International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 13 (2017) pp. 3933-3937

Cryptanalysis on Efficient Two-factor User Authentication Scheme with Unlinkability for Wireless Sensor Networks

Hae-Won Choi[1], Hyunsung Kim[2,3,*]

[1]Department of Computer Engineering, Kyungwoon University, Gumi, Kyungbuk 39160, Korea.

[2]Department of Cyber Security, Kyungil University, Kyungsan, Kyungbuk 38428, Korea.

[3]Department of Mathematical Sciences, Chancellor College, University of Malawi, P.O.Box 280, Zomba, Malawi.

*(*Corresponding Author)*

Abstract

To provide secure authentication for wireless sensor networks (WSNs), recently Jiang et al. proposed an efficient two-factor user authentication scheme with unlinkability. They argued that the scheme provides resilience of privileged insider attack, stolen-verifier attack, password guessing attack, weak stolen smart card attack, replay attack, forgery attack, identity guessing attack and tracking attack. Unfortunately, this paper provides cryptanalysis on Jiang et al.'s scheme focused on denial of service attacks on gateway node and user, respectively, and password guessing attack with the assumption on stolen smart card attack feasibility. Furthermore, this paper provides simple directions of the counterpart's solutions on them.

Keywords: Wireless Sensor Networks, Cryptanalysis, Denial of Service Attack, Password Guessing Attack, Unlinkability.

INTRODUCTION

Recent technology advances in integration and miniaturization of physical sensors have enabled a new generation of wireless sensor networks (WSNs) [1-3]. WSNs are formed by a set of sensor nodes for data sensing in remote areas, which has computation and communication capabilities. It is impractical or inconvenient to access real time data from the sensor nodes through base stations or gateway nodes (GWNs) only. For the alternative solution, registered users could collect data from sensors by helping of GWNs [4-5].

Security and privacy are very critical for the success of WSNs. WSNs are subject to various attacks such as eavesdropping, modification, interception, insertion and deletion because their open and dynamic nature of wireless communications. Furthermore, they are weak against physical security attacks due to their unattended property. Thereby, authentication is the basic security service for the WSNs security.

After Das proposed a two-factor authentication scheme using the smart card and passwords as the evidence to corroborate the user identity, a series of schemes were subsequently put forward to improve it [6-10]. After that, Vaidya et al. showed several security weaknesses in [11] under the assumption that a smart card is lost or stolen and the adversary can extracts parameters from the smart card [7-8]. Sun et al. identified that Khan and Alghathar's scheme in [7] still suffers from the GWN impersonation attack, the GWN bypassing attack and the privileged insider attack [12]. To fix the security weaknesses, they also proposed a new user authentication scheme, which was also shown that it could not provide user privacy protection and mutual authentication and session key agreement.

Recently, Xue et al. proposed a temporal-credential based mutual authentication and key agreement scheme for WSNs, which only involves hash and XOR operations [13]. However, Jiang et al. showed that Xue et al.'s scheme is subject to identity guessing attack, tracking attack, privileged insider attack and weak stolen smart card attack. After that, they proposed an improved scheme with untraceability property [14].

There are two purposes of this paper: one is to provide cryptanalysis on Jiang et al.'s user authentication scheme and the other is to provide research direction in brief to solve the problems in Jiang et al.'s scheme. First of all, this paper provides cryptanalysis focused on three vulnerabilities in Jiang et al.'s user authentication scheme focused on denial of service attacks on GWN and user, respectively, and password guessing attack with the assumption on stolen smart card attack feasibility. Then, this paper will also provide future research directions in brief to give a proper direction of the research.

The rest of this paper is organized as follows. Network

configuration is reviewed at Section 2. In Section 3, Jiang et al.'s scheme is reviewed. Section 4 provides cryptanalysis on Jiang et al.'s scheme and brief solution direction on each attack. Finally, section 5 concludes the paper.

NETWORK CONFIGURATION

The network environment for Jiang et al.'s scheme has three main parties as shown in Fig. 1, which aims to harvest sensing data by user. It is a bit more revised for the better understanding of the environment, which is formed with sensor nodes, GWN, and user [15].

