Cryptanalysis of Protocol for Heterogeneous Wireless Sensor Networks for the Internet of Things Environment

Jihyeon Ryu
Department of Computer Science and Engineering
Sungkyunkwan University
Suwon, Korea
jhryu@security.re.kr

Hyoungshick Kim
Department of Computer Science and Engineering
Sungkyunkwan University
Suwon, Korea
hyoung@skku.edu

Youngsook Lee
Cyber Security
Howon University
Gunsan, Korea
ysooklee@howon.ac.kr

Dongho Won*
Department of Computer Science and Engineering
Sungkyunkwan University
Suwon, Korea
dhwon@security.re.kr

***Abstract*—Access and connectivity to everything on the Internet of Things are closely tied to the wireless sensor network environment. In an IoT environment, a user can access a desired single sensor node without first connecting to the gateway node. Chen et al. proposed an efficient and safe protocol in this environment. Unfortunately, their plans have security weakness.**

We describe the protocol proposed by Chen et al. and describe two attack techniques for that protocol. The first is that it is vulnerable to password guessing attacks. Also, their protocols cannot defend against session key attacks. Finally, this paper proves that the target protocol is unsafe.

***Index Terms*—Remote user authentication, Internet of Things, Wireless sensor network**

I. Introduction

Today, there are using so numerous sensor devices. Therefore, research on the sensor device is also actively progressing [1]–[7]. Modern sensor devices are used to automatically and remotely support the sensing process in various living areas. Sensor nodes can be placed in homogeneous or heterogeneous networks. Homogeneous sensor networks use equal frequency resources rather than each sensor node using different frequency domains, while heterogeneous sensor networks use different frequency domains at each sensor node. In practice, homogeneous sensor networks are rarely used because all sensors use different frequency resources.

Many heterogeneous wireless sensor networks are used in conjunction with the Internet of things (IoT), especially. IoT is a technology that provides a connection between all devices by embedding sensors and wired/wireless communication functions of various objects. In the IoT environment, different heterogeneous wireless sensor networks are used, depending on the device used and the purpose of the data being measured. General wireless sensor networks can be used well in IoT environments, but depending on the quality of data required, IoT environments require faster and more secure wireless sensor networks. In particular, we need to provide security protocols to ensure security properties such as confidentiality, integrity and reliability even if data packets are captured and modified in the WSN used for IoT.

This paper deals with Chen et al. [1]'s protocol for heterogeneous wireless sensor networks tailored to the IoT environment. We introduce the relevant work in section II. Section III introduces the prior knowledge used in Chen et al.'s protocol and reviews the entire protocol in section IV. In section V analyzes the protocol and concludes the paper with section VI.

II. Related Work

There are lots of user authentication systems have been proposed for WSNs [1]–[7]. Because authentication is limited in WSNs, it should not be too energy-consuming and easy to steal messages from the middle, making it more secure in terms of security. This section describes how the authentication scheme before Chen et al. [1]'s authentication protocol has changed.

Wong et al. [3] suggested a two-step user authentication method for WSN using only user identity and password. This protocol has a very lightweight structure using hash-based operations. However, Tseng et al. [4] also suggested an imporved protocol because Wong et al. [3]'s method was weak to forgery attack and replay attack. Vaidya et al. [5] found problems with the impersonation and DoS attack of this protocol and suggested an imporved protocol [6]. However, their protocol was still vulnerable to DoS and forgery attacks [7].

Das et al. [8] suggested a three-factor protocol that includes smart card, user identity and password. However, their plans were not feasible for implementation, and after a recent Xue et al. [9] suggested a new protocol, but it proved insecure [10].

In 2014, a lightweight mutual authentication protocol for heterogeneous ad-hoc wireless sensor networks was proposed [11]. The protocol is very fast, using only hash and XOR operations, adjusted to the WSN's resource constraint structure. However, Farash et al. [12] have found problems with disclosure of the session key, no sensor node anonymity, user traceability, so new protocol has been proposed. Regrettably, in 2019, Chen et al. [1] showed that Farash et al. [12]'s protocol

978-1-7281-5453-4/20/$31.00 ©2020 IEEE

is also vulnerable to password guessing attacks and that the anonymity of users and sensor nodes is still not guaranteed and proposed a new protocol.

III. Background

This section describes the properties of the hash function used in the target paper and briefly describes the notation of the target paper [1].

A. Hash function

The hash function encrypts plain text. This encryption process, also known as obfuscation, satisfies the following properties: [13].

1) preimage-resistance: For a given hash result, it is computationally infeasible to find an input that produces that hash result. ex) given that y of unknown input, finding the preimage $x^{'}$ s.t. $h\ (x^{'}) = y$. Functions without this property are weak to preimage attacks.

