International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 17 (2017) pp. 6962-6969

Weaknesses of Temporal Credential-Based Mutual Authentication with a Multiple-Password Scheme for Wireless Sensor Networks

Younsung Choi
Department of Cyber Security, Howon University, 64, 3-gil, Gunsan, Jeollabuk-do, 54058, Republic of Korea.

Orcid ID: 0000-0002-3185-8670 and Scopus Author ID: 56173148800

Abstract

Wireless sensor networks are significant technologies in various fields. For example, they are used for monitoring dangerous places, medical and environmental monitoring, and military surveillance. Various studies have focused on the authentication scheme for wireless sensor networks. However, it is difficult to achieve perfect security performance and low overhead. Liu et al. proposed a scheme that uses multiple passwords to achieve three-factor security performance and generate a session key between the user and sensor nodes. They claim that security analysis shows that their scheme can withstand related attacks, including a lost password threat. Additionally, the comparison phase shows that Liu et al. scheme involves a relatively small overhead. However, this paper shows that Liu et al.'s scheme is vulnerable to off-line password attack, lack of anonymity, DoS attack, privileged insider attacks, and unclear transmission from the sensor node to the user.

Keywords: Security analysis, Authentication scheme, Wireless sensor networks.

INTRODUCTION

Multi-functional sensor nodes with low battery consumption have been rapidly developed because of development of microelectronic and wireless communication techniques, And the Internet of Things has become increasingly universal so wireless sensor networks (WSNs) are widely used in various application fields such as monitoring military surveillance, nuclear-reactor control systems, vehicle safety systems, and medical monitoring. Various researchers have recently studied the authentication scheme for WSNs, and several investigations have surveyed the security of WSNs [1-5]. These studies have analyzed the main problems faced by WSN security research. The majority of these schemes aim to achieve improved security performance and reducing the overhead. Watro et al. [6] study and suggest a security scheme based on mutual authentication with the RSA cryptosystem and the Diffie—Hellman key agreement. And Nam et al. [7] proposed an anonymous scheme with lightweight computation. They used elliptic curve cryptography to enhance security and user anonymity. Wong et al. [8] suggest security enhanced password-based authentication scheme that only uses hash functions. Moreover, Wong et al's proposed scheme is more efficient than Watro et al.'s schemes. However, M. L. Das et al. showed that their scheme is vulnerable to numerous attacks and proposed a two-factor scheme with a password and a smart card. Although vulnerable to numerous attacks, the scheme prompted other researchers to improve two-factor authentication for WSNs. Xue et al. [9] study temporal credential authentication for WSNs. Their scheme allows the gateway nodes (GW) to issue a temporal credential to users and sensor nodes for mutual authentication. This scheme is efficient for using the hash function and XOR operation. Jiang et al. [10] claim that Xue et al.'s scheme cannot provide an identity guessing, a privileged insider, weak stolen smart card, and tracking attacks. Jiang et al. suggest a two-factor user authentication scheme for WSNs. Though they improve upon the weakness of Xue et al.'s approach, Thereafter, Khan and Alghathbar [11] indicated that M. L. Das's scheme cannot withstand bypassing attacks and is weak on privileged insider attacks. After their study, Choo and Hitchcock provide proof models and allow different options for the key-sharing requirement in formulation [12]. Numerous researchers have worked on fulfilling this requirement; listing these works in this paper is unnecessary.

Liu et al. proposed a temporal credential-based mutual authentication with a multiple-password scheme for WSNs. Comparison with related works shows that Liu et al.'s proposed scheme exhibits improved security performance with low overhead. However, this paper shows that Liu et al.'s scheme is vulnerable to off-line password attack, lack of anonymity, DoS attack, privileged insider attacks, and unclear transmission from sensor node to the user. The remainder of the paper is organized as follows. In section 2, This paper describes Liu et al.'s mutual authentication scheme, and in section 3, This paper point out the weaknesses of Liu et al.'s authentication scheme. Finally, this paper draws conclusions in section 4.

REVIEW OF LIU ET AL.'S MUTUAL AUTHENTICATION SCHEME

This section shows Liu et al.'s a temporal credential-based mutual authentication technique with a multiple-password scheme for *WSNs*. Table 1 shows the notations used in this paper.

