International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.367-374
http://dx.doi.org/10.14257/ijsia.2015.9.8.32

Enhanced User Authentication Scheme for Wireless Sensor Networks

Hee-Joo Park[*]

[*]*Dept. of Cyber Security, Kyungil University*
hjpark@kiu.ac.kr

Abstract

To provide unlinkability for wireless sensor network, Jiang et al. proposed an efficient two factor user authentication scheme. The scheme provides some good aspects for wireless sensor network. However, this paper shows that Jiang et al.'s scheme has some security weaknesses and proposes an enhanced scheme to remove the weaknesses in Jiang et al.'s scheme. The proposed scheme does not use verification table and synchronized values between communication parties. It provides user anonymity and un-traceability by adopting dynamic identifier depending on each session dependent random number and time stamps. Comparing with the other authentication schemes, the proposed scheme is more secure while maintaining efficiency.

Keywords: *Wireless sensor network, information security, authentication, smart card, password*

1. Introduction

Wireless sensor networks have emerged as a promising computing model for various internet of things applications such as military target tracking and surveillance, natural disaster relief, biomedical health monitoring and hazardous environment sensing. It is usually consisted with a large number of low-cost, battery-powered sensor nodes that are of limited computation and communication capacity [1-5]. While the nodes are left unattended after deployment, they can adaptively form a routing graph and continuously collect data for events of interests and deliver the data to a designated destination. In a hierarchical wireless sensor network, a sensory data is periodically gathered in cluster head and then forwarded to the sink. This method to collect data makes wireless sensor networks very vulnerable to adversary's malicious attacks [1-5].

Users generally want to log in to a wireless sensor network via sink node or gateway nodes (GWNs). However, it is not easy to access real time data from the sensor nodes via GWNs only. Thereby, user needs to take direct access to the sensor nodes to acquire data whenever he (or she) requires. Research into security and privacy focused on wireless sensor networks has been challenging issues to researchers [6-15]. Wireless sensor networks are subject to various attacks including eavesdropping, modification, interception, replay, tracking and identity exposure because of their open and dynamic nature. Especially, it is great important that only authorized user could access sensor nodes and data from them. Furthermore, their communication between user and sensor node should be secured by using session dependent key.

To solve the above mentioned problem, Das proposed a two factor authentication scheme based on smart card and password [10]. After that, series of security schemes are proposed to improve the scheme [11-15]. Recently, Xue et al. proposed a temporal credential based mutual authentication and key agreement scheme for wireless sensor networks, which only involves hash and XOR operations [14]. However, Jiang et al. showed that Xue et al.'s scheme is weak against identity guessing attack, tracking

ISSN: 1738-9976 IJSIA

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 [15].

There are two purposes of this paper: one is to show security weaknesses in Jiang et al.'s authentication scheme and the other is to propose an enhanced authentication scheme to solve the problems in Jiang et al.'s scheme. First of all, this paper shows two weaknesses in Jiang et al.'s scheme focused on effects from the usage of verification table and from the usage of synchronization values. Then, this paper proposes a new enhanced user authentication scheme over wireless sensor networks 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 and time stamps.

The rest of this paper is organized as follows. In Section 2, Jiang et al.'s user authentication scheme is reviewed. Section 3 presents weakness analyses on Jiang et al.'s scheme. An enhanced user authentication scheme is proposed to solve the weakness problems in Jiang et al.'s protocol and to provide the required security aspects in the wireless sensor networks in Section 4. In Section 5, we provide security analysis for the proposed authentication scheme. Section 6 concludes the paper.

2. Jiang *et al.'s* Efficient Two-factor User Authentication Scheme

This section reviews Jiang et al.'s efficient two-factor user authentication scheme with unlinkability for wireless sensor networks [15]. Jiang *et al.'s* user authentication scheme is consisted with three phases: registration phase, login and authentication phase, and password update phase.

2.1. Registration Phase

User registers with GWN. A user who wants to become a new legal 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 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.

2.2 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 $TC_i=H(K_{GWN\text{-}U}||ID_i||TE_i)$ 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 $TC_j=H(K_{GWN\text{-}S}||SID_j)$, $C_{GWN}=H(TID_i||TC_j||TS_5)$ 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 $T_j{*}\text{-}\ TS_5 > \Delta T$, 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.

2.3. 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'.

3. Weakness Analysis on Jiang *et al.'s* User Authentication Scheme

This section provides weakness analyses on Jiang *et al.'s* user authentication scheme. The scheme has bad effect due to the usage of verification table and furthermore, is weak against unsynchronization attack.

3.1 Effect on Verification Table

The stolen-verifier attack is infeasible to a scheme when an attacker cannot impersonate the client to the server if the attacker compromises the server and obtains a verifier of a user. Even if Jiang *et al.'s* user authentication scheme could provide infeasibility, it has potential weakness to expose linkability due to (TID_i, ID_i, TE_i) in the verification table. Thereby, it is recommendable to the security schemes that do not use verification table to check the authenticity of users.

