Wuhan University
Journal of Natural Sciences

2023, Vol.28 No.6, 541-552

Article ID 1007-1202(2023)06-0541-12
DOI https://doi.org/10.1051/wujns/2023286541

Analysis and Improvement on an Authentication Scheme for Wireless Sensor Networks in Internet of Things Environment

LI Anqian[1], KANG Baoyuan[1], ZUO Xinyu[1], HUO Yuyan[1], NIU Shufang[2], SUN Zhu[3]

1. School of Software, Tiangong University, Tianjin 300387, China;
2. School of Computer Science and Technology, Tiangong University, Tianjin 300387, China;
3. International Cultural Exchange College, Xinjiang University, Urumqi 830046, Xinjiang, China

Abstract: Nowadays, Internet of Everything has become a major trend, and Internet of Things (IoT) has emerged. Wireless sensor networks (WSNs) are core technologies for IoT to sense the real world. Due to the unattended and resource-constrained characteristics of WSNs, it is a great challenge to design an efficient and secure authentication scheme for communication between users and sensor nodes in WSNs. Recently, Hu *et al* proposed an authentication scheme for WSNs in an IoT environment. They claimed that their scheme could maximize the balance between security and computational cost as well as efficiency, and be resistant to many known attacks. However, we find that the scheme is difficult to resist stolen smart card attack and denial-of-service attack. Moreover, during the login and key negotiation phase of the scheme, Gateway (GWN) is unable to extract key values for subsequent computation based on the messages sent by the sensor nodes, which in turn leads to the inability to achieve mutual authentication and key agreement. To overcome these shortcomings, we propose an improved scheme. The proposed scheme enables real-time data exchange and transmission as well as secure communication between users and sensor nodes.

Key words: Internet of Things (IoT); Wireless Sensor Networks (WSNs); authentication; elliptical curve cryptography (ECC)
CLC number: TP309.2

0 Introduction

The ability to bring physical things into the digital world is becoming increasingly possible because of the high level of development of wireless communication and smart device technologies[1]. A very significant opportunity for wireless sensor networks (WSNs) has been offered by the rise of Internet of Things (IoT) era and the development of communication technology. As a combination of wireless networks and IoT sensors, WSNs have attracted more and more attention worldwide because of the excellent performance in industrial control, smart home, environmental monitoring and other aspects[2].

However, owing to the openness of the network and the broadcast nature of wireless communication, WSNs are facing a variety of threats that ordinary wireless networks may suffer from, such as replay attacks, information leakage, denial-of-service (DOS) attacks, in

Received date: 2023-04-26
Biography: LI Anqian, female, Master candidate, research direction: cryptography. E-mail: lianqian98@163.com

addition to the vulnerability of sensor nodes to physical access and disassembly until these sensor nodes are fully controlled by attackers. Sensor devices in WSNs are disposed in public environments to collect information in real time[3]. If one of the sensor nodes is compromised, its linkability will become a focal point. An attacker can use the compromised device as a springboard to attack other devices and systems. Coupled with the sensitive and critical nature of the transmitted data, the data must be protected by end-to-end services as it is transmitted between WSNs and entities outside of WSNs[4]. Therefore, it is crucial to provide an authentication scheme for WSNs that can guarantee secure communication between users and sensor nodes. In WSNs, the communication between devices requires the use of various protocols that will define the purpose of the communication, the sequence of steps to be performed during the communication, and the encryption techniques used to protect the transmitted information[5].

In recent years, researchers have been developing efficient ways to merge WSNs into IoT environments and have done a lot of research on authentication schemes that balance efficiency and security in WSNs, but numerous schemes have security concerns[6]. In 2019, Ostad-Sharif *et al*[6] proposed a secure and lightweight authenticated key agreement scheme for WSNs, and they claimed that their scheme not only was efficient but also provided perfect forward secrecy and was resistant to common attacks. In 2020, Chen *et al*[7] pointed out that Ostad-Sharif *et al*'s scheme[6] not only had design errors in the login and authentication phase, which resulted in legitimately registered users not being able to access the system, but also did not provide password change and update capabilities. In 2021, Chunka *et al*[8] presented a smart card-based user authentication and session key agreement scheme. They claimed that their scheme not only was efficient but also was resistant to attacks such as sensor node capture attacks, gateway key leakage and so on. However, Lee *et al*[9] confirmed that Chunka *et al*'s scheme[8] was vulnerable to known session-specific temporary information attacks, identity/password pair guessing attacks, impersonation attacks, etc. In 2022, Hu *et al*[10] proposed a two-factor authentication scheme for WSNs in IoT environment, and they claimed that their scheme could maximized the balance of security and computational cost as well as efficiency, and was able to resist many common attacks. However, we found that there were security risks in Hu *et al*'s scheme. Firstly, this scheme could not resist stolen smart card attacks and DOS attacks. Secondly, during the login and key agreement phase of Hu *et al*'s scheme, gateway (GWN) could not extract key values for subsequent computation based on the messages sent by the sensor nodes, resulting in the scheme's failure to achieve mutual authentication and key agreement.

Hu *et al*'s authentication scheme is briefly reviewed in Section 1. In Section 2, we analyze the shortcomings of the Hu *et al*'s scheme. An improved scheme is given in Section 3. In Section 4, we analyze the security for the improved scheme. The performance evaluation for the proposed scheme in different metrics and the comparison with the same type of schemes are presented in Section 5. In Section 6, we conclude the paper.

1 Review of Hu *et al*'s Scheme

In Hu *et al*'s scheme[10], users and sensor nodes complete mutual authentication and agree on session keys with the help of GWN. The scheme consists of four phases: initialization phase, registration phase, login and key agreement phase, and password and expiration time update phase. The notations involved in the scheme and their definitions are shown in Table 1.

1.1 Intialization Phase

GWN chooses two random numbers $K_{\mathrm{GU}}, K_{\mathrm{GS}} \in Z_q^*$ as the private key of GWN. P is the generator in the elliptic curve. The public key of GWN is P_{pub} and the calculation formula is $P_{\mathrm{pub}} = K_{\mathrm{GU}} \cdot P$.

1.2 Registration Phase

The current phase consists of a user registration phase and a sensor node registration phase. In this phase, the data is transmitted over a secure channel.

1.2.1 Registration for users

When a new user wants to access the services provided by WSNs, he/she must register with the gateway at first. The details of the user registration phase are as follows.

Step 1 U_i chooses ID_i and PW_i, generates a random number r_i, and calculates

$$A_i = h(\mathrm{ID}_i \| \mathrm{PW}_i \| r_i).$$

Then, U_i sends a message $\{\mathrm{ID}_i, A_i\}$ to the GWN over a secure channel.

Step 2 Once GWN receives a message from U_i, it selects an expiration time TE_i for the temporary credentials of U_i.

Table 1 Notations used in Hu *et al*'s scheme

Notation	Definition
U_i, GWN, S_j	The i-th user, gateway and the j-th sensor node
ID_i	Identity of the i-th user
PID_i	Pseudonymous identity of the i-th user
$\mathrm{ID}_{\mathrm{GWN}}$	Identity of gateway
SID_j	Identity of the j-th sensor node
PW_i	Password of the i-th user
SC	Smart card
K_{GU}, K_{GS}	Private keys only known to GWN
TC_i	The temporal credential of the i-th user
TC_j	The temporal credential of the j-th sensor node
TE_i	Expiration time of a U_i's temporal credential
P	Basic point of the elliptic curve
N_1, N_2, N_3, x, x_1, x_2, x_3	Random numbers
SK, SK_{ij} (= SK_{ji})	The session key between U_i and S_j
$\oplus$	Bitwise XOR operation
$\|\|$	Concatenation operation
$h(\cdot)$	A secure Hash function

GWN calculates the public key $P_{\mathrm{pub}}=K_{\mathrm{GU}}\cdot P$ and U_i's temporal credential $\mathrm{TC}_i=h(\mathrm{ID}_i||\mathrm{ID}_{\mathrm{GWN}}||K_{\mathrm{GU}}||\mathrm{TE}_i)$.