Table 1: Notation

Notation	Description	Notation	Description
GW	a gateway node	*U*	the user
SN	the sensor node	*SC*	the smart card of U
A	the adversary	ID_U	the identity of U
ID_{GW}	the identity of GW	ID_{SC}	the identity of SC
ID_{SN}	the identity of SN	PW_U	the password of U
n	the number of passwords	T_U, T_{GW}, T_S	the current timestamp
SK	the session key in the future	V_i	Verification information of U
DID_{SC}, PID_j	the pseudonym of SC and SN, respectively	k_i, k_{GW}, k_i	the secret number for U, GW, and SN, respectively
RPW_i	the protected information for the multiple–password	PTC_i, PTC_j	the protected temporal credential of U and SN,
e_i, PK_{GW}, PK_j	the protected information for the secret number of U, GW, and SN, respectively	σ_U, σ_{GW}	the HMAC output with secret keys k UG and k GS, respectively
(Mac, Ver)	a keyed-hashing for message-authentication codes	*(Enc, Dec)*	symmetric encryption /decryption functions
H(·)	hash function	*K*	bitwise concatenation

According to Choo's research [13], the temporary SK has many advantages relative to using long-term keys. Liu et al.'s scheme not only inherits the excellent properties of Nam et al.'s scheme but also improves upon the weaknesses of their scheme. Because Liu et al.'s scheme uses multiple passwords to replace the Tate-pairing computation and the fuzzy extractor function, it can achieve the same security performance with smaller overhead [14]. Unlike Nam et al.'s scheme, Liu et al. proposed scheme consists of five phases: a registration phase, login phase, authentication and key exchange phase, password update phase, and dynamic-node addition phase[15]. These phases are described in detail, as follows:

Registration Phase

In registration phase, user registers a legal user *U* and sensor nodes *SN*. The registration phase is executed in a secure environment prior to the deployment of *WSNs*. Before registration phase, *GW* assigns the unique identities ID_{SN}, ID_{SC}, and ID_{GW} to *SNs*, *SC*, and *GW*, respectively. And then, *GW* generates a secret number k_{GW}. The hash function H(·), message authentication check scheme *MAC*(·), and *Ver*(·) are stored in *SC*, *GW*, and *SN*. The registration phase is described in detail, as follows:

[Registration phase for legal user] In registration phase for legal user, the user registers the legal user *U* through the following steps.

[Re-LU-1] *U* inserts their SC and inputs their multiple-password PW_1, PW_2 ⋯ PW_n. *U* generates a random secret number K_i and gets the unique identifier ID_{SC}. *U* computes $RPW_i = H(ID_{SC} \| PW_1 \| PW_2 \| \cdots \| PW_n \| n \| k_i)$ and retrieves the timestamp TS_1. Finally, *U* sends (RPW_i, TS_1, ID_{SC}) to *GW*.

[Re-LU-2] After received the message, *GW* checks the freshness of TS_1. If TS_1 do not provide freshness, *GW* rejects the request. If not, *GW* obtains the unique identifier ID_{GW}. And then, *GW* computes $TC_i = H(k_{GW} \| ID_{GW} \| ID_{SC})$, $PTC_i = TC_i \oplus RPW_i$, and $PK_{GW} = PTC_i \oplus k_{GW}$. GW then issues the current timestamp TS_2. Finally, *GW* stores (ID_{GW}, ID_{SC}, PK_{GW}) in verification table and sends (PTC_i, TS_2, ID_{GW}) to *U*.

[Re-LU-3] After received the message, *U* checks the freshness of TS_2. If TS_2 do not provide freshness, *U* rejects the request. If not, *U* computes $e_i = k_i \oplus H(n \| PW_1 \| PW_2 \| \cdots \| PW_n)$, $V_i = H(e_i \| RPW_i \| ID_{SC} \| k_i \| n)$. Finally, *U* stores ($e_i$, V_i, PTC_i, ID_{SC}, ID_{GW}) in the *SC*.

In registration phase for legal user, the adversary *A* cannot restore the sensitive number because of the property of the hash function and the confidentiality properties of the *XOR* operation, as well as the information stored in GW and SC. The random secret numbers k_i and k_{GW} are not stored in *GW*. This phase is shown in Figure 1.

[Registration for sensor node] In registration for sensor node of Liu et al.' scheme, each legal *SN* is required to register in *GW* so that GW can verify the legal *SN* and add the new *SN* to WSNs. Before *SN* registration phase, the legality of *U* should be verified. These steps are described below.

[Re-SN-1] *SN* generates a random secret number k_j and gets the unique identifier ID_{SN}. Then, *SN* computes $PID_j = H(ID_{SN} \| k_j)$, $PK_j = PID_j \oplus k_j$ and replaces ID_{SN} with PID_j. Finally, SN retrieves timestamp TS_3 and sends (PID_j, TS_3) to *GW*.