2) 2nd-preimage resistance: For a given input value, it is computationally infeasible to change the input without changing the hash result of that input. ex) finding a 2nd-preimage $x^{'} \neq x$ s.t. $h\ (x) = h\ (x^{'})$. Functions without this property are weak to second-preimage attacks.

3) collision resistance: Finding two inputs that produce the same hash result must be calculationally infeasible. ex) any two different inputs x, $x^{'}$ that after hashing get same output like $h\ (x) = h\ (x^{'})$.

B. Notations

In this paper, we use the following variables:

U_i	: i-th user
GWN	: Gateway node
S_j	: j-th sensor
$\mathcal{A}$	: The malevolent attacker
ID_i	: Identity of the i-th user
PW_i	: Password of the i-th user
SID_j	: The j-th sensor node's identity
X_{GWN}	: Gateway secret key
X_{GWN-U_i}	: The secret key shared with i-th user and gateway node
X_{GWN-S_j}	: The secret key shared with the j-th sensor and gateway node
SC	: Smart card
SK	: Session key between sensor and user
$X? = Y$	: Comparing value X with Y
$h\ (\cdot)$	: Cryptographic hash function
$X \parallel Y$	: Concatenation
$\oplus$	: A binary bit-wise XOR operation

IV. Review of the target scheme

A. Registration Phase

The registration phase consists of two phases: (1) user registration phase, and (2) sensor registration phase. In the registration phase, necessary variables are exchanged and stored. In this way, variables necessary for the login and authentication process are issued and stored in advance.

1) User registration phase: In the user registration phase, when the user logs in, the gateway node encrypts the necessary information and receives it on SC. Finally, the user can log in later with the information stored on SC. The detailed steps are as follows:

1) User U_i makes ID_i and PW_i, selects a random number r_i. Next, U_i calculates $MP_i = h(r_i \parallel PW_i)$ and sends the information $\{ID_i, MP_i\}$ to GWN.
2) Gateway node GWN calculates $e_i = h(MP_i \parallel ID_i)$, $d_i = h(ID_i \parallel X_{GWN})$, $g_i = h(h(X_{GWN}) \oplus h(e_i \oplus ID_i \oplus d_i)) \oplus h(MP_i \parallel d_i)$, $f_i = d_i \oplus h(MP_i \parallel e_i)$, $SC = \{e_i, f_i, g_i\}$. And GWN sends the SC to U_i.
3) User gets the SC and inserts r_i into SC. Finally, SC stores the information $\{r_i, f_i, e_i, g_i\}$.

2) Sensor registration phase: In the sensor registration phase, S_j encrypts GWN's secret key to be used with GWN to the GWN and stores it in the memory. The stored information is then used for user login:

1) S_j selects a random r_j and calculates $MN_j = X_{GWN-S_j} \oplus r_j$. Also computes $MP_j = h(X_{GWN-S_j} \parallel r_j \parallel SID_j \parallel T_1)$. And S_j sends the information $\{SID_j, MP_j, MN_j, T_1\}$ to gateway node GWN.
2) GWN checks the time-stamp T_1 that $|T_1 - T_c| < \triangle T$ and calculates $r_j^{'} = MN_j \oplus X_{GWN-S_j}$. After obtaining $r_j^{'}$, confirms $MP_j^{'}? = h(X_{GWN-S_j} \parallel r_j^{'} \parallel SID_j \parallel T_1)$. Then $y_j = h(X_{GWN}) \oplus r_j$, $x_j = h(SID_j \oplus X_{GWN} \oplus y_j)$, $e_j = x_j \oplus X_{GWN-S_j}$, $d_j = h(X_{GWN} \parallel 1) \oplus h(X_{GWN-S_j} \parallel T_2)$ and $f_j = h(x_j \parallel d_j \parallel X_{GWN-S_j} \parallel T_2)$ are calculated. After all operations have been completed, the GWN sends the following information $\{e_j, f_j, d_j, T_2\}$ to S_j.
3) S_j checks the time-stamp T_2 that $|T_2 - T_c| < \triangle T$ and computes $x_j = e_j \oplus X_{GWN-S_j}$. S_j confirms $f_j? = h(x_j \parallel d_j \parallel X_{GWN-S_j} \parallel T_e)$ after obtaining x_j. And then $h(X_{GWN} \parallel 1) = d_j \oplus h(X_{GWN-S_j} \parallel T_2)$ and stores x_j, $h(X_{GWN} \parallel 1)$ into a memory.

