{K_{GWN-U}}$ and computes $TC_i^*=H(K_{GWN-U}||ID_i)$ and $C_i^*=H(ID_i^*||PU_i^{K_{GWN-U}}||TC_i^*)$. If $C_i^*\neq C_i$, GWN rejects it and sends REJ message to U_i. Otherwise, GWN authenticates U_i successfully.

Then GWN computes the accessed sensor node S_j's temporal credential $TC_j^*=H(K_{GWN-S}||SID_j)$ and $C_{GWN}=H(DID_i||TC_j^*||PU_i)$. Finally, GWN sends {$DID_i$, PU_i, C_{GWN}} to S_j.

Step 3: Upon receiving the message, S_j computes $C_{GWN}^*=H(DID_i||TC_j||PU_i)$ and checks the validity of GWN by verifying $C_{GWN}^*=C_{GWN}$. S_j confirms that the sender of the received message is a legitimate GWN only if the verification is successful. Then S_j generates a random key K_j and computes $PU_j=g^{K_j}$, $C_j=H(SID_j||PU_{GWN-S}{}^{K_j}||TC_j)$, $KEY_{ij}=PU_i^{K_j}$, and $C_{ij}=H(PU_i||PU_j||KEY_{ij})$. Finally, S_j sends {SID_j, PU_j, C_j, C_{ij}} to GWN.

Step 4: After receiving the message, GWN computes $C_j^*=H(SID_j||PU_j^{K_{GWN-S}}||TC_j^*)$. If $C_i^*=C_i$, it can confirm that S_j is a legitimate sensor node. GWN computes $E_{GWN}=H(ID_i||SID_j||TC_i||PU_i||PU_j)$. Finally, GWN sends {$SID_j$, PU_j, C_{ij}, E_{GWN}} to U_i.

Step 5: After receiving the message, U_i computes $E_{GWN}^*=H(ID_i||SID_j||TC_i||PU_i||PU_j)$, $KEY_{ij}^*=PU_j^{K_i}$ and $C_{ij}^*=H(PU_i||PU_j||KEY_{ij}^*)$. If $E_{GWN}^*=E_{GWN}$ and $C_{ij}^*=C_{ij}$, U_i can confirm that both S_j and GWN are legitimate. Finally, U_i and S_j can use KEY_{ij} to secure the communications between them.

5.3. Password Update Phase

Whenever user wants to change his/her password, he/she could perform this phase without helping of GWN. If a legal user U_i wants to change his password, U_i enters his password PW_i and a new password PW_i^*, computes $RPW_i^*=H(r||PW_i)$ and $PTC_i^*=TC_i\oplus RPW_i^*\oplus H(r||PW_i^*)$, and replaces PTC_i with PTC_i^*.

6. Security Analysis

This section provides the security analysis of the proposed scheme focused on no requirement of global time synchronization, providing forward secrecy provision, and secure against password guessing attack, replay attack and user identity guessing attack.

6.1. Global Time Synchronization

The proposed scheme is based on the challenge-response mechanism, which does not use time stamp to provide session freshness. The proposed scheme uses session fresh random numbers K_i and K_j. There is no way an attacker knows them due to the difficulty of the discrete logarithm problems of PU_i and PU_j. Therefore, the proposed scheme is very good to be deployed at WSNs.

6.2. Forward Secrecy

We could have the same assumptions as in Juang et al.'s security analysis that attacker could get the system's long term secret keys K_{GWN-U} and K_{GWN-S} and could steal and read the smart card of U_i. Then, attacker could get { $H(\cdot)$, g, PTC_i, PU_{GWN-U} } from the smart card and { PU_i, DID_i, C_i}, {DID_i, PU_i, C_{GWN}}, {SID_j, PU_j, C_j, C_{ij}} and {SID_j, PU_j, C_{ij}, E_{GWN}} from the intercepted messages among U_i, GWN and S_j. There is only way that the attacker could get the session key KEY_{ij} by knowing K_i or K_j from PU_i and PU_j, respectively. However, they are based on the difficulty of the discrete logarithm problems. Furthermore, even GWN could not compute the session key KEY_{ij} between U_i and S_j neither. Thereby, the proposed scheme could provide forward secrecy.

6.3. Resilience of Password Guessing Attack

We could assume that an attacker could get a legal user's smart card and read the memory on it and any intercepted messages on the process of the scheme run. Then only information the attacker could get are { $H(\cdot)$, g, PTC_i, PU_{GWN-U} } from the memory of the smart card. Additionally, the attacker could get the intercepted messages of { PU_i, DID_i, C_i}, {DID_i, PU_i, C_{GWN}}, {SID_j, PU_j, C_j, C_{ij}} and {SID_j, PU_j, C_{ij}, E_{GWN}} from the previous sessions. Even if the attacker could get the information, it is not possible to derive the password PW_i or the identifier ID_i from them due to the one-wayness of the hash function. There is only PTC_i that the attacker could have, which is related with the password. To find the correct password, the attacker needs to know r, ID_i, and K_{GWN-U} at the same time. However, there is no way that the attacker knows these values. Thereby, it is impossible to perform password guessing attack against the proposed scheme.

