Hindawi
Security and Communication Networks
Volume 2021, Article ID 2037188, 17 pages
https://doi.org/10.1155/2021/2037188

Research Article

An Efficient and Provable Multifactor Mutual Authentication Protocol for Multigateway Wireless Sensor Networks

Shuailiang Zhang,[1,2] **Xiujuan Du**,[1,2] **and Xin Liu**[1,2]

[1]*Computer Department, Qinghai Normal University, Xining 810008, China*
[2]*Academy of Plateau Science and Sustainability, Xining 810008, China*

Correspondence should be addressed to Xiujuan Du; dxj@qhnu.edu.cn

Received 19 April 2021; Revised 25 June 2021; Accepted 19 July 2021; Published 4 August 2021

Academic Editor: James Ying

As the most popular way of communication technology at the moment, wireless sensor networks have been widely concerned by academia and industry and plays an important role in military, agriculture, medicine, and other fields. Identity authentication offers the first line of defence to ensure the security communication of wireless sensor networks. Since the sensor nodes are resource-limited in the wireless networks, how to design an efficient and secure protocol is extremely significant. The current authentication protocols have the problem that the sensor nodes need to execute heavy calculation and communication consumption during the authentication process and cannot resist node capture attack, and the protocols also cannot provide perfect forward and backward security and cannot resist replay attack. Multifactor identity authentication protocols can provide a higher rank of security than single-factor and two-factor identity authentication protocols. The multigateway wireless sensor networks' structure can provide a larger communication coverage area than the single-gateway network structure, so it has become the focus of recent studies. Therefore, we design a novel multifactor authentication protocol for multigateway wireless sensor networks, which only apply the lightweight hash function and are given biometric information to achieve a higher level of security and efficiency and a larger communication coverage area. We separately apply BAN logic, random oracle model, and AVISPA tool to validate the security of our authentication protocol in Case 1 and Case 2. We put forward sixteen evaluation criteria to comprehensively evaluate our authentication protocol. Compared with the related authentication protocols, our authentication protocol is able to achieve higher security and efficiency.

1. Introduction

As the prevalent way of communication and the significant section of the Internet of Things, wireless sensor networks are composed of massive sensor nodes, which have collection and computing abilities, and communicate with the corresponding communication parties via wireless technology [1]. Wireless sensor networks' communications are widely applied in military, industrial, agricultural monitoring, wearable health monitoring systems, smart home environment, intelligent transportation systems, and other fields. These sensor nodes are small and resource-constrained, and they are often randomly deployed in unattended or hostile region under the regulation of one or more gateway nodes to gather and transmit the information on public network channel [2]. Due to the characteristics of the communication channel in wireless sensor network, the communication information is prone to various types of attacks. Mutual authentication plays a significant role in guaranteeing the security among the existing security mechanisms [3] and is considered as the basic access control that the user must first pass through the verification of the sensor node before accessing the gathered information [4].

The current identity authentication technology can be divided into three types: password based single-factor authentication technology, password and smart card based two-factor authentication technology, and password, smart card, and biometric based three-factor authentication technology [5]. The aforementioned third type is the most commonly used authentication technology, and it enhances

the security of the wireless network works to a higher level [6, 7]. At present, most of the researches are keen on the identity authentication technology of single gateway, while only a few people are engaged in identity authentication technology of multigateway structure [8]. We can apply multiple gateway nodes to extend the communication coverage area and increase scalability [9]. However, the current multigateway authentication technology has some disadvantages such as high computational complexity and heavy storage consumption and is vulnerable to various attacks. Therefore, for the sake of eliminating the security flaws and increasing the computation efficiency, we design a novel lightweight mutual authentication protocol for the multiple gateway nodes networks.

1.1. Network Model. As shown in Figure 1, it involves three communication entities, that is, sensor nodes, home/foreign gateway node, and user in case 1. The sensor node and user should complete registration at the gateway node. After registration, the user delivers the login request to the gateway node. The gateway authenticates are in charge of transmitting authentication information between the user and the sensor node. After completing authentication process, the registered user has ability to obtain information gathered by the sensors under the negotiated session key.

As shown in Figure 2, it involves four communication entities, that is, sensor nodes, home gateway node, foreign gateway node, and user in case 2. In addition to completing the authentication of case 1, it is also necessary to achieve the authentication between the home gateway node and the foreign gateway node.

1.2. Related Works. Gope and Hwang [10] proposed an efficient and secure authentication scheme and claimed that their scheme is able to preserve the user anonymity for roaming services in global mobility networks by way of using the one-way hash function operation. Xu et al. [11] discovered that the scheme of Gope and Hwang is vulnerable to reply attacks and has a heavy storage cost. Similarly, Lu et al. [3] also pointed out that scheme of Gope and Hwang is susceptible to specific known information attack, and the password alteration section is inaccurate. Fan et al. [12] found that the scheme of Gope and Hwang is vulnerable to offline guessing attack and the desynchronization attack and does not retain robust forward security. Then, they proposed a novel efficient mutual and key agreement scheme with desynchronization for anonymous roaming service in global mobility networks. However, Mohit and Narendra [13] reviewed the scheme of Wu and showed that the scheme has the problem of the traceability of the mobile user and inefficient wrong password detection.

In order to preserve security and privacy and reduce communication and computation costs, Das et al. [14] proposed a biometric-based authentication protocol for the Industrial Internet of Things. Unfortunately, Hussain and Chaudhry [15] discovered that the protocol of Das et al. is unable to prevent the assailant from obtaining the public parameters kept in the smart device and fails to resist session key attack and achieve perfect forward secrecy. So, against offline password guessing attack and user impersonation attack, Amin et al. [16] demonstrated a secure three-factor mutual authentication protocol, and this protocol lengthens the lifetime of network by means of decreasing the cost of sensor nodes. Later, Sharif et al. [17] claimed that the protocol of Amin et al. cannot boycott strong reply attacks and cannot realize the prefect forward secrecy. However, Wu et al. [18] pointed out that both of the two protocols [14, 17] suffer from under offline surmising attack.

To overcome user and sensor node impersonation attacks, He et al. [19] introduced a novel mutual authentication design based on the temporal credential for wireless sensor networks. Afterwards, Kumari et al. [20] demonstrated that there are seven security problems in the design of He et al. Jiang et al. [21] revealed that the design of He et al. is prone to malicious user impersonation attack, stolen smart card attack, and tracking attack in the authentication process and proposed an untraceable and secure two-factor authentication design based on elliptic curve cryptography for wireless sensor networks. After analyzing the design of Jiang et al., Xiong et al. [22] received the result that the design has no detection mechanism for unauthorized login and clock synchronization problem and introduced a three-factor anonymous authentication design for wireless sensor networks by applying the fuzzy commitment to deal with biometric information.

For the purpose of withstanding the node capture attack, impersonation attack, and man-in-the-middle attack, Das [23] then put forward an original biometric-based mutual authentication design for wireless sensor networks. In the same year, Lu et al. [24] found that the design of Das does not really implement the three-factor security and user anonymity and has no ability to boycott user impersonation attack. Li et al. [25] pointed out that the design of Ruhul et al. [26] is vulnerable to DoS attack and lacks forward secrecy. In view of previous studies, Li introduced a three-factor mutual authentication design with forward secrecy for wireless medical sensor networks, which settles the contradiction of local password verification and mobile device lost attack via fuzzy verifier and honey_list technology. Nevertheless, Mo and Chen [27] discovered that the protocol of Xiong et al. [22] is vulnerable to resist stolen smart card attack and divulge the biometric information. Mo and Chen [27] pointed out that the protocol of Lu et al. [24] is prone to known session-specific temporary information attack and cannot realize three-factor security and backward secrecy. Mo and Chen [27] found that the protocol of Li et al. [25] is susceptible to withstanding replay attack.

Mutual authentication is used to supply the fundamental security requirement by confirming the legality of the communication parities for various network applications, such as smart city [28, 29], Internet of Drones [30, 31], vehicular networks [32, 33], multiserver environment [34, 35], and mobile devise [36, 37].

1.3. Organization. The remainder of the paper is organized as follows. In part 2, we discuss the preliminaries. In part 3, we present our proposed mutual authentication protocol. In

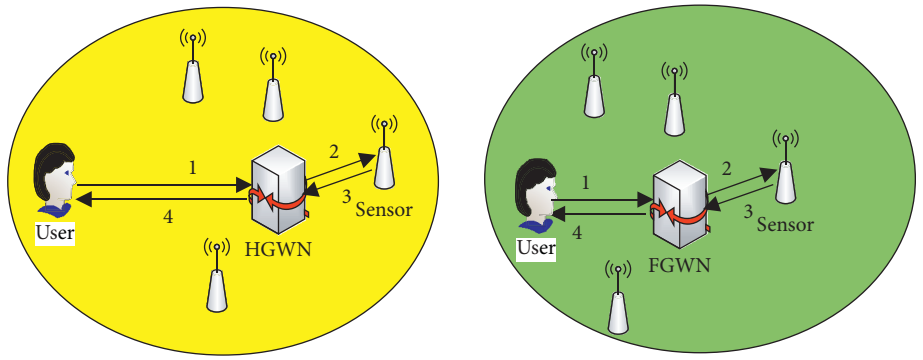

Figure 1: Network architecture in case 1.

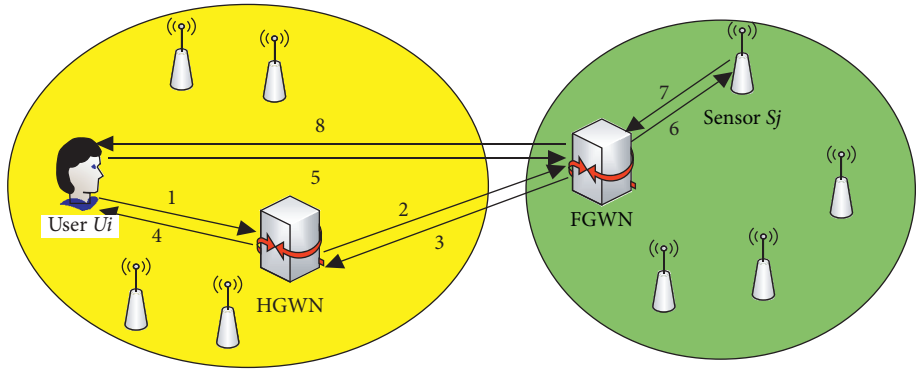

Figure 2: Network architecture in case 2.

part 4, we show formal analysis of our proposed mutual authentication protocol through three methods, that is, BAN logic, random oracle model, and AVISPA. In part 5, we demonstrate informal analysis of our proposed mutual authentication protocol through sixteen security authentication protocol evaluation criteria. In part 6, we compare our proposed mutual authentication protocol with other related authentication protocols in terms of security, computation time, and communication cost. Finally, we come to a conclusion in part 7.

2. Preliminaries

This part presents the preliminaries in our designed mutual authentication protocol involving biometric fuzzy extractor, threat model, and protocol evaluation criteria.

2.1. Biometric Fuzzy Extractor. So as to prevent the given biometric information BIO_i from various noises in the process of information acquisition, this paper introduces the biometric fuzzy extractor. There are two functions in biometric fuzzy extractor [28, 36]:GEN function and REP function. The concrete representations of the two functions are as follows:

(1) $\mathrm{GEN}(\mathrm{BIO}_i) = (\sigma_i, \tau_i)$. GEN is a probabilistic generation function that separates out the secret string σ_i and an auxiliary string τ_i from the given biometric information BIO_i

(2) $\mathrm{REP}(\mathrm{BIO}_i, \tau_i) = \sigma_i$. REP is a deterministic function that recovers the secret string σ_i from the given biometric information BIO_i with the assistance of the auxiliary string τ_i

2.2. Threat Model. The threat model presents the possibilities of an assailant obtaining the information about the authentication protocol without authorizing and the competence of potential destruction. Before evaluating the security authentication protocol, we assume that the assailant has the following abilities in the authentication process:

(1) The assailant is able to revise, intercept, delete, and transmit the communication information on the public network channel [38, 39]

(2) The assailant is able to obtain the parameters kept in the smart card via power analysis attack [40], in case the smart card is stolen or lost

(3) The assailant is able to carry out the online and offline password guessing attack [35]

(4) The assailant is able to implement the impersonation attack [4]

(5) The assailant is aware of the authentication protocol system [41]

(6) The assailant may be a legitimate user or an external entity [42, 43]

2.3. Protocol Evaluation Criteria. Since the information is interacted on the public network channel, the assailant is able to intercept and manipulate the interactive information [41, 44]. To guarantee the security of the interactive information on the public network channel, we design a mutual authentication and session key agreement protocol among the communication parties for the multiple gateway nodes networks. From four aspects of users, gateway nodes, sensor nodes, and communication protocol itself, we define the following sixteen security authentication protocol evaluation criteria:

(1) Session key security
(2) Three-factor security
(3) Perfect forward and backward security
(4) Resist sensor node capture attack
(5) Resist stolen smart card attack
(6) Resist user impersonation attack
(7) Resist gateway impersonation attack
(8) Resist sensor node impersonation attack
(9) Resist reply attack
(10) Resist privileged insider attack
(11) Resist online password-guessing attack
(12) Resist offline password-guessing attack
(13) Resist user tracking attack
(14) Biometric template protection
(15) Mutual authentication
(16) User anonymity

3. The Proposed Protocol

In this part, we will demonstrate our three-factor remote user authentication and key agreement protocol in the wireless sensor network environment with multiple gateways. Our protocol is related to five sections, which are initialization section, registration section, login section, authentication and key agreement section, and password change section.