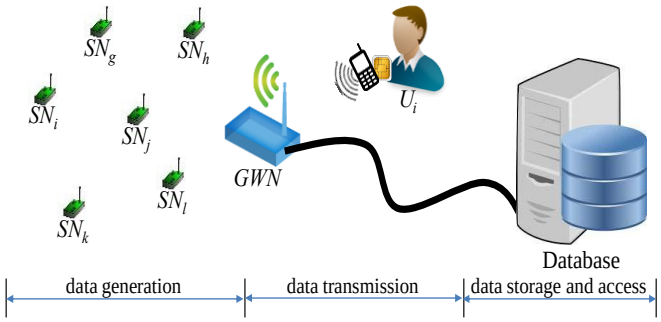

Figure 1: Network configuration for data harvesting based on user

WSN is defined by IEEE 802.15 as a communication standard optimized for low power devices. WSNs have unique requirements in terms of bandwidth, latency, power usage and signal distance. A WSN is consisted with multiple sensor nodes (S_j), a gateway node (GWN) and user (U_i) or database server. WSNs are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location [15]. Main roles of each participant are as follows

- Sensor node (S_j) : S_j is a node in a WSN that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. The main components of S_j are a microcontroller, transceiver, external memory, power source and one or more sensors. Sensors are used by S_j to capture data from their environment. To be services, S_j needs to be registered to GWN. It only allows the access of data via GWN.
- GWN : GWN manages the WSN and aggregates data from distributed sensor nodes. It connects to a wired backbone network or the mobile users. When GWN needs to harvest data from the WSN, it communicates wirelessly to sensor nodes in the network. Traffic between different sensor nodes is relayed by GWN and wired backbone. GWN works as a registration center for the security and privacy.
- User (U_i): U_i works as a mobile data harvesting center, which needs to take mobile computer equipped with wireless communication feasibility. U_i could collect sensing data only via GWN not directly from S_j for the security and privacy reasons. To be serviced for a certain application, U_i needs to be registered to GWN.

JIANG ET AL.'S EFFICIENT TWO-FACTOR USER AUTHENTICATION SCHEME FOR WSN

This section reviews Jiang et al.'s efficient two-factor user authentication scheme with unlinkability for WSNs [14]. Jiang et al.'s authentication scheme is consisted with three phases: registration phase, login and authentication phase and password update phase. Table 1 summarizes the notations used throughout this paper.

Table 1. Notations

Symbol	Description
GWN	WSN gateway node
$H(.)$	Cryptographic hash function
U_i	User i
K_{GWN-U}, K_{GWN-S}	Gateway master keys
KEY_{ij}	Shared session key between U_i and S_j
ID_i	Identity of U_i
PW_i	Password of U_i
S_j	Sensor node j
SID_j	Sensor node j's identity
TE_i	Expiration time of U_i's temporal credential
TS_i	Current timestamp of entity i
P_i, TID_i	Pseudonym of U_i
$\|\|$	Bitwise concatenation
$\oplus$	Bitwise exclusive-or

Registration Phase :

In this phase, the user registers or re-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, a password PW_i and

generates a random value r. Then, U_i 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 $TC_i=H(K_{GWN-U}||ID_i||TE_i)$, $PTC_i=TC_i\oplus RPW_i$. 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 $\{H(.), TID_i, TE_i, PTC_i\}$ 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 only known to GWN 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.

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 then 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 verifies the validity of ID_i and rejects the registration request if ID_i is invalid. Then, GWN checks whether the transmission delay is within the allowed time interval ΔT. T_{GWN}^* is the current time. If $T_{GWN}^*- TS_4>\Delta T$, 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 $TC_i=H(\boldsymbol{K_{GWN-U}}||ID_i||TE_i)$, $C_i^*=H(ID_i||K_i||TC_i||TS_4)$. 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 computes $C_{GWN}^*=H(TID_i||TC_j||TS_5)$. If $C_{GWN}^*\neq C_{GWN}$, S_j rejects it. 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 $C_j=H(K_j||TID_i||SID_j||TS_6)$, $PKS_j=K_j\oplus H(K_i||TS_6)$. 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 $C_j^*=H(K_j||ID_i||SID_j||TS_6)$.If $C_j^*=C_j$, it can confirm that S_j is a legitimate sensor node. GWN generates a new temporary identity TID_i', 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/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.

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'.

CRYPTANALYSIS AND REMARKS ON JIANG ET AL.'S USER AUTHENTICATION SCHEME

This section provides cryptanalysis and simple solutions on Jiang et al.'s user authentication scheme with unlinkability for WSNs in [14]. Jiang et al.'s scheme is weak against denial of service attacks on GWN and user, respectively, and password guessing attack with the assumption on stolen smart card attack feasibility.

