https://doi.org/10.33778/kcsa.2021.21.1.055

Security Improvement of User Authentication Protocol for Heterogeneous Wireless Sensor Networks for the Internet of Things Environment

Young sook Lee*

ABSTRACT

Recently, the use of sensor devices is gradually increasing. As various sensor device emerge and the related technologies advance, there has been a dramatic increase in the interest in heterogeneous wireless sensor networks (WSNs). While sensor device provide us many valuable benefits, automatically and remotely supported services offered and accessed remotely through WSNs also exposes us to many different types of security threats. Most security threats were just related to information leakage and the loss of authentication among the involved parties: users, sensors and gateways. An user authentication protocol for wireless sensor networks is designed to restrict access to the sensor data only to user. In 2019, Chen et al. proposed an efficient user authentication protocol. However, Ryu et al. show that it's scheme still unstable and inefficient. It cannot resist offline password guessing attack and session key attack. In this paper, we propose an improved protocol to overcome these security weaknesses by storing secret data in device. In addition, security properties like session-key security, perfect forward secrecy, known-key security and resistance against offline password attacks are implied by our protocol.

Heterogeneous Wireless Sensor Networks 환경에서의 안전한 사용자 인증 프로토콜

이 영 숙*

요 약

최근 센서를 이용한 장치들의 사용은 증가추세이다. 이런 센서 장치들은 이종무선 센서네트워크 환경에서 최신 기술들과 연관 지어 폭발적으로 증가하고 있다. 이런 환경에서 센서디바이스의 사용은 우리에게 편리함을 제공하기는 하나 여러 형태의 보안위협이 도사리고 있는 실정이다. 무선센서네트워크를 이용하여 원격으로 접속하여 제공받는 서비스에 존재하는 보안위협 중 대부분은 전송되는 정보의 유출과 사용자, 센서, 게이트웨이 사이의 인증에 대한 손실이 대부분이다. 2019년 Chen 등이 이종무선 센서 네트워크에 안전한 사용자 인증 프로토콜을 제안하였다. 그러나 Ryu 등이 제안한 논문에서 그들이 제안 프로토콜은 password guessing attack과 session key attack에 취약하다는 것을 주장하였다. 본 논문은 이전에 제안된 논문의 취약점을 개선하여 더욱 안전하고 효율적인 사용자 인증 프로토콜을 제안하였다.

Key words : User Authentication Protocol, Heterogeneous, Off-line Password guessing attack, Session Key

접수일(2021년 2월 26일), 게재확정일(2021년 03월 31일)

* 호원대학교 IT소프트웨어보안학과

1. Introduction

Recently, the use of sensor devices is gradually increasing. As various sensors emerge and the related technologies advance, there has been a dramatic increase in the interest in wireless sensor networks(WSNs) [1-9]. Today, billions of physical, chemical and biological sensors are being deployed into various types of WSNs for numerous applications, including military surveillance, wildlife monitoring, vehicular tracking and healthcare diagnostics[14]. Sensor nodes can be placed in homogeneous or heterogeneous networks. Homogeneous sensor networks use equal frequency resources, 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[12].

Sensor device provide us many valuable benefits, automatically and remotely supported services offered and accessed remotely through WSNs. However, providing an application service in a WSN environment introduces significant security challenges to be addressed among the involved parties: users, sensors and gateways. One important challenge is to achieve authentication between users and sensors (via the assistance of a gateway), thereby preventing illegal access to the sensor data and their transmissions[14]. User authentication in heterogeneous WSNs is more challenging to achieve than in traditional networks due to the sensor network characteristics, such as resource constraints, unreliable communication channel and unattended operation[11].

2. Related Work

User authentication protocols for WSNs(Wireless Sensor Networks) are designed to address these security challenges [1-9], and are a subject of active research in network security and cryptography. Generally speaking, the design of user authentication schemes for WSNs is error-prone, and their security analysis is time-consuming.

In 2009, Das proposed a smart-card-based user authentication scheme for wireless sensor networks; throughout the paper, we call such a scheme a SUA-WSN scheme. Since then, the design of SUA-WSN schemes has received significant attention from researchers due to their potential to be widely deployed, and a number of solutions offering various levels of efficiency and security have been subsequently proposed[10, 11]. One important security requirement for SUA-WSN schemes is to ensure that only a user who is in possession of both a smart card and the corresponding password can pass the authentication check of the gateway and gain access to the sensor network and data. A SUA-WSN scheme that meets this requirement is said to achieve two-factor security. To properly capture the notion of two-factor security, the adversary against SUA-WSN schemes is assumed to be able to either extract the sensitive information in the smart card of a user possibly via a side-channel attack or learn the password of the user through shoulder-surfing or by exploiting a malicious card reader, but not both. Clearly, there is no means to prevent the adversary from impersonating a user if both the password of the user and the information in the smart card are disclose[11, 12, 13, 14]

Chen et al proposed an efficient user authentication protocol using smart card in 2019[1]. However, in [12], Ryu et al. uncover Chen et al.'s protocol also showed weaknesses and protocol's progress was incomplete. They show that

it's protocol still unstable and inefficient. It cannot resist offline password guessing attack and session key attack.