3.1. Initialization Section. SA picks the distinctive identity $\mathrm{ID}_{\mathrm{SN}j}$ and private key $\mathrm{SX}_{\mathrm{SN}j}$, for the SN, calculates the value $\mathrm{SNX}_j = h(\mathrm{ID}_{\mathrm{SN}j} \| \mathrm{SX}_{\mathrm{SN}j})$ and dispatches the information $\{\mathrm{ID}_{\mathrm{SN}j}, \mathrm{SNX}_j\}$ to the SN. SA chooses the distinctive identity ID_{GWNh} and private key SX_{GWNh} for the HGWN. SA selects the distinctive identity ID_{GWNf} and private key SX_{GWNf} for the FGWN in the same way. Each pair of HGWN and FGWN keeps a private session key K_{hf}.

3.2. Registration Section. The registration section is divided into two parts, namely, sensor node registration and user registration.

3.2.1. Sensor Node Registration. A1: in the light of the received information $\{\mathrm{ID}_{\mathrm{SN}j}, \mathrm{SNX}_j\}$ in the initialization section, SN_j calculates $\mathrm{MSN}_j = \mathrm{SNX}_j \oplus h(\mathrm{ID}_{\mathrm{SN}j})$ and dispatches the information $\{\mathrm{ID}_{\mathrm{SN}j}, \mathrm{MSN}_j\}$ to GWN_H. A2: after obtaining the information sent by the SN, HGWN computes $\mathrm{SNX}_j = \mathrm{MSN}_j \oplus h(\mathrm{ID}_{\mathrm{SN}j})$, preserves the information $\{\mathrm{ID}_{\mathrm{SN}j}, \mathrm{MSN}_j\}$, and replies to the sensor node with a confirmation message.

3.2.2. User Registration

A1: U_i picks the essential parameters, identity ID_i, password PW_i, and two stochastic digits r_i and r_p and counts $\mathrm{UID}_i = h(\mathrm{ID}_i \| r_i)$ and $\mathrm{UPW}_i = h(\mathrm{PW}_i \| r_i \| r_p)$. After the calculation, U_i delivers UID_i and UPW_i to HGWN as the registration request.

A2: after getting the registration request, HGWN generates a stochastic digit $r_{\mathrm{GWN}h}$ and computes $\mathrm{GUID}_i = h(r_{\mathrm{GWN}h} \| \mathrm{SX}_{\mathrm{GWN}h} \| \mathrm{ID}_{\mathrm{GWN}h}) \oplus \mathrm{UID}_i$, $\mathrm{GE}_i = h(\mathrm{UID}_i \| \mathrm{UPW}_i)$, and $\mathrm{GF}_i = \mathrm{GE}_i \oplus \mathrm{GUID}_i \oplus \mathrm{UID}_i$ in combination with its own privacy parameters. HGWN loads GE_i and GF_i into the smart card and transmits the smart card to U_i.

A3: after reception of the smart card, U_i imprints his or her unique biometric BIO_{Ui} on the sensor device specific terminal and further counts $\mathrm{GEN}(\mathrm{BIO}_{Ui}) = (\sigma_{Ui}, \tau_{Ui})$, $\mathrm{USC}_1 = r_i \oplus h(\mathrm{ID}_i \| \mathrm{PW}_i \| \sigma_{Ui})$, $\mathrm{USC}_2 = r_p \oplus h(\sigma_{Ui} \| r_i)$, and $\mathrm{USC}_3 = h(\mathrm{UID}_i \| \mathrm{UPW}_i \| \sigma_{Ui} \| r_i \| r_p)$. Then, U_i loads $(\mathrm{USC}_1, \mathrm{USC}_2, \mathrm{USC}_3)$ into the smart card.

3.3. Login Section. A1: U_i inserts smart card and inputs his or her identity ID_i, password PW_i, and biometric BIO_{Ui}. A2: smart card counts $\mathrm{REP}(\mathrm{BIO}_{Ui}, \tau_{Ui}) = \sigma_{Ui}$, $r_i^* = \mathrm{USC}_1 \oplus h(\mathrm{ID}_i \| \mathrm{PW}_i \| \sigma_{Ui})$, $r_p^* = \mathrm{USC}_2 \oplus h(\sigma_{Ui} \| r_i)$, $\mathrm{UID}_i^* = h(\mathrm{ID}_i \| r_i^*)$, $\mathrm{UPW}_i^* = h(\mathrm{PW}_i \| r_i^* \| r_p^*)$, and $\mathrm{USC}_3^* = h(\mathrm{UID}_i^* \| \mathrm{UPW}_i^* \| \sigma_{Ui} \| r_i^* \| r_p^*)$ and confirms the correctness of the formula $\mathrm{USC}_3^* = \mathrm{USC}_3$. A3: if it is not right, smart card suspends the session promptly. Otherwise, smart card picks stochastic identity SCN_i, stochastic digit $r_{\mathrm{SC}n}$, and time stamp T_{sc} and counts $\mathrm{SCG}_1 = \mathrm{GUID}_i \oplus \mathrm{SCN}_i$, $\mathrm{SCG}_2 = r_{\mathrm{SC}n} \oplus h(\mathrm{SCN}_i \| T_{sc})$, $\mathrm{SCG}_3 = \mathrm{GF}_i \oplus h(\mathrm{UID}_i \| \mathrm{UPW}_i)$, and $\mathrm{SCG}_4 = h(\mathrm{SCN}_i \| r_{\mathrm{SC}n} \| T_{\mathrm{sc}} \| \mathrm{GUID}_i \| \mathrm{SCG}_3 \| \mathrm{ID}_{\mathrm{SN}j})$. Finally, U_i delivers the login request $(\mathrm{SCG}_1, \mathrm{SCG}_2, \mathrm{SCG}_4, \mathrm{T_{sc}}, \mathrm{UID}_i, \mathrm{ID}_{\mathrm{SN}j})$ to GWN_H.

3.4. Authentication and Key Agreement Section. On the basis of UID_i in the login request, GWN_H computes $\mathrm{GUID}_i = h(r_{\mathrm{GWN}h} \| \mathrm{SX}_{\mathrm{GWN}h} \| \mathrm{ID}_{\mathrm{GWN}h}) \oplus \mathrm{UID}_i$, $\mathrm{SCN}_i^* = \mathrm{GUID}_i \oplus \mathrm{SCG}_1$, $r_{\mathrm{SC}n}^* = \mathrm{SCG}_2 \oplus h(\mathrm{SCN}_i^* \| T_{\mathrm{sc}})$, $\mathrm{SCG}_3^* = \mathrm{GUID}_i \oplus \mathrm{UID}_i$, and $\mathrm{SCG}_4^* = h(\mathrm{SCN}_i^* \| r_{\mathrm{SC}n}^* \| T_{\mathrm{sc}} \| \mathrm{GUID}_i \| \mathrm{SCG}_3^* \| \mathrm{ID}_{\mathrm{SN}j})$ and confirms the correctness of the formula $\mathrm{SCG}_4^* = \mathrm{SCG}_4$. If it is not right, GWN_H terminates the session promptly. Otherwise, GWN_H finds whether $\mathrm{ID}_{\mathrm{SN}j}$ is in the information about the sensor node it preserves. If it is in the information, execute case 1 as shown in Figure 3; if it is not, execute case 2 as shown in Figure 4.

Case 1:

A1: GWN_H generates time stamp $T_{\mathrm{gwn}h}$ and computes the freshness of the login request by the formula

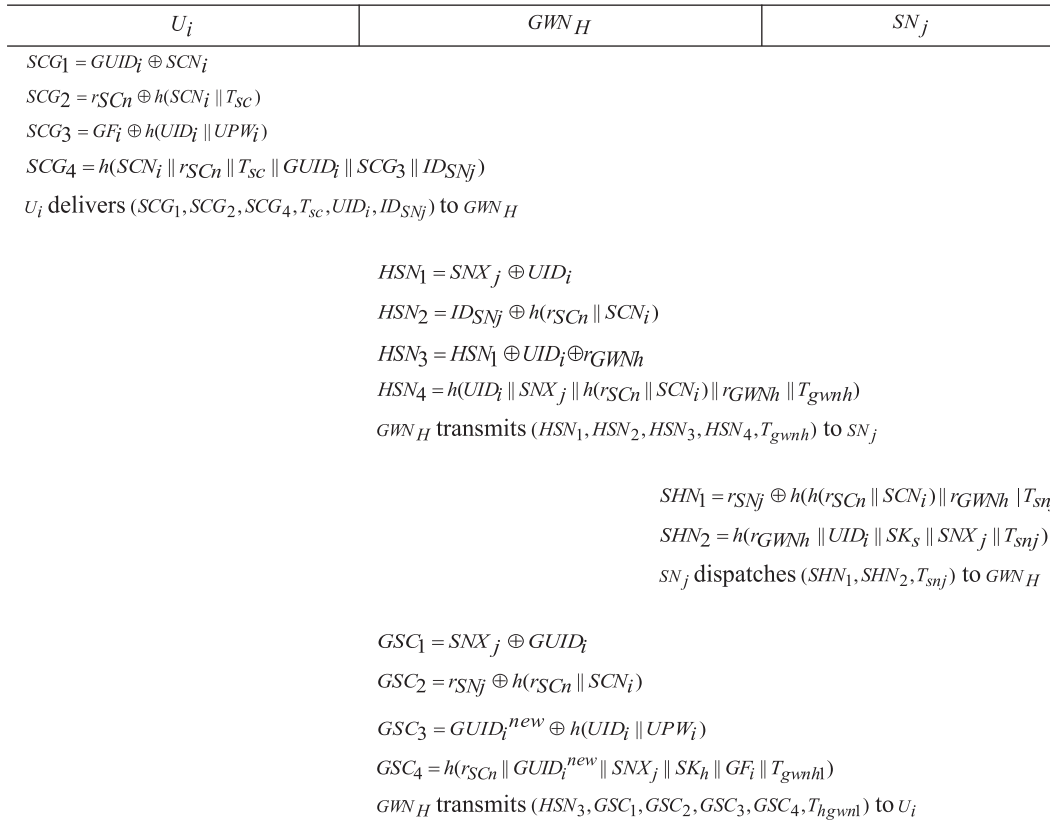

Figure 3: The main authentication steps in case 1.

$|T_{\text{gwn}h} - T_{\text{sc}}| \le \Delta T$. If it is not right, GWN_H terminates the session promptly. Otherwise, GWN_H computes $\text{HSN}_1 = \text{SNX}_j \oplus \text{UID}_i$, $\text{HSN}_2 = \text{ID}_{\text{SN}j} \oplus h(r_{\text{SC}n} \| \text{SCN}_i)$, $\text{HSN}_3 = \text{HSN}_1 \oplus \text{UID}_i \oplus r_{\text{GWN}h}$, and $\text{HSN}_4 = h(\text{UID}_i \| \text{SNX}_j \| h(r_{\text{SC}n} \| \text{SCN}_i) r_{\text{GWN}h} T_{gwnh})$ and transmits the information $(\text{HSN}_1, \text{HSN}_2, \text{HSN}_3, \text{HSN}_4, T_{\text{gwn}h})$ to SN_j.

A2: upon receiving the information $(\text{HSN}_1, \text{HSN}_2, \text{HSN}_3, \text{HSN}_4, T_{\text{gwn}h})$ at time $T_{\text{sn}j}$, SN_j calculates the freshness of the information by the formula $|T_{\text{sn}j} - T_{\text{gwn}h}| \le \Delta T$. If it is not right, SN_j ends the session promptly. Otherwise, SN_j calculates $\text{UID}_i^* = \text{SNX}_j \oplus \text{HSN}_1$, $h(r_{\text{SC}n} \| \text{SCN}_i)^* = \text{ID}_{\text{SN}j} \oplus \text{HSN}_2$, $r_{\text{GWN}h}^* = \text{HSN}_1 \oplus \text{UID}_i^* \oplus \text{HSN}_3$, and $\text{HSN}_4^* = h(\text{UID}_i^* \| \text{SNX}_j \| h(r_{\text{SC}n} \| \text{SCN}_i)^* \| r_{\text{GWN}h}^* \| T_{\text{gwn}h})$ and confirms the correctness of the formula $\text{HSN}_4^* = \text{HSN}_4$.

A3: if it is not right, SN_j ends the session promptly. Otherwise, SN_j selects stochastic digit $r_{\text{SN}j}$ and calculates $\text{SK}_s = h(r_{\text{SN}j} \| r_{\text{GWN}h} \| \text{UID}_i \| h(r_{\text{SC}n} \| \text{SCN}_i) \| \text{SNX}_j)$, $\text{SHN}_1 = r_{\text{SN}j} \oplus h(h(r_{\text{SC}n} \| \text{SCN}_i) \| r_{\text{GWN}h} | T_{snj})$, and $\text{SHN}_2 = h(r_{\text{GWN}h} \| \text{UID}_i \| \text{SK}_s \| \text{SNX}_j \| T_{\text{sn}j})$. Then, SN_j dispatches the information $(\text{SHN}_1, \text{SHN}_2, T_{\text{sn}j})$ to GWN_H.

A4: upon receiving the information $(\text{SHN}_1, \text{SHN}_2, T_{\text{sn}j})$ at time $T_{\text{gwn}h1}$, GWN_H computes the freshness of the information by the formula $|T_{\text{gwn}h1} - T_{\text{sn}j}| \le \Delta T$. If it is not right, GWN_H terminates the session promptly. Otherwise, GWN_H computes $r_{\text{SN}j}^* = \text{SHN}_1 \oplus h(h(r_{\text{SC}n} \| \text{SCN}_i) \| r_{\text{GWN}h} | T_{\text{sn}j})$, $\text{SK}_h = h(r_{\text{SN}j}^* | r_{\text{GWN}h} \| \text{UID}_i \| h(r_{\text{SC}n} \| \text{SCN}_i) \| \text{SNX}_j)$, and $\text{SHN}_2^* = h(r_{\text{GWN}h} \| \text{UID}_i \| \text{SK}_h \| \text{SNX}_j \| T_{\text{sn}j})$ and confirms the correctness of the formula $\text{SHN}_2^* = \text{SHN}_2$.

