A Security Analysis of "A Privacy-Preserving Three-Factor Authentication System for IoT-Enabled Wireless Sensor Networks"

Seunghwan Son
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, South Korea
sonshawn@knu.ac.kr

DeokKyu Kwon
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, South Korea
kdk145@knu.ac.kr

Youngho Park
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, South Korea
parkyh@knu.ac.kr

***Abstract*—Wireless sensor network (WSN) is a main component of the internet of things (IoT) technology, it can be predicted to apply in various areas including smart city, smart home, healthcare, vehicular network, and so on. However, in WSN environments, sensors and data users communicate wirelessly and it can be prone to malicious attacks such as forgery, impersonation, denial-of-service. Therefore, many researchers have proposed to establish a session key securely in WSN environments. In 2024, Thakur *et al.* designed a three-factor based authentication protocol for IoT-enabled WSNs. They indicated that Sahoo *et al.*'s protocol has weaknesses, and therefore, they suggested an enhanced scheme that resolved the previous security weaknesses. Nevertheless, we reviewed Thakur *et al.*'s scheme and we analyze that their scheme fails to support mutual authentication and does not provide perfert forward secrecy. Furthermore, their scheme is also prone to DoS attack because of lack of mutual authentication. We provide a detailed analysis of Thakur *et al.*'s scheme and propose countermeasures to address them.**

***Index Terms*—Internet of Things (IoT), wireless sensors networks (WSNs), sensor, security, mutual authentication**

I. Introduction

As the internet of things (IoT) technology develops and gains attention, the utilization of wireless sensor networks (WSNs) technology is increasing [1], [2]. WSN is a network that is composed of a lot sensor nodes, which are connected to the network in wireless channels. In WSNs, sensors can collect physical data from their surroundings and transmit it to data users and a central server. WSNs are not limited by time or place and cost effective, and therefore, it can be applied in various areas such as smart farm, healthcare, drone environments, smart city, etc. Generally, WSNs consist of a user, sensor, and gateway. A user can request and receive data from sensors, and a sensor collects surrounding data and transmits it to a user, and a gateway acts as middleman between the user and the sensor.

This study was supported by the "BK21 Four project funded by the Ministry of Education, Korea (4199990113966)"

However, these communications are performed via a wireless channel, which is vulnerable to various attacks such as denial-of-service (DoS), impersonation, and replay attacks [3]–[6]. Attackers can steal personal information transmitted in WSNs and abuse the stolen information. These attacks can be severe depending on the communication environments. For example, in wireless medical sensor networks, a patient's personal health information can be collected by sensors and transmitted through a wireless channel, and it can violate the patient's privacy. Furthermore, a sensor node can be easily stolen and captured by an attacker, and the sensor impersonation attack must be considered in WSN environments. Therefore, to prevent these attacks, it is essential to design a secure session key agreement protocol between a user and sensor.

Recently, many studies about mutual authentication scheme have been proposed for WSNs. In 2024, Thakur *et al.* suggested a three-factor based mutual authentication protocol which provides privacy preservation for IoT-enabled WSNs [12]. They identified Sahoo *et al.*'s scheme has security weaknesses and designed an enhanced scheme. However, our analysis revealed that Thakur *et al.*'s enhanced scheme continues to exhibit vulnerabilities to denial-of-service (DoS) attacks and neglects to guarantee mutual authentication and perfect forward secrecy. Therefore, their approach may be difficult to apply to WSNs. In this paper, we present countermeasures to address these security concerns.

The structure of this paper is outlined as following. Section II presents the WSNs communication environments. Section IV shows the scheme of Thakur *et al.*, and Section V demon-

strates the weaknesses of Thakur *et al.*'s scheme. Section VI presents the countermeasures to resolve the security issues, and Section VII concludes the paper.