GWN will store $\{\mathrm{ID}_{\mathrm{GWN}}, \mathrm{TE}_i, P_{\mathrm{pub}}, h(\cdot), \mathrm{PTC}_i\}$ in a smart card SC and send SC to U_i over a secure channel.

Step 3 U_i computes $\mathrm{TC}_i=\mathrm{PTC}_i\oplus A_i$, $B_i=\mathrm{TC}_i\oplus h(\mathrm{ID}_i||\mathrm{PW}_i)$, and stores $\{B_i\}$ in SC.

1.2.2 Registration for sensor nodes

Each sensor node must register with GWN and only once, and its registration phase consists of the following operations.

Step 1 GWN selects an identity SID_j for the sensor node S_j and calculates

$$\mathrm{TC}_j=h(K_{\mathrm{GS}}||\mathrm{SID}_j).$$

GWN sends a message $\{\mathrm{TC}_j, \mathrm{SID}_j\}$ to S_j over a secure channel.

Step 2 S_j receives the message from GWN and stores $\{\mathrm{TC}_j, \mathrm{SID}_j\}$.

1.3 Login and Key Agreement Phase

In this phase, U_i and S_j agree on a session key with the help of GWN, thus performing a mutually authenticated key agreement to ensure further secure communication between them. The specific steps are as follows.

Step 1 U_i inserts SC and enters his/her identity ID_i and password PW_i. SC then generates two random numbers N_1 and x_1 based on the stored information and the extracted

$$\mathrm{TC}_i=B_i\oplus h(\mathrm{ID}_i||\mathrm{PW}_i)$$

entered by U_i, and calculates

$$T_1=x_1\cdot P,$$

$$T_2=(\mathrm{ID}_i||\mathrm{TE}_i||\mathrm{SID}_j||N_1)\oplus h(x_1\cdot P_{\mathrm{pub}}),$$

where $P_{\mathrm{pub}}=K_{\mathrm{GU}}\cdot P$ is the public key of GWN,

$$T_3=h(T_1||\mathrm{ID}_i||\mathrm{ID}_{\mathrm{GWN}}||\mathrm{TC}_i||N_1||\mathrm{TE}_i||\mathrm{SID}_j).$$

U_i sends a login request message $M_1=\{T_1, T_2, T_3\}$ to GWN.

Step 2 After receiving the message $M_1=\{T_1, T_2, T_3\}$ from U_i, GWN calculates

$$\mathrm{ID}_i||\mathrm{TE}_i||\mathrm{SID}_j||N_1=T_2\oplus h(K_{\mathrm{GU}}\cdot T_1)$$

and checks the validity of TE_i. If it fails, GWN will reject U_i's login request. Otherwise, GWN calculates

$$\mathrm{TC}_i=h(\mathrm{ID}_i||\mathrm{ID}_{\mathrm{GWN}}||K_{\mathrm{GU}}||\mathrm{TE}_i),$$

$$T_3^*=h(T_1||\mathrm{ID}_i||\mathrm{ID}_{\mathrm{GWN}}||\mathrm{TC}_i||N_1||\mathrm{TE}_i||\mathrm{SID}_j).$$

GWN checks whether $T_3^*=T_3$ is correct or not. If not, GWN terminates the current phase. Otherwise, GWN generates three random numbers N_2, x as well as x_2 and computes

$$\mathrm{TC}_j=h(K_{\mathrm{GS}}||\mathrm{SID}_j),$$

$$T_4=x_2\oplus h(\mathrm{TC}_j||N_2||\mathrm{ID}_{\mathrm{GWN}}),$$

$$T_5=h(\mathrm{ID}_i||\mathrm{TE}_i||x)\oplus h(N_2||\mathrm{TC}_j),$$

$$T_6=h(T_1||h(\mathrm{ID}_i||\mathrm{TE}_i||x)||x_2||N_2).$$

Then, GWN sends a message $M_2=\{T_1, T_4, T_5, T_6, N_2\}$ to S_j over a secure channel.

Step 3 After receiving the message from GWN, S_j recovers

$$x_2=T_4\oplus h(\mathrm{TC}_j||N_2||\mathrm{ID}_{\mathrm{GWN}}),$$

$$h(\mathrm{ID}_i||\mathrm{TE}_i||x)=T_5\oplus h(N_2||\mathrm{TC}_j),$$

and calculates

$$T_6^*=h(T_1||h(\mathrm{ID}_i||\mathrm{TE}_i||x)||x_2||N_2).$$

S_j checks whether $T_6^*=T_6$ holds or not. if it does, S_j generates two random numbers N_3, x_3, and computes

$$\mathrm{SK}=h(h(\mathrm{ID}_i||\mathrm{TE}_i||x)||\mathrm{SID}_j||x_3\cdot T_1||T_1||T_7),$$

$$T_8=h(\mathrm{SK}||N_3),$$

$$T_9=(T_8||T_7||N_3)\oplus h(\mathrm{TC}_j||N_2),$$

$$T_{10}=h(\mathrm{TC}_j||T_7||N_2||T_8).$$

S_j transmits a message $M_3=\{T_9, T_{10}\}$ to GWN.

Step 4 After receiving the message from S_j, GWN extracts

$$T_8||T_7||N_3 = T_9 \oplus h(\mathrm{TC}||N_2)$$

and calculates $T_{10}{*} = h(\mathrm{TC}_j||T_7||N_2||T_8)$.

Then, GWN verifies whether $T_{10}{*} = T_{10}$ or not. If not, GWN will terminate the current phase immediately. Otherwise, GWN calculates

$$T_{11} = (T_8||N_1||T_7||N_3||x) \oplus h(N_1||\mathrm{TC}_i).$$

GWN sends the message $M_4 = \{T_{11}\}$ to U_i.

Step 5 Once U_i receives M_4, it extracts

$$T_8||N_1||T_7||N_3||x = T_{11} \oplus h(N_1||\mathrm{TC}_i)$$

and calculates the session key

$$\mathrm{SK} = h(h(\mathrm{ID}_i||\mathrm{TE}_i||x)||\mathrm{SID}_j||x_3 \cdot T_1||T_1||T_7),$$
$$T_8{*} = h(\mathrm{SK}||N_3).$$

U_i checks whether $T_8{*} = T_8$ holds or not. If it does, it means that U_i and S_j have successfully reached the session key.

1.4 Password and Expiration Time Update Phase

If U_i wants to update or change his/her password, he/she inserts a smart card SC and enters ID_i, PW_i. After that, SC will calculate

$$B_i^{\mathrm{new}} = B_i \oplus h(\mathrm{ID}_i||\mathrm{PW}_i) \oplus h(\mathrm{ID}_i||\mathrm{PW}_i^{\mathrm{new}}),$$

and then replaces B_i with B_i^{new}.

If GWN wants to update the expiration time TE_i for TC_i, GWN can reselect a TE_i' and recalculate

$$\mathrm{TC}_i' = h(\mathrm{ID}_i||\mathrm{ID}_{\mathrm{GWN}}||K_{\mathrm{GU}}||\mathrm{TE}_i'),$$
$$T_{11}' = (T_8||N_1||T_7||N_3||\mathrm{TC}_i'||\mathrm{TE}_i') \oplus h(N_1||\mathrm{TC}_i)$$

in Step 4 of the login and key agreement phase. After that, U_i can extract TE_i' and TC_i' from T_{11}, update B_i and TE_i in his/her own smart card.