6.4. Resilience Of Replay Attack

Suppose that an attacker could intercept the messages { PU_i, DID_i, C_i}, {DID_i, PU_i, C_{GWN}}, {SID_j, PU_j, C_j, C_{ij}} and {SID_j, PU_j, C_{ij}, E_{GWN}} from the previous sessions. Then the attacker tries to replay these messages in a certain session. However, the proposed scheme uses session fresh random numbers K_i or K_j and they effects to each message's integrity check value C. Thereby, it is impossible to perform replay attack against the proposed scheme.

6.5. Resilience of User Identity Guessing Attack

Suppose that an attacker could intercept the messages { PU_i, DID_i, C_i}, {DID_i, PU_i, C_{GWN}}, {SID_j, PU_j, C_j, C_{ij}} and {SID_j, PU_j, C_{ij}, E_{GWN}} from the previous sessions. Then the attacker tries to get certain parameters from these messages, but these messages are treated to be random strings due to the randomness of K_i and K_j and the uniqueness of C_i, C_{GWN}, C_j, and C_{ij}. Therefore, in case of the attacker does not know about these K_i and K_j, the attacker will face to solve the discrete logarithm problem to get the correct identity from DID_i. Hence, the proposed scheme can resist from the user identity guessing attack.

7. Conclusion

This paper has shown the weakness analyses on Jiang et al.'s recent user authentication scheme for WSNs. They were the requirement of global synchronization time and lack of forward secrecy to the session key. Furthermore, we proposed an authenticated key agreement scheme with forward secrecy over WSNs to solve the weaknesses in Jiang et al.'s scheme. The proposed scheme does not use global synchronized time stamp but use session dependent random numbers to provide session freshness. It provides user anonymity and un-traceability by adopting dynamic identifier depending on each session's random numbers. The proposed authenticated key agreement scheme could be used as a security building block for the WSNs security.

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] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: A Survey", Computer Networks **(2002)** Vol. 38, pp. 393-422.
[2] T. Nhon and D. Kim, "Relay Selection Scheme for Hierarchical Wireless Sensor Networks", International Journal of Control and Automation **(2014)** Vol. 7, pp. 147-160.
[3] H. Choi, K. Kim and H. Kim, "Separated Dual-layering Routing Scheme (SDRS) for Hierarchical Wireless Sensor Networks", The Journal of Korea Navigation Institute **(2009)** Vol. 13, pp. 551-558.
[4] H. Kim and S. Lee, "Enhanced Novel Access Control Protocol over Wireless Sensor Networks", IEEE Transactions on Consumer Electronics **(2009)** Vol. 55, pp. 492-498.
[5] J. Hong and N. Kim, "An Efficient Power Management for Wireless Sensor Systems", International Journal of Control and Automation **(2015)** Vol. 8, pp. 275-286.
[6] G. V. Merrett and Y. K. Tan, "Wireless Sensor Networks: Application – Centric Design", INTECH **(2010)**
[7] K. H. M. Wong, Y. Zheng, J. Cao and S. Wang, "A dynamic user authentication scheme for wireless sensor networks", Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing **(2007)** pp. 32-58.
[8] M. Das, "Two-factor user authentication in wireless sensor networks", IEEE Transactions on Wireless Communications **(2009)** Vol. 8, pp. 1086–1090.
[9] D. Nyang and M. Lee, "Improvement of Das's two-factor authentication protocol in wireless sensor networks", IACR eprint Archive **(2009)** 631.
[10] M. Khan and K. Alghathbar, "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks", Sensors **(2010)** Vol. 10, pp. 2450–2459.
[11] T. H. Chen and W. K. Shih, "A robust mutual authentication protocol for wireless sensor networks", ETRI Journal **(2010)** Vol. 32, pp. 704-712.
[12] K. Xue, C. Ma, P. Hong and R. Ding, "A Temporal-Credential-based Mutual Authentication and Key Agreement Scheme for Wireless Sensor Networks", Journal of Network and Computer Applications **(2013)** Vol. 36, pp. 316-323.
[13] Q. Jiang, J. Ma, X. Lu and Y. Tian, "An Efficient Two-factor User Authentication Scheme with Unlinkability for Wireless Sensor Networks", Peer-to-Peer Networking and Applications **(2014)** DOI:10.1007/s12083-014-0285-z.
[14] M. L. Sichitiu and C. Veerarittiphan, "Simple, accurate time synchronization for wireless sensor networks", Proceedings of WCNC 2003 **(2003)** pp. 1266-1273.
[15] S. Ganeriwal, R. Kumar and M. B. Srivastava, "Timing-sync protocol for sensor networks", Proceedings of SenSys 03 **(2003)** pp. 138-149.
[16] M. Maroti, B. Kusy, G. Simon and A. Ledeczi, "The flooding time synchronization protocol", Proceedings of SenSys '04 **(2004)** pp. 39-49.
[17] X. Du, M. Guizani, Y. Xiao and H. Chen, "Secure and Efficient Time Synchronization in Heterogeneous Sensor Networks", IEEE Transactions on Vehicular Technology **(2008)** Vol. 57, pp. 2387-2394.
[18] H. Song, S. Zhu and G. Cao, "Attack-resilient time synchronization for wireless sensor networks", Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems 2005 **(2005)** pp. 765-772.
[19] H. Kim, "AUTH_HOTP-HOTP Based Authentication Scheme over Home Network Environment", Lecture Notes in Computer Science **(2011)** Vol. 6784, pp. 622-637.

Authors

Hyunsung Kim, He 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, He 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.