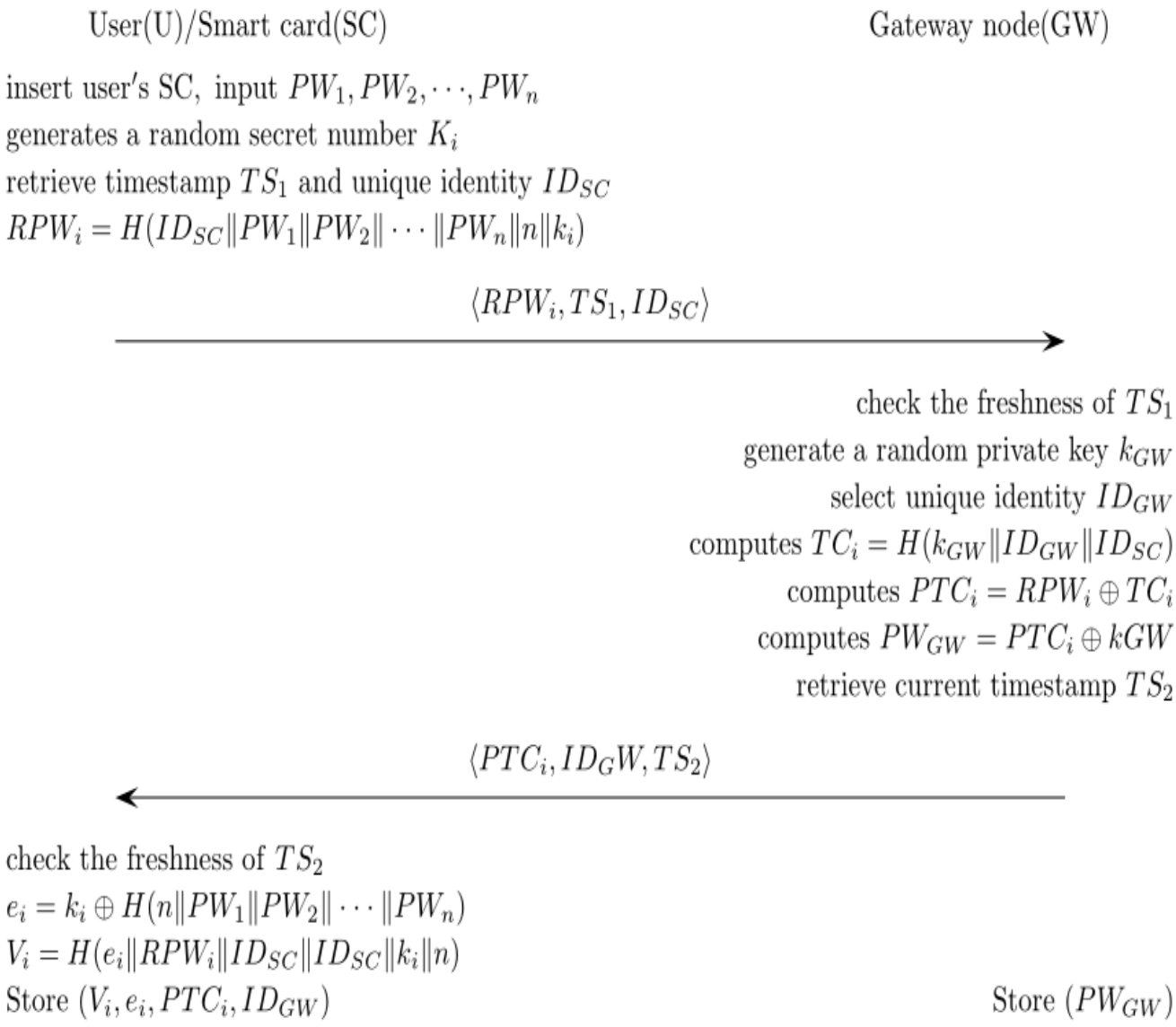

Figure 1: Registration phase for a legal user in Liu et al.'s authentication scheme

[Re-SN-2] After received the message, *GW* checks the freshness of TS_3. If TS_3 is not fresh, *GW* rejects the request. Otherwise, *GW* computes $TC_j = H(k_{GW} \| PID_j)$, $PTC_j = TC_j \oplus PID_j$. Then, *GW* retrieves the timestamp TS_4 and stores PID_j. Finally, *GW* sends (TS_4, PTC_j) to *SN*.

[Re-SN-3] After received the message, *SN* checks the freshness of TS_4. If TS_4 do not provide the freshness, *GW* rejects the request. Otherwise, *SN* stores (PK_j, PTC_j).

Different *SNs* possess different values of PID_j and PK_j, and the random secret number K_j is not stored in *SN*. Therefore, Liu et al.'s scheme can withstand node capture attacks, as discussed in the asecurity analysis section. This phase is shown in Figure 2. After finishing the entire registration scheme, *GW* deletes k_{GW}, *SC* deletes K_i, and *SN* deletes K_j before the *WSNs* are deployed.

