IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 19, 2021, accepted July 12, 2021, date of publication July 26, 2021, date of current version August 2, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3099299

An Improved Authentication Protocol for Smart Healthcare System Using Wireless Medical Sensor Network

WANG YUANBING[1,2], LIU WANRONG[2], AND LI BIN[2]
[1]School of Biomedical Engineering, Shanghai Jiao Tong University, Shanghai 200030, China
[2]Shanghai Sixth People's Hospital Affiliated to Shanghai Jiao Tong University, Shanghai 200233, China

Corresponding author: Li Bin (libin2001@hotmail.com)

This work was supported in part by the National Key Research and Development Program of the Ministry of Science and Technology of China under Grant 2019YFC0121805.

ABSTRACT With the rapid development and evolution of wireless network technology, electronic health has shown great potential in continuously monitoring the health of patients. The wireless medical sensor network (WMSN) has played an important role in this field. In WMSN, medical sensors are placed on patients to collect relevant health data and transmitted to medical professionals in hospitals or at home through insecure channels. These health data need to be highly protected because they contain patient-related private information. Once the information is leaked or maliciously modified, it will cause the wrong diagnosis and endanger the health of patients. To protect information privacy and security from being stolen by illegal users, this article reviews the solutions of Farash *et al.* and further points out the existing vulnerabilities, such as privileged insider attack, user anonymity invalidation, and offline password guessing attack. In order to overcome these drawbacks, we use the Elliptic Curve Cryptography to propose an improved anonymous authentication protocol for a smart healthcare system. The security of our protocol is verified by Burrows-Abadi-Needham logic and Automated Validation of Internet Security Protocols and Applications (AVISPA) tools, and security features and efficiency analysis are performed with other related schemes. The results show that the improved protocol provides better security protection while ensuring computational and communication efficiency.

INDEX TERMS Authentication, patient monitor, security analysis, wireless medical sensor network.

I. INTRODUCTION

In recent years, with the rapid growth of hospitalized patients, it has become an increasingly difficult task to continuously monitor the health of patients by relying solely on medical professionals (such as doctors or nurses) [1]. Electronic health (e-Health) and mobile health provide the possibility to solve this problem. E-Health is an application based on Internet of Things which contains a series of healthcare information services [2], [3]. In this system, medical sensors are placed on the patient in advance to collect relevant physiological information, such as ECG, body temperature, blood pressure, pulse, etc. After that, the doctor can obtain medical information about the patient at any time and any place. This can not only reduce medical costs and make full use of limited medical resources but also help doctors make an early diagnosis and improve the quality of life of patients [1], [3], [4].

As a typical application in e-Health, Wireless Medical Sensor Network (WMSN) uses Wireless Sensing Network (WSN) to complete the task of monitoring the health status of patients. It comprises numerous lightweight smart devices with limited storage space, computation power, transmission range, and battery life [5]–[7]. Besides, when the patient's health data are transmitted through an unsafe public channel, information protection and privacy protection become prominent problems and big challenges [8].

If we transmit patient medical data without any encryption through an unsafe public channel, it is very likely that these information can be obtained by someone illegally, then the patient's privacy will be exposed. Meanwhile, a malicious user may modify the intercepted data and disguise it

The associate editor coordinating the review of this manuscript and approving it for publication was Gautam Srivastava.

as original information and then send it to remote medical professionals, which will lead to inappropriate diagnosis and affect patient treatment. User authentication and key agreement mechanism plays a vital role in protecting the patient's real-time data from unauthorized users; it can not only provide mutual authentication between all participating entities but also negotiate session keys to encrypt the transmitted data from eavesdropping [6], [8]–[11].