2 Security Analysis of Hu *et al*'s Scheme

This section analyzes the security of Hu *et al*'s scheme[10], and demonstrates that Hu *et al*'s scheme[9] has the following risks.

2.1 Vulnerability to Stolen Smart Card Attack and DOS Attack

If an attacker steals a smart card SC of one user U_i, and then attempts to log in by inserting the SC and entering his/her own identity ID_k and password PW_k, since SC does not verify whether the current user has registered legally, based on the information $\{\mathrm{ID}_{\mathrm{GWN}}, \mathrm{TE}_i, P_{\mathrm{pub}}, h(\cdot), B_i\}$ stored in SC, the attacker can directly perform a series of calculations by using equation (1) and then send $M_1 = \{T_1', T_2', T_3'\}$ to GWN. Although the attacker can neither pass the authentication

$$T_3{*} = h(T_1||\mathrm{ID}_i||\mathrm{ID}_{\mathrm{GWN}}||\mathrm{TC}_i||N_1||\mathrm{TE}_i||\mathrm{SID}_j)$$

of GWN nor participate in the subsequent operations, GWN has already carried out a series of calculations through equation (2), consuming a large amount of computational resources. If mass forged login requests are sent, GWN's resources will be exhausted, and GWN cannot process normal requests from legitimate users timely. In other words, legitimate users will not be able to get responses from the service.

Generate N_1', x_1'

$$\begin{cases} \mathrm{TC}_i' = B_i \oplus h(\mathrm{ID}_k||\mathrm{PW}_k) \\ T_1' = x_1' \cdot P \\ T_2' = (\mathrm{ID}_k||\mathrm{TE}_i||\mathrm{SID}_j||N_1') \oplus h(x_1' \cdot P_{\mathrm{pub}}) \\ T_3' = h(T_1'||\mathrm{ID}_k||\mathrm{ID}_{\mathrm{GWN}}||\mathrm{TC}_i'||N_1'||\mathrm{TE}_i||\mathrm{SID}_j) \end{cases} \tag{1}$$

$$\begin{cases} \mathrm{ID}_i||\mathrm{TE}_i||\mathrm{SID}_j||N_1 = T_2 \oplus h(K_{\mathrm{GU}}T_1) \\ \mathrm{TC}_i = h(\mathrm{ID}_i||\mathrm{ID}_{\mathrm{GWN}}||K_{\mathrm{GU}}||\mathrm{TE}_i) \\ T_3{*} = h(T_1||\mathrm{ID}_i||\mathrm{ID}_{\mathrm{GWN}}||\mathrm{TC}_i||N_1||\mathrm{TE}_i||\mathrm{SID}_j) \end{cases} \tag{2}$$

2.2 GWN Cannot Extract Key Values

Hu *et al*[10] claimed that their scheme satisfied user anonymity, meaning that the user's identity ID_i was only included in T_2, T_3, T_4, T_5 and not transmitted over a public channel. However, GWN not only served multiple sensor nodes and users simultaneously, but also received a huge amount of messages.

Since the identity of the sensor node and the identity of the specific user were missing in the message $M_3 = \{T_9, T_{10}\}$ sent by the sensor node to GWN, GWN was unable to recognize which sensor node was trying to contact which user after receiving M_3. Therefore, GWN could not determine which temporary credential was used to calculate equation (3). Then, the following operations cannot work.

$$\begin{cases} T_8||T_7||N_3 = T_9 \oplus h(\mathrm{TC}_j||N_2) \\ T_{10}{*} = h(\mathrm{TC}_j||T_7||N_2||T_8) \end{cases} \tag{3}$$

2.3 Failure Mutual Authentication and Key Agreement

As described in Section 2.2, GWN cannot obtain SID_j and ID_i from the message $M_3 = \{T_9, T_{10}\}$ sent by S_j during login and key agreement phase, so GWN is unable to compute equation (3), much less conduct further authentication by verifying whether $T_{10}{*} = T_{10}$ or not. It means that Hu *et al*'s scheme[10] cannot continue to work. Therefore, the scheme fails to achieve mutual authentication and key agreement.

3 The Proposed Scheme

To overcome the shortcomings in Hu *et al*'s scheme[10], this paper presents an improved scheme. Firstly, proposed scheme adds a user's pseudo-identity PID_i in the registration phase of users for the transmission of identity information in a public channel. The pseudo-identity is dynamic and updated promptly after each communication. Secondly, the proposed scheme incorporates a key authentication in the login phase of user, where the smart card verifies whether the current user is the legitimate registered one. Finally, the proposed scheme adds some necessary identity information in the transmitted messages. This measure ensures that GWN, upon receiving a message from a sensor node, can clearly know which sensor node wants to communicate with which user.

The proposed scheme satisfies mutual authentication and effectively enhances the anonymity of users. In addition, the proposed scheme not only resists the stolen smart card attacks and DOS attacks mentioned above, but also solves the problem that GWN cannot extract key values. For the sake of brevity, this section only describes the initialization phase, the registration phase, and the login and key agreement phase. The specific steps are as follows.

3.1 Initialization Phase

GWN selects an additive group G of order q and a generator P of G on an elliptic curve E. GWN chooses two private keys $K_{\mathrm{GU}} \in Z_q^*$ and $K_{\mathrm{GS}} \in Z_q^*$, and computes its public key $P_{\mathrm{pub}} = K_{\mathrm{GU}} \cdot P$.

3.2 Registration Phase

Any user and sensor can register with GWN. Unregistered entities are not able to communicate subsequently. The above approach can effectively guarantee the security of data transmission, thereby ensuring the network security of the whole system. This phase is divided into a user registration phase and a sensor node registration phase.

3.2.1 Registration of users

When a new user wants to access an IoT service and communicate with one of the sensor nodes, he/she must first register with GWN and obtain his/her SC through a secure channel. GWN stores the user's registration information in order to verify his/her identity during the login phase. In Fig. 1, this phase is divided into three steps and the process is as follows.

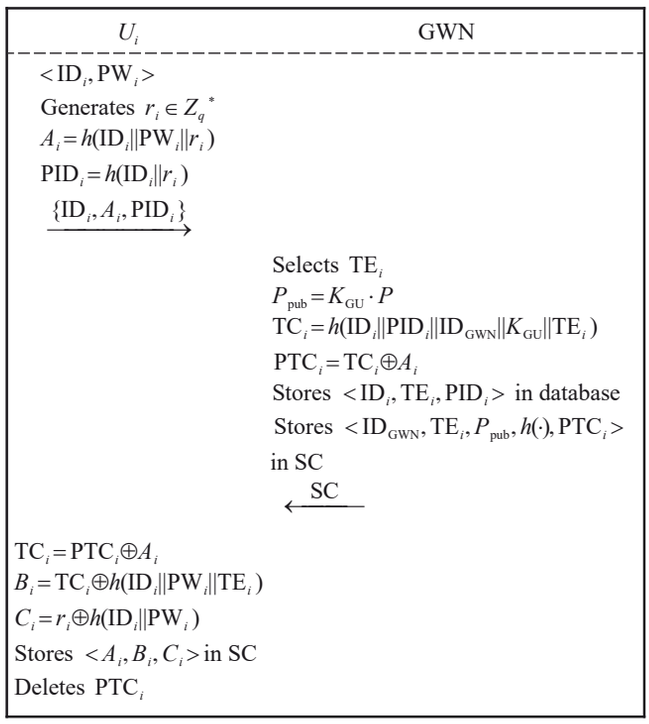

Fig. 1 Registration of users

Step 1 User U_i selects his/her unique identity ID_i and password PW_i, generates a random number $r_i \in Z_q^*$, and calculates A_i and pseudo-identity PID_i according to equation (4). Then, U_i sends a registration message $\{\mathrm{ID}_i, A_i, \mathrm{PID}_i\}$ to the GWN over a secure channel.