A5: if it is not right, GWN_H terminates the session promptly. Otherwise, GWN_H generates new stochastic digit $r_{\text{GWN}h}^{\text{new}}$ and computes $\text{GUID}_i^{\text{new}} = h(r_{\text{GWN}h}^{\text{new}} \| \text{SX}_{\text{GWN}h} \| \text{ID}_{\text{GWN}h}) \oplus \text{UID}_i$,

$\text{GSC}_1 = \text{SNX}_j \oplus \text{GUID}_i$, $\text{GSC}_2 = r_{\text{SN}j} \oplus h(r_{\text{SC}n} \| \text{SCN}_i)$, $\text{GSC}_3 = \text{GUID}_i^{\text{new}} \oplus h(\text{UID}_i \| \text{UPW}_i)$, and $\text{GSC}_4 = h(r_{\text{SC}n} \| \text{GUID}_i^{\text{new}} \| \text{SNX}_j \| \text{SK}_h \| \text{GF}_i \| T_{\text{gwn}h1})$. Then, GWN_H transmits the information $(\text{HSN}_3, \text{GSC}_1, \text{GSC}_2, \text{GSC}_3, \text{GSC}_4, T_{\text{hgw}n1})$ to U_i.

A6: upon receiving the information $(\text{HSN}_3, \text{GSC}_1, \text{GSC}_2, \text{GSC}_3, \text{GSC}_4, T_{\text{hgw}n1})$ at time T_{ui}, U_i computes the freshness of the information by the formula $|T_{ui} - T_{\text{gwn}h1}| \le \Delta T$. If it is not right, U_i suspends the session promptly. Otherwise, U_i counts $\text{SNX}_j^* = \text{GSC}_1 \oplus \text{GUID}_i$, $r_{\text{SN}j}^* = \text{GSC}_2 \oplus h(r_{\text{SC}n} \| \text{SCN}_i)$,

$r_{\text{GWN}h}^* = \text{SNX}_j^* \oplus \text{HSN}_3$, $\text{SK}_u = h(r_{\text{SN}j}^* \| r_{\text{GWN}h}^* \| \text{UID}_i \| h(r_{\text{SC}n} \| \text{SCN}_i) \| \text{SNX}_j^*)$, $\text{GUID}_i^{\text{new}} = \text{GSC}_3 \oplus h(\text{UID}_i \| \text{UPW}_i)$, and $\text{GSC}_4^* = h(r_{\text{SC}n} \| \text{GUID}_i^{\text{new}} \| \text{SNX}_j^* \| \text{SK}_u \| \text{GF}_i \| T_{\text{gwn}h1})$ and confirms the correctness of the formula $\text{GSC}_4^* = \text{GSC}_4$.

U_i	GWN_H	GWN_F	SN_j

$SCG_1 = GUID_i \oplus SCN_i$

$SCG_2 = r_{SCn} \oplus h(SCN_i \| T_{sc})$

$SCG_3 = GF_i \oplus h(UID_i \| UPW_i)$

$SCG_4 = h(SCN_i \| r_{SCn} \| T_{sc} \| GUID_i \| SCG_3 \| ID_{SNj})$

U_i delivers $(SCG_1, SCG_2, SCG_4, T_{sc}, UID_i, ID_{SNj})$ to GWN_H

GWN_H transmits (ID_{SNj}, ID_{GWNh}) to GWN_F

$FHN_1 = h(SNX_j \| K_{FH}) \oplus SX_{GWNf}$

$FHN_2 = K_{FH} \oplus SNX_j$

$FHN_3 = ID_{SNj} \oplus ID_{GWNf}$

$FHN_4 = h(K_{FH} \| ID_{GWNh} \| ID_{GWNf} \| SNX_j \| ID_{SNj} \| SX_{GWNf})$

GWN_F transmits $(FHN_1, FHN_2, FHN_3, FHN_4)$ to the GWN_H

$FHN_2 = K_{FH} \oplus SNX_j$

$GSC_5 = h(SNX_j \| ID_{SNj})$

$GSC_6 = UID_i \oplus SNX_j$

$GSC_7 = FHN_1 \oplus GSC_5$

GWN_H transmits (FHN_2, GSC_6, GSC_7) to U_i

$SCF_5 = h(SNX_j \| K_{FH}) \oplus r_{ui}$

$SCF_6 = UID_i \oplus FHN_1$

$SCF_7 = h(r_{ui} \| UID_i \| T_{ui} \| SX_{GWNf} \| K_{FH} \| SNX_j)$

U_i delivers $(SCF_5, SCF_6, SCF_7, T_{ui})$ to GWN_F

$FSN_1 = SNX_j \oplus UID_i$

$FSN_2 = ID_{SNj} \oplus h(UID_i \| r_{ui})$

$FSN_3 = r_{GWNf} \oplus UID_i \oplus h(r_{ui} \| UID_i)$

$FSN_4 = h(UID_i \| SNX_j \| h(r_{ui} \| UID_i) \| r_{GWNf} \| T_{gwnf})$

GWN_F transmits $(FSN_1, FSN_2, FSN_3, FSN_4, T_{gwnf})$ to SN_j

$SFN_2 = r_{SNj} \oplus h(r_{GWNf} \| UID_i \| SNX_j)$

$SFN_3 = h(r_{SNj} \| r_{GWNf} \| SK_s \| UID_i \| SNX_j \| T_{snj})$

SN_j dispatches (SFN_2, SFN_3, T_{snj}) to GWN_F

$FSC_1 = K_{FH} \oplus r_{GWNf}$

$FSC_2 = r_{SNj} \oplus h(SNX_j \| K_{FH} \| SX_{GWNf})$

$FSC_3 = GUID_i^{new} \oplus h(UID_i \| r_{ui})$

$FSC_4 = h(r_{SNj} \| GUID_i^{new} \| SNX_j \| K_{FH} \| SX_{GWNf} \| SK_f \| T_{gwnf1})$

GWN_F transmits $(FSC_1, FSC_2, FSC_3, FSC_4, T_{gwnf1})$ to U_i

Figure 4: The main authentication steps in case 2.

A7: if it is not right, U_i suspends the session promptly. Otherwise, U_i counts $\mathrm{GF}_i^{\mathrm{new}} = \mathrm{GE}_i \oplus \mathrm{GUID}_i^{\mathrm{new}} \oplus \mathrm{UID}_i$ and substitutes $(\mathrm{GF}_i^{\mathrm{new}}, \mathrm{GUID}_i^{\mathrm{new}})$ for $(\mathrm{GF}_i, \mathrm{GUID}_i)$ in smart card.

Case 2:

A1: first, GWN_H broadcasts the information $(\mathrm{ID}_{\mathrm{SN}j}, \mathrm{ID}_{\mathrm{GWN}h})$ among all gateway nodes. GWN_F finds whether $\mathrm{ID}_{\mathrm{SN}j}$ is in the information about the

sensor node it preserves. If it is in the information, GWN_F finds SNX_j based on ID_{SNj}. Next, GWN_F finds and computes $FHN_1 = h(SNX_j \| K_{FH}) \oplus SX_{GWNf}$, $FHN_2 = K_{FH} \oplus SNX_j$, $FHN_3 = ID_{SNj} \oplus ID_{GWNf}$, and $FHN_4 = h(K_{FH} \| ID_{GWNh} \| ID_{GWNf} \| SNX_j \| ID_{SNj} \| SX_{GWNf})$. Then, GWN_F transmits the information $(FHN_1, FHN_2, FHN_3, FHN_4)$ to GWN_H.

A2: after reception of the information $(FHN_1, FHN_2, FHN_3, FHN_4)$, GWN_H computes $ID_{GWNf} = ID_{SNj} \oplus FHN_3$. GWN_H finds the private key K_{FH} between them according to identity ID_{GWNf} of GWN_F and computes $SNX_j^* = K_{FH} \oplus FHN_2$, $SX_{GWNf}^* = h(SNX_j^* \| K_{FH}) \oplus FHN_1$, and $FHN_4^* = h(K_{FH} \| ID_{GWNh} \| ID_{GWNf} \| SNX_j^* \| ID_{SNj} \| SX_{GWNf}^*)$. Then, GWN_H confirms the correctness of the formula $FHN_4^* = FHN_4$.

A3: if it is not right, GWN_H terminates the session promptly. Otherwise, GWN_H computes $GSC_5 = h(SNX_j \| ID_{SNj})$, $GSC_6 = UID_i \oplus SNX_j$, and $GSC_7 = FHN_1 \oplus GSC_5$ and transmits the information (FHN_2, GSC_6, GSC_7) to U_i.

A4: after reception of the information (FHN_2, GSC_6, GSC_7), U_i counts $SNX_j = UID_i \oplus GSC_6$, $K_{FH} = FHN_2 \oplus SNX_j$, $FHN_1 = GSC_7 \oplus h(ID_{SNj} \| SNX_j)$, and $SX_{GWNf} = h(SNX_j \| K_{FH}) \oplus FHN_1$. Then, U_i picks the stochastic digit r_{ui} and time stamp T_{ui} and counts $SCF_5 = h(SNX_j \| K_{FH}) \oplus r_{ui}$, $SCF_6 = UID_i \oplus FHN_1$, and $SCF_7 = h(r_{ui} \| UID_i \| T_{ui} \| SX_{GWNf} \| K_{FH} \| SNX_j)$. Finally, U_i delivers the information $(SCF_5, SCF_6, SCF_7, T_{ui})$ to GWN_F.

A5: upon receiving the information $(SCF_5, SCF_6, SCF_7, T_{ui})$ at time T_{gwnf}, GWN_F computes the freshness of the information by the formula $|T_{gwnf} - T_{ui}| \le \Delta T$. If it is not right, GWN_F terminates the session promptly. Otherwise, GWN_F computes $r_{ui}^* = h(SNX_j \| K_{FH}) \oplus SCF_5$, $UID_i^* = SCF_6 \oplus FHN_1$, and $SCF_7^* = h(r_{ui}^* \| UID_i^* \| T_{ui} \| SX_{GWNf} \| K_{FH} \| SNX_j)$ and confirms the correctness of the formula $SCF_7^* = SCF_7$.

A6: if it is not right, GWN_F terminates the session promptly. Otherwise, GWN_F generates stochastic digit r_{GWNf} and computes $FSN_1 = SNX_j \oplus UID_i$, $FSN_2 = ID_{SNj} \oplus h(UID_i \| r_{ui})$, $FSN_3 = r_{GWNf} \oplus UID_i \oplus h(r_{ui} \| UID_i)$, and $FSN_4 = h(UID_i \| SNX_j \| h(r_{ui} \| UID_i) \| r_{GWNf} \| T_{gwnf})$. Then, GWN_F transmits the information $(FSN_1, FSN_2, FSN_3, FSN_4, T_{gwnf})$ to SN_j.

A7: upon receiving the information $(FSN_1, FSN_2, FSN_3, FSN_4, T_{gwnf})$ at time T_{snj}, SN_j calculates the freshness of the information by the formula $|T_{snj} - T_{gwnf}| \le \Delta T$. If it is not right, SN_j ends the session promptly. Otherwise, SN_j calculates $UID_i^* = SNX_j \oplus FSN_1$, $h(r_{ui} \| UID_i)^* = ID_{SNj} \oplus FSN_2$, $r_{GWNf}^* = FSN_3 \oplus UID_i^* \oplus h(r_{ui} \| UID_i)^*$, and $FSN_4^* = h(UID_i^* \| SNX_j \| h(r_{ui} \| UID_i)^* \| r_{GWNf}^* \| T_{gwnf})$ and confirms the correctness of the formula $FSN_4^* = FSN_4$.

A8: if it is not right, SN_j ends the session promptly. Otherwise, SN_j selects stochastic digit r_{SNj} and calculates $SK_s = h(r_{SNj} \| r_{GWNf} \| UID_i \| h(r_{ui} \| UID_i))$, $SFN_1 = h(UID_i \| r_{GWNf} | SNX_j)$, $SFN_2 = r_{SNj} \oplus h(r_{GWNf} \| UID_i \| SNX_j)$, and $SFN_3 = h(r_{SNj} \| r_{GWNf} \| SK_s \| UID_i \| SNX_j \| T_{snj})$. Then, SN_j dispatches the information (SFN_2, SFN_3, T_{snj}) to GWN_F.

A9: upon receiving the information (SFN_2, SFN_3, T_{snj}) at time T_{gwnf1}, GWN_F computes the freshness of the information by the formula $|T_{gwnf1} - T_{snj}| \le \Delta T$. If it is not right, GWN_F terminates the session promptly. Otherwise, GWN_F computes $r_{SNj}^* = SFN_2 \oplus h(r_{GWNf} \| UID_i \| SNX_j)$, $SK_f = h(r_{SNj}^* \| r_{GWNf} \| UID_i \| h(r_{ui} \| UID_i))$, and $SFN_3^* = h(r_{SNj}^* \| r_{GWNf} \| SK_f \| UID_i \| NX_j \| T_{snj})$ and confirms the correctness of the formula $SFN_3^* = SFN_3$.

A10: if it is not right, GWN_F terminates the session promptly. Otherwise, GWN_F generates new stochastic digit r_{GWNf}^{new} and computes $GUID_i^{new} = h(r_{GWNf}^{new} \| SX_{GWNf} \| ID_{GWNf}) \oplus UID_i$, $FSC_1 = K_{FH} \oplus r_{GWNf}$, $FSC_2 = r_{SNj} \oplus h(SNX_j \| K_{FH} \| SX_{GWNf})$, $FSC_3 = GUID_i^{new} \oplus h(UID_i \| r_{ui})$, and $FSC_4 = h(r_{SNj} \| GUID_i^{new} \| SNX_j \| K_{FH} \| SX_{GWNf} \| SK_f \| T_{gwnf1})$. Then, GWN_F transmits the information $(FSC_1, FSC_2, FSC_3, FSC_4, T_{gwnf1})$ to U_i.