II. Related Works

We introduce the related papers of Thakur *et al.*'s. In 2014, Turkanovic *et al.* [7] presented a mutual authentication protocol that can be utilized for ad hoc WSNs users. They designed their scheme using only hash and exclusive-or operations considering limited computing power of user and sensor nodes. They asserted that their scheme can guarantee user anonymity and can defend smart card breach attack. However, Farash *et al.* [8] pointed out that the scheme of [7] cannot guarantee user untraceability and sensor anonymity, and cannot prevent smart card stolen and impersonation attacks. Finally, they found that the scheme of [7] cannot provide session key security. They proposed an improved scheme that is secure against above attacks. In 2016, Amin *et al.* [9] found that the scheme of [8] cannot guarantee the security of gateway secret key, user anonymity, resistance to user impersonation through off-line guessing attack. They proposed an anonymity-preserving key agreement scheme for WSNs. Their scheme resolved several security issues of the Farash *et al.*'s scheme. However, Ostad-Sharif *et al.* [10] indicated that the scheme of [9] is prone to strong replay attack and cannot guarantee perfect forward secrecy, and proposed an improved scheme for IoT networks. In 2023, Sahoo *et al.* [11] pointed out the scheme of [10] has problems such as inefficient login, drawback in password change and session key computation, and cannot provide user anonymity. They proposed an enhanced scheme and asserted that their scheme can resolve the above issues and can be securely used in WSNs. However, in 2024, Thakur *et al.* [12] *et al.* indicated that the scheme of [11] cannot sensor identity guessing, sensor node impersonation, ephemeral session random number leakage attacks. They proposed an enhanced scheme using elliptic curve cryptosystem (ECC) to improve the security of their scheme. Unfortunately, we found that Thakur *et al.*'s mutual authentication protocol does not support mutual authentication and perfect forward secrecy, and is vulnerable to DoS attack.

III. System Model

WSNs are composed of a user, a gateway, and a sensor. The descriptions of each elements are as follows:

- **User:** A user request data from a sensor through a gateway. A user sends request message to the nearby gateway, and the gateway relays the message to the sensor. The user can receive the return message generated from the gateway.
- **Gateway:** A gateway acts as a middleman between a user and a sensor. When a request message is transmitted from a user, the gateway checks the validity of the message and relays it to the sensor. Then, when the return message is transmitted from the sensor, the gateway checks the validity of the message and sends it to the user.
- **Sensor:** A sensor collects surrounding data and sends it to data users. When a data request message sent from a user, the sensor authenticates the user and sends a response message.

IV. Review of Thakur *et al.*'s Scheme

Before analyzing Thakur *et al.*'s scheme, We provide the review of their scheme. We denote U_i, GWY, and SN_j are respectively i-th user, a gateway, and j-th sensor node. We presents notations and their meaning in Table I.

TABLE I
Notations and their meanings

Notation	Description
UID_i, UPW_i	Identity and password of U_i
B_i	Biometric information of U_i
N_1, N_2, N_3	Session random numbers
x_i	Secret keys of U_i
x_{GW}	Secret key of GWY
x_j	Secret key of SN_j
P_i	Public key of U_i
P_{GW}	Public key of GWY
P_j	Public key of SN_j
$T_i (i = 1, 2, ...)$	Timestamps
SK_{ij}	Session key between U_i and SN_j

A. Initialization Phase

GWY initializes the system and publishes public parameters. GWY selects a elliptic curve of the system, chooses a generator P of the selected curve and a master secret key k. Then, GWY computes $P_{GW} = k.P$ and publishes P, P_{GW}.

Then, GWY selects a unique identity ID_j and computes $PID_j = h(ID_j||k)$, and sends PID_j to SN_j. SN_j stores PID_j.

B. Registration Phase

U_i registers to GWY in the registration phase. U_i generates UID_i, UPW_i, and B_i, which are respectively a identity, a password, and a biometric information. Then, U_i computes $Gen_i = (w_i, \theta_i)$, selects a random nonce b_i, and calculates $SID_i = h(UID_i||w_i||b_i)$ and $SPW_i = h(UPW_i||w_i||b_i)$. After that, U_i sends (SID_i, SPW_i) to GWY.