$$\begin{cases} A_i = h(\mathrm{ID}_i \| \mathrm{PW}_i \| r_i) \\ \mathrm{PID}_i = h(\mathrm{ID}_i \| r_i) \end{cases} \tag{4}$$

Step 2 GWN receives the registration message from U_i and chooses an expiration time TE_i for U_i. GWN calculates its own public key P_{pub}, the user's temporary credentials TC_i and PTC_i by equation (5). GWN stores $\{\mathrm{ID}_i, \mathrm{TE}_i, \mathrm{PID}_i\}$ into its own database and embeds $\{\mathrm{ID}_{\mathrm{GWN}}, \mathrm{TE}_i, P_{\mathrm{pub}}, h(\cdot), \mathrm{PTC}_i\}$ into a smart card SC. GWN then issues SC to U_i over a secure channel.

$$\begin{cases} P_{\mathrm{pub}} = K_{\mathrm{GU}} \cdot P \\ \mathrm{TC}_i = h(\mathrm{ID}_i \| \mathrm{PID}_i \| \mathrm{ID}_{\mathrm{GWN}} \| K_{\mathrm{GU}} \| \mathrm{TE}_i) \\ \mathrm{PTC}_i = \mathrm{TC}_i \oplus A_i \end{cases} \tag{5}$$

Step 3 Once the SC is received, U_i performs equation (6) for the calculation in order to create the values required for the authentication in the next stage. After that, U_i stores $\{A_i, B_i, C_i\}$ in SC and removes PTC_i. As of now, the values stored in SC are $\{\mathrm{ID}_{\mathrm{GWN}}, \mathrm{TE}_i, P_{\mathrm{pub}}, h(\cdot), A_i, B_i, C_i\}$.

$$\begin{cases} \mathrm{TC}_i = \mathrm{PTC}_i \oplus A_i \\ B_i = \mathrm{TC}_i \oplus h(\mathrm{ID}_i \| \mathrm{PW}_i \| \mathrm{TE}_i) \\ C_i = r_i \oplus h(\mathrm{ID}_i \| \mathrm{PW}_i) \end{cases} \tag{6}$$

3.2.2 Registration of sensor nodes

Any sensor node that interacts with GWN for the first time must register first. The registration process of sensor nodes is shown in Fig. 2, with the following steps.

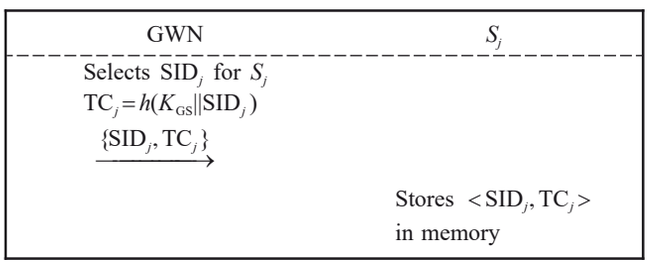

Fig. 2 Registration of sensor nodes

Step 1 For a newly installed sensor node S_j, GWN first selects an identity SID_j for it and calculates the temporary credential TC_j by $\mathrm{TC}_j = h(K_{\mathrm{GS}}||\mathrm{SID}_j)$.

Step 2 S_j receives a message $\{\mathrm{SID}_j, \mathrm{TC}_j\}$ sent from GWN over a secure channel and stores $\{\mathrm{SID}_j, \mathrm{TC}_j\}$ in memory.

3.3 Login and Key Agreement Phase

In this stage, the legally registered user U_i can share a session key with registered sensor node S_j that wants to register via GWN[11]. As shown in Fig.3, U_i authenticates with S_j mutually and establishes a session key for secure communication with the help of GWN. The detailed steps are described below.

Step 1 U_i inserts the smart card SC and enters his/her identity ID_i and password PW_i. After that, SC uses equation (7) for the calculation.

$$\begin{cases} r_i^* = C_i \oplus h(\mathrm{ID}_i||\mathrm{PW}_i) \\ A_i^* = h(\mathrm{ID}_i||\mathrm{PW}_i||r_i^*) \end{cases} \tag{7}$$

SC checks $A_i^* = A_i$ holds or not. If this check fails, SC will reject the user's login request. Otherwise, it means that this user is the legitimate holder of SC, and also indicates $r_i^* = r_i$. Then, SC recovers the temporary credentials TC_i for U_i and computes pseudo-identity PID_i by equation (8).

$$\begin{cases} \mathrm{TC}_i = B_i \oplus h(\mathrm{ID}_i||\mathrm{PW}_i||\mathrm{TE}_i) \\ \mathrm{PID}_i = h(\mathrm{ID}_i||r_i) \end{cases} \tag{8}$$

After that, SC selects two random numbers $N_1 \in Z_q^*$, $x_1 \in Z_q^*$ and calculates the values F_1, F_2, F_3 according to equation (9). U_i sends message $M_1 = \{F_1, F_2, F_3, \mathrm{PID}_i\}$ to GWN over a public channel.

$$\begin{cases} F_1 = x_1 \cdot P \\ F_2 = (\mathrm{ID}_i||\mathrm{TE}_i||\mathrm{SID}_j||N_1) \oplus h(x_1 \cdot P_{\mathrm{pub}}) \\ F_3 = h(F_1||\mathrm{ID}_i||\mathrm{ID}_{\mathrm{GWN}}||\mathrm{TC}_i||N_1||\mathrm{TE}_i||\mathrm{SID}_j) \end{cases} \tag{9}$$

Step 2 Once GWN receives the message M_1 from U_i, it extracts the values needed for subsequent authentication according to equation (10).

$$\mathrm{ID}_i||\mathrm{TE}_i||\mathrm{SID}_j||N_1 = F_2 \oplus h(K_{\mathrm{GU}} \cdot F_1) \tag{10}$$

GWN verifies the effectiveness of TE_i. If the verification fails, GWN rejects U_i's login request. Otherwise, GWN calculates the TC_i and F_3^* by equation (11).

$$\begin{cases} \mathrm{TC}_i = h(\mathrm{ID}_i||\mathrm{PID}_i||\mathrm{ID}_{\mathrm{GWN}}||K_{\mathrm{GU}}||\mathrm{TE}_i) \\ F_3^* = h(F_1||\mathrm{ID}_i||\mathrm{ID}_{\mathrm{GWN}}||\mathrm{TC}_i||N_1||\mathrm{TE}_i||\mathrm{SID}_j) \end{cases} \tag{11}$$

GWN verifies whether $F_3^* = F_3$ holds or not. GWN rejects U_i's login request if the condition fails. Or else, it proves that U_i is a legitimate user who has registered with GWN. Then, GWN selects three random numbers $N_2 \in Z_q^*$, $x \in Z_q^*$, $x_2 \in Z_q^*$ and calculates the temporary credentials TC_j of S_j and three values F_4, F_5, F_6 according to equation (12).

$$\begin{cases} \mathrm{TC}_j = h(K_{\mathrm{GS}}||\mathrm{SID}_j) \\ F_4 = x_2 \oplus h(\mathrm{TC}_j||N_2||\mathrm{ID}_{\mathrm{GWN}}) \\ F_5 = h(\mathrm{ID}_i||\mathrm{TE}_i||x) \oplus h(N_2||\mathrm{TC}_j) \\ F_6 = h(F_1||h(\mathrm{ID}_i||\mathrm{TE}_i||x)||x_2||N_2) \end{cases} \tag{12}$$

Lately, GWN sends a message $M_2 = \{F_1, F_4, F_5, F_6, N_2, \mathrm{PID}_i\}$ to S_j over a public channel.