A11: upon receiving the information $(FSC_1, FSC_2, FSC_3, FSC_4, T_{gwnf1})$ at time T_{ui}, U_i computes the freshness of the information by the formula $|T_{ui} - T_{gwnf1}| \le \Delta T$. If it is not right, U_i suspends the session promptly. Otherwise, U_i counts $r_{GWNf}^* = K_{FH} \oplus FSC_1$, $r_{SNj}^* = FSC_2 \oplus h(SNX_j \| K_{FH} \| SX_{GWNf})$, $GUID_i^{new} = FSC_3 \oplus h(UID_i \| r_{ui})$, $SK_u = h(r_{SNj}^* \| r_{GWNf}^* \| UID_i \| h(r_{ui} \| UID_i))$, $r_{GWNh}^* = SNX_j^* \oplus HSN_3$, and $FSC_4 = h(r_{SNj}^* \| GUID_i^{new} \| SNX_j \| K_{FH} \| SX_{GWNf} \| SK_u \| T_{gwnf1})$ and confirms the correctness of the formula $FSC_4^* = FSC_4$.

A12: if it is not right, U_i suspends the session promptly. Otherwise, U_i counts $GF_i^{new} = GE_i \oplus GUID_i^{new} \oplus UID_i$ and substitutes $(GF_i^{new}, GUID_i^{new})$ for $(GF_i, GUID_i)$ in smart card.

3.5. Password and Biometric Change Section

A1: U_i inserts smart card and inputs his or her identity ID_i, password PW_i, and biometric BIO_{Ui}.

A2: smart card counts $REP(BIO_{Ui}, \tau_{Ui}) = \sigma_{Ui}$, r_i^*, r_p^*, UID_i^*, UPW_i^*, and USC_3^* and confirms the correctness of the formula $USC_3^* = USC_3$.

A3: if it is not right, smart card suspends the session promptly. Otherwise, U_i picks the new parameters,

identity ID_i, password PW_i^{new}, and two stochastic digits r_i and r_p, and counts $UID_i = h(ID_i \| r_i)$ and $UPW_i^{new} = h(PW_i \| r_i \| r_p)$. After the calculation, U_i delivers UID_i and UPW_i^{new} to HGWN as the change request.

A4: after getting the change request, HGWN generates a stochastic digit r_{GWNh} and computes $GUID_i^{new}$, GE_i^{new}, and GF_i^{new} in combination with its own privacy parameters. HGWN loads GE_i^{new} and

GF_j^{new} into the smart card and transmits the smart card to U_i.

A5: after reception of the smart card, U_i imprints his or her unique biometric BIO_{Ui}^{new} on the sensor device specific terminal and further counts $GEN(BIO_{Ui}^{new}) = (\sigma_{Ui}^{new}, \tau_{Ui}^{new})$, USC_1^{new}, USC_2^{new}, and USC_3^{new}. Then, U_i loads $(USC_1^{new}, USC_2^{new}, USC_3^{new})$ into the smart card to replace the old parameters.

4. Formal Security Analysis of Protocol

In this section, we separately apply BAN logic and AVISPA tool to validate the security of our proposed authentication and key agreement protocol in case 1 and case 2.

4.1. BAN Logic (Case 1). In this section, we will validate our proposed designed authentication protocol by applying the BAN logic in case 1.

BAN logic notations are as follows:

(1) $\partial| \equiv \beta$: ∂ trusts the realness in β

(2) $\partial \triangleleft \beta$: ∂ obtains or sees information β

(3) $\partial| \sim \beta$: ∂ sent or said information β

(4) $\partial| \Rightarrow \beta$: ∂ has jurisdiction over β

(5) $\#(\beta)$: β is fresh

(6) $\partial \overset{SK}{\longleftrightarrow} \beta$: SK is the private session key between ∂ and β

(7) $(\beta)_{SK}$: β is encrypted with the private session key SK

BAN logic postulate rules:

PR1: Message-meaning rule: $(\partial| \equiv \beta \overset{SK}{\longleftrightarrow} \partial, \partial \triangleleft \{M\}_k)/\partial| \equiv \beta| \sim M$

PR2: Nonce-verification rule: $(\partial| \equiv \#(M), \partial| \equiv \beta| \sim M)/\partial| \equiv \beta| \equiv M$

PR3: Jurisdiction rule: $(\partial| \equiv \beta| \equiv M, \partial| \equiv \beta| \Rightarrow M)/\partial| \equiv M$

PR4: Fresh rule: $(\partial| \equiv \#(M))/\partial| \equiv \#(M, P)$

PR5: Belief rule: $(\partial| \equiv \beta| \equiv (M, P))/\partial| \equiv \beta| \equiv M$

Security goals are as follows:

Goal 1: $U_i| \equiv (U_i \overset{SK}{\longleftrightarrow} GWN_h)$

Goal 2: $U_i| \equiv GWN_h| \equiv (U_i \overset{SK}{\longleftrightarrow} GWN_h)$

Goal 3: $GWN_h| \equiv (U_i \overset{SK}{\longleftrightarrow} GWN_h)$

Goal 4: $GWN_h| \equiv U_i| \equiv (U_i \overset{SK}{\longleftrightarrow} GWN_h)$

Goal 5: $SN_j| \equiv (SN_j \overset{SK}{\longleftrightarrow} GWN_h)$

Goal 6: $SN_j| \equiv GWN_h| \equiv (SN_j \overset{SK}{\longleftrightarrow} GWN_h)$

Goal 7: $GWN_h| \equiv (SN_j \overset{SK}{\longleftrightarrow} GWN_h)$

Goal 8: $GWN_h| \equiv SN_j| \equiv (SN_j \overset{SK}{\longleftrightarrow} GWN_h)$

Rational assumptions are as follows:

RA1: $GWN_h| \equiv (U_i \overset{GUID_i}{\longleftrightarrow} GWN_h)$

RA2: $GWN_h| \equiv (\#T_{sc})_{SNX_j}$

RA3: $SN_j| \equiv (GWN_h \longleftrightarrow SN_j)$

RA4: $SN_j| \equiv (\#SNX_j)$

RA5: $GWN_h| \equiv (SN_j \overset{r_{SNj}}{\longleftrightarrow} GWN_h)$

RA6: $GWN_h| \equiv (\#T_{snj})$

RA7: $GWN_h| \equiv SN_j| \Rightarrow (SN_j \overset{SK}{\longleftrightarrow} GWN_h)$

RA8: $U_i| \equiv (GWN_h \overset{GF_i}{\longleftrightarrow} U_i)$

RA9: $U_i| \equiv (\#T_{hgwn1})$

RA10: $U_i| \equiv GWN_h| \Rightarrow (U_i \overset{SK}{\longleftrightarrow} GWN_h)$

RA11: $SN_j| \equiv GWN_h| \Rightarrow (SN_j \overset{SK}{\longleftrightarrow} GWN_h)$

RA12: $GWN_h| \equiv U_i| \Rightarrow (U_i \overset{SK}{\longleftrightarrow} GWN_h)$

The idealized form of the information is as follows:

Inf 1: $U_i \longrightarrow GWN_h \quad (SCG_1, SCG_2, SCG_4, T_{sc}, UID_i, ID_{SNj})$

Inf 2: $GWN_h \longrightarrow SN_j \quad (HSN_1, HSN_2, HSN_3, HSN_4, T_{gwnh})$

Inf3: $SN_j \longrightarrow GWN_h \quad (SHN_1, SHN_2, T_{snj})$

Inf4: $GWN_h \longrightarrow U_i \quad (HSN_3, GSC_1, GSC_2, GSC_3, GSC_4, T_{hgwn1})$

In view of Inf1, we are ready to receive the following:

F1: $GWN_h \triangleleft (SCG_1, SCG_2, SCG_4, T_{sc}, UID_i, ID_{SNj})_{GUID_i}$

In view of F1, RA1, and PR1, we are ready to receive the following:

F2: $GWN_h| \equiv U_i| \sim (SCG_1, SCG_2, SCG_4, T_{sc}, UID_i, ID_{SNj})$

The equivalent form of F2 is the following:

F3: $GWN_h| \equiv U_i| \sim (UID_i, SCN_i, r_{SCn}, T_{sc})$

In view of F3, RA2, PR4, and PR2, we are ready to receive the following:

F4: $GWN_h| \equiv U_i| \equiv (UID_i, SCN_i, r_{SCn}, T_{sc})$

In view of F4 and PR5, we are ready to receive the following:

F5: $GWN_h| \equiv U_i| \equiv (UID_i, SCN_i, r_{SCn})$

In view of Inf2, we are ready to receive the following:

F6: $SN_j \triangleleft (HSN_1, HSN_2, HSN_3, HSN_4, T_{gwnh})_{SNX_j}$

In view of F6, RA3, and PR1, we are ready to receive the following:

F7: $SN_j| \equiv GWN_h| \sim (HSN_1, HSN_2, HSN_3, HSN_4, T_{gwnh})$

The equivalent form of F7 is the following:

F8: $SN_j| \equiv GWN_h| \sim (SNX_j, UID_i, r_{SCn}, SCN_i, r_{GWNh}, T_{gwnh})$

In view of F8, RA4, PR4, and PR2, we are ready to receive the following:

F9: $\mathrm{SN}_j| \equiv \mathrm{GWN}_h| \equiv (\mathrm{SNX}_j, \mathrm{UID}_i, r_{\mathrm{SC}n}, \mathrm{SCN}_i, r_{\mathrm{GWN}h}, T_{\mathrm{gwn}h})$

In view of F9 and PR5, we are ready to receive the following:

F10: $\mathrm{SN}_j| \equiv \mathrm{GWN}_h| \equiv (\mathrm{SNX}_j, \mathrm{UID}_i, r_{\mathrm{SC}n}, \mathrm{SCN}_i, r_{\mathrm{GWN}h})$

In view of Inf3, we are ready to receive the following:

F11: $\mathrm{GWN}_h \triangleleft (\mathrm{SHN}_1, \mathrm{SHN}_2, T_{snj})_{r_{\mathrm{SN}j}}$

In view of F11, RA5, and PR1, we are ready to receive the following:

F12: $\mathrm{GWN}_h| \equiv \mathrm{SN}_j| \sim (\mathrm{SHN}_1, \mathrm{SHN}_2, T_{snj})$

The equivalent form of F12 is the following:

F13: $\mathrm{GWN}_h| \equiv SN_j| \sim (r_{\mathrm{SN}j}, r_{\mathrm{GWN}h}, r_{\mathrm{SC}n}, \mathrm{SCN}_i, T_{snj}, \mathrm{UID}_i, \mathrm{SNX}_j)$

In view of F13, RA6, PR4, and PR2, we are ready to receive the following:

F14: $\mathrm{GWN}_h| \equiv \mathrm{SN}_j| \equiv (r_{\mathrm{SN}j}, r_{\mathrm{GWN}h}, r_{\mathrm{SC}n}, \mathrm{SCN}_i, T_{snj}, \mathrm{UID}_i, \mathrm{SNX}_j)$

In view of F14 and PR5, we are ready to receive the following:

F15: $\mathrm{GWN}_h| \equiv \mathrm{SN}_j| \equiv (r_{\mathrm{SN}j}, r_{\mathrm{GWN}h}, r_{\mathrm{SC}n}, \mathrm{SCN}_i, \mathrm{UID}_i, \mathrm{SNX}_j)$

The private session key is $\mathrm{SK} = h(r_{\mathrm{SN}j} \| r_{\mathrm{GWN}h} \| \mathrm{UID}_i \| h(r_{\mathrm{SC}n} \| \mathrm{SCN}_i) \| \mathrm{SNX}_j)$

In view of F15, we are ready to receive the following:

F16: $\mathrm{GWN}_h| \equiv \mathrm{SN}_j| \equiv (\mathrm{SN}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_h)$ Goal 8

In view of F16, RA7, and PR3, we are ready to receive the following:

F17: $\mathrm{GWN}_h| \equiv (\mathrm{SN}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_h)$ Goal 7

In view of Inf4, we are ready to receive the following:

F18: $U_i \triangleleft (\mathrm{HSN}_3, \mathrm{GSC}_1, \mathrm{GSC}_2, \mathrm{GSC}_3, \mathrm{GSC}_4, T_{\mathrm{hgwn}1})_{\mathrm{GF}_i}$

In view of F18, RA8, and PR1, we are ready to receive the following:

F19: $U_i| \equiv \mathrm{GWN}_h| \sim (\mathrm{HSN}_3, \mathrm{GSC}_1, \mathrm{GSC}_2, \mathrm{GSC}_3, \mathrm{GSC}_4, T_{\mathrm{hgwn}1})$

The equivalent form of F19 is the following:

F20: $U_i| \equiv \mathrm{GWN}_h| \sim (\mathrm{SNX}_j, \mathrm{UID}_i, r_{\mathrm{GWN}h}, r_{\mathrm{SN}j}, r_{\mathrm{SC}n}, \mathrm{SCN}_i, T_{\mathrm{hgwn}1})$

In view of F20, RA9, PR4, and PR2, we are ready to receive the following:

F20: $U_i| \equiv \mathrm{GWN}_h| \equiv (\mathrm{SNX}_j, \mathrm{UID}_i, r_{\mathrm{GWN}h}, r_{\mathrm{SN}j}, r_{\mathrm{SC}n}, \mathrm{SCN}_i, T_{\mathrm{hgwn}1})$

In view of F20 and PR5, we are ready to receive the following:

F21: $U_i| \equiv \mathrm{GWN}_h| \equiv (\mathrm{SNX}_j, \mathrm{UID}_i, r_{\mathrm{GWN}h}, r_{\mathrm{SN}j}, r_{\mathrm{SC}n}, \mathrm{SCN}_i)$