Denial of Service Attack on GWN :

Availability makes sure that the network can accomplish basic tasks while under attacks. A variety of attacks can compromise the availability. Denial of service is one of very important attack against availability. Denial of Service is not only for that the attacker attempt to disrupt, subvert or destroy WSNs, but also for any event that diminishes or eliminates WSN's capability to perform its excepted function [16].

As mentioned above, attacker could easily modify any message

over the wireless communication. Jiang et al.'s scheme uses a verification table which stores all user's (TID_i, ID_i, TE_i) information. After that, the information is used in the second step of login and authentication phase. Denial of service attack is feasible against to Jiang et al.'s scheme only if attacker just form a new TID_i^*, which is like a random number, and just switch a legal message $\{TID_i, C_i, PKS_i, TS_4\}$ as $\{TID_i^*, C_i, PKS_i, TS_4\}$. Then GWN needs to check the overall user's information for the authentication check of the message. The attack could be more easy if attacker uses a number of faked messages with different random TID_i^* and the copied timestamp of TS_4, respectively.

The most common approach to cope from this attack is not to use verification table. So, it is recommendable to use checkable TID_i by using GWN's secret information. The only reason of the usage of TID_i is for the unlinkability. However, it needs to be synchronized between user and GWN, which is not easy. Thereby, it would be better to use hashed identity related information with any amplified secret information of GWN.

Denial of Service Attack on User:

This attack is also concerned with availability of the service to user. With the same concept of the GWN case, attacker could easily perform denial of service attack to user.

For the attack, a legal user U_i could perform the password update phase of Jiang et al.'s scheme with PW_i and PW_i'. Then, smart card will compute $PTC_i'=TC_i \oplus RPW_i \oplus H(r||PW_i')$ and replace PTC_i with PTC_i'. U_i could not be serviced by using the login and authentication phase because the computed PTC_i' has $H(K_{GWN\text{-}U}||ID_i||TE_i) \oplus H(r||PW_i) \oplus H(r||PW_i')$. It means that GWN will reject the login request because the computed C_i is $H(ID_i||K_i||TC_i \oplus H(r||PW_i)||TS_4)$ but not $H(ID_i||K_i||TC_i||TS_4)$, which will be rejected at step 2 of the phase by GWN. Thereby, any legal user U_i could not be serviced after performing the password update phase due to the lack of security scheme design concerns.

Even if the scheme computes $PTC_i'=TC_i \oplus H(r||PW_i')$ and replaces PTC_i with PTC_i' for the password update, it is still feasible for the denial of service attack. For the attack, attacker just performs the password update phase of Jiang et al.'s scheme when the legal user temporarily vacates his (or her) seat. Attacker needs to input two random numbers r_1 and r_2. Then, the smart card will think r_1 as PW_i and r_2 as PW_i', respectively, compute $PTC_i'=TC_i \oplus H(r||r_2)$ and replace PTC_i' with PTC_i. When the legal user U_i want to use service, the login and authentication request will be always rejected by GWN due to the same reason as in the previous case.

The most common approach to cope from this attack is to provide ownership check of the smart card. So, it is recommendable to use any validation mechanism of smart card ownership before it is serviced in Jiang et al.'s scheme.

Password Guessing Attack :

Password guessing attack is one of password cracking, which is the process of recovering passwords from data that have been stored in or transmitted by a computer system [17]. A common approach is to try guesses repeatedly for the password and check them against an available cryptographic hash of the password. The purpose of the password guessing attack is to gain unauthorized access to a system.

For the password guessing attack against Jiang et al.'s scheme, we need two assumptions that attacker could get a legal user's session messages and steal the user's smart card as described in [14]. Then the attacker could have $\{TID_i, C_i, PKS_i, TS_4\}$, $\{TS_5, TID_i, C_{GWN}, PKS_{GWN}\}$, $\{SID_j, TS_6, C_j, PKS_j\}$ and $\{SID_j, TS_7, PKS_j, D_{GWN}, E_{GWN}\}$ from the session messages and $\{H(.), TID_i, TE_i, PTC_i, r\}$ from the smart card memory. Actually, the attacker needs to get only the information $\{TID_i, C_i, PKS_i, TS_4\}$ from the first message and $\{PTC_i, r\}$ from the smart card.

Attacker could perform password guessing attack by selecting a new guessed password PW_i^* and computing $TC_i^*=PTC_i \oplus H(r||PW_i^*)$, $K_i^*=PKS_i \oplus H(TC_i^*||TS_4)$ and $C_i^*=H(ID_i||K_i^*||TC_i^*||TS_4)$. After that the attacker checks whether C_i^* is equal to C_i. If the validity fails, the attacker performs the attack with another password candidate. However, the attack is successful if the validation is successful, which means that the attacker could get the password of the registered user.