Now, we proposed enhanced Chen et al.'s protocol for user authentication environment. This study proposes a security enhanced remote user authentication protocol and provides a security analysis and formal analysis. Finally, the efficiency analysis reveals that the proposed protocol can protect against several possible types of attacks with only a slightly high computational cost.

3. The proposed a User Authentication Protocol for Heterogeneous Wireless Sensor Networks

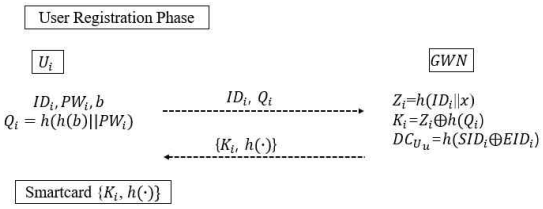
This section presents our user authentication protocol for heterogeneous wireless sensor networks. The scheme participants include a remote user, a sensor, and gateway node. For simplicity, we denote the remote user by U_i, the server by S_j, and gateway node by GWN. Our protocol consists of three phases: registration phase, login phase, and authentication phase. The registration phase is performed only once per user when a new user registers itself. The authentication phase is carried out whenever a user wants to gain access to the remote server and the gateway node. The system parameters listed in Table 1 are assumed to have been established in advance before the scheme is used in practice.

<Table 1> Notation

	i-th user
S_j	j-th server
ID_i	identity of an entity U_i
PW_i	password of an entity U_i
SID_j	identity of a server S_j
GWN	gateway node
$,y$	the secret key of the gateway node
T_i	timestamp of current time i
ΔT	the maximum allowed time interval for transmission delay
$h()$	one-way hash function
$\|\|$	concatenation operation
	XOR operation

3.1 Registration Phase

This is the phase where a new registration of a user and a sensor takes place. The registration phase consist of two phase : (1) user registration phase, and (2) sensor registration phase. The user registration phase and sensor registration phase are described in Figure1 and Figure2 respectively. The registration proceeds as follows:



(Figure 1) User Registration Phase

(1) User Registration Phase

Step 1. User U_i chooses its identity ID_i, password TPW_i, and random number b. U_i computes $Q_i = h(h(b)\|PW_i)$. Then sends the registration request message $\langle ID_i, Q_i \rangle$ to remote sensor S_j via a secure channel.

Step 2. Upon receiving the request $\langle ID_i, Q_i \rangle$, remote gateway node GWN computes

$Z_i = h(ID_i\|x)$,

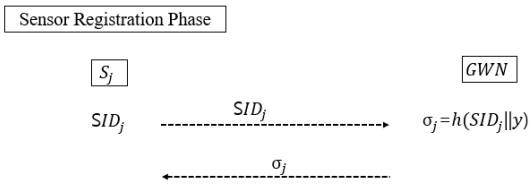
$K_i = Z_i \quad h(Q_i)$,.

Then, the gateway node issues a smart card and stored { , h(·)} into a smart card and sends it to U_i via a secure channel.

(2) Sensor Registration Phase

Step 1. The sensor S_j chooses its identity SID_j and sends SID_j to the gateway node GWN via a secure channel.

Step 2. Upon receiving the request $\langle SID_j \rangle$, GWN computes $_j = h(SID_j \| y)$ and then sends σ_j to the sensor nodes S_j via a secure channel.



(Figure 2) Sensor Registration Phase

3.2 Login and Authentication Phase

This phase is carried out whenever the user wants to gain access to the sensor S_j. The sensor node S_j checks whether the user is in correct and accesses the gateway node. The sensor node share session key to the user after the authentication process. This scheme carry the login phase and authentication phase out as shown in Figure 3 and in Figure 4, respectively.