Step 3 Upon receiving the message M_2, S_j calculates a series of values according to equation (13).

$$\begin{cases} x_2 = F_4 \oplus h(\mathrm{TC}_j||N_2||\mathrm{ID}_{\mathrm{GWN}}) \\ h(\mathrm{ID}_i||\mathrm{TE}_i||x) = F_5 \oplus h(N_2||\mathrm{TC}_j) \\ F_6^* = h(F_1||h(\mathrm{ID}_i||\mathrm{TE}_i||x)||x_2||N_2) \end{cases} \tag{13}$$

S_j verifies whether $F_6^* = F_6$ holds or not, and aborts the current phase if equation is not matched. Otherwise, S_j generates two random numbers $N_3 \in Z_q^*$, $x_3 \in Z_q^*$ and calculates the session key SK_{ji} and a set of values by equation (14).

$$\begin{cases} F_7 = x_3 \cdot P \\ \mathrm{SK}_{ji} = h(\mathrm{PID}_i||\mathrm{SID}_j||x_3 \cdot F_1||F_1||F_7) \\ F_8 = h(\mathrm{SK}_{ji}||N_3) \\ F_9 = (F_8||F_7||N_3) \oplus h(\mathrm{TC}_j||\mathrm{PID}_i) \\ F_{10} = h(\mathrm{TC}_j||F_7||N_3||F_8) \end{cases} \tag{14}$$

S_j sends a message $M_3 = \{F_9, F_{10}, \mathrm{SID}_j, \mathrm{PID}_i\}$ to GWN over a public channel.

Step 4 As soon as GWN receives M_3, it extracts the values to be used for the subsequent operation and the validation value F_{10}^* by equation (15).

$$\begin{cases} F_8||F_7||N_3 = F_9 \oplus h(\mathrm{TC}_j||\mathrm{PID}_i) \\ F_{10}^* = h(\mathrm{TC}_j||F_7||N_3||F_8) \end{cases} \tag{15}$$

GWN verifies whether $F_{10}^* = F_{10}$ holds or not. If

U_i	GWN	S_j
Inserts SC		
Inputs $<\mathrm{ID}_i, \mathrm{PW}_i>$		
$r_i^* = C_i \oplus h(\mathrm{ID}_i \| \mathrm{PW}_i)$		
$A_i^* = h(\mathrm{ID}_i \| \mathrm{PW}_i \| r_i^*)$		
Checks $A_i^* = A_i$		
$TC_i = B_i \oplus h(\mathrm{ID}_i \| \mathrm{PW}_i \| \mathrm{TE}_i)$		
Generates $N_1 \in Z_q^*, x_1 \in Z_q^*$		
$F_1 = x_1 \cdot P$		
$F_2 = (\mathrm{ID}_i \| \mathrm{TE}_i \| \mathrm{SID}_j \| N_1) \oplus h(x_1 \cdot P_{\mathrm{pub}})$		
$F_3 = h(F_1 \| \mathrm{ID}_i \| \mathrm{ID}_{\mathrm{GWN}} \| \mathrm{TC}_i \| N_1 \| \mathrm{TE}_i \| \mathrm{SID}_j)$		
$M_1 = \{F_1, F_2, F_3, \mathrm{PID}_i\} \longrightarrow$		
	$\mathrm{ID}_i \| \mathrm{TE}_i \| \mathrm{SID}_j \| N_1 = F_2 \oplus h(K_{\mathrm{GU}} \cdot F_1)$	
	Checks the validity of TE_i	
	$\mathrm{TC}_i = h(\mathrm{ID}_i \| \mathrm{PID}_i \| \mathrm{ID}_{\mathrm{GWN}} \| K_{\mathrm{GU}} \| \mathrm{TE}_i)$	
	$F_3^* = h(F_1 \| \mathrm{ID}_i \| \mathrm{ID}_{\mathrm{GWN}} \| \mathrm{TC}_i \| N_1 \| \mathrm{TE}_i \| \mathrm{SID}_j)$	
	Checks $F_3^* = F_3$	
	Generates $N_2 \in Z_q^*, x \in Z_q^*, x_2 \in Z_q^*$	
	$\mathrm{TC}_j = h(K_{\mathrm{GS}} \| \mathrm{SID}_j)$	
	$F_4 = x_2 \oplus h(\mathrm{TC}_j \| N_2 \| \mathrm{ID}_{\mathrm{GWN}})$	
	$F_5 = h(\mathrm{ID}_i \| \mathrm{TE}_i \| x) \oplus h(N_2 \| \mathrm{TC}_j)$	
	$F_6 = h(F_1 \| h(\mathrm{ID}_i \| \mathrm{TE}_i \| x) \| x_2 \| N_2)$	
	$M_2 = \{F_1, F_4, F_5, F_6, N_2, \mathrm{PID}_i\} \longrightarrow$	
		$x_2 = F_4 \oplus h(\mathrm{TC}_j \| N_2 \| \mathrm{ID}_{\mathrm{GWN}})$
		$h(\mathrm{ID}_i \| \mathrm{TE}_i \| x) = F_5 \oplus h(N_2 \| \mathrm{TC}_j)$
		$F_6^* = h(F_1 \| h(\mathrm{ID}_i \| \mathrm{TE}_i \| x) \| x_2 \| N_2)$
		Checks $F_6^* = F_6$
		Generates $N_3 \in Z_q^*, x_3 \in Z_q^*$
		$F_7 = x_3 \cdot P$
		$\mathrm{SK}_{ji} = h(\mathrm{PID}_i \| \mathrm{SID}_j \| x_3 \cdot F_1 \| F_1 \| F_7)$
		$F_8 = h(\mathrm{SK}_{ji} \| N_3)$
		$F_9 = (F_8 \| F_7 \| N_3) \oplus h(\mathrm{TC}_j \| \mathrm{PID}_i)$
		$F_{10} = h(\mathrm{TC}_j \| F_7 \| N_3 \| F_8)$
		$M_3 = \{F_9, F_{10}, \mathrm{SID}_j, \mathrm{PID}_i\} \longleftarrow$
	$F_8 \| F_7 \| N_3 = F_9 \oplus h(\mathrm{TC}_j \| \mathrm{PID}_i)$	
	$F_{10}^* = h(\mathrm{TC}_j \| F_7 \| N_3 \| F_8)$	
	Checks $F_{10}^* = F_{10}$	
	$\mathrm{PID}_i^{\mathrm{new}} = \mathrm{PID}_i \oplus h(N_3 \| \mathrm{TC}_i)$	
	$F_{11} = \mathrm{PID}_i^{\mathrm{new}} \oplus h(\mathrm{ID}_{\mathrm{GWN}} \| \mathrm{TC}_i \| N_1)$	
	$F_{12} = h(\mathrm{PID}_i^{\mathrm{new}} \| \mathrm{TC}_i)$	
	$F_{13} = (F_8 \| F_7 \| N_3) \oplus h(\mathrm{PID}_i^{\mathrm{new}})$	
	$M_4 = \{F_{11}, F_{12}, F_{13}\} \longleftarrow$	
$\mathrm{PID}_i^{\mathrm{new}*} = F_{11} \oplus h(\mathrm{ID}_{\mathrm{GWN}} \| \mathrm{TC}_i \| N_1)$		
$F_{12}^* = h(\mathrm{PID}_i^{\mathrm{new}*} \| \mathrm{TC}_i)$		
Checks $F_{12}^* = F_{12}$		
$F_8 \| F_7 \| N_3 = F_{13} \oplus h(\mathrm{PID}_i^{\mathrm{new}})$		
$\mathrm{SK}_{ij} = h(\mathrm{PID}_i \| \mathrm{SID}_j \| x_1 \cdot F_7 \| F_1 \| F_7)$		
$F_8^* = h(\mathrm{SK}_{ij} \| N_3)$		
Checks $F_8^* = F_8$		