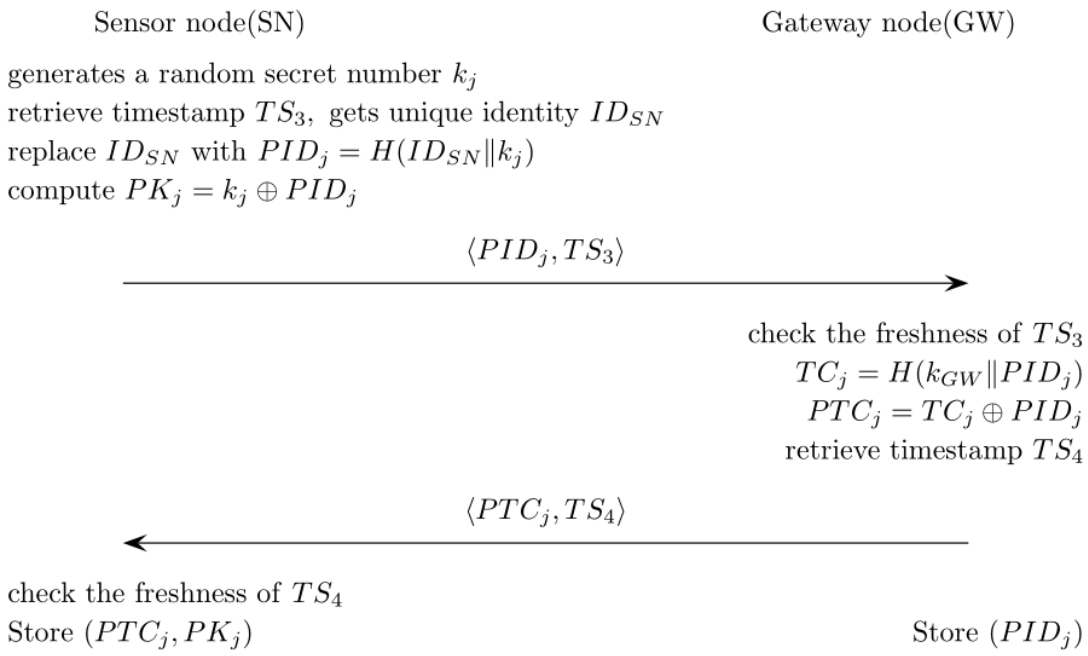

Figure 2: Registration for sensor nodes in Liu et al.'s authentication scheme

Login Phase

The login phase procedure is described in detail and shown in Figure 3 as follows. If *U* attempts to login to WSNs and gets the data from *SN*, the following steps are executed.

[Lo-1] *U* inserts their *SC* and inputs the registered multiple-password PW_1, PW_2, ⋯, PW_n.

[Lo-2] SC gets the unique identifier ID_{SC} and computes $k_i = e_i \oplus H(n \| PW_1 \| PW_2 \| \cdots \| PW_n)$, $RPW_i = H(ID_{SC} \| PW_1 \| PW_2 \| \cdots // PW_n \| n \| k_i)$.

[Lo-3] *SC* checks whether $H(e_i \| RPW_i \| k_i \| n \| ID_{SC})$ is equal to V_i. If it is not same, *SC* rejects the request. Otherwise, *SC* retrieves timestamp TS_1 and computes $TC_i = PTC_i \oplus RPW_i$, $PKS_i = k_i \oplus H(TC_i \| TS_1)$, $C_i = MAC_{ki}(TC_i \| TS_1 \| RPW_i)$, $DID_{SC} = ID_{SC} \oplus H(TS_1 \| ID_{GW})$.

[Lo-4] Finally, *U* sends $(PTC_i, C_j, PKS_i, TS_1, DID_{SC})$ to *GW*.

Authentication and Key Exchange Phase

This paper describes the authentication mechanism through *U*, *GW*, and *SC*. The mechanism achieves mutual authentication and generates the *SK* for future use. The details are presented, as follows:

[Au-Ke-1] After received the message, *GW* checks the freshness of TS_1. If it does not provide the freshness, GW aborts the session. Otherwise, *GW* retrieves the unique identity ID_{GW} and computes $ID_{SC} = DID_{SC} \oplus H(TS_1 \| ID_{GW})$. *GW* obtains the PK_{GW} corresponding to ID_{SC} in the verification table. Then, *GW* computes $k_{GW} = PK_{GW} \oplus PTC_i$, $TC_i = H(k_{GW} \| ID_{GW})$, $RPW_i = PTC_i \oplus TC_i$, and $k_i = PKS_i \oplus H(TC_i \| TS_1)$. *GW* checks whether Ver_{ki} $(TC_i \| TS_1 \| RPW_i, C_i)$ is equal to 1. If it is not equal, *GW* aborts the session. Otherwise, *GW* retrieves timestamp TS_2 and computes $TC_j = H(k_{GW} \| PID_j)$, $PKS_{GW} = k_i \oplus H(TC_j \| TS_2)$, $C_{GW} = MAC_{TCj}(k_i \| TS_2 \| PID_j)$. Finally, *GW* sends $(PID_j, C_{GW}, PKS_{GW}, TS_2)$ to *SN*.