GWY receives the message and computes $C_i = h(SID_i||ID_{GW}||X_{GW})$ and $D_i = SID_i \oplus SPW_i \oplus h(C_i)$. Then, GWY sends $(D_i, h(.))$ to U_i.

After U_i receives the message, U_i computes $X_i = D_i \oplus h(UID_i||SID_i||w_i)$, $Y_i = b_i \oplus h(UID_i||UPW_i||w_i||D_i)$, and $Z_i = h(UID_i||SPW_i||D_i||w_i||b_i)$. Then, U_i Stores $\{X_i, Y_i, Z_i, \theta_i\}$ in smart card SC_i. Fig. 2 summerizes the registration phase.

C. User Login and Mutual Authentication Phase

U_i inputs UID_i, UPW_i, and B_i to SC_i, then SC_i computes $w_i = Rep(B_i, \theta_i)$, $C_i = X_i \oplus h(UID_i||w_i)$, $b_i = Y_i \oplus h(UID_i||UPW_i||w_i||C_i)$, $SID_i = h(UID_i||w_i||b_i)$, $SPW_i = h(UPW_i||w_i||b_i)$, and $Z_i^{'} = h(SID_i||SPW_i||X_i||w_i||b_i)$. If $Z_i^{'} \stackrel{?}{=} Z_i$, U_i is successfully logging in to SC_i.

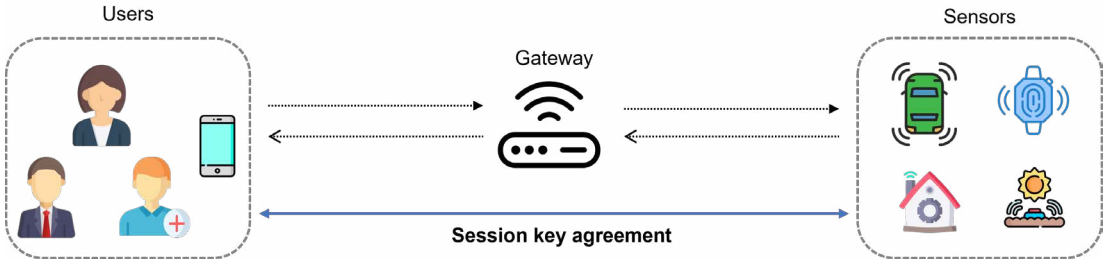

Fig. 1. WSN model.

U_i		GWY
Selects UID_i and UPW_i		
Generates B_i		
Computes $Gen_i = (w_i, \theta_i)$		
Generates a random b_i		
Computes $SID_i = h(UID_i\|\|w_i\|\|b_i)$		
$SPW_i = h(UPW_i\|\|w_i\|\|b_i)$		
	$\xrightarrow{(SID_i, SPW_i)}$	
	Computes $h(SID_i\|\|ID_{GWY}\|\|X_{GWY})$	C_i =
	$D_i = SID_i \oplus SPW_i \oplus h(C_i)$	
	$\xleftarrow{(D_i, h(.))}$	
Computes $X_i = D_i \oplus h(UID_i\|\|SID_i\|\|w_i)$		
$Y_i = b_i \oplus h(UID_i\|\|UPW_i\|\|w_i\|\|D_i)$		
$Z_i = h(UID_i\|\|SPW_i\|\|D_i\|\|w_i\|\|b_i)$		
Stores $\{X_i, Y_i, Z_i, \theta_i\}$		

Fig. 2. Registration phase of Thakur *et al.*'s scheme.

SC_i generates N_i and T_1, computes $W_1 = h(UID_i||N_1||x_i||T_1)$, $M_{i1} = W_1.P$, $M_{i2} = W_1.P_j$, $M_{i3} = h(M_{i1}||M_{i2}||T_1)$. Then, U_i sends (M_{i1}, M_{i2}, T_1) to GWY.