Fig. 3 Login and key agreement phase

the condition fails, this session is aborted immediately. Otherwise, GWN updates PID_i by equation (16) and calculates some values.

$$\begin{cases} \mathrm{PID}_i^{\mathrm{new}} = \mathrm{PID}_i \oplus h(N_3 \| \mathrm{TC}_i) \\ F_{11} = \mathrm{PID}_i^{\mathrm{new}} \oplus h(\mathrm{ID}_{\mathrm{GWN}} \| \mathrm{TC}_i \| N_1) \\ F_{12} = h(\mathrm{PID}_i^{\mathrm{new}} \| \mathrm{TC}_i) \\ F_{13} = (F_8 \| F_7 \| N_3) \oplus h(\mathrm{PID}_i^{\mathrm{new}}) \end{cases} \tag{16}$$

GWN then sends a message $M_4 = \{F_{11}, F_{12}, F_{13}\}$ to U_i over a public channel.

Step 5 After receiving the message from GWN, U_i extracts the updated pseudo-identity $\mathrm{PID}_i^{\mathrm{new}}*$ and calculates $F_{12}*$ through equation (17) .

$$\begin{cases} \mathrm{PID}_i^{\mathrm{new}}* = F_{11} \oplus h(\mathrm{ID}_{\mathrm{GWN}} \| \mathrm{TC}_i \| N_1) \\ F_{12}* = h(\mathrm{PID}_i^{\mathrm{new}}* \| \mathrm{TC}_i) \end{cases} \tag{17}$$

U_i checks whether $F_{12}* = F_{12}$ holds or not. U_i terminates the session on the mismatch of equality. Otherwise, it indicates that U_i authenticates GWN and the accuracy of the transmitted message, and also means that $\mathrm{PID}_i^{\mathrm{new}}* = \mathrm{PID}_i^{\mathrm{new}}$. Then, U_i recovers and calculates some values by equation (18).

$$\begin{cases} F_8 \| F_7 \| N_3 = F_{13} \oplus h(\mathrm{PID}_i^{\mathrm{new}}) \\ \mathrm{SK}_{ij} = h(\mathrm{PID}_i \| \mathrm{SID}_j \| x_1 \cdot F_7 \| F_1 \| F_7) \\ F_8* = h(\mathrm{SK}_{ij} \| N_3) \end{cases} \tag{18}$$

U_i verifies whether $F_8* = F_8$ holds or not. If the verification fails, U_i terminates the current session immediately. Otherwise, it means that U_i and S_j have successfully negotiated a session key, which can be used to secure subsequent communications.

4 Security Analysis

The most basic requirement of any authentication scheme is security. In this section, we give a security analysis of the proposed scheme. The proposed scheme provides mutual authentication, satisfies user anonymity and untraceability, and is resistant to many common attacks as described below.

4.1 User Anonymity

For the sake of ensuring user's privacy, the authentication scheme must guarantee anonymity. In the proposed scheme, the identity ID_i of U_i is neither transmitted in a public channel nor stored in SC. As shown in equation (19), the proposed scheme encrypts ID_i with a random number r_i chosen by U_i thereby generating the user's pseudo-identity PID_i. In the login and key agreement phase, the proposed scheme transmits the identity information in the public channel as PID_i instead of ID_i, and even if an attacker intercepts PID_i, he/she cannot crack ID_i due to the protection of $h(\cdot)$ with a random number r_i. In summary, the proposed scheme satisfies user anonymity.

$$\mathrm{PID}_i = h(\mathrm{ID}_i \| r_i) \tag{19}$$

4.2 User Untraceability

U_i sends a login message $M_1 = \{F_1, F_2, F_3, \mathrm{PID}_i\}$ to GWN through a public channel, and an attacker can intercept M_1. However, as equation (20) shows, $\{F_1, F_2, F_3\}$ are all related to the random numbers x_1 or N_1, and the random numbers are different in each session. Similarly, the random numbers make PID_i vary from session to session. That is, all values in M_1 cannot be associated with a specific user. Therefore, the attacker cannot trace the user's actions during the login and key agreement phase. Meanwhile, after GWN authenticates S_j in the login and key agreement phase, it updates PID_i by equation (21) and transmits it to U_i, which means that U_i's pseudo-identity is dynamic. Usually, an attacker intercepts messages from different sessions and tries to find the relationship between them to determine whether they belong to the same device[12]. In the proposed scheme, GWN does not transmit $\mathrm{PID}_i^{\mathrm{new}}$ directly through a public channel after it updates PID_i, but protects $\mathrm{PID}_i^{\mathrm{new}}$ by equation (22) before transmitting F_{11}. In this way, attacker cannot obtain the correlation between PID_i and $\mathrm{PID}_i^{\mathrm{new}}$ by intercepting both of them. As shown above, proposed scheme not only satisfies user untraceability, but also enhances user anonymity because of dynamic identity.

$$\begin{cases} F_1 = x_1 \cdot P \\ F_2 = (\mathrm{ID}_i \| \mathrm{TE}_i \| \mathrm{SID}_i \| N_1) \oplus h(x_1 \cdot P_{\mathrm{pub}}) \\ F_3 = h(F_1 \| \mathrm{ID}_i \| \mathrm{ID}_{\mathrm{GWN}} \| \mathrm{TC}_i \| N_1 \| \mathrm{TE}_i \| \mathrm{SID}_j) \end{cases} \tag{20}$$

$$\mathrm{PID}_i^{\mathrm{new}} = F_{11} \oplus h(\mathrm{ID}_{\mathrm{GWN}} \| \mathrm{TC}_i \| N_1) \tag{21}$$

$$F_{11} = \mathrm{PID}_i^{\mathrm{new}} \oplus h(\mathrm{ID}_{\mathrm{GWN}} \| \mathrm{TC}_i \| N_1) \tag{22}$$

4.3 Mutual Authentication

The three parties involved in the communication, i.e., U_i, GWN, and S_j, must authenticate each other to ensure the legitimacy of either party. In the login phase, SC authenticates the currently logged-in user as the legitimate holder of SC by verifying A_i in equation (23). GWN authenticates U_i by verifying F_3 in equation (23), in particular TC_i contained therein, before responding to U_i's login request. GWN authenticates S_j by checking F_{10} in equation (23) according to integrity and accuracy, es-

pecially TC_j contained therein. S_j achieves authentication of GWN by examining F_6 in equation (23), especially $h(ID_i||TE_i||x)$ contained therein. U_i authenticates GWN by verifying F_{12} in equation (23), and verifies that the session key reached with S_j is consistent by checking F_8. In conclusion, if the whole authentication process can be completed, the participants can trust each other, which means that proposed scheme supports mutual authentication.