The private session key is $\mathrm{SK} = h(r_{\mathrm{SN}j} \| r_{\mathrm{GWN}h} \| \mathrm{UID}_i \| h(r_{\mathrm{SC}n} \| \mathrm{SCN}_i) \| \mathrm{SNX}_j)$

In view of F21, we are ready to receive the following:

F22: $U_i| \equiv \mathrm{GWN}_h| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_h)$ Goal 2

In view of F22, RA10, and PR3, we are ready to receive the following:

F23: $U_i| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_h)$ Goal 1

The private session key is $\mathrm{SK} = h(r_{\mathrm{SN}j} \| r_{\mathrm{GWN}h} \| \mathrm{UID}_i \| h(r_{\mathrm{SC}n} \| \mathrm{SCN}_i) \| \mathrm{SNX}_j)$

In view of F10 and F15, we are ready to receive the following:

F24: $\mathrm{SN}_j| \equiv \mathrm{GWN}_h| \equiv (\mathrm{SN}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_h)$ Goal 6

In view of F24, RA11, and PR3, we are ready to receive the following:

F25: $\mathrm{SN}_j| \equiv (\mathrm{SN}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_h)$ Goal 5

The private session key is $\mathrm{SK} = h(r_{\mathrm{SN}j} \| r_{\mathrm{GWN}h} \| UID_i \| h(r_{\mathrm{SC}n} \| \mathrm{SCN}_i) \| \mathrm{SNX}_j)$

In view of F5 and F21, we are ready to receive the following:

F26: $\mathrm{GWN}_h| \equiv U_i| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_h)$ Goal 4

In view of F26, RA12, and PR3, we are ready to receive the following:

F27: $\mathrm{GWN}_h| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_h)$ Goal 3

4.2. AVISPA Tool (Case 1). In this section, we will validate our proposed designed authentication protocol by applying the AVISPA tool in case 1. In AVISPA tool, four validation models are supported: OFMC, ATSE, SATMC, and TA4SP. The security of our designed authentication protocol is simulated by applying the HLPSL (High Level Protocol Specifications Language). Figures 5 and 6 present the result of the simulation by applying the OFMC and ATSE.

4.3. BAN Logic (Case 2). In this section, we will validate our proposed designed authentication protocol by applying the BAN logic in case 2.

Goal 1: $U_i| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$

Goal 2: $U_i| \equiv \mathrm{GWN}_f| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$

Goal 3: $\mathrm{GWN}_f| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$

Goal 4: $\mathrm{GWN}_f| \equiv U_i| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$

Goal 5: $\mathrm{SN}_j| \equiv (\mathrm{SN}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$

Goal 6: $\mathrm{SN}_j| \equiv \mathrm{GWN}_f| \equiv (\mathrm{SN}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$

Goal 7: $\mathrm{GWN}_f| \equiv (\mathrm{SN}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$

Goal 8: $\mathrm{GWN}_f| \equiv \mathrm{SN}_j| \equiv (\mathrm{SN}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$

Rational assumptions are as follows:

RA1: $\mathrm{GWN}_f| \equiv (U_i \overset{\mathrm{UID}_i}{\longleftrightarrow} \mathrm{GWN}_f)$

RA2: $\mathrm{GWN}_f| \equiv (\#T_{ui})_{r_{\mathrm{GWN}f}}$

RA3: $\mathrm{SN}_j| \equiv (\mathrm{GWN}_f \overset{}{\longleftrightarrow} \mathrm{SN}_j)$

RA4: $\mathrm{SN}_j| \equiv (\#T_{\mathrm{gwn}f})$

RA5: $\mathrm{GWN}_f| \equiv (\mathrm{SN}_j \overset{\mathrm{FSN}_1}{\longleftrightarrow} \mathrm{GWN}_f)$

RA6: $\mathrm{GWN}_f| \equiv (\#T_{snj})$

RA7: $\mathrm{GWN}_f| \equiv \mathrm{SN}_j| \Rightarrow (\mathrm{SN}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$

RA8: $U_i| \equiv (\mathrm{GWN}_f \overset{\mathrm{FSC}_1}{\longleftrightarrow} U_i)$

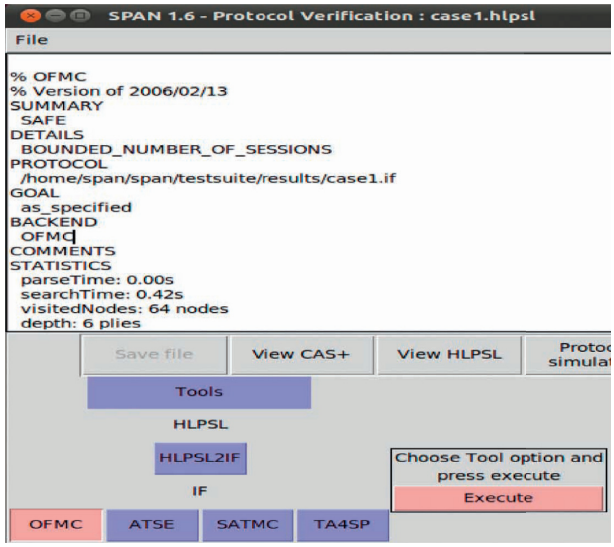

Figure 5: The simulation result of OFMC.

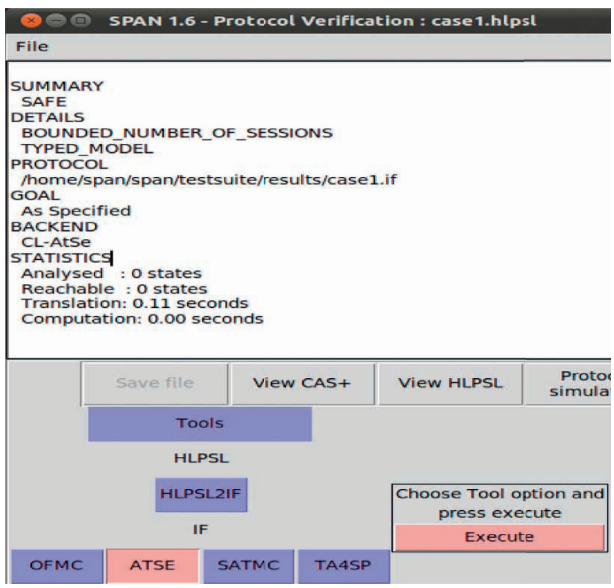

Figure 6: The simulation result of ATSE.

RA9: $U_i| \equiv (\#T_{\text{gwn}f1})$

RA10: $U_i| \equiv \text{GWN}_f| \Rightarrow (U_i \overset{\text{SK}}{\longleftrightarrow} \text{GWN}_f)$

RA11: $\text{SN}_j| \equiv \text{GWN}_f| \Rightarrow (\text{SN}_j \overset{\text{SK}}{\longleftrightarrow} \text{GWN}_f)$

RA12: $\text{GWN}_f| \equiv U_i| \Rightarrow (U_i \overset{\text{SK}}{\longleftrightarrow} \text{GWN}_f)$

The idealized form of the information is as follows:

Inf1: $U_i \longrightarrow \text{GWN}_f\,(\text{SCF}_5, \text{SCF}_6, \text{SCF}_7, T_{ui})$

Inf2: $\text{GWN}_f \longrightarrow \text{SN}_j\,(\text{FSN}_1, \text{FSN}_2, \text{FSN}_3, \text{FSN}_4, T_{\text{gwn}f})$

Inf3: $\text{SN}_j \longrightarrow \text{GWN}_f\,(\text{SFN}_2, \text{SFN}_3, T_{snj})$

Inf4: $\text{GWN}_f \longrightarrow U_i\,(\text{FSC}_1, \text{FSC}_2, \text{FSC}_3, \text{FSC}_4, T_{\text{gwn}f1})$

In view of Inf1, we are ready to receive the following:

F1: $\text{GWN}_f \triangleleft (\text{SCF}_5, \text{SCF}_6, \text{SCF}_7, T_{ui})_{\text{UID}_i}$

In view of F1, RA1, and PR1, we are ready to receive the following:

F2: $\text{GWN}_f| \equiv U_i| \sim (\text{SCF}_5, \text{SCF}_6, \text{SCF}_7, T_{ui})$

The equivalent form of F2 is the following:

F3: $\text{GWN}_f| \equiv U_i| \sim (\text{SNX}_j, K_{\text{FH}}, r_{ui}, \text{UID}_i, \text{ID}_{\text{SN}j}, \text{SX}_{\text{GWN}f}, T_{ui})$

In view of F3, RA2, PR4, and PR2, we are ready to receive the following:

F4: $\text{GWN}_f| \equiv U_i| \equiv (\text{SNX}_j, K_{\text{FH}}, r_{ui}, \text{UID}_i, \text{ID}_{\text{SN}j}, \text{SX}_{\text{GWN}f}, T_{ui})$

In view of F4 and PR5, we are ready to receive the following:

F5: $\text{GWN}_f| \equiv U_i| \equiv (r_{ui}, \text{UID}_i)$

In view of Inf2, we are ready to receive the following:

F6: $SN_j \triangleleft (\text{FSN}_1, \text{FSN}_2, \text{FSN}_3, \text{FSN}_4, T_{\text{gwn}f})_{r_{\text{GWN}f}}$

In view of F6, RA3, and PR1, we are ready to receive the following:

F7: $\text{SN}_j| \equiv \text{GWN}_f| \sim (\text{FSN}_1, \text{FSN}_2, \text{FSN}_3, \text{FSN}_4, T_{\text{gwn}f})$

The equivalent form of F7 is the following:

F8: $\text{SN}_j| \equiv \text{GWN}_f| \sim (\text{SNX}_j, \text{UID}_i, \text{ID}_{\text{SN}j}, r_{ui}, r_{\text{GWN}f}, T_{\text{gwn}f})$

In view of F8, RA4, PR4, and PR2, we are ready to receive the following:

F9: $\text{SN}_j| \equiv \text{GWN}_f| \equiv (\text{SNX}_j, \text{UID}_i, \text{ID}_{\text{SN}j}, r_{ui}, r_{\text{GWN}f}, T_{\text{gwn}f})$

In view of F9 and PR5 we are ready to receive the following:

F10: $\text{SN}_j| \equiv \text{GWN}_f| \equiv (\text{UID}_i, r_{ui}, r_{\text{GWN}f})$

In view of Inf3, we are ready to receive the following:

F11: $\text{GWN}_f \triangleleft (\text{SFN}_2, \text{SFN}_3, T_{snj})_{\text{SFN1}}$

In view of F11, RA5, and PR1, we are ready to receive the following:

F12: $\text{GWN}_f| \equiv \text{SN}_j| \sim (\text{SFN}_2, \text{SFN}_3, T_{snj})$

The equivalent form of F12 is the following:

F13: $\text{GWN}_f| \equiv \text{SN}_j| \sim (r_{\text{SN}j}, r_{\text{GWN}f}, r_{ui}, \text{UID}_i, \text{SNX}_j, T_{snj})$

In view of F13, RA6, PR4, and PR2, we are ready to receive the following:

F14: $\text{GWN}_f| \equiv \text{SN}_j| \equiv (r_{\text{SN}j}, r_{\text{GWN}f}, r_{ui}, \text{UID}_i, \text{SNX}_j, T_{snj})$

In view of F14 and PR5, we are ready to receive the following:

F15: $\text{GWN}_f| \equiv \text{SN}_j| \equiv (r_{\text{SN}j}, r_{\text{GWN}f}, r_{ui}, \text{UID}_i)$

The private session key is $\text{SK} = h(r_{\text{SN}j} \| r_{\text{GWN}f} \| \text{UID}_i \| h(r_{ui} \| \text{UID}_i))$

In view of F15, we are ready to receive the following:

F16: $\text{GWN}_f| \equiv \text{SN}_j| \equiv (\text{SN}_j \overset{\text{SK}}{\longleftrightarrow} \text{GWN}_f)$ Goal 8

In view of F16, RA7, and PR3, we are ready to receive the following:

F17: $\text{GWN}_f| \equiv (\text{SN}_j \overset{\text{SK}}{\longleftrightarrow} \text{GWN}_f)$ Goal 7

In view of Inf4, we are ready to receive the following:

F18: $U_i \triangleleft (\text{FSC}_1, \text{FSC}_2, \text{FSC}_3, \text{FSC}_4, T_{\text{gwn}f1})_{\text{FSC}_1}$

In view of F18, RA8, and PR1, we are ready to receive the following:

F19: $U_i| \equiv \mathrm{GWN}_f| \sim (\mathrm{FSC}_1, \mathrm{FSC}_2, \mathrm{FSC}_3, \mathrm{FSC}_4, T_{\mathrm{gwn}f1})$

The equivalent form of F19 is the following:

F20: $U_i| \equiv \mathrm{GWN}_f| \sim (K_{\mathrm{FH}}, r_{\mathrm{GWN}f}, r_{\mathrm{SN}j}, \mathrm{SNX}_j, \mathrm{UID}_i, r_{ui}, \mathrm{SX}_{\mathrm{GWN}f}, T_{\mathrm{gwn}f1})$

In view of F20, RA9, PR4, and PR2, we are ready to receive the following:

F20: $U_i| \equiv \mathrm{GWN}_f| \equiv (K_{\mathrm{FH}}, r_{\mathrm{GWN}f}, r_{\mathrm{SN}j}, \mathrm{SNX}_j, \mathrm{UID}_i, r_{ui}, \mathrm{SX}_{\mathrm{GWN}f}, T_{\mathrm{gwn}f1})$

In view of F20 and PR5, we are ready to receive the following:

F21: $U_i| \equiv \mathrm{GWN}_f| \equiv (r_{\mathrm{GWN}f}, r_{\mathrm{SN}j}, \mathrm{UID}_i, r_{ui})$

The private session key is $\mathrm{SK} = h(r_{\mathrm{SN}j} \| r_{\mathrm{GWN}f} \| \mathrm{UID}_i \| h(r_{ui} \| \mathrm{UID}_i))$

In view of F21, we are ready to receive the following:

F22: $U_i| \equiv \mathrm{GWN}_f| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$ Goal 2

In view of F22, RA10, and PR3, we are ready to receive the following:

F23: $U_i| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$ Goal 1

The private session key is $\mathrm{SK} = h(r_{\mathrm{SN}j} \| r_{\mathrm{GWN}f} \| \mathrm{UID}_i \| h(r_{ui} \| \mathrm{UID}_i))$

In view of F10 and F15, we are ready to receive the following:

F24: $\mathrm{SN}_j| \equiv \mathrm{GWN}_f| \equiv (\mathrm{SN}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$ Goal 6

In view of F24, RA11, and PR3, we are ready to receive the following:

F25: $\mathrm{SN}_j| \equiv (\mathrm{SN}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$ Goal 5

The private session key is $\mathrm{SK} = h(r_{\mathrm{SN}j} \| r_{\mathrm{GWN}f} \| \mathrm{UID}_i \| h(r_{ui} \| \mathrm{UID}_i))$

In view of F5 and F21, we are ready to receive the following:

F26: $\mathrm{GWN}_f| \equiv U_i| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$ Goal 4

In view of F26, RA12, and PR3, we are ready to receive the following:

F27: $\mathrm{GWN}_f| \equiv (U_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{GWN}_f)$ Goal 3

4.4. AVISPA Tool (Case 2). In this section, we will validate our proposed designed authentication protocol by applying the AVISPA tool in case 2. Figures 7 and 8 present the result of the simulation by applying the ATSE and OFMC.