B. Login and Authentication Phase

In this phase, U_i accesses S_j via ID_i, PW_i and SC. The sensor node checks whether the user is correct and access the gateway node. Gateway node shares session key to the user after the authentication process. The detailed procedure is as follows:

1) User U_i enters his/her smartcard SC into a terminal and inserts his/her $ID_i^{'}$ and $PW_i^{'}$. SC calculates $MP_i^{'} = h(r_i \parallel PW_i^{'})$ and checks $e_i? = h(MP_i^{'} \parallel ID_i^{'})$. After that, U_i calculates $d_i = f_i \oplus h(MP_i^{'} \parallel e_i)$, $h(X_{GWN}) = g_i \oplus h(MP_i^{'} \parallel d_i)$, $M_{12} = h(e_i \oplus ID_i \oplus d_i)$, $M_1 = ID_i \oplus h(h(h(X_{GWN}) \oplus M_{12}) \parallel T_1)$. And he/she chooses K_i and computes $M_2 = K_i \oplus h(d_i \parallel T_1)$, $M_3 = h(M_1 \parallel M_2 \parallel K_i \parallel T_1)$. Finally, user U_i sends $\{M_1, M_2, M_3, M_{12}, T_w\}$ to sensor node S_j.
2) S_j checks the time-stamp T_1 that $|T_1 - T_c| < \triangle T$ and if satisfied, computes $ESID_j = SID_j \oplus h(h(X_{GWN} \parallel 1) \parallel T_2) \oplus y_j$. In that order, sensor chooses a random

K_j and computes $M_4 = h(x_j \parallel T_1 \parallel T_2) \oplus K_j$, $M_5 = h(SID_j \parallel M_4 \parallel T_1 \parallel T_2 \parallel K_j)$. Lastly, S_j broadcasts the message $\{M_1$, M_2, M_3, M_{12}, T_1, T_2, $ESID_j$, M_4, $M_5\}$ to GWN.

3) GWN checks the time-stamp T_2 that $|T_2 - T_c| < \triangle T$ and if satisfied, calculates $SID_j^{'} = ESID_j \oplus h(h(X_{GWN} \parallel 1) \parallel T_2)$, $x_j^{'} = h(SID_j^{'} \parallel X_{GWN})$ and $K_j^{'} = M_4 \oplus h(x_j^{'} \parallel T_1 \parallel T_2)$. GWN then checks the message $M_5? = h(SID_j^{'} \parallel M_4 \parallel T_1 \parallel T_2 \parallel K_j^{'})$. If so, GWN computes $ID_i^{'} = M_1 \oplus h(h(X_{GWN} \oplus M_{12}) \parallel T_1)$, $d_i^{'} = h(ID_i^{'} \parallel X_{GWN})$ and $K_i^{'} = M_2 \oplus h(d_i^{'} \parallel T_1)$. And also GWN confirms the message $M_3? = h(M_1 \parallel M_2 \parallel K_i^{'} \parallel T_1)$. If M_3 is correct, perform the following operations in sequence: $M_6 = K_j^{'} \oplus h(d_i^{'} \parallel T_3)$, $M_7 = K_i^{'} \oplus h(x_j^{'} \parallel T_3)$ and $M_8 = h(M_6 \parallel d_i^{'} \parallel T_3)$. And finally, GWN also calculates $M_9 = h(M_7 \parallel x_j^{'} \parallel T_3)$. If all operations are over, GWN sends message $\{M_6$, M_7, M_8, M_9, $T_3\}$ to S_j.
4) S_j checks the time-stamp T_3 that $|T_3 - T_c| < \triangle T$ and $M_9? = h(M_7 \parallel x_j \parallel T_3)$. If satisfied, S_j computes $K_i^{'} = M_7 \oplus h(x_j \parallel T_3)$, $SK = h(K_i^{'} \oplus K_j)$. Finally, S_j also calculates $M_{10} = h(SK \parallel M_6 \parallel M_8 \parallel T_3 \parallel T_4)$. When everything is done, S_j sends $\{M_6$, T_4, M_8, M_{10}, $T_3\}$ to user U_i.
5) The user U_i examines the time-stamp T_4 that $|T_4 - T_c| < \triangle T$ and $M_8? = h(M_6 \parallel d_i \parallel T_3)$. User U_i calculates $K_j^{'} = M_6 \oplus h(d_i \parallel T_3)$ and $SK = h(K_j^{'} \oplus K_i)$. Finally, user U_i confirms the message $M_{10}? = h(SK \parallel M_6 \parallel M_8 \parallel T_3 \parallel T_4)$.

C. Password Change Phase

The user changes the password through the following process.

User U_i inserts his/her SC into a terminal and inputs his/her ID_i, PW_i and new password $PW_i^{'}$. And smartcard SC computes $MP_i = h(r_i \parallel PW_i)$ and confirms $e_i? = h(MP_i \parallel ID_i)$. If so then $d_i = f_i \oplus h(MP_i \parallel d_i)$, $MP_i^{'} = h(r_i \parallel PW_i^{'})$, $e_i^{'} = h(MP_i^{'} \parallel ID_i)$, $f_i^{'} = d_i \oplus h(MP_i^{'} \parallel e_i^{'})$ and $g_i^{'} = h(x_{GWN}) \oplus h(MP_i^{'} \parallel d_i)$. And changes variables $\{e_i$, f_i, $g_i\}$ to $\{e_i^{'}$,$f_i^{'}$, $g_i^{'}\}$.