3.2 Necessity to Synchronization

Two parties in Jiang *et al.'s* user authentication scheme require to be synchronized with the temporal identity TID_i. Otherwise, both of them treat the counterpart as the fake one. However, Jiang et al.'s user authentication scheme could easily make it unsynchronized by just changing E_{GWN} with any random bit string of the step 4 message at the login and authentication phase. After GWN replacing TID_i with TID_i' in the verification table, U_i will reject the session due to the validation failure on E_{GWN} check when U_i receives the altered message. Thereby, they are unsynchronized between each other. Thereby, it is recommendable to the security schemes that do not use synchronization mechanism.

4. Enhanced User Authentication Scheme

This section proposes an enhanced user authentication scheme over wireless sensor networks to solve the weakness problems in Jiang et al.'s user authentication scheme. The aim of the proposed scheme is to remove the usage of the verification table in GWN and is not based on the synchronized temporal identity between two parties. The proposed scheme is composed of three phases, registration, login and authentication, and password update.

4.1. Registration Phase

Let $K_{GWN\text{-}U}$ and $PU_{GWN\text{-}U}=g^{K_{GWN\text{-}U}}$ denote GWN's private key and its corresponding public key, where s is kept secret by GWN and $PU_{GWN\text{-}U}$ 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 $TC_i=H(K_{GWN\text{-}U}||ID_i)$ and $PTC_i=TC_i \oplus RPW_i$, where $K_{GWN\text{-}U}$ is the long term secret key of GWN. Finally, GWN issues the card containing $\{ H(\cdot), g, PTC_i, PU_{GWN\text{-}U} \}$ 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 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 $TC_j=H(K_{GWN\text{-}S}||SID_j)$, where $K_{GWN\text{-}S}$ 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.

4.2 Login and Authentication 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 $r^*=R \oplus ID_i \oplus PW_i$, $TC_i^*=PTC_i \oplus H(r^*||PW_i)$, $PKS_i=K_i \oplus H(TC_i^*||TS_1)$, $PU_i=g^{K_i}$, $DID_i=PU_{GWN\text{-}U}{}^{K_i} \oplus ID_i$ and $C_i=H(ID_i||K_i||TC_i^*||TS_1)$, where TS_1 is the timestamp of the smart card. Finally, U_i sends $\{PU_i, DID_i, PKS_i, TS_1, C_i\}$ to GWN.

Step 2 : Upon receiving the message, GWN checks whether the transmission delay is within the allowed time interval ΔT. GWN terminates the current session if T_{GWN}^*- $TS_1 > \Delta T$, which T_{GWN}^* is the current time, and sends REJ message back to U_i; Otherwise, GWN continues to obtain ID_i by computing $ID_i^*=DID_i \oplus PU_i^{K_{GWN\text{-}U}}$ and computes $TC_i^*=H(K_{GWN\text{-}U}||ID_i)$, $K_i^*=PKS_i \oplus H(TC_i^*||TS_1)$ and $C_i^*=H(ID_i^*||K_i^*||TC_i^*||TS_1)$. 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 $TC_j=H(K_{GWN-S}||SID_j)$, $C_{GWN}=H(DID_i||TC_j||TS_2)$ and $PKS_{GWN}=K_i^*\oplus H(TC_j||TS_2)$, where TS_2 is the timestamp of GWN. Finally, GWN sends $\{TS_2, DID_i, C_{GWN}, PKS_{GWN}\}$ 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^*- $TS_2 > \Delta T$, where T_j^* is the current time of S_j, S_j terminates the current session. Otherwise, S_j confirms that the sender of the received message is a legitimate GWN, and computes $K_i'=PKS_{GWN}\oplus H(TC_j||TS_2)$. Then S_j generates a timestamp TS_3 and a random key K_j and computes $C_j=H(K_j||DID_i||SID_j||TS_3)$, $PKS_j=K_j\oplus H(K_i'||TS_3)$ and $KEY_{ij}=H(K_i'\oplus K_j)$. Finally, S_j sends $\{SID_j, TS_3, C_j, PKS_j\}$ to GWN.

Step 4 : After verifying the timeliness of TS_3, GWN computes and $K_j^*=PKS_j\oplus H(K_i^*||TS_3)$ and $C_j^*=H(K_j^*||DID_i||SID_j||TS_3)$. If $C_i^*=C_i$, it can confirm that S_j is a legitimate sensor node. GWN computes $D_{GWN}=ID_i\oplus H(K_i^*||TS_4)$ and $E_{GWN}=H(ID_i||SID_j||TC_i||D_{GWN}||K_j^*||TS_4)$. Finally, GWN sends $\{SID_j, TS_4, PKS_j, D_{GWN}, E_{GWN}\}$ to U_i.

Step 5 : After verifying the timeliness of TS_4, U_i computes $ID_i'=D_{GWN}\oplus H(K_i||TS_4)$, $K_j'=PKS_j \oplus H(K_i||TS_4)$ and $E_{GWN}^*=H(ID_i'||SID_j||TC_i||D_{GWN}||K_j'||TS_4)$. If $E_{GWN}^*=E_{GWN}$, he (or she) can confirm that both S_j and GWN are legitimate. U_i 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.

4.3. 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 $PTC_i' = TC_i\oplus RPW_i\oplus H(r||PW_i')$, and replaces PTC_i with PTC_i'.