$$\begin{cases} A_i = h(ID_i||PW_i||r_i) \\ F_3 = h(F_1||ID_i||ID_{GWN}||TC_i||N_1||TE_i||SID_j) \\ F_{10} = h(TC_j||F_7||N_3||F_8) \\ F_6 = h(F_1||h(ID_i||TE_i||x)||x_2||N_2) \\ F_{12} = h(PID_i^{new}||TC_i) \\ F_8 = h(SK_{ij}||N_3) \end{cases} \tag{23}$$

4.4 Resistance to Replay Attack

Although the proposed scheme still does not use timestamps as Hu *et al*'s scheme[10], all values transmitted in a public channel are added with random numbers N_1, x_1, N_2, x, x_2, N_3, x_3 chosen randomly by U_i, S_j, and GWN in the login and key agreement phase, and these random numbers vary from session to session. Even if an attacker intercepts messages M_1, M_2, M_3, M_4 over a public channel and replays them, the attacker cannot compute the correct session key. As shown in equation (24), if the attacker wants to compute the session key, he/she must know F_7 at first. However, he/she cannot obtain F_7 in the session key from the intercepted messages. It is because the attacker must first obtain the random number x_3 chosen by S_j and the base point P of the elliptic curve in order to compute F_7, but he/she cannot know these values from the messages transmitted over the public channel, so the attacker cannot compute the session key. It follows that the proposed scheme is able to resist replay attacks.

$$SK_{ji} = h(PID_i||SID_j||x_3 \cdot F_1||F_1||F_7) \tag{24}$$

4.5 Resistance to Man-in-the-Middle(MITM) Attack

If an attacker tries to eavesdrop, manipulate, or intercept messages transmitted in the public channel, he/she will be detected by the mutual authentication mechanism at each entity involved in the communication. As shown in Sections 4.3 and 4.4, such a malicious attempt will not succeed even if the attacker attempts to replay or tamper with the values in the transmitted message. Thus, the proposed scheme is resistant to MITM attacks.

4.6 Resistance to DOS Attack

An attacker may send a large number of fake request messages to the target device multiple times in an attempt to prevent legitimate users from accessing the service, resulting in the target device being unable to provide normal service. In the proposed scheme, SC verifies the U_i's login information. In equation (25), ID_i and PW_i are the identity and password entered by U_i, and r_i is recovered from $h(\cdot)$ and C_i, both of which are stored in SC inserted by U_i. Therefore, SC can verify whether U_i is the legitimate holder of SC or not by verifying A_i. In addition to this, each message in the proposed scheme authenticates the sender before proceeding to the next operation. If authentication is successful, the session will proceed normally. Otherwise, it will be terminated immediately. Thus, the proposed scheme is resistant to DOS attacks.

$$\begin{cases} r_i = C_i \oplus h(ID_i||PW_i) \\ A_i = h(ID_i||PW_i||r_i) \end{cases} \tag{25}$$

4.7 Perfect Forward Secrecy

In the proposed scheme, a new session key will be generated between U_i and S_j after each communication is completed. If this session key is corrupted by an attacker, however, the attacker cannot find significant correlation between past, present and future session keys because the random numbers x_1 and x_3 contained in each session key change from session to session. As a result, the proposed scheme achieves perfect forward secrecy.

4.8 Resistance to Impersonation Attack

An attacker may impersonate U_i to launch an attack. In the proposed scheme, U_i communicates by using a pseudo-identity PID_i, which is updated at the end of each authentication phase. Therefore, it is difficult for the attacker to impersonate a legitimate user using some outdated pseudo-identity. Even if the attacker happens to guess the identity of U_i, he/she can never send a valid message to the GWN to prove his/her identity. It is because the attacker cannot know the temporary credential TC_i and the expiration time TE_i issued by GWN to the legitimate user. In summary, the proposed scheme is able to resist impersonation attacks.

4.9 Resistance to Stolen Smart Card Attack

If the attacker steals the smart card SC, then he/she may impersonate U_i to log in, insert SC, and then enter his/her own identity and password. However, the attacker cannot pass the authentication of equation (26). That is, even if the attacker steals SC and leaks the data

stored inside, he/she still cannot obtain the important authentication information. So the proposed scheme is resistant to stolen smart card attacks.

$$\begin{cases} A_i^* = h(\mathrm{ID}_i \| \mathrm{PW}_i \| r_i^*) \\ \text{Checks } A_i^* = A_i \end{cases} \tag{26}$$

4.10 Resistance to Known Session Key Attack

If an attacker wants to use an old or compromised session key for a session, the scheme is considered vulnerable to known session key attacks. As shown in equation (27), the session key in the proposed scheme contains random numbers x_1 and x_3 that are refreshed with each communication, so the attacker is hard to know F_1 and F_7. Meanwhile, due to the complexity of computational Diffie-Hellman problem (CDH), it is infeasible for the attacker to obtain new information from the old session key and extract $\{x_1, x_3\}$ from $\{F_1, F_7\}$.

$$\begin{cases} \mathrm{SK}_{ji} = \mathrm{SK}_{ij} = h(\mathrm{PID}_i \| \mathrm{SID}_j \| x_3 \cdot F_1 \| F_1 \| F_7) \\ \qquad = h(\mathrm{PID}_i \| \mathrm{SID}_j \| x_1 \cdot F_7 \| F_1 \| F_7) \\ F_1 = x_1 \cdot P \\ F_7 = x_3 \cdot P \end{cases} \tag{27}$$

4.11 Resistance to Off-Line Password Guessing Attack

Suppose an attacker tries to guess PW_i of the legitimate user using the stolen smart card or any previously transmitted message, so as to pass the verification of equation (27), he/she must know the real identity ID_i and r_i^* of the legitimate user. However, the attacker cannot obtain ID_i based on the intercepted message. Moreover, r_i is an independent and unique random number chosen arbitrarily by the legitimate user during the registration phase. The user must extract r_i^* at the login stage based on the registered ID_i and PW_i as well as C_i stored in the SC in order to pass the verification of equation (27). That is, even if the attacker guesses PW_i correctly by chance, it will not be able to pass the verification of SC. Therefore, the proposed scheme can resist the off-line password guessing attacks.

4.12 No Key Control

Each entity in the session cannot compute the session key separately by controlling the key negotiation process. Not only x_1 and x_3, but also F_1 and F_7 are chosen and computed independently by U_i and S_j, respectively. As shown in equation (27), if U_i does not extract F_7 created by S_j based on the received message M_4, then SK_{ij} cannot be computed. Similarly, if S_j does not extract F_1 created by U_i based on M_2, then SK_{ji} cannot be computed.

5 Performance Analysis

This section presents a comparison of Hu *et al*'s scheme[10] with the proposed scheme and other schemes of the same type in terms of both performance and security features.

5.1 Implementation Setup

We refer to the experimental results of Xie *et al*[13]. To make it easier, we only consider four main cryptographic operations: ① one-way Hash function, ② point multiplication, ③ symmetric encryption and decryption, and ④ fuzzy extraction function. We do not consider the XOR operation because it can be neglected. The encryption times of the Hash function, encryption/decryption, point multiplication in elliptic curves, and fuzzy extraction function are denoted as T_h, T_s, T_e, and T_f, and the estimated time are 0.068, 0.56, 2.501, and 2.501 ms, respectively.