In 2012, Kumar *et al.* [12] proposed a user authentication protocol for medical monitoring. According to their security analysis, their solution can resist a variety of common security attacks and fully protect patient data from illegal users. However, Khan and Khan [13] and He *et al.* [14] pointed out that the protocol proposed by Kumar *et al.* [12] cannot resist insider privilege attack and offline password guessing attack, and lacks user anonymity and a complete mutual authentication mechanism. In order to overcome the above shortcomings, Khan and Khan [13] and He *et al.* [14] each proposed an improved two-factor user authentication protocol. Later in 2015, Wu *et al.* [15] found that He *et al.* scheme [14] could not resist offline password guessing attack, user impersonation attack, and sensor node capture attack. Then in 2016, Li *et al.* [16] found that He *et al.*'s scheme [14] had many problems during the login and authentication phases, and could not establish a correct session key. Besides, there is no check to verify whether the password inputted by user is correct until the information is delivered to the gateway node (GWN), and this may even cause the user to fail the authentication process after updating the password with a wrong old password. Therefore, Li *et al.* [16] introduced biometrics in their improved user authentication protocol to try to eliminate the previous drawbacks. Unfortunately, Das *et al.* [17] confirmed that Li *et al.*'s scheme [16] still could not resist various attacks such as privileged-insider attack.

In 2014, Turkanovć *et al.* [18] designed a novel lightweight user authentication and key agreement protocol for resource-constrained WSN which is claimed to have high security and can resist various common attacks. Unfortunately, in 2016, Farash *et al.* [19] showed Turkanovć *et al.*'s scheme [18] is very vulnerable to man-in-the-middle attack and stolen smart card attack. Besides, there was a lack of user untraceability and a secure session key protection mechanism. Subsequently, Amin and Biswas [20] further pointed out that any attacker can easily guess out a user's identity and password in [18]. Later, the analysis results of Amin *et al.* [21] showed that the improved user authentication scheme of Farash *et al.* [19] still has multiple security flaws. Similarly, in 2016, Wu *et al.* [22] showed that the scheme of Amin and Biswas [20] has the problem of mission key leakage and forgery attacks.

In 2016, in order to reduce the communication cost of sensing nodes mentioned in [20], Amin *et al.* [23] designed a new lightweight user authentication scheme that is used in patient monitoring systems. However, in 2017, Jiang *et al.* [24] showed that Amin *et al.*'s protocol [23] could not withstand the stolen mobile device attack, session key leakage, and desynchronization attack. Later, Wu *et al.* [25] in 2017 and Ali *et al.* [26] in 2018 further pointed out system insiders can use their own privileges to obtain the password of any user, and an unauthorized attacker can also pass the system authentication through forged login information in Amin *et al.*'s protocol [23]. But in 2018, Li *et al.* [27] analyzed Wu *et al.*'s scheme [25] and pointed out that the scheme is not user-friendly and does not provide forward security. In 2019, Chandrakar [9] mentioned that the protocol of Wu *et al.* [25] has some drawbacks such as it cannot prevent replay attack. In the same year, in order to solve the historical flaws in the authentication protocol used for remote patient monitoring (including the lack of forward security and desynchronization attack problem), Shuai *et al.* [28] designed a three-factor authentication scheme using hash functions and pseudonyms. In 2020, Mo *et al.* [29] pointed out that Ali *et al.*'s and Shuai *et al.*'s schemes [26], [28] are not as perfect as their own security analysis. Both of them have the same security problems, i.e., there is still the possibility of privileged insider attack and offline dictionary guessing attack. To make matters worse, once the user changes his/her password, they will be permanently rejected by GWN from login the network using the updated password.

In 2017, Challa *et al.* [30] designed a three-factor user authentication protocol for use in healthcare environments that takes into account both computational efficiency and security. In their scheme, in addition to providing a regular password update function, the user can also update his/her biometrics. In addition, a user re-registration function is added to the scheme to prevent the user's smart card from being lost or stolen. In 2019, Soni *et al.* [31] found many weaknesses in Challa *et al.*'s scheme [30]. Firstly, the attacker can easily calculate the session key; secondly, the attacker may destroy the normal connection process between the user and the sensor node; thirdly, the user re-registration process does not consider the issue of the revocation of the old smart card, which may cause the smart card flood. In 2020, Xu *et al.* [32] introduced chaotic maps and Rabin cryptosystem to improve Soni *et al.*'s scheme [31], providing a higher level of security and less computational consumption, which is more suitable for WMSN. Besides, Yazdinejad *et al.* [33] shortened the time for authentication in the hospital network by using the idea of blockchain.