5. Security Analysis

This section provides the security analysis of the proposed scheme focused on stolen verifier attack, unsynchronization attack, password guessing attack, replay attack and user identity guessing attack.

5.1 Resilience of Stolen Verifier Attack

Stolen verifier attack means that an attacker steals or modifies the verifiers stored in GWN. In our scheme, GWN does not need to maintain any verifiers in GWN. So, there is no possibility that an attacker could get any useful information for the registered user or modify any information in GWN. Therefore, our scheme is secure against stolen verifier attack.

5.2 Resilience of Unsynchronization Attack

Synchronization is necessary to a security scheme that uses any synchronized value between two communication parties. However, the proposed scheme does not need to keep any synchronization value between any parties in the wireless sensor network. Therefore, our scheme is secure against unsynchronization attack.

5.3 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 $\{ H(\cdot), g, PTC_i, PU_{GWN-U}, R \}$ from the memory of the smart card. Additionally, the attacker could get the intercepted messages of {PU_i, DID_i, PKS_i, TS_1, C_i}, {TS_2, DID_i, C_{GWN}, PKS_{GWN}}, {SID_j, TS_3, C_j, PKS_j}, and {SID_j, TS_4, PKS_j, D_{GWN}, E_{GWN}} from the previous sessions. Even if an 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 $K_{GWN\text{-}U}$ at the same time. However, there is no way that the attacker knows these values. In the other aspect, the attacker could have the identifier related value DID_i. However, the attacker could not get any identifier information from $DID_i=PU_{GWN\text{-}U}^{K_i}\oplus ID_i$ due to the discrete logarithm problem. Thereby, it is impossible to perform password guessing attack against the proposed scheme.

5.4 Resilience of User Identity Guessing Attack

Suppose that an attacker could intercept the messages {PU_i, DID_i, PKS_i, TS_1, C_i}, {TS_2, DID_i, C_{GWN}, PKS_{GWN}}, {SID_j, TS_3, C_j, PKS_j}, and {SID_j, TS_4, PKS_j, D_{GWN}, 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 TS_1, TS_2, TS_3, and TS_4. 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.

6. Conclusion

This paper has shown the weakness analyses on a recent user authentication scheme for wireless sensor networks proposed by Jiang et al. focused on effect on verification table and unsynchronization possibility. Furthermore, we proposed an enhanced user authentication scheme to solve the weaknesses in Jiang *et al.'s* scheme. The proposed scheme does not use verification table and synchronized values between communication parties. It provides user anonymity and un-traceability by adopting dynamic identifier depending on each session dependent random number and time stamps. The proposed user authentication scheme could be used as a security building block for the wireless sensor network security.

References

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

[2] S. He, J. Chen, P. Cheng, J. Gu, T. He and Y. Sun, "Maintaining Quality of Sensing with Actors in Wireless Sensor Network", IEEE Transactions on Parallel and Distributed Systems, vol. 23, **(2012),** pp. 1657-1667.

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

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

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: A Survey", Computer Networks, vol. 38, **(2002),** pp. 393-422

[6] H. Zhu, S. Du, Z. Gao, M. Dong and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay tolerant networks", IEEE Transactions on Parallel and Distributed Systems, vol. 25, **(2014),** pp. 22–32.

[7] Z. Gao, H. Zhu, S. Li, S. Du and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks", IEEE Wireless Communications, vol. 19, **(2012),** pp. 106–112.

[8] H. Li, R. Lu, L. Zhou, B. Yang and X. Shen, "An efficient Merkle tree based authentication scheme for smart grid", IEEE Systems Journal, vol. 8, **(2013),** pp. 655 – 663.

[9] B. Vaidya, J. Rodrigues and J. H. Park, "User authentication schemes with pseudonymity for ubiquitous sensor network in NGN", International Journal of Communication Systems, vol. 23, **(2010),** pp. 1201–1222.

[10] M. Das, "Two-factor user authentication in wireless sensor networks", IEEE Transactions on Wireless Communications, vol. 8, **(2009),** pp. 1086–1090.

[11] D. Nyang and M. Lee, "Improvement of Das's two-factor authentication protocol in wireless sensor networks", IACR eprint Archive, vol. 631, **(2009).**

[12] M. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks", Sensors, vol. 10, **(2010),** pp. 2450–2459.

[13] T. H. Chen and W. K. Shih, "A robust mutual authentication protocol for wireless sensor networks", ETRI Journal, vol. 32, **(2010),** pp. 704-712.

[14] 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, vol. 36, **(2013),** pp. 316-323.

[15] 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, DOI:10.1007/s12083-014-0285-z, **(2014).**

Authors

Hee-Joo Park, He is a professor at the Department of Cyber Security, Kyungil University, Republic of Korea from 2012. He received the B.S. and M.S. degrees in Electrical Engineering from Yeungnam University, Republic of Korea, in 1978 and 1981, respectively. He received the Ph.D. degree in Computer Science and Statistics from Catholic University of Daegu, Republic of Korea, in 1995. He had been a professor from 1982 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include information security, neural network, pattern recognition, ad-hoc network and sensor network.