V. Security Weakness of Chen et al.'s Scheme

We have identified two vulnerabilities in Chen et al.'s protocol. The details are as follows:

A. Password Guessing Attack

The attacker $\mathcal{A}$ can perform a password guessing attack through the information captured during the registration process of the user. The details are as follow:

1) In user registration phase, attacker $\mathcal{A}$ steals MP_i.
2) And attacker $\mathcal{A}$ also can get r_i in U_i's smartcard SC.
3) Finally, attacker can guess PW_i using the equation $MP = h(r_i \parallel PW_i)$.

As a result, the attacker $\mathcal{A}$ can guess the user U_i's password PW_i through the user's smartcard information and the registration request message.

B. Session Key Attack

The attacker $\mathcal{A}$ can extract the session key from the information stolen during the user registration process and user authentication process. $\mathcal{A}$ can attack by the following steps.

1) In user registration phase, attacker $\mathcal{A}$ steals MP_i.
2) And attacker $\mathcal{A}$ also can get e_i, f_i in U_i's smartcard SC.
3) The attacker $\mathcal{A}$ can compute $d_i = f_i \oplus h(MP_i \parallel e_i)$ through the obtained MP_i, e_i and f_i.
4) $\mathcal{A}$ eavesdrops the login request message M_2, T_1 and calculates $K_i = M_2 \oplus h(d_i \parallel T_1)$.
5) $\mathcal{A}$ eavesdrops the authentication message M_6, T_3 and calculates $K_j = M_6 \oplus h(d_i \parallel T_3)$.
6) Finally, the attacker $\mathcal{A}$ recovers the session key of U_i and S_j as $SK = h(K_i \oplus K_j)$

This result shows that target paper scheme does not secure.

VI. Conclusion

Chen et al. suggested a new protocol for heterogeneous wireless sensor network tailored for IoT. However, we found that this protocol is very weak to password guessing attack and session key attack. We described these attack methods and proved a problem with using Chen et al.'s protocol. In future work, new protocols are needed to improve this protocol.

Acknowledgment

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2019R1A2C1010159)

References

[1] Y. Chen, J. S. Chou, H. S. Wu, "Improved on an efficient user authentication scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," Journal of Engineering Technology, 8(1), pp. 143–157, 2019.

[2] J. Ryu, H. Lee, H. Kim, D. Won, "Secure and Efficient Three-Factor Protocol for Wireless Sensor Networks," Sensors, 18(12), 4481, 2018.

[3] K. H. Wong, Y. Zheng, J. Cao, S. Wang, "A dynamic user authentication scheme for wireless sensor networks," In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), 1(8), 2006.

[4] H. R. Tseng, R. H. Jan, W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," In IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference, pp. 986–990, 2007.

[5] B. Vaidya, J. S Silva, J. J. Rodrigues, "Robust dynamic user authentication scheme for wireless sensor networks," In Proceedings of the 5th ACM symposium on QoS and security for wireless and mobile networks, pp. 88–91, 2009.

[6] B. Vaidya, M. Chen, J. J. Rodrigues, "Improved robust user authentication scheme for wireless sensor networks," In 2009 Fifth International Conference on Wireless Communication and Sensor Networks (WCSN), pp. 1–6, IEEE, 2009.

[7] Y. Faye, I. Niang, H. Guyennet, "A user authentication-based probabilistic risk approach for Wireless Sensor Networks," In 2012 International Conference on Selected Topics in Mobile and Wireless Networking, IEEE, pp. 124–129, 2012.

[8] A. K. Das, P. Sharma, S. Chatterjee, J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," Journal of Network and Computer Applications, 35(5), pp. 1646-1656, 2012.

[9] K. Xue, C. Ma, P. Hong, R. Ding, "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, 2013.

[10] D. He, N. Kumar, N. Chilamkurti, “A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks,” In International Symposium on Wireless and pervasive Computing (ISWPC), pp. 1–6. IEEE, 2013.

[11] M. Turkanovi, B. Brumen, M. Hlbl, “A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion,” Ad Hoc Networks, 20, pp. 96–112, 2014.

[12] M. S. Farash, M. Turkanovi, S. Kumari, M. Hlbl, “An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment,” Ad Hoc Networks, 36, pp. 152–176, 2016.

[13] J. Katz, A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, “Handbook of applied cryptography,” CRC press, 1996.