GWY first checks the validity of T_1. Then, GWY computes $M_{i2} = s_b.M_{i1}$, checks $M_{i3} \stackrel{?}{=} h(M_{i1}||M_{i2}||T_1)$. After GWY verifies the equality, GWY generates N_2 and T_2. After that, GWY computes $W_2 = h(ID_j||PID_j||N_2||x_{GWY}||T_2)$, $M_4 = W_2.P$, $M_5 = W_2.P_j$, and $M_6 = h(ID_j||M_{i1}||M_5||T_2)$, and sends (M_{i1}, M_4, M_6, T_2) to SN_j.

SN_j checks the validity of the T_2, computes $M_5 = x_j.M_4$, and checks $M_6 \stackrel{?}{=} h(ID_j||M_{i1}||M_5||T_2)$. After SN_j verifies the equality, SN_j generates N_3 and T_3, computes $S_{j1} = N_3.P$, $S_{j2} = N_3.P_i$, and $S_3 = x_j.P_i$, $S_4 = h(S_{j2}||S_3||M_{i1})$, and $SK_{ij} = h(HID_j||S_{j2}||S_3||T_3)$, and sends (S_{j1}, S_4, T_3) to GWY.

GWY checks the validity of T_3, computes $M_7 = ID_j \oplus h(M_{i2}||T_4)$, and sends $(S_{j1}, S_4, M_7, T_3, T_4)$ to U_i.

U_i checks the validity of the T_4, computes $ID_j = M_7 \oplus h(M_{i2}||T_4)$, $S_{j2} = S_{j1}.x_i$, and $S_3 = x_i.P_j$. and checks $S_4 \stackrel{?}{=} h(S_{j2}||S_3||M_{i1})$. If it is verifiedq, U_i computes $SK_{ij} = h(ID_j||S_{j2}||S_3||T_3)$. Then, U_i and SN_j have the same session key SK_{ij}. Fig. 3 summarizes the authentication phase.

D. Password update phase

The password of U_i can be updated without the help of GWY. U_i inputs (UID_i, UPW_i, B_i) to SC_i, then SC_i computes $w_i = Rep(B_i, \theta_i)$, $D_i = X_i \oplus h(UID_i||w_i)$, $b_i = Y_i \oplus h(UID_i||UPW_i||w_i||D_i)$, $SID_i = h(UID_i||w_i||b_i)$, $SPW_i = h(UPW_i||w_i|||b_i)$, and $Z_i = h(SID_i||SPW_i||X_i||w_i||b_i)$. Then, U_i successfully logs in to SC_i and can enter new password UPW_i^{new}.

V. Weaknesses of Thakur *et al.*'s scheme

We demonstrate the weaknesses of Thakur *et al.*'s protocol in detail. Thakur *et al.*'s scheme do not has resistance to DoS attack and cannot provide mutual authentication and perfect forward secrecy.

A. Lack of mutual authentication

In the first message of Thakur *et al.*'s scheme, U_i sends (M_{i1}, M_{i3}, T_1) to GWY. The message do not include information about the identity of U_i. Although $M_{i1} = W_1.P$ and W_1 should be calculated by $W_1 = h(UID_i||N_1||x_i||T_1)$, GWY and SN_j cannot distinguish W_1 and a random number. Therefore, GWY and SN_j cannot authenticate U_i correctly.

B. Vulnerable to DoS attack

Due to the lack of mutual authentication, Thakur *et al.*'s protocol cannot prevent DoS attack. An attacker can perform a DoS attack targeting the gateway. An adversary A can impersonate a user and send an authentication request message. First, A can generate a random number n_A and a timestamp T_A. Then, A computes $M_{A1} = n_A.P$, $M_{A2} = W_1.P_{GW}$, and $M_{A3} = h(M_{A1}||M_{A2}||T_A)$ and transmits (M_{A1}, M_{A2}, T_A) to GWY. After GWY receives the message, GWY computes $M_{A2} = x_{GWY}.M_{i1}$ and checks $M_{A3} \stackrel{?}{=} h(M_{A1}||M_{A2}||T_A)$. It must be equal and GWY computes following operations and sends message to SN_j. SN_j also checks the validity of the message and return the response message. Therefore, A can randomly generate lots of messages and can cause DoS to the network.