[Au-Ke-2] After received the message, *SN* checks the freshness of TS_2. If it does not provide the freshness, *SN* disconnect the session. Otherwise, *SN* computes $TC_j = PTC_j \oplus PID_j$, $k_i = PKS_{GW} \oplus H(TC_j \| TS_2)$. Then, *SN* checks whether $Ver_{TCj}(k_i \| TS_2 \| PID_j; C_{GW})$ is equal to 1. If it is not equal, SN aborts the session. Otherwise, SN retrieves timestamp TS_3 and computes $k_i = PK_i \oplus PID_j$, $PKS_j = k_j \oplus H(k_i \| TS_3)$, $C_j = MAC_{kj}(k_j \| TS_3 \| k_i)$, and $SK = H(k_i \oplus k_j)$ as the *SK*. Finally, *SN* sends (C_j, PKS_j, TS_3) to U.

[Au-Ke-3] After then, *U* checks the freshness of TS_3. If it does not provide the freshness, *U* aborts the session. Otherwise, the *SC* of *U* computes $k_j = PKS_j \oplus H(k_i \| TS_3)$. Then, *SC* checks whether $Ver_{kj}(k_j \| TS_3 \| k_i; C_j)$ is equal to 1. If it is not equal, SC aborts the session. Otherwise, SC computes $SK = H(k_i \oplus k_j)$ as the SK for future use.

Liu et al claimed that Liu et al's proposed scheme not only achieves mutual authentication and key establishment, but it also checks the integrity of the message. Each message authentication-check function in *U*, *SN*, and *GW* uses different secret encryption keys for secure communication. The authentication and key exchange phase are shown in Figure 3.

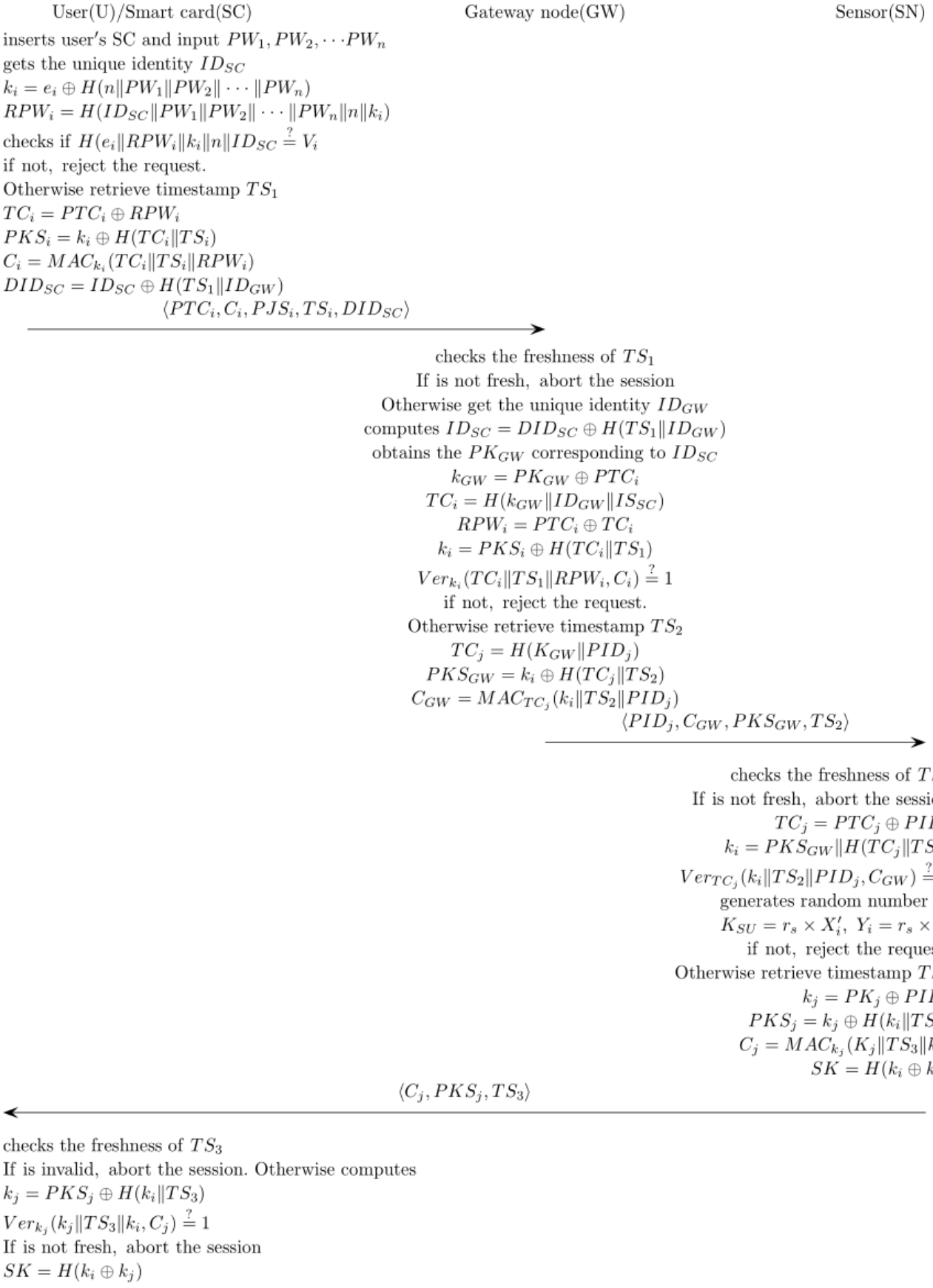

Figure 3: Login, authentication, and key exchange phase in Liu et al.'s authentication scheme