3.2.1 Login Phase

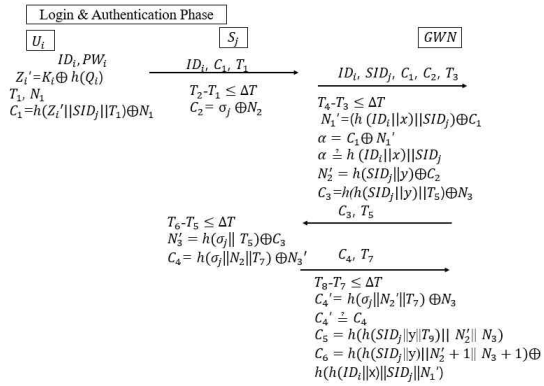
Step 1. U_i inserts its smart card into card reader, and inputs ID_i, PW_i.

Step 2. Smart card continually picks up rhe current timestamp T_1 and generates the random nonce N_1, and computes

$Z_i' = K_i \quad h(Q_i)$,

$C_1 = h(Z_i' \| SID_j \| T_1) \quad N_1$.

Step 3. After that, U_i sends $<ID_i, C_1, T_1>$ to the sensor S_j via public channel.



(Figure 3) Login Phase

3.2.2 Authentication Phase

With the three login request message $\langle ID_i, C_1, T_1 \rangle$, the scheme enters the authentication phase during which S_j and GWN perform the following steps:

Step 1. When the login request arrives $\langle ID_i, C_1, T_1 \rangle$, the sensor S_j retrieves the current timestamp and verifies the freshness of the U_i's timestamp T_1 using $T_2 - T_1) \quad \Delta T$. The sensor S_j aborts if the check T_1 fail. Otherwise, generates a random number N_2 and retrieves the current timestamp T_3. The sensor S_j computes $C_2 = \sigma_j \quad N_2$.

After that, the sensor S_j sends the message $\langle ID_i, SID_j, C_1, C_2, T_3 \rangle$ to the gateway node GWN.

Step 2. After receiving $\langle ID_i, SID_j, C_1, C_2, T_3 \rangle$ from S_j, the gateway node GWN obtains the current timestamp T_4 and computes

$N_1' = (h(ID_i \| x) \| SID_j) \quad C_1$,

$\alpha = C_1 \quad N_1'$,

$N_2' = h(SID_j \| y) \quad C_2$.

GWN verifies that (1) $T_4 - T_3 \quad \Delta T$ (2) α equals $h(ID_i \| x) \| SID_j$. If both of these conditions are

hold, *GWN* accepts as authentic the sensor and t he user. Otherwise, *GWN* stop the following proc edure.

Step 3. *GWN* generates a random number N a nd retrieves the current timestamp T_5. The gate way node *GWN* computes C_3 $h(h(SID_j\|y)\|T_5)$. Then, sends $\langle C_3, T_5 \rangle$ to the sensor S_j.

Step 4. After receiving the response $\langle C_3, T_5 \rangle$, S_j generates a new timestamp T_6 and verifies t hat $(T_6 - T_5)$ ΔT. If this condition hold, S_j b elieves that the responding party is the genuine g ateway node. Otherwise, S_j aborts this protocol. The sensor S_j retrieves the current timestamp and computes $C_4 = h(\sigma_j\|N_2\|T_7)$ and sends $\langle C_4, T_7 \rangle$ to the gateway *GWN*.

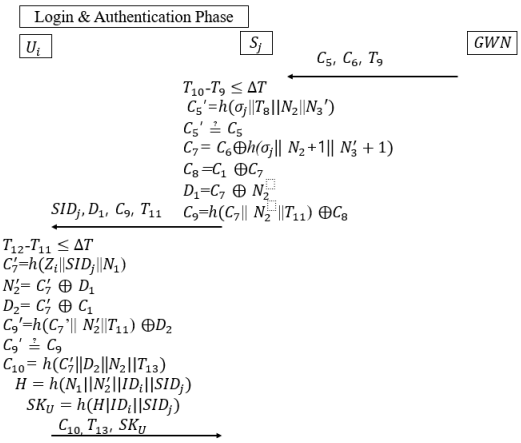
Step 5. Upon receiving the message $\langle C_4, T_7 \rangle$, t he gateway node *GWN* obtains the current times tamp T_8 and verifies that: (1) $(T_8 - T_7)$ ΔT, where ΔT is the maximum allowed time differenc e between T_8 and T_7, and (2) C_4 is equal to $h(\sigma_j\|N_2'\|T_7)$ N_3. If any of these is untrue, *GWN* rejects the login request and aborts the pr otocol. Otherwise, *GWN* accepts the login reques t. *GWN* generates a new timestamp T_9 and com putes

$C_5 = h(h(SID_j\|y)\|T_9)\|N_2'\|N_3),$

$C_6 = h(h(SID_j\|y)\|N_2' + 1\|N_3 + 1)$

$h(h(ID_i\|x)\|SID_j\|N_1').$

And then, *GWN* sends the message $\langle C_5, C_6, T_9 \rangle$ to the sensor S_j.