A. MOTIVATION, METHODOLOGY AND CONTRIBUTION

The scheme of Farash *et al.* has been studied and analyzed by a large number of researchers, and many enhanced schemes have been proposed afterwards. However, most of the schemes did not adopt the architecture of Farash *et al.* for protocol design. Although Farash *et al.*'s protocol still uses the GWN to perform the authentication process, it does not need to interact with the GWN directly and can only obtain aggregated information about the sensor node as in other schemes. The user can directly connect and access a specific sensor node, thus providing a more direct approach.

Therefore, we believe that the design idea of Farash *et al.* is worth learning.

In this article, we first point out the security problems that still exist in Farash *et al.*'s scheme (i.e., privileged insider attack, user anonymity problem, and stolen smart card attack). Furthermore, we want to overcome these weaknesses. Therefore, we use the principle of elliptic curve cryptography (ECC) to improve the scheme. There is a CDH (Computational Diffie-Hellman) problem in ECC. The CDH problem believes that when given random numbers a, b and point P, it is easy to calculate abP; but when only the information of P, aP, and bP is given, it is impossible to calculate the value of abP in a limited time. Besides, we preserve the timestamp mechanism to ensure the freshness of the message in our protocol.

Based on the above principles, we propose an improved anonymous user authentication and key agreement protocol for health monitoring. In the subsequent security analysis, we proved the security of our protocol through Burrows-Abadi-Needham (BAN) logic and Automated Validation of Internet Security Protocols and Applications (AVISPA) tools. The performance comparison and efficiency analysis results confirm that the improved protocol provides a higher security level while ensuring computation efficiency.

B. ORGANIZATION OF THE PAPER

The remainder of this paper is organized as follows. In Section II, we briefly reviewed Farash *et al.*'s scheme and further pointed out the drawbacks of the scheme in Section III. In order to eliminate these shortcomings, we proposed an improved user authentication protocol for intelligent medical systems in Section IV. In Section V and VI, the security analysis of the proposed protocol is showed, including informal security analysis and mutual authentication proof using BAN logic. Further, we depict the simulation outputs using AVISPA in Section VII. The security features comparison and effectiveness analysis with other related schemes are illustrated in Section VIII. Finally, the conclusion is represented in Section IX.

II. REVIEW OF FARASH *et al.*'s SCHEME

In this section, we will briefly review Farash *et al.*'s scheme [19] in order to better understanding their content. According to Farash *et al.*'s description, their scheme includes five phases. For the purpose of this article, we will only describe the first four phases in detail except for the dynamic node addition phase. TABLE 1 depicts all notations used in the scheme.

A. PRE-DEPLOYMENT PHASE

In order to enable the network to operate normally, the system administrator *SA* must first perform the pre-deployment phase in offline mode. At this stage, *SA* will select a secure password X_{GWN} which is known only to the *GWN*. Each sensor node S_j will be pre-defined with its identity SID_j, and the gateway node *GWN* will generate and store a password X_{GWN-Sj} which is familiar by only GWN and the related S_j ($1 \leq j \leq m$), where m represents the number of sensor nodes. The shared key X_{GWN-Sj} will be used in the next sensor node registration phase. It is worth noting that when S_j is successfully registered, the password X_{GWN-Sj} will be deleted from the memory of S_j. Meanwhile, the gateway node *GWN* will also lose this information forever. In addition, the information of the sensor identity SID_j will also be deleted from the *GWN*, which allows the *GWN* to add a huge number of additional sensor nodes to this network, regardless of the *GWN* memory limit.

TABLE 1. Notations.

Notation	Description
U_i	user
ID_i	the identity of U_i
PW_i	the password of U_i
SC	smart card
S_j	sensor node
SID_j	the identity of S_j
$ESID_j$	masked identity of S_j
GWN	gateway node
X_{GWN}	secure password known only to the *GWN*
$X_{GWN\text{-}Sj}$	secure password shared with S_j
MP_i, MP_j	masked password of U_i and S_j
MN_j	masked nonce of S_j
T_x	timestamp
ΔT	time interval for the allowed transmission delay
SK	session key
$\oplus$, $\|\|$, $h()$	XOR, concatenation, and hash operation
r_i, r_j, K_i, K_j	random numbers

B. REGISTRATION PHASE

In this stage, a user needs to get a legal identity to access the system and sensors need to complete the rest initialization to normal work. In the subsequent login and authentication phases, only registered users and sensor nodes can be verified by *GWN*, then negotiate the session key between each other and achieve successful mutual communication. User and sensor node registration are shown in FIGURE 1 and 2.