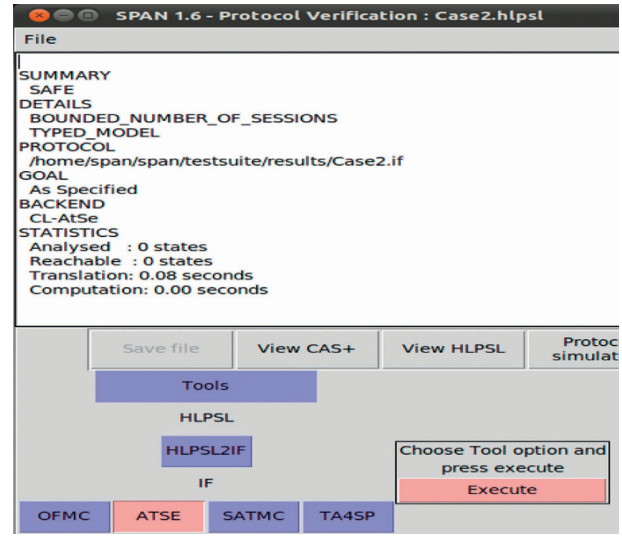

Figure 7: The simulation result of ATSE.

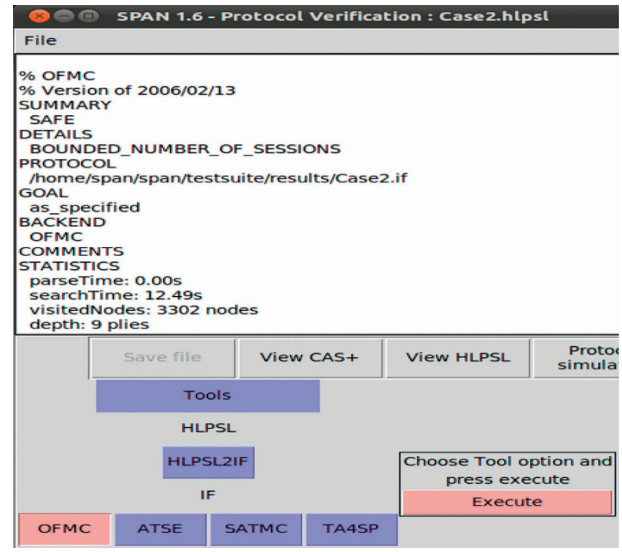

Figure 8: The simulation result of OFMC.

5. Informal Security Analysis of Protocol

In this section, we demonstrate informal security analysis of our proposed mutual authentication protocol through sixteen evaluation criteria as defined in Section 2.3.

5.1. Session Key Security. In our designed protocol, the private session key is derived from the relevant privacy parameters of the three parties involved in the communication process through hash function operation. In case 1, the private session key is $\mathrm{SK} = h(r_{\mathrm{SN}j} \| r_{\mathrm{GWNh}} \| \mathrm{UID}_i \| h(r_{\mathrm{SCn}} \| \mathrm{SCN}_i) \| \mathrm{SNX}_j)$. The information $(\mathrm{HSN}_3, \mathrm{GSC}_1, \mathrm{GSC}_2, \mathrm{GSC}_3, \mathrm{GSC}_4, T_{\mathrm{hgwn1}})$ transmitted from GWN_H to U_i comprises the session key; that is, $\mathrm{GSC}_4 = h(r_{\mathrm{SCn}} \| \mathrm{GUID}_i^{\mathrm{new}} \| \mathrm{SNX}_j \| \mathrm{SK}_h \| \mathrm{GF}_i \| T_{\mathrm{gwnh1}})$. Let us assume that the assailant captures the information; then the assailant intends to figure out $\mathrm{SK}^* = h(r_{\mathrm{SN}j} \| r_{\mathrm{GWNh}} \| \mathrm{UID}_i \| h(r_{\mathrm{SCn}} \| \mathrm{SCN}_i) \| \mathrm{SNX}_j)$ by creating $r_{\mathrm{SN}j}$, r_{GWNh}, r_{SCn}, $\mathrm{SNX}_j = h(\mathrm{ID}_{\mathrm{SN}j} \| \mathrm{SX}_{\mathrm{SN}j})$, $h(r_{\mathrm{SCn}} \| \mathrm{SCN}_i)$, and $\mathrm{UID}_i = h(\mathrm{ID}_i \| r_i)$. In case 2, the private session key is $\mathrm{SK}_s = h(r_{\mathrm{SN}j} \| r_{\mathrm{GWN}f} \| \mathrm{UID}_i \| h(r_{ui} \| \mathrm{UID}_i))$. The information $(\mathrm{SFN}_2, \mathrm{SFN}_3, T_{snj})$ dispatched from SN_j to GWN_F includes the session key; that is, $\mathrm{SFN}_3 = h(r_{\mathrm{SN}j} \| r_{\mathrm{GWN}f} \| \mathrm{SK}_s \| \mathrm{UID}_i \| \mathrm{SNX}_j \| T_{snj})$. By creating

r_{SNj}, r_{GWNh}, $UID_i = h(ID_i \| r_i)$, and $h(r_{Ui} \| UID_i)$, the assailant is able to figure out the session key $SK^* = h(r_{SNj} \| r_{GWNf} \| UID_i \| h(r_{ui} \| UID_i))$. Nevertheless, it is impracticable for the assailant to figure out the session key without knowing these privacy parameters and finishing inversion of hash function in polynomial time. Thus, our designed protocol is capable of achieving session key security.

5.2. Three-Factor Security. In our designed protocol, if the assailant only knows two of three factors, he is unable to launch an attack in our designed protocol. The first possibility is that the assailant only knows smart card and biometric. In this condition, assume that the assailant captures $(GE_i, GF_i, USC_1, USC_2, USC_3)$ kept in smart card and regains σ_{Ui} by the formula $GEN(BIO_{Ui}) = (\sigma_{Ui}, \tau_{Ui})$. Later, the assailant will speculate ID_i, PW_i, r_i, and r_p to figure out $UID_i^* = h(ID_i^* \| r_i^*)$, $UPW_i^* = h(PW_i^* \| r_i^* \| r_p^*)$, and $USC_3 = h(UID_i \| UPW_i \| \sigma_{Ui} \| r_i \| r_p)$ and confirms the correctness of the formula $USC_3^* = USC_3$. Nevertheless, the assailant cannot obtain password and sensitive parameters at the same time [4]. The smart card will suspend the session promptly after the assailant inputs the speculated password and sensitive parameters. The second possibility is that the assailant only knows password and biometric. Although the assailant has no ability to regain σ_{Ui} by the formula $REP(BIO_{Ui}, \tau_{Ui}) = \sigma_{Ui}$, he is able to capture the communication information $(SCG_1, SCG_2, SCG_4, T_{sc}, UID_i, ID_{SNj})$. Even if the assailant obtains the correct password and biometric, he still cannot pass the verification of the smart card and cannot simulate the communication information. The third possibility is that the assailant only knows smart card and password. Assume that the assailant captures $(GE_i, GF_i, USC_1, USC_2, USC_3)$ kept in smart card, where $USC_1 = r_i \oplus h(ID_i \| PW_i \| \sigma_{Ui})$, $USC_2 = r_p \oplus h(\sigma_{Ui} \| r_i)$, and $USC_3 = h(UID_i \| UPW_i \| \sigma_{Ui} \| r_i \| r_p)$. Due to the uniqueness of biometric, the assailant has no ability to regain σ_{Ui} by the formula $GEN(BIO_{Ui}) = (\sigma_{Ui}, \tau_{Ui})$. Without obtaining accurate biometric information to figure out USC_1, USC_2, and USC_3, it is impossible for the assailant to imitate user to log into the gateway.

5.3. Perfect Forward and Backward Security. In our designed protocol, the private session key in case 1 is $SK = h(r_{SNj} \| r_{GWNh} \| UID_i \| h(r_{SCn} \| SCN_i) SNX_j)$ and it is counted by the stochastic digits r_{SNj}, r_{GWNh}, r_i, and r_{SCn}, the identities ID_i, SCN_i, and ID_{SNj}, and the private key SX_{SNj}. The private session key in case 2 is $SK = h(r_{SNj} \| r_{GWNf} \| UID_i \| h(r_{ui} \| UID_i))$ and it is counted by the stochastic digits r_{SNj}, r_{GWNh}, r_{ui}, and r_i and the identity ID_i. The private session key is counted by the hash function and the stochastic digits are variable in each session. Even if the assailant compromises the private session key SK in case 1 and case 2, he is unable to obtain any previous or future private session keys. Consequently, our designed protocol is capable of achieving perfect forward and backward security.

5.4. Resist Sensor Node Capture Attack. In our designed protocol, the assailant is able to capture the sensor node and obtain the information (ID_{SNj}, SNX_j) kept in the sensor nodes, since the sensor nodes are placed in an unattended environment. SNX_j is calculated as $SNX_j = h(ID_{SNj} \| SX_{SNj})$ and SX_{SNj} is the private key of sensor node that is only known to himself. Even if the assailant compromises the information kept in the sensor nodes, he is unable to accurately figure out the private parameters in sensor nodes and create the effective information in the communication process. Consequently, our designed protocol is capable of resisting sensor node capture attack.

5.5. Resist Stolen Smart Card Attack. In our designed protocol, smart card is one of the three factors; hence, the case where the smart card is stolen is supposed to be taken into consideration. Smart card includes GE_i, GF_i, USC_1, USC_2, and USC_3, where $GE_i = h(UID_i \| UPW_i)$, $GF_i = GE_i \oplus GUID_i \oplus UID_i$, $USC_1 = r_i \oplus h(ID_i \| PW_i \| \sigma_{Ui})$, $USC_2 = r_p \oplus h(\sigma_{Ui} \| r_i)$, and $USC_3 = h(UID_i \| UPW_i \| \sigma_{Ui} \| r_i \| r_p)$; r_i and r_p are stochastic digits picked by U_i; and σ_{Ui} is counted by GEN. Assume that the smart card is stolen by the assailant through power analysis method and the information $(GE_i, GF_i, USC_1, USC_2, USC_3)$ kept in smart card is available to the assailant. The assailant is unable to speculate ID_i, PW_i, and σ_{Ui} through USC_1 and is also unable to speculate r_{GWNh} and SX_{GWNh} through $GUID_i$. Without these important parameters, the assailant is unable to imitate the smart card information. Thus, our designed protocol is capable of resisting stolen smart card attack.

5.6. Resist User Impersonation Attack. In our designed protocol, assume that the login request information $(SCG_1, SCG_2, SCG_4, T_{sc}, UID_i, ID_{SNj})$ is known by the assailant. In order to compute SCG_1, the assailant has to calculate $GUID_i$ and SCN_i. In order to compute SCG_2, the assailant has to calculate r_{SCn} and $h(SCN_i \| T_{sc})$. In order to compute SCG_4, the assailant has to calculate $GUID_i$, SCG_3, r_{SCn}, and SCN_i. To implement impersonation attack, the assailant has to speculate accurate parameters $(r_{SCn}, SCN_i, T_{sc}, r_{GWNh}, SX_{GWNh}, ID_{GWNh}, ID_i, PW_i, r_i, r_p)$. However, it is impossible for the assailant to gain these parameters. Without these important parameters, the assailant is unable to imitate the user to participate in the communication process. Thus, our designed protocol is capable of resisting user impersonation attack.

5.7. Resist Gateway Impersonation Attack. In our designed protocol, when U_i delivers the registration request (UID_i, UPW_i) to GWN_H, where $UID_i = h(ID_i \| r_i)$ and $UPW_i = h(PW_i \| r_i \| r_p)$, the assailant is able to capture this registration information and demands to reply information (GE_i^*, GF_i^*) to U_i, where $GF_i^* = GE_i^* \oplus GUID_i^* \oplus UID_i^*$, $GE_i^* = h(UID_i^* \| UPW_i^*)$, and $GUID_i^* = h(r_{GWNh}^* \| SX_{GWNh}^* \| ID_{GWNh}^*) \oplus UID_i^*$. In order to accurately calculate these parameters, the assailant needs to speculate $(r_{GWNh}, r_i, r_p, ID_i, PW_i, SX_{GWNh}, ID_{GWNh})$. As the stochastic

digits (r_{GWNh}, r_i, r_p) are variable in each session, this reply will not be successful. Consequently, our designed protocol is capable of resisting gateway impersonation attack.