Password-updating Phase

To enhanced the security of phase, *U* needs to change their password periodically. In this phase, Liu et al. propose the password-updating phase to change the password of *U*, and *U* can change the sequence of passwords and the number of passwords. The details of this phase are described below.

[Pu-1] *U* inserts their *SC* and inputs the older multiple-password $PW_1, PW_2, \cdots, PW_n$.

[Pu-2] *SC* gets the unique identifier ID_{SC} and computes $k_i = e_i \oplus H(n \,||\, PW_1 \,||\, PW_2 \,||\cdots||\, PW_n)$, $RPW_i = H(ID_{SC} \,||\, PW_1 \,||\, PW_2 \,||\, \cdots \,||\, PW_n \,||\, n \,||\, k_i)$.

[Pu-3] SC checks whether $H(e_i \,||\, RPW_i \,||\, k_i \,||\, n \,||\, ID_{SC})$ is equal to V_i. If it is not equal, SC rejects the request. Otherwise, SC computes $TC_i = PTC_i \oplus RPW_i$. Then, U inputs their new multiple-password PW_1^{new}, PW_2^{new},$\cdots$, PW_m^{new}

[Pu-4] After inputting the new multiple-password, SC computes $RPW_i^{new} = H(ID_{SC} \,||\, PW_1^{new} \,||\, PW_2^{new} \,||\, \cdots \,||\, PW_m^{new} \,||\, m \,||\, k_i)$, $PTC_i^{new} = TC_i \oplus RPW_i^{new}$, $e_i^{new} = k_i \oplus H(m \,//\, PW_1^{new} \,||\, PW_2^{new} \,||\, \cdots \,||\, PW_m^{new})$, $V_i^{new} = H(e_i^{new} \,||\, RPW_i^{new} \,||\, ID_{SC} \,||\, k_i \,||\, m)$. U sends PTC_i, PTC_i^{new}, and the current TS to GW. Finally, SC replaces (e_i, V_i, PTC_i) with $(e_i^{new}, V_i^{new}, PTC_i^{new})$.

[Pu-5] After receiving PTC_i^{new}, GW checks the freshness of TS. If it is not fresh, GW rejects the request. Otherwise, GW computes $k_{GW} = PK_{GW} \oplus PTC_i$, $PK_{GW}^{new} = PTC_i^{new} \oplus k_{GW}$. Then, GW replaces PK_{GW} with PK_{GW}^{new}.

Dynamic Node Addition Phase

Deploying the new node is inevitable for WSNs because nodes may be lost, exhausted, or destroyed. In node addition phase, Liu et al's proposed scheme allows *U* to add a new *SN* to *WSNs* after deployment. Liu et al.'s scheme strictly requires that only the legal user must execute the dynamic node addition phase. Therefore, Liu et al's authentication scheme must initially verify the legality of *U*. Liu et al. assume that a new sensor node is going to join the *WSNs*, and the following steps must be executed.

[Da-1] First, *U* inserts their *SC* and inputs the registered multiple-password $PW_1, PW_2, \cdots, PW_n$.

[Da-2] And then, *SC* gets the unique identifier ID_{SC} and computes $RPW_i = H(ID_{SC} \,||\, PW_1 \,||\, PW_2 \,||\, \cdots \,||\, PW_n \,||\, n \,||\, k_i)$ and $k_i = e_i \oplus H(n \,||\, PW_1 \,||\, PW_2 \,||\, \cdots \,||\, PW_n)$.

[Da-3] *SC* checks whether $H(e_i \,||\, RPW_i \,||\, k_i \,||\, n \,||\, ID_{SC})$ is equal to V_i. If it does not provide the freshness, *SC* rejects the request. Otherwise, *SC* sends PTC_i and the current *TS* to *GW*.

[Da-4] *GW* checks the freshness of TS. If it is not fresh, *GW* rejects the request. Otherwise, GW computes $k_{GW} = PK_{GW} \oplus PTC_i$ and assigns the new unique identifier ID_{SC}^{new} to SN^{new} via a secure channel.

[Da-5] *SN* executes the registration phase for the sensor node. In this phase, the dynamic addition phase must be executed by a legal *U* that has been authenticated by *SC*. This mechanism can provide to withstand malicious sensor node attacks.