U_i/SC_i	GWY	SN_j
Inputs UID_i, UPW_i, B_i		
Computes $w_i = Rep(B_i, \theta_i)$		
$C_i = X_i \oplus h(UID_i\|\|w_i)$		
$b_i = Y_i \oplus h(UID_i\|\|UPW_i\|\|w_i\|\|C_i)$		
$SID_i = h(UID_i\|\|w_i\|\|b_i)$		
$SPW_i = h(UPW_i\|\|w_i\|\|b_i)$		
$Z_i^{'} = h(SID_i\|\|SPW_i\|\|X_i\|\|w_i\|\|b_i)$		
Checks $Z_i^{'} \stackrel{?}{=} Z_i$		
Generates N_i and T_1		
Computes $W_1 = h(UID_i\|\|N_1\|\|x_i\|\|T_1)$		
$M_{i1} = W_1.P$, $M_{i2} = W_1.P_{GW}$		
$M_{i3} = h(M_{i1}\|\|M_{i2}\|\|T_1)$		
$\xrightarrow{(M_{i1}, M_{i2}, T_1)}$		
	Checks the validity of T_1	
	Computes $M_{i2} = x_{GWY}.M_{i1}$	
	Checks $M_{i3} \stackrel{?}{=} h(M_{i1}\|\|M_{i2}\|\|T_1)$	
	Generates N_2 and T_2	
	Computes	
	$W_2 = h(ID_j\|\|PID_j\|\|N_2\|\|x_{GWY}\|\|T_2)$	
	$M_4 = W_2.P$, $M_5 = W_2.P_j$	
	$M_6 = h(ID_j\|\|M_{i1}\|\|M_5\|\|T_2)$	
	$\xrightarrow{(M_{i1}, M_4, M_6, T_2)}$	
		Checks the validity of the T_2
		computes $M_5 = x_j.M_4$
		Checks $M_6 \stackrel{?}{=} h(ID_j\|\|M_{i1}\|\|M_5\|\|T_2)$
		Generates N_3 and T_3
		Computes $S_{j1} = N_3.P$
		$S_{j2} = N_3.P_i$
		$S_3 = x_j.P_i$
		$S_4 = h(S_{j2}\|\|S_3\|\|M_{i1})$
		$SK_{ij} = h(HID_j\|\|S_{j2}\|\|S_3\|\|T_3)$
		$\xleftarrow{(S_{j1}, S_4, T_3)}$
	Checks the validity of T_3	
	Computes $M_7 = ID_j \oplus h(M_{i2}\|\|T_4)$	
	$\xleftarrow{(S_{j1}, S_4, M_7, T_3, T_4)}$	
Checks the validity of the T_4		
Computes $ID_j = M_7 \oplus h(M_{i2}\|\|T_4)$		
$S_{j2} = S_{j1}.x_i$		
$S_3 = x_i.P_j$		
$S_4 \stackrel{?}{=} h(S_{j2}\|\|S_3\|\|M_{i1})$		
Computes $SK_{ij} = h(ID_j\|\|S_{j2}\|\|S_3\|\|T_3)$		

Fig. 3. The mutual authentication phase proposed by Thakur *et al.*.

C. Lack of perfect forward secrecy

In the proposed scheme, secret keys x_i, x_{GWY}, x_j are used during authentication process. Let assume that the network is compromised and A obtains these long-term keys. Then, A can computes $S_{j2} = S_{j1}.x_i$, $S_3 = x_i.x_j.P$ and then computes $SK_{ij} = h(ID_j||S_{j2}||S_3||T_3)$. Using the session key, A can decrypt the transmitted message in the previous sessions, and user data can be leaked.

VI. Countermeasures

We suggests countermeasures to resist the above security issues.