5.8. Resist Sensor Node Impersonation Attack. In our designed protocol, the assailant is able to capture the information $(HSN_1, HSN_2, HSN_3, HSN_4, T_{gwnh})$ and counts $UID_i^* = SNX_j \oplus HSN_1$, $h(r_{SCn}\|SCN_i)^* = ID_{SNj} \oplus HSN_2$, and $r_{GWNh}^* = HSN_1 \oplus UID_i^* \oplus HSN_3$. Then, the assailant chooses stochastic digit r_{ASSk} and time T_{ass} to count $SK_s = h(r_{ASSK}\|r_{GWNh}\|UID_i\|h(r_{SCn}\|SCN_i)\|SNX_j)$, $SHN_1 = r_{ASSk} \oplus h(h(r_{SCn}\|SCN_i)\|r_{GWNh}|T_{ass})$, and $SHN_2 = h(r_{GWNh}\|UID_i\|SK_s\|SNX_j\|T_{ass})$ as the valid sensor nodes. Nevertheless, SNX_j includes the private key SX_{SNj} of SN; hence, the assailant is unable to count the accurate information (SHN_1, SHN_2, T_{ass}) and the session key SK_A. The aforementioned sensor node impersonation attack is in case 1, and case 2 is identical to case 1. Consequently, our designed protocol is capable of resisting the sensor node impersonation attack.

5.9. Resist Reply Attack. In our designed protocol, we apply the time stamp in our communication information to resist reply attack. Suppose that the assailant captures the foregone communication information $(SCG_1, SCG_2, SCG_4, T_{sc}, UID_i, ID_{SNj})$ and intends to imitate the legitimate user to reply the information. GWN_H computes the freshness of the information by the formula $|T_{gwnh} - T_{sc}| \le \Delta T$. If it is not right, GWN_H terminates the session promptly. Suppose that the assailant captures the foregone communication information $(HSN_1, HSN_2, HSN_3, HSN_4, T_{gwnh})$ and intends to imitate the legitimate gateway to reply the information. SN_j calculates the freshness of the information by the formula $|T_{snj} - T_{gwnh}| \le \Delta T$. If it is not right, SN_j terminates the session promptly. Consequently, our designed protocol is capable of resisting reply attack.

5.10. Resist Privileged Insider Attack. In our designed protocol, U_i delivers UID_i and UPW_i to GWN_H as the registration request in registration section, where $UID_i = h(ID_i\|r_i)$ and $UPW_i = h(PW_i\|r_i\|r_p)$. If the identity and password are leaked to any privileged insider at GWN_H, this will lead to abundant security risks. The privileged insider is unable to extract the accurate identity ID_i and password PW_i from UID_i and UPW_i in the registration section on account of the irreversible one-way hash function $h(\cdot)$. Unaware of the stochastic digits r_i and r_p, the privileged insider is also unable to extract the accurate identity ID_i and password PW_i from UID_i and UPW_i in the registration section. Consequently, our designed protocol is capable of resisting privileged insider attack.

5.11. Resist Online Password-Guessing Attack. In our designed protocol, password PW_i never emerges in the delivered information in the communication process. Although the assailant is able to capture the communication information $(SCG_1, SCG_2, SCG_4, T_{sc}, UID_i, ID_{SNj})$, $(HSN_1, HSN_2, HSN_3, HSN_4, T_{gwnh})$, (SHN_1, SHN_2, T_{snj}), and $(HSN_3, GSC_1, GSC_2, GSC_3, GSC_4, T_{hgwn1})$, all the communication information does not directly associate with password PW_i. The aforementioned condition is in case 1, and case 2 is identical to case 1. Consequently, our designed protocol is capable of resisting online password-guessing attack.

5.12. Resist Offline Password-Guessing Attack. In our designed protocol, the assailant is able to capture the smart card and obtain the kept information GE_i, GF_i, USC_1, USC_2, and USC_3. The smart card contents containing password are $USC_1 = r_i \oplus h(ID_i\|PW_i\|\sigma_{Ui})$ and $USC_3 = h(UID_i\|UPW_i\|\sigma_{Ui}\|r_i\|r_p)$. For the purpose of speculating the password accurately, the assailant has to obtain ID_i and σ_{Ui} at the same time for USC_1 and has to obtain ID_i, r_i, r_p, and σ_{Ui} at the same time for USC_3. It is impossible for the assailant to accurately compute these parameters at the same time. Consequently, our designed protocol is capable of resisting offline password-guessing attack.

5.13. Resist User Tracking Attack. In our designed protocol, parameter $GUID_i$ computed by the gateway node for the user is transformed into $GUID_i^{new} = GSC_3 \oplus h(UID_i\|UPW_i)$ after finishing the authentication process in case 1. Parameter $GUID_i$ computed by the gateway node for the user is transformed into $GUID_i^{new} = h(r_{GWNf}^{new}\|SX_{GWNf}\|ID_{GWNf}) \oplus UID_i$ after finishing the authentication process in case 2. Without knowing the relevant parameter, only known U_i, the assailant is unable to figure out the following $GUID_i^{new}$. Consequently, our designed protocol is capable of resisting user tracking attack.

5.14. Biometric Template Protection. In our designed protocol, the biometric information kept in smart card is first counted via $GEN(BIO_{Ui}) = (\sigma_{Ui}, \tau_{Ui})$ and the masked with the irreversible one-way hash function $USC_1 = r_i \oplus h(ID_i\|PW_i\|\sigma_{Ui})$, $USC_2 = r_p \oplus h(\sigma_{Ui}\|r_i)$, and $USC_3 = h(UID_i\|UPW_i\|\sigma_{Ui}\|r_i\|r_p)$. Even though the smart card is captured by the assailant, he is incapable of gaining any useful biometric information because the hash function is irreversible operation. Consequently, our designed protocol is capable of protecting the biometric template.

5.15. Mutual Authentication. In our designed protocol, U_i delivers the login request $(SCG_1, SCG_2, SCG_4, T_{sc}, UID_i, ID_{SNj})$ to GWN_H. After reception of the information, GWN_H authenticates U_i by computing SCG_4^*. GWN_H transmits $(HSN_1, HSN_2, HSN_3, HSN_4, T_{gwnh})$ to SN_j. After reception of the information, SN_j authenticates GWN_H by computing HSN_4^*. SN_j dispatches (SHN_1, SHN_2, T_{snj}) to GWN_H. After reception of the information, GWN_H authenticates SN_j by computing SHN_2^*. GWN_H transmits $(HSN_3, GSC_1, GSC_2, GSC_3, GSC_4, T_{hgwn1})$ to U_i. After reception of the information, U_i authenticates GWN_H by computing GSC_4^*. The aforementioned mutual authentication is in case 1, and case 2 is identical to case 1.

Consequently, our designed protocol is capable of achieving the mutual authentication.

5.16. User Anonymity. In our designed protocol, the assailant is able to capture the login request $(SCG_1, SCG_2, SCG_4, T_{sc}, UID_i, ID_{SNj})$ and obtain the kept information GE_i, GF_i, USC_1, USC_2, and USC_3 in the stolen smart card. The assailant will figure out identity ID_i via $h(UID_i \| UPW_i) = GF_i \oplus SCG_3$, where $UID_i = h(ID_i \| r_i)$. In order to figure out GF_i, the assailant has to speculate parameters r_{GWNh} and SX_{GWNh}, which are only known to GWN_H. Moreover, UPW_i includes parameters PW_i and r_p, which are only known to U_i. Consequently, our designed protocol is capable of achieving user anonymity.

6. Performance Comparison

In this section, we will demonstrate performance comparisons of our proposed mutual authentication protocol with other related mutual authentication protocols in terms of security, computation time, and communication cost.

6.1. Security Comparison. The security comparison result is shown in Table 1. From [1], we know that [25] cannot resist offline and online password-guessing attack. As shown in [25], the authors' security analysis does not mention or refer to IF5, IF7, IF10, and IF13. As shown in [46], the authors' security analysis does not mention or refer to IF2, IF4, and IF11. From [1], we know that [45] and [9] cannot resist IF5 and cannot achieve IF16 and IF3. As shown in [50], the authors' security analysis does not mention or refer to IF2, IF4, IF11, IF12, and IF14. As shown in [8], the authors' security analysis does not mention or refer to IF3, IF5, IF7, and IF14. From [47], we know that [48] cannot resist reply and sensor node capture attacks. As shown in [47], the authors' security analysis does not mention or refer to IF2, IF11, and IF12. As shown in [49], the authors' security analysis does not mention or refer to IF2, IF13, IF14, and IF15.

6.2. Computation Time Comparison. The computation time comparison result is presented in Table 2. We directly obtain the communication costs in the corresponding references as shown in Table 2. We can see that some references [47–49] add fingerprint operations to communication cost, while some references [8, 9, 25, 45] do not. In order to make a unified communication cost comparison, we will not add the fingerprint operations to communication cost. In this comparison, we specify that H represents the time of hash function operation, E/D represents the time of encryption and decryption operation, MM represents the time of modular multiplication operation, and EM represents the time of ECC point multiplication operation. We apply the experimental results of EM = 0.0171 s [46], H = 0.00032 s [7], E/D = 0.0056 s [7], and MM = 0.0002586 s [47] to compute computation cost. The total communication time in our designed protocol is $27H = 0.00864$ s in case 1 and $43H = 0.0137$ s in case 2. Although the communication cost is higher than the communication time in [7], our designed protocol has higher level of security. Compared with other authentication protocols, no matter in case 1 or in case 2, our designed protocol has higher level of computation cost and is more suitable for the resource-constrained wireless sensor networks.

Table 1: Security comparison.

	[45]	[9]	[46]	[25]	[47]	[48]	[8]	[49]	[50]	Ours
IF1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IF2	Y	Y	N	Y	N	Y	Y	N	N	Y
IF3	N	N	Y	Y	Y	Y	N	Y	Y	Y
IF4	Y	Y	N	Y	Y	N	Y	Y	N	Y
IF5	N	N	Y	N	Y	Y	N	Y	Y	Y
IF6	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IF7	Y	Y	Y	N	Y	Y	N	Y	Y	Y
IF8	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IF9	Y	Y	Y	Y	Y	N	Y	Y	Y	Y
IF10	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
IF11	Y	Y	N	N	N	Y	Y	Y	N	Y
IF12	Y	Y	Y	N	N	Y	Y	Y	N	Y
IF13	Y	Y	Y	N	Y	Y	Y	N	Y	Y
IF14	Y	Y	Y	Y	Y	Y	N	N	N	Y
IF15	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
IF16	N	N	Y	Y	Y	Y	Y	Y	Y	Y

IF1: session key security; IF2: three-factor security; IF3: perfect forward and backward security; IF4: resist sensor node capture attack; IF5: resist stolen smart card attack; IF6: resist user impersonation attack; IF7: resist gateway impersonation attack; IF8: resist sensor node impersonation attack; IF9: resist reply attack; IF10: resist privileged insider attack; IF11: resist online password-guessing attack; IF12: resist offline password-guessing attack; IF13: resist user tracking attack; IF14: biometric template protection; IF15: mutual authentication; IF16: user anonymity; Y: yes; N: no or not mentioned.

6.3. Communication Cost Comparison. The communication cost comparison result is revealed in Table 3. In order to make a unified and thorough communication cost comparison, we make the following assumptions that the identity of user is 160 bits, the identity of gateway node or base station is 160 bits, the identity of sensor node is 32 bits, the stochastic digit is 128 bits, the result of symmetric encryption/decryption is 128 bits, the time stamp size is 32 bits, the result of hash function is 160 bits, and the result of ECC point multiplication operation is 160 bits.

In case 1, the communication cost of the information $(SCG_1, SCG_2, SCG_4, T_{sc}, UID_i, ID_{SNj})$ delivered from U_i to GWN_H is 160 bits + 160 bits + 160 bits + 32 bits + 160 bits + 32 bits = 704 bits; the communication cost of the information $(HSN_1, HSN_2, HSN_3, HSN_4, T_{gwnh})$ transmitted from GWN_H to SN_j is 160 bits + 160 bits + 128 bits + 160 bits + 32 bits = 640 bits; the communication cost of the information (SHN_1, SHN_2, T_{snj}) dispatched from SN_j to GWN_H is 160 bits + 160 bits + 32 bits = 352 bits; and the communication cost of the information $(HSN_3, GSC_1, GSC_2, GSC_3, GSC_4, T_{hgwn1})$ transmitted from GWN_H to U_i is 160 bits + 160 bits + 160bits + 160 bits + 160 bits + 32 bits = 832 bits.

Table 2: Computation time comparison.