SECURITY WEAKNESS ANALYSIS FOR LIU ET AL.'S MUTUAL AUTHENTICATION SCHEME

Liu et al. proposed a temporal credential-based mutual authentication with a multiple-password scheme for WSNs. Comparison with other related works shows that Liu et al.'s proposed scheme exhibits improved security performance with low overhead. However, this paper analyzes Liu et al.'s mutual authentication scheme and identifies various security weaknesses such as off-line password attack, lack of anonymity, DoS attack, privileged insider attack, and unclear transmission from sensor node to user.

Off-line Password Attack

An attacker can use the power analysis attack to extract information stored in the SC. Therefore, the attacker obtains (e_i, V_i, PTC_i, ID_{GW}) from SC. Additionally, the attacker gets DID_{SC} and TS_1 from the communication between the user and GW. $DID_{SC} = ID_{SC} \oplus H(TS_1 \,||\, ID_{GW})$

$H(e_i \,||\, RPW_i \,||\, k_i \,||\, n \,||\, ID_{SC}) = V_i$, $RPW_i = H(ID_{SC} \,||\, PW_1 \,||\, PW_2 \,||\, PW_3 \,||\, \cdots \,||\, PW_n)$

$\rightarrow H(e_i \,||\, H(ID_{SC} \,||\, PW_1 \,||\, PW_2 \,||\, PW_3 \,||\, \cdots \,||\, PW_n) \,||\, k_i \,||\, n \,||\, ID_{SC}) = V_i$,

$k_i = e_i \oplus H(n \,||\, PW_1 \,||\, PW_2 \,||\, PW_3 \,||\, \cdots \,||\, PW_n)$, $ID_{SC} = DID_{SC} \oplus H(TS_1 \,||\, ID_{GW})$

$\rightarrow H(e_i \,||\, H(ID_{SC} \,||\, PW_1 \,||\, PW_2 \,||\, \cdots \,||\, PW_n) \,||\, e_i \oplus H(n \,||\, PW_1 \,||\, PW_2 \,||\, \cdots \,||\, PW_n) \,||\, n \,||\, ID_{SC}) = V_i$

$\rightarrow H(e_i \,||\, H(DID_{SC} \oplus H(TS_1 \,||\, ID_{GW}) \,||\, PW_1 \,||\, PW_2 \,||\, \cdots \,||\, PW_n) \,||\, e_i \oplus H(n \,||\, PW_1 \,||\, PW_2 \,||\, \cdots \,||\, PW_n) \,||\, n \,||\, DID_{SC} \oplus H(TS_1 \,||\, ID_{GW})) = V_i$

The adversary then knows all of the values in this formula, except for n and $PW_1 \,||\, PW_2 \,||\, \cdots \,||\, PW_n$. Therefore, the adversary can easily determine the user's password PWi by mounting an off-line password guessing attack. Let $|\, \mathcal{D}_{pw} \,|$ denote the number of passwords in $\mathcal{D}_{pw}$. The running time of the aforementioned attack procedure is $\mathcal{O}(|\, \mathcal{D}_{pw} \,| * T_H)$, where T_H is the running time for the hash function; both the password and identity are human-memorable short strings and not high-

entropy keys. That is, they are often chosen from two corresponding dictionaries that are small in size. As $| \mathcal{D}_{pw} |$ are very limited in practice, i.e., $| \mathcal{D}pw | \leq 10^6$, $| \mathcal{D}pw | * n$ is not sufficient to protect off-line password attack. Therefore, the aforementioned attack can be completed in polynomial time. Therefore, the attacker can compute *PW* using an off-line password attack with information taken from a user's smart card and *RPW* in the public channel.

Lack of Anonymity

In Liu et al.'s authentication scheme, an anonymous identity DID_{SC} is used to provide anonymity; however, an attacker can obtain some information (ID_{SC}) using DID_{SC}. The user of Liu et al.'s authentication scheme sends DID_{SC} to GW for authentication via public communication; thus, the attacker can obtain all of the DID_{SC} coming to the server because the user can obtain all of DID_{SC}.

$DID_{SC} = ID_{SC} \oplus H(TS_1 || ID_{GW})$

$\rightarrow ID_{SC} = DID_{SC} \oplus H(TS_1 || ID_{GW})$

The attacker can obtain DID_{SC} and TS_1 via public communication. Additionally, the attacker can get ID_{GW} from a user's smart card by using a power analysis attack because a smart card has e_i, V_i, PTC_i and ID_{GW}. The attacker can also obtain ID_{SC}; thus, Liu et al.'s authentication scheme cannot provide anonymity.