(Figure 4) Authentication Phase

Step 6. After receiving $\langle C_5, C_6, T_9 \rangle$ from *GWN*, t he sensor S_j obtains the current timestamp T_{10}. S_j verifies that (1) $T_{10} - T_9$ ΔT (2) C_5 equals $h(\sigma_j\|T_9\|N_2\|N_3')$. If both of these conditions are hol d S_j accepts as authentic the gateway node. Otherw ise, S_j stop the following procedure. The sensor S_j r etrieves the current timestamp T_{11} and computes

$C_7 = C_6$ $h(\sigma_j\|N_2 + 1\|N_3' + 1),$

$C_8 = C_1$ $C_7,$

$D_1 = C_7$ $N_2,$

$C_9 = h(C_7\|N_2\|T_{11})$ $C_8.$

The sensor S_j sends to $\langle SID_j, D_1, C_9, T_{11} \rangle$ to the user U_i

Step 7. U_i having received $\langle SID_j, D_1, C_9, T_{11} \rangle$ f rom S_j computes

$C_7' = h(Z_i\|SID_j\|N_1),$

$N_2' = C_7'$ $D_1,$

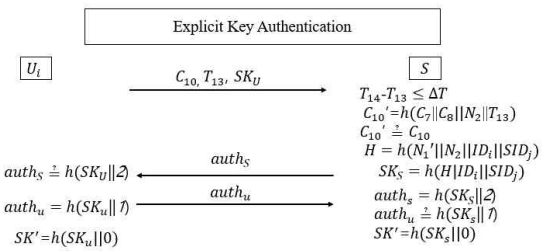
$D_2 = C_7'$ $C_1,$

$C_9' = h(C_7'\|N_2'\|T_{11})$ D_2. U_i verifies that (1) $T_{12} - T_{11}$ ΔT (2) C_9' equals C_9. If both of these conditions are hold, U_i accepts as authentic the sens or and the gateway node. Otherwise, U_i stop the pr otocol. Now the user U_i retrieves the current timest amp T_{13} and computes

0 $h(C_7' \| D_2 \| N_2' \| T_{13})$,
$H = h(N_1 \| N_2' \| ID_i \| SID_j)$,
$SK = h(H \| ID_i \| SID_j)$. And then, U_i sends the message $\langle C_{10}, SK_U, T_{13} \rangle$ to the sensor S_j.

3.2.3 Explicit Key Authentication

Step 1. Upon receiving $\langle C_{10}, SK_U, T_{13} \rangle$ from U_i, the sensor S_j obtains the current timestamp T_{14} and verifies that (1) $T_{14} - T_{13}$ ΔT (2) C_{10} eq uals $h(C_{10} \| C_8 \| N_2 \| T_{13})$. If both of these condition s are hold, U_i computes $SK_S = h(H \| ID_i \| SID_j)$ $(H = h(N_1' \| N_2 \| ID_i \| SID_j))$.



(Figure 5) Explicit Key Authentication

Step 2. U_i computes $SK_U = h(H \| ID_i \| SID_j)$ $(H = h(N_1 \| N_2' \| ID_i \| SID_j)$, $auth_u = h(SK_u \| 1)$ and sends $auth_u$ to the senso r. Similarly, S_j computes $auth_s = h(SK_s \| 2)$ and sends $auth_s$ to the user.

Step 3. Upon receiving $auth_s$, the user U_i check s the equality $auth_s \stackrel{?}{=} h(SK_u \| 2)$. If they are equa l, then U_i computes it final session key SK' as $SK' = h(SK_u \| 0)$. Otherwise U_i aborts the scheme. Likewise, the sensor S_j, after receiving $auth_u$, ve rifies that $auth_u$ equals $h(SK_s \| 1)$. If so, then S_j computes the final session key SK' as $SK' = h(SK_s \| 0)$. Otherwise, S_j aborts the scheme. This procedure of adding explicit authentication is outli ned in Figure 5.

4. Security Analysis in the Proposed Protocol.

This section describes the security analysis to confirm the our proposed protocol. We need to provide the following definitions to then compare the proposed protocol to other authentication protocols, including that 2019 proposed by Chen et al's protocol.

Definition 1. A strong secret key (α, β) has a high value of entropy K that cannot be find out in polynomial time.

Definition 2. A secure one-way hash function $= h(x)$ is the following. Given x to compute y is easy but y to compute x is very hard.

Definition 3. For a given input value, it is computationally infeasible to find any second input which has the same output as that of a specified input; given x, it is difficult to find a second preimage x' x such that $h(x) = h(x')$.