It is not easy to cope from password guessing attack to an authentication scheme, which needs to design carefully. However, Jiang et al.'s scheme uses combination with random number to amplify the password and provide validation from the transmitted message. Thereby, it needs to add some more information of user related secret to cope from the attack.

CONCLUSION

This paper has provided the cryptanalysis on recent two-factor user authentication scheme with unlinkability for WSNs proposed by Jiang et al., which does not provide security against denial of service attack on GWN, denial of service attack on user and password guessing attack. Furthermore, we provided solution directions on each weakness. This paper's remarks could be very helpful and useful to enhance the security and privacy of user based remote data harvesting applications based on WSNs, which is the very core operation for the success of the applications.

For the future work, it is desirable to devise a uniform framework for the security and privacy for WSNs, which has basic subfunctions of authentication, confidentiality, integrity, access control, nonrepudiation, and privacy.

However, the framework should consider various applications' requirements. Thereby, it needs to be simplified at the very beginning and needs to be expanded by adding the required aspects from various entities on remote data harvesting applications over WSNs.

ACKNOWLEDGEMENTS

Corresponding author is Hyunsung Kim. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598) and (NRF-2017R1D1A1B03035050).

REFERENCES

[1] Kim, H., Ryu, E.-K., and Lee, S.-W., 2013, "Security Considerations on Cognitive Radio based on Body Area Networks for u-Healthcare," Journal of Security Engineering, 10(1), pp. 9-20.

[2] Kim, H., 2014, "Efficient and non-interactive hierarchical key agreement in WSNs," International Journal of Security and Its Applications, 7(2), pp. 159-170.

[3] Kim, H., and Lee, S. W., 2015, "Freshness Preserving Secure Data Gathering Protocol over Wireless Sensor Networks," International Journal of Control and Automation, 8(6), pp. 411-420.

[4] Park, H.-J., 2015, "Enhanced User Authentication Scheme for Wireless Sensor Networks," International Journal of Security and Its Applications, 9(8), pp. 367-374.

[5] Kim, H., and Lee, S. W., 2009, "Enhanced Novel Access Control Protocol over Wireless Sensor Networks," IEEE Transactions on Consumer Electronics, 55(2), pp. 492-498.

[6] Das, M., 2009, "Two-factor User Authentication in Wireless Sensor Networks," IEEE Transactions on Wireless Communications, 8(3), pp. 1086-1090.

[7] Khan, M., and Alghathbar, K., 2010, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks," Sensors, 10(3), pp. 2450-2459.

[8] Chen, T. H., and Shih, W. K., 2010, "A robust mutual authentication protocol for wireless sensor networks," ETRI Journal, 32(5), pp. 704-712.

[9] Yeh, H.-L., Chen, T. H., Liu, P. C., Kim, T. H., and Wei, H. W., 2011, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," Sensors, 11(5), pp. 4767-4779.

[10] Jiang, Q., Ma, Z., Ma, J., and Li, G., 2012, "Security enhancement of robust user authentication framework for wireless sensor networks," China Communications, 9(10), pp. 103-111.

[11] Vaidya, B., Makrakis, D., and Mouftah, H., 2012, "Two-factor mutual authentication with key agreement in wireless sensor networks," Security and Communication Networks, doi:10.1002/sec.517.

[12] Sun, D., Li, J., Feng, Z., Cao, Z., and Xu, Z., 2012, "On the security and improvement of a two-factor user authentication scheme in wireless sensor networks," Personal and Ubiquitous Computing, 17(5), pp. 895-905.

[13] Xue, K., Ma, C., Hong, P., and Ding, R., 2013, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," Journal of Network and Computer Applications, 36(1), pp. 316-323.

[14] Jiang, Q., Ma, J., Lu, X., and Tian, Y., 2015, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," Peer-to-Peer Networking and Applications, 8(6), pp. 1070-1081.

[15] Wikipedia, 2017, https://en.wikipedia.org/wiki/ Wireless_sensor_network.

[16] Gong, Y., Ruan, F., Fan, Z., Hou, J., Mei, P. and Li, P., 2016, "Security Architecture and Requirements for Wireless Sensor Networks," International Journal of Security and Its Applications, 10(8), pp. 295-302. Wikipedia, 2017, https://en.wikipedia.org/wiki/ Password_cracking.