DoS Attack

A DoS attack is an attempt to make a machine or network resource unavailable so legal users cannot use the regular resources of the machine or network. Although the methods, motives, and targets of DoS attacks vary, they generally involve efforts to temporarily or indefinitely interrupt or suspend the services of a host connected to the Internet. In Liu et al.'s authentication scheme, sensor nodes can verify the freshness of a message by using TS_2. Therefore, when an attacker sends a previous message to the sensor node, the sensor node knows whether this message is a current message or a previous message. However, after an attacker gets the previous message $\{ PID_J, C_{GW}, PKS_{GW}, TS_2 \}$, the attacker can resend the message changing only TS_2 to the current timestamp. To check the legitimacy of the message, the sensor node needs to execute various computations, such as the hash function (once), verification function (three times), timestamp checking (once), and exclusive OR (once). The sensor node has limited battery power and computational ability, so it is possible for a sensor node to perform its normal functions when an attacker executes a DoS attack on the sensor node.

Privileged Insider Attacks

In Liu et al.'s authentication scheme, GW has all of the information required to perform authentication between a server and a user. This means that an insider of the server can impersonate all registered users if the insider steals information stored in the server. To impersonate the registered user, an attacker needs to obtain $\{PID_J, C_{GW}, PKS_{GW}, TS_2\}$ and compute the session key SK from PKS_j. This is because GW has all of the information, including a user's ID_{SC} and secret key k_{GW}. To solve this problem, the server should store less login and authentication information and add a secure value between the server and sensor node (due to the security of the session key).

Unclear Transmission from the Sensor Node to the User

In the last phase of Liu et al.'s authentication scheme, a user can check that the regular sensor node sends messages using $Ver_{kj} (k_j || TS_3 || k_i, C_j) = 1$. The user can determine that a message is normal and can use *SK* for the session key: $SK = H(k_i \oplus k_j)$. Thus, the last phase is important to the sensor node and user. However, the sensor node cannot know which user contacted the sensor node. Thus, the sensor node cannot assure the user that the sensor sent a message. This is the reason that the sensor node does not have any information about the user that want to communicate with the sensor node. Thus, it is essential to provide the user's information to the sensor node.

CONCLUSION

Liu et al. proposed a temporal credential-based mutual authentication technique with a multiple-password scheme for WSNs. Through comparison with other schemes, Liu et al. have proven that their scheme exhibits better security performance than the other schemes. However, based on the security analysis of this paper, it is known that Liu et al.'s authentication scheme is susceptible to off-line password attack, lack of anonymity, DoS attack, privileged insider attacks, and unclear transmission from the sensor node to the user.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea grant funded by Korea government (Ministry of Science, ICT & Future Planning) (NRF-2017R1C1B5017492) and this research was supported by financial support of Howon University in 2017

REFERENCES

[1] Yang G, Chen W, Cao X. The security of Wireless sensor networks: Sciences Press; 2010.

[2] Nguyen KT, Laurent M, Oualha N. Survey on secure communication protocols for the Internet of Things.

Ad Hoc Networks. 2015.

[3] Roman R, Alcaraz C, Lopez J, Sklavos N. Key management systems for sensor networks in the context of the Internet of Things. Computers & Electrical Engineering. 2011; 37(2):147–59.

[4] Wang Y, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks. 2006.

[5] Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer networks. 2010; 54(15):2787–805.

[6] Watro R, Kong D, Cuti S-f, Gardiner C, Lynn C, Kruus P, editors. TinyPK: securing sensor networks with public key technology. Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks; 2004: ACM.

[7] Nam J, Choo K-KR, Han S, Kim M, Paik J, Won D. Efficient and Anonymous Two-Factor User Authentication in Wireless Sensor Networks: Achieving User Anonymity with Lightweight Sensor Computation. 2015

[8] Wong KH, Zheng Y, Cao J, Wang S, editors. A dynamic user authentication scheme for wireless sensor networks. Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006 IEEE International Conference on; 2006: IEEE.

[9] Xue K, Ma C, Hong P, Ding R. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. Journal of Network and Computer Applications. 2013; 36 (1):316–23.

[10] Jiang Q, Ma J, Lu X, Tian Y. An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. Peer-to-Peer Networking and Applications. 2014:1–12.

[11] Khan MK, Alghathbar K. Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'. Sensors. 2010; 10(3):2450–9. doi: 10.3390/s100302450 PMID: 22294935

[12] Choo KKR, Hitchcock Y. Security Requirements for Key Establishment Proof Models: Revisiting Bellare—Rogaway and Jeong—Katz—Lee Protocols: Springer Berlin Heidelberg; 2005. 429–42 p.

[13] Choo KKR. On the Security Analysis of Lee, Hwang & Lee (2004) and Song & Kim (2000) Key Exchange / Agreement Protocols. Informatica. 2006; 17(4):467–80

[14] jia C. Wireless sensor network security research [D]: Zhejiang University; 2008.

[15] Liu, Xin, Ruisheng Zhang, and Qidong Liu. "A Temporal Credential-Based Mutual Authentication with Multiple-Password Scheme for Wireless Sensor Networks." PloS one 12.1 (2017): e0170657.