Definition 4. A hash function is collision resistant if it is hard to find two inputs that hash to the same output; that is, two inputs a and b such that $h(a) = h(b)$.

4.1 Offline password guessing attack

The vulnerability of Chen et al.'s scheme to the password guessing attack is due to the fol- lowing fact: to find out the password of the user, they suffice to obtain the information stor- ed in its smart card and read the exchanged message between the sensor and the remote user. More concretely, the problem with chen et al.'s scheme is that whoever obtains the value of

stored in $_i$'s smart card and the value of $h(r_i \| PW_i)$, the part of the user U_i's login message $MP_i(=h(r_i \| PW_i))$ can break password of user U_i. In this attack, an attacker may try to guess a password and then to check the correctness of the guessed password off-line. If his guess fails, the attacker tries again with another password, until he find the proper one. In our proposed scheme, the only information related to password is $Q_i(=h(h(b) \| PW_i)$, but because b is the secret information that the user only knows, this value does not help the attacker to verify directly the correctness of guessed password. Thus, off-line password guessing attack would be unsuccessful against the proposed our protocol.

4.2 Session Key Attack

The vulnerability of Chen et al.'s scheme to the session key attack is due to the following fact: to find out the session key, they suffice to obtain the information stored in its smart card and read the exchanged message between the sensor and the remote user. More tangibly, the problem with chen et al.'s scheme is that whoever obtains these values of e_i, f_i, r_i stored in U_i's smart card, the part of the user U_i's login message and authentication message can learn the session key $sk = h(K_i \| K_j)$. In the proposed scheme, the only information related to session key is $SK(=h(H \| ID_i \| SID_j)$, but because H is the secret information that the user and sensor only know, this value does not help the attacker to find directly the session key. Thus, session key would be unsuccessful against the proposed scheme.

4.3 Known Key Attack

Known key security is said to be provided if compromise of some session keys does not help an attacker learn about any other session keys or impersonate a party in some later session. In our protocol, the session keys generated in different sessions are independent since the short-lived secret values N_1 and N_2 are chosen independently at random from session to session. Thus, known key attack would be unsuccessful against the proposed our protocol.

5. Conclusion

Now, we proposed improved Chen et al..'s user authentication protocol for heterogeneous wireless sensor networks . Some modifications are accomplished to improve their protocol. In our proposed scheme, the only information related to password is the secret information that the user only knows, this value does not help the attacker to verify directly the correctness of guessed password. Thus, off-line password guessing attack would be unsuccessful against the proposed our protocol. In addition, our protocol achieves mutual authentication; i.e., the user and the sensor can authenticate each other.

Reference

[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] Rawat, P.; Singh, K.; Chaouchi, H.; Bonnin, J. Wireless sensor networks: A survey on recent developments and potential synergies. J. Supercomput. 68, 1 - 48, 2014.

[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] Kumar, P.; Choudhury, A.; Sain, M.; Lee, S.; Lee, H. RUASN: A robust user authentication framework for wireless sensor networks. Sensors, 11, 5020 - 5046, 2011.

[9] Khan, M.; Kumari, S. An improved user authentication protocol for healthcare services via wireless medical sensor networks. Int. J. Distrib. Sens. Netw. 2014, 2014, No. 347169, 2014.

[10] Das, M. Two-factor user authentication in wireless sensor networks. IEEE Trans. Wirel. Commun. 2009, 8, 1086 - 1090, 2009.

[11] J. Nam, M. Kim, J. Paik, Y. Lee, D. Won, "A Provably-Secure ECC-Based Authentication Scheme for Wireless Sensor Networks", Sensors, 14, pp. 21023 - 21044, 2014.

[12] J. Ryu, H. kim, Y. Lee, D. Won, "Cryptanalysis of protocol for Heterogenous of the Internet of Thihs Environment", IMCOM 2020, Taichung, Taiwan, pp. 1-4, 2020.

[13] Y. Lee, "Security Improvement to a Remote User Authentication Scheme for Multi-Server Environment", The Korea-Society of Digital Industry& Information Management, 7(4), 23—30, 2011.

[14] Y. Lee, "Security Enhancement to an Biometric Authentication Protocol for WSN Environment", Convergence Security Journal, 16(6), 83-88, 2016.

[저 자 소 개]

이 영 숙 (Youngsook Lee)

2009년 ~ 현재 호원대학교 IT소프트웨어보안학과 교수
2008년 8월 성균관대학교 컴퓨터공학과 공학박사
2005년 2월 성균관대학교 정보보호학과 공학석사
1987년 2월 성균관대학교 정보공학과 공학사

email : ysooklee@howon.ac.kr