	User	Sensor node	Home gateway/base station	Foreign gateway/base station	Total time
[45]	$6H + 2E/D$	$5H + 1E/D$	$8H + 3E/D$	$5H + 2E/D$	$24H + 8E/D = 0.0524$ s
[9]	$14H$	$4H$	$17H$	0	$35H = 0.0112$ s
[46]	$8H + 3$EM	0	$7H + 3$EM	0	$15H + 6$EM $= 0.107$ s
[25]	$8H + 3$EM	$4H + 2$EM	$8H +$ EM	0	$20H + 6$EM $= 0.109$ s
[47]	$9H + 2$EM	$5H$	$10H + 1$EM	0	$24H + 3$EM $= 0.0589$ s
[48]	$9H + 1E/D$	$4H + 2E/D$	$6H + 3E/D + 2$MM	0	$19H + 6E/D + 2$MM $= 0.0412$ s
[8]	Case 1: $13H$ Case 2: $18H$	Case 1: $6H$ Case 2: $6H$	Case 1: $17H$ Case 2: $10H$	Case 1: $0H$ Case 2: $14H$	Case 1: $36H = 0.0115$ s Case 2: $48H = 0.0153$ s
[49]	Case 1: $12H + 3$EM Case 2: $12H + 4$EM	Case 1: $5H$ Case 2: $5H$	Case 1: $6H + 3$ EM Case 2: 0	Case 1: 0 Case 2: $8H + 3$EM	Case 1: $23H + 6$EM $= 0.1099$ s Case 2: $25H + 6$EM $= 0.111$ s
[50]	Case 1: $7H + 2$EM Case 2: $7H + 2$EM	Case 1: $4H + 2$EM Case 2: $4H + 2$EM	Case 1: $11H$ Case 2: $9H + 1$EM	Case 1: $0H$ Case 2: $8H + 1$EM	Case 1: $22H + 4$EM $= 0.0754$ s Case 2: $28H + 6$EM $= 0.1116$ s
Ours	Case 1: $12H$ Case 2: $16H$	Case 1: $5H$ Case 2: $7H$	Case 1: $12H$ Case 2: $6H$	Case 1: $0H$ Case 2: $14H$	Case 1: $27H = 0.00864$ s Case 2: $43H = 0.0137$ s

Table 3: Communication cost comparison.

	User (bits)	Sensor node (bits)	Home gateway/base station (bits)	Foreign gateway/base station (bits)	Total cost (bits)
[45]	608	352	448	736	2144
[9]	983	352	1344	0	2679
[46]	864	0	512	0	1376
[25]	640	480	960	0	2080
[47]	928	416	1312	0	2656
[48]	512	160	1440	0	2112
[8]	Case 1: 864 Case 2: 512	Case 1: 352 Case 2: 352	Case 1: 1344 Case 2: 1184	Case 1: 0 Case 2: 1376	Case 1: 2560 Case 2: 3424
[49]	Case 1: 1024 Case 2: 1024	Case 1: 352 Case 2: 352	Case 1: 800 Case 2: 544	Case 1: 0 Case 2: 800	Case 1: 2176 Case 2: 2720
[50]	Case 1: 864 Case 2: 864	Case 1: 1728 Case 2: 1728	Case 1: 640 Case 2: 832	Case 1: 0 Case 2: 1504	Case 1: 3232 Case 2: 4928
Ours	Case 1: 704 Case 2: 512	Case 1: 352 Case 2: 352	Case 1: 1472 Case 2: 480	Case 1: 0 Case 2: 1920	Case 1: 2528 Case 2: 3264

In case 2, the communication cost of the information $(\mathrm{FHN}_1, \mathrm{FHN}_2, \mathrm{FHN}_3, \mathrm{FHN}_4)$ transmitted from GWN_F to GWN_H is 160 bits + 160 bits + 128 bits + 160 bits = 608 bits; the communication cost of the information $(\mathrm{FHN}_2, \mathrm{GSC}_6, \mathrm{GSC}_7)$ transmitted from GWN_H to U_i is 160 + 160 + 160 = 480 bits; the communication cost of the information $(\mathrm{SCF}_5, \mathrm{SCF}_6, \mathrm{SCF}_7, T_{ui})$ delivered from U_i to GWN_F is 160 bits + 160 bits + 160 bits + 32 bits = 512 bits; the communication cost of the information $(\mathrm{FSN}_1, \mathrm{FSN}_2, \mathrm{FSN}_3, \mathrm{FSN}_4, T_{\mathrm{gwn}f})$ transmitted from GWN_F to SN_j is 160 bits + 160 bits + 160 bits + 160 bits + 32 bits = 672 bits; the communication cost of the information $(\mathrm{SFN}_2, \mathrm{SFN}_3, T_{snj})$ dispatched from SN_j to GWN_F is 160 bits + 160 bits + 32 bits = 352 bits; and the communication cost of the information $(\mathrm{FSC}_1, \mathrm{FSC}_2, \mathrm{FSC}_3, \mathrm{FSC}_4, T_{\mathrm{gwn}f1})$ transmitted from GWN_F to U_i is 128 bits + 160 bits + 160 bits + 160 bits + 32 bits = 640 bits.

Compared with the other authentication protocols, the total communication cost in our protocol is a bit higher than those in the other protocols [25, 45, 46, 48, 49]. During the authentication process, the number of information exchanges in the protocols in [46, 48, 49] is less than ours and the sensor nodes require more communication cost than the gateway node in the protocol in [50]. Because the sensor nodes are resource-constrained, the communication costs of the sensor nodes shall be reduced. The sensor nodes' communication costs in our protocol are lower than those in the other comparison protocols. The communication cost is acceptable as our designed authentication protocol achieves additional security features and has lower computation time.

7. Conclusion

To overcome the problems that the sensor nodes need to execute heavy calculation and communication consumption during the authentication process and cannot resist node capture attack and that the protocols also cannot provide perfect forward and backward security and cannot resist replay attack, we put forward a novel multifactor user authentication and key agreement scheme for multigateway wireless sensor networks in this paper. In our authentication protocol, we apply the lightweight hash function and given biometric information to achieve a higher level of security and efficiency, as well as a larger communication coverage area. Our authentication protocol meets sixteen evaluation criteria. We separately apply BAN logic, random oracle

model, and AVISPA tool to validate the security of our authentication protocol. Our authentication protocol is able to achieve higher security and is more efficient in communication and computation costs as compared with the related authentication protocols.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China, under Grant no. 61962052, IoT Innovation Team Foundation of Qinghai Office of Science and Technology, under Grant no. 2020-ZJ-903, Key Laboratory of IoT of Qinghai (2020-ZJ-Y16), and Hebei IoT Monitoring Center (3142016020).

References

[1] C. Wang, D. Wang, Y. Tu et al., "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2020.

[2] D. Singh, B. Kumar, S. Singh et al., "Evaluating authentication schemes for real-time data in wireless sensor network," *Wireless Personal Communications*, vol. 114, no. 3, 2020.

[3] Y. Lu, G. Xu, L. Li et al., "Robust privacy-preserving mutual authenticated key agreement scheme in roaming service for global mobility networks," *IEEE Systems Journal*, vol. 13, pp. 1–12, 2019.

[4] D. Wang, W. Li, and P. Wang, "Measuring two-factor Authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4081–4092, 2018.

[5] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: approaches, threats and trends," *Computer Networks*, vol. 170, no. 2, Article ID 107118, 2020.

[6] S. Jangirala, D. A. Kumar, W. Mohammad, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, p. 1, 2018.

[7] M. Wazid, A. K. Das, V. Odelu et al., "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, p. 1, 2017.

[8] H. Guo, Y. Gao, T. Xu et al., "A secure and efficient three-factor multi-gateway authentication protocol for wireless sensor networks," *Ad Hoc Networks*, vol. 95, Article ID 101965.1, 2019.

[9] R. Amin, S. K. H. Islam, N. Kumar, and K. K. R. Choo, "An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks," *Journal of Network and Computer Applications*, vol. 104, 2018.

[10] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Systems Journal*, vol. 10, no. 4, pp. 1–10, 2016.

[11] G. Xu, J. Liu, Y. Lu, X. Zeng, Y. Zhang, and X. Li, "A novel efficient MAKA protocol with desynchronization for anonymous roaming service in Global Mobility Networks," *Journal of Network and Computer Applications*, vol. 107, pp. 83–92, 2018.

[12] W. Fan, L. Xu, S. Kumari et al., "An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks," *Annals of Telecommunications*, vol. 72, no. 3-4, pp. 1–14, 2016.

[13] G. Mohit and S. C. Narendra, "Anonymous two factor authentication protocol for roaming service in global mobility network with security beyond traditional limit," *Ad Hoc Networks*, vol. 84, pp. 56–67, 2019.

[14] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4900–4913, 2018.

[15] S. Hussain and S. A. Chaudhry, "Comments on "biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment"" *IEEE Internet of Things Journal*, vol. 6, no. 6, Article ID 10936, 2019.

[16] 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," *Computer Networks*, vol. 101, pp. 42–62, 2016.

[17] A. O. Sharif, H. Arshad, M. Nikooghadam et al., "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," *Future Generation Computer Systems*, vol. 100, 2019.

[18] F. Wu, X. Li, L. Xu et al., "A novel three-factor Authentication protocol for wireless sensor networks with IoT notion," *IEEE Systems Journal*, vol. 15, no. 99, pp. 1–10, 2020.

[19] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Information Sciences*, vol. 321, pp. 263–277, 2015.

[20] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Generation Computer Systems*, vol. 63, pp. 56–75, 2016.

[21] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 76, pp. 37–48, 2016.

[22] L. Xiong, J. Niu, S. Kumari et al., "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications*, vol. 103, 2018.

[23] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *International Journal of Communication Systems*, vol. 30, no. 1, Article ID e2933.1, 2017.

[24] Y. Lu, G. Xu, L. Li et al., "Anonymous three-factor authenticated key agreement for wireless sensor networks," *Wireless Networks*, vol. 25, 2017.

[25] X. Li, J. Peng, M. S. Obaidat et al., "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," *IEEE Systems Journal*, vol. 14, no. 99, pp. 1–12, 2019.

[26] A. Ruhul, S. K. HafizulIslam, G. P. Biswas, M. Khurram Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generations Computer Systems Fgcs*, vol. 80, 2018.

[27] J. Mo and H. Chen, "A lightweight secure user authentication and key agreement protocol for wireless sensor networks," *Security and Communication Networks*, vol. 2019, no. 4, pp. 1–17, 2019.

[28] L. Xiong, J. Niu, S. Kumari et al., "A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city," *Future Generation Computer Systems*, vol. 83, pp. 607–618, 2017.

[29] L. Xiong, A. K. Sangaiah, S. Kumari, F. Wu, J. Shen, and M. K. Khan, "An efficient authentication and key agreement scheme with user anonymity for roaming service in smart city," *Personal & Ubiquitousuting*, vol. 21, 2017.

[30] B. Yza, B. Dha, L. A. Li et al., "A lightweight authentication and key agreement scheme for Internet of Drones," *Computer Communications*, vol. 154, pp. 455–464, 2020.

[31] M. Wazid, A. K. Das, N. Kumar et al., "Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of Drones deployment," *IEEE Internet of Things Journal*, vol. 6, p. 1, 2018.

[32] P. Vijayakumar, V. Chang, L. J. Deborah et al., "Computationally efficient privacy preserving anonymous mutual and batch Authentication schemes for vehicular ad hoc networks," *Future Generation Computer Systems*, vol. 78, 2016.

[33] C. Xu, X. Huang, M. Ma, and H. Bao, "An anonymous handover authentication scheme based on LTE-A for vehicular networks," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 6251219, 15 pages, 2018.

[34] S. Chatterjee, S. Roy, A. K. Das et al., "Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 99, p. 1, 2016.

[35] T. Sudhakar, V. Natarajan, M. Gopinath, and J. Saranyadevi, "An enhanced authentication protocol for multi-server environment using password and smart card," *Wireless Personal Communications*, vol. 115, no. 2, 2020.

[36] S. Qiu, D. Wang, G. Xu et al., "Practical and provably secure three-factor Authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2020.

[37] W. Ding, C. Haibo, H. Debiao, and W. Ping, "On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices," *IEEE Systems Journal*, vol. 12, 2016.

[38] L. Xiong, W. Fan, M. K. Khan et al., "A secure chaotic map-based remote authentication scheme for telecare medicine information systems," *Future Generation Computer Systems*, vol. 84, pp. 149–159, 2017.

[39] J. Mo, W. Shen, and W. Pan, "An improved anonymous authentication protocol for wearable health monitoring systems," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 5686498, 13 pages, 2020.

[40] A. Irshad, S. A. Chaudhry, Q. Xie et al., "An enhanced and provably secure chaotic map-based authenticated key agreement in multi-server architecture," *Arabian Journal for Science and Engineering*, vol. 43, 2017.

[41] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Networks*, vol. 36, no. 1, pp. 58–80, 2016.

[42] S. Jangirala, S. Mukhopadhyay, and A. K. Das, "A multi-server environment with secure and efficient remote user authentication scheme based on dynamic ID using smart cards," *Wireless Personal Communications*, vol. 95, 2017.

[43] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," *Ad Hoc Networks*, vol. 54, pp. 147–169, 2017.

[44] D. Kumar, S. Chand, and B. Kumar, "Cryptanalysis and improvement of an authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 1, pp. 1–20, 2018.

[45] A. Rifaqat, P. Alrup Kumar, K. Saru, K. Marimuthu, and C. Mauro, "A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring," *Future Generation Computer Systems*, vol. 84, 2018.

[46] Y. Chen and J. Chen, "A secure three-factor-based authentication with key agreement protocol for e-Health clouds," *The Journal of Supercomputing*, vol. 77, no. 3, 2020.

[47] H. Far, M. Bayat, A. K. Das et al., "LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT," *Wireless Networks*, vol. 27, no. 4, pp. 1–24, 2021.

[48] R. Vinoth, L. J. Deborah, P. Vijayakumar, and N. Kumar, "Secure multifactor Authenticated key agreement scheme for industrial IoT," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3801–3811, 2021.

[49] A. K. Sutrala, A. K. Das, N. Kumar, A. G. Reddy, A. V. Vasilakos, and J. J. P. C. Rodrigues, "On the design of secure user authenticated key management scheme for multigateway-based wireless sensor networks using ECC," *International Journal of Communication Systems*, vol. 31, no. 8, Article ID e3514, 2018.

[50] J. Guo and Y. Du, "A secure three-factor anonymous roaming authentication protocol using ECC for space information networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 9, pp. 1–19, 2021.