5.2 Computation Comparisons

Table 3 shows the comparison of proposed scheme

Table 3 Computational cost of the schemes

Scheme	User	GWN	Senor node	Total	Estimated time/ms
Hu *et al*[10]	$7T_\mathrm{h}+3T_\mathrm{e}$	$10T_\mathrm{h}+T_\mathrm{e}$	$6T_\mathrm{h}+2T_\mathrm{e}$	$23T_\mathrm{h}+6T_\mathrm{e}$	16.570
Sutrala *et al*[14]	$16T_\mathrm{h}+5T_\mathrm{e}+T_\mathrm{f}$	$9T_\mathrm{h}+3T_\mathrm{e}$	$8T_\mathrm{h}+4T_\mathrm{e}$	$33T_\mathrm{h}+12T_\mathrm{e}+T_\mathrm{f}$	34.757
Xie *et al*[15]	$8T_\mathrm{h}+3T_\mathrm{e}+T_\mathrm{s}$	$7T_\mathrm{h}+T_\mathrm{e}+2T_\mathrm{s}$	$5T_\mathrm{h}+2T_\mathrm{e}+T_\mathrm{s}$	$20T_\mathrm{h}+6T_\mathrm{e}+4T_\mathrm{s}$	18.606
Srinivas *et al*[16]	$17T_\mathrm{h}+6T_\mathrm{e}+T_\mathrm{f}$	$12T_\mathrm{h}+3T_\mathrm{e}$	$8T_\mathrm{h}+4T_\mathrm{e}$	$37T_\mathrm{h}+13T_\mathrm{e}+T_\mathrm{f}$	37.530
Sahoo *et al*[17]	$10T_\mathrm{h}+4T_\mathrm{e}+2T_\mathrm{s}+T_\mathrm{f}$	$5T_\mathrm{h}+2T_\mathrm{e}+T_\mathrm{s}$	$5T_\mathrm{h}+2T_\mathrm{e}+2T_\mathrm{s}$	$20T_\mathrm{h}+8T_\mathrm{e}+5T_\mathrm{s}+T_\mathrm{f}$	26.669
Proposed	$11T_\mathrm{h}+3T_\mathrm{e}$	$14T_\mathrm{h}+T_\mathrm{e}$	$7T_\mathrm{h}+2T_\mathrm{e}$	$32T_\mathrm{h}+6T_\mathrm{e}$	17.182

with other similar schemes. Although proposed scheme has a slightly longer running time than Hu *et al'* s scheme[10], it has better security and can effectively improve the security flaws of Hu *et al*'s scheme[10]. Moreover, the computational cost of proposed scheme is significantly lower than the schemes of Sutrala *et al*[14], Xie *et al*[15], Srinivas *et al*[16] and Sahoo *et al*[17] .

5.3 Comparison of Safety Features and Functions

Table 4 shows that the existing schemes do not meet all the security requirements, and the proposed scheme provides sufficient security advantages compared to other schemes and is suitable for wireless sensor networks in the IoT environment.

Table 4 Security comparison among relevant schemes

Scheme	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11
Hu *et al*[10]	√	√	√	√	√	×	√	√	×	√	√
Sutrala *et al*[14]	×	×	√	×	√	√	√	√	×	√	√
Xie *et al*[15]	√	√	×	√	×	√	√	×	√	√	√
Srinivas *et al*[16]	×	√	×	×	×	√	×	√	×	√	×
Sahoo *et al*[17]	√	√	×	√	√	×	√	√	√	×	√
Proposed scheme	√	√	√	√	√	√	√	√	√	√	√

R1: User anonymity; R2: User untraceability; R3: Mutual authentication; R4: Resistance to reply attack; R5: Resistance to MITM attack; R6: Resistance to DOS attack; R7: Forward security; R8: Resistance to impersonation attack; R9: Resistance to stolen smart card attack; R10: Resistance to known session key attack; R11: Resistance to off-line password guessing attack; √ denotes the scheme can provide the corresponding attribute; × denotes the scheme cannot provide the corresponding attribute

6 Conclusion

In this paper, we review a two-factor authentication scheme proposed by Hu *et al* for WSNs in an IoT environment, and point out some flaws of it. Then, we propose an improved scheme that addresses Hu *et al'* s scheme security concerns, and takes into account computational efficiency. We demonstrate the security of proposed scheme through security analysis, and show that proposed scheme is resistant to a wide range of known attacks and meets all security requirements. In addition, we compare and analyze the performance of proposed scheme and Hu *et al'* s scheme as well as similar schemes in recent years. The analysis results show that proposed scheme achieves desired efficiency and is compatible with low-cost, restricted IoT devices.

References

[1] Tran-Dang H, Krommenacker N, Charpentier P, *et al*. Toward the Internet of Things for physical Internet: Perspectives and challenges[J]. *IEEE Internet of Things Journal*, 2020, **7**(6): 4711-4736.

[2] Bin Abu Bakar K, Zuhra F T, Isyaku B, *et al*. A review on the immediate advancement of the Internet of Things in wireless telecommunications[J]. *IEEE Access*, 2023, **11**: 21020-21048.

[3] Du J Q, Kang B Y, Han Y B. Improvement on a biometric based user authentication scheme in wireless sensor networks using smart cards[J]. *Wuhan University Journal of Natural Sciences*, 2020, **25**(2): 155-161.

[4] Chander B, Kumaravelan G. An improved 2-factor authentication scheme for WSN based on ECC[J]. *IETE Technical Review*, 2023, **40**(2): 167-178.

[5] Szymoniak S, Kesar S. Key agreement and authentication protocols in the Internet of Things: A survey[J]. *Applied Sciences*, 2022, **13**(1): 404.

[6] Ostad-Sharif A, Arshad H, Nikooghadam M, *et al*. Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme [J]. *Future Generation Computer Systems*, 2019, **100**: 882-892.

[7] Chen C T, Lee C C, Lin I C. Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments [J]. *PLoS One*, 2020, **15**(4): e0232277.

[8] Chunka C, Banerjee S, Goswami R S. An efficient user authentication and session key agreement in wireless sensor

network using smart card[J]. *Wireless Personal Communications*, 2021, **117**(2): 1361-1385.

[9] Lee J, Oh J, Kwon D, *et al.* PUFTAP-IoT: PUF-based three-factor authentication protocol in IoT environment focused on sensing devices[J]. *Sensors*, 2022, **22**(18):7075.

[10] Hu B, Tang W, Xie Q. A two-factor security authentication scheme for wireless sensor networks in IoT environments[J]. *Neurocomputing*, 2022, **500**: 741-749.

[11] Li R, Kang B Y, Mai K Q. Analysis and improvement on a hash-based authentication scheme for multi-server architecture[J]. *Wuhan University Journal of Natural Sciences*, 2021, **26**(5): 394-404.

[12] Yang S, Zheng X, Liu G, *et al.* IBA: A secure and efficient device-to-device interaction-based authentication scheme for Internet of Things[J]. *Computer Communications*, 2023, **200**: 171-181.

[13] Xie Q, Wong D S, Wang G, *et al.* Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model[J]. *IEEE Transactions on Information Forensics and Security*, 2017, **12**(6): 1382-1392.

[14] Sutrala A K, Obaidat M S, Saha S, *et al*. Authenticated key agreement scheme with user anonymity and untraceability for 5G-enabled softwarized industrial cyber-physical systems [J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, **23**(3): 2316-2330.

[15] Xie Q, Li K H, Tan X, *et al*. A secure and privacy-preserving authentication protocol for wireless sensor networks in smart city[J]. *EURASIP Journal on Wireless Communications and Networking*, 2021(2021**)**: 119.

[16] Srinivas J, Das A K, Wazid M, *et al*. Designing secure user authentication protocol for big data collection in IoT-based intelligent transportation system[J]. *IEEE Internet of Things Journal*, 2021, **8**(9): 7727-7744.

[17] Sahoo S S, Mohanty S, Majhi B. A secure three factor based authentication scheme for health care systems using IoT enabled devices[J]. *Journal of Ambient Intelligence and Humanized Computing*, 2021, **12**(1): 1419-1434.

□