A. Support mutual authentication

U_i should include information that can authenticate U_i in the first message. It is possible to add user's identity in the message, yet this method cannot guarantee user anonymity and untraceability. Therefore, it is appropriate to create a temporary identity of U_i and update it at the end of each session. This can result in increasing computation on the user side, so it is important to design it with minimal computational costs.

B. Resistance to DoS attack

After GWY receives the message, it should be possible to verify the legitimate of the sender and the integrity of the message. If ECC operations are required during this process, GWY can be overloaded and it can cause network delay. Therefore, GWY should be able to authenticate the message using only hash and exclusive-or operations.

C. Support perfect forward secrecy

To solve this problem, it is recommended to use a symmetric key that utilizes a random number and a long-term key for the session key simultaneously. For example, x_i and N_1 is a secret key and random number of U_i, respectively, and x_j and N_3 are a secret key and a random number of SN_j, respectively. In the proposed scheme, $SK_{ij} = h(ID_j||N_3.x_i.P||x_i.x_j.P||T_3)$, and it can be secured if a symmetric key of random numbers such as $N_1.N_3.P$ is included for calculating the session key.

VII. Conclusions

WSNs are a potential technology and predicted to be utilized in various fields. Thakur *et al.* proposed a mutual authentication protocol to guarantee secure communication for WSNs environments. However, we found that their scheme cannot resist DoS attack and cannot support support mutual authentication and perfect forward secrecy. Although Thakur *et al.*'s scheme has improvements over the existing schemes and contributed to design a secure key agreement protocol for WSNs, it is difficult to be practically utilized in WSNs environments. In this paper, we proposed countermeasures to address the above issues. In future research, we plan to design a key agreement scheme that can be practically used in WSNs by utilizing the proposed countermeasures.

References

[1] I. F. Akyildiz and M. C. Vuran, *Wireless Sensor Networks*, vol. 4. Hoboken, NJ, USA: Wiley, 2010.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Comput. Netw*., vol. 52, no. 12, pp. 2292–2330, Aug. 2008.

[3] S. Yu and Y. Park, "A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions," *IEEE Internet Things J*., vol. 9, no. 20, pp. 20214–20228, Oct. 2022.

[4] K. Park and Y. Park, "Miot-cdps: Complete decentralized privacypreserving scheme for medical internet of things," *Internet of Things*, p. 101250, 2024

[5] D. Kwon, S. Son, M. Kim, J. Lee, A. K. Das, and Y. Park, "A secure self-certified broadcast authentication protocol for intelligent transportation systems in UAV-assisted mobile edge computing environments," *IEEE Trans. Intell. Transp. Syst.*, early access, 22 July, 2024, doi : 10.1109/ TITS.2024.3428491.

[6] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain based lightweight V2I handover authentication protocol for VANET," *IEEE Trans. Netw. Sci. Eng*., vol. 9, no. 3, pp. 1346–1358, May 2022.

[7] M. Turkanovic, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Netw*., vol. 20, pp. 96–112, Sep. 2014.

[8] M. S. Farash, M. Turkanovic, S. Kumari, and M. Hölbl, "An efficient ´ user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw*., vol. 36, pp. 152–176, Jan. 2016

[9] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," *Comput. Netw*., vol. 101, pp. 42–62, Jun. 2016.

[10] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," *Future Gener. Comput. Syst*., vol. 100, pp. 882–892, Nov. 2019.

[11] S. S. Sahoo, S. Mohanty, K. S. Sahoo, M. Daneshmand, and A. H. Gandomi, "A three-factor-based authentication scheme of 5g wireless sensor networks for iot system," *IEEE Internet Things J*., vol. 10, no. 17, pp. 15 087–15 099, 2023.

[12] G. Thakur, S. Prajapat, P. Kumar, and C.-M. Chen, "A privacy-preserving three-factor authentication system for iot-enabled wireless sensor networks," *J. Syst. Archit.*, vol 154. p. 103245, 2024.