C. LOGIN AND AUTHENTICATION PHASE

This phase is shown in FIGURE 3.

D. PASSWORD CHANGE PHASE

This phase is shown in FIGURE 4.

III. WEAKNESSES OF FARASH *et al.*'s SCHEME

A. WEAKNESS 1: PRIVILEGED INSIDER ATTACK

A privileged insider attack is an attack initiated by a privileged but malicious person. Although the *GWN* is generally

U_i		GWN
$Chooses < ID_i, PW_i >$		
$Generates\ a\ nonce\ r_i$		
$Calculates\ MP_i = h(r_i \| PW_i)$		
	$\xrightarrow{\{MP_i, ID_i\}}$	$Calculates\ e_i = h(MP_i \| ID_i)$
		$d_i = h(ID_i \| X_{GWN})$
		$g_i = h(X_{GWN}) \oplus h(MP_i \| d_i)$
		$f_i = d_i \oplus h(MP_i \| e_i)$
	$\xleftarrow{\{SC\}}$	$Stores\ \{e_i, f_i, g_i\} into\ a\ SC$
$Stores\ r_i\ into\ SC$		
$SC\ contains\ parameters\ \{r_i, e_i, f_i, g_i\}$		

FIGURE 1. User registration phase of Farash *et al.*'s scheme [19].

S_j		GWN
$stores\ its\ SID_j\ and\ X_{GWN-S_j}$		$knows\ its\ master\ key\ X_{GWN}$
		$for\ each\ S_j\ stores their\ SID_j\ and\ X_{GWN-S_j}$
$Generates\ a\ nonce\ r_j$		
$Calculates\ MP_j = h(X_{GWN-S_j} \| r_j \| SID_j \| T_1)$		
$MN_j = r_j \oplus X_{GWN-S_j}$		
	$\xrightarrow{\{SID_j, MP_j, MN_j, T_1\}}$	$Checks\ \lvert T_1 - T_c \rvert < \Delta T\ ?$
		$Calculates\ r_j^{'} = MN_j \oplus X_{GWN-S_j}$
		$Checks\ MP_j^{'} = ?\ h(X_{GWN-S_j} \| r_j^{'} \| SID_j \| T_1)$
		$Calculates\ x_j = h(SID_j \| X_{GWN}), e_j = x_j \oplus X_{GWN-S_j}$
		$d_j = h(X_{GWN} \| 1) \oplus h(X_{GWN-S_j} \| T_2)$
$Checks \lvert T_2 - T_c \rvert < \Delta T\ ?$	$\xleftarrow{\{e_j, f_j, d_j, T_2\}}$	$f_j = h(x_j \| d_j \| X_{GWN-S_j} \| T_2)$
$Calculates\ x_j = e_j \oplus X_{GWN-S_j}$		
$Checks\ f_j = ?\ h(x_j \| d_j \| X_{GWN-S_j} \| T_2)$		
$Calulates\ h(X_{GWN} \| 1) = d_j \oplus h(X_{GWN-S_j} \| T_2)$		
$Stores < x_j, h(X_{GWN} \| 1) > into\ memory$		
$Deletes\ X_{GWN-S_j}\ from\ memory$		
	$\xrightarrow{confirmation}$	$Deletes < SID_j, X_{GWN-S_j} > from\ memory$

FIGURE 2. Sensor registration phase of Farash *et al.*'s scheme [19].

considered as a trusted subject in the authentication scheme, the system administrator may also use his/her privileges to try to obtain some sensitive information, such as user identity, user password, session key, and so on. Assuming that adversary A is a privileged attacker, A can compute the session key of a session through the following steps:

Step1: A gets X_{GWN} from the GWN memory.

Step2: During the login and authentication phase, A can receive the message $\{M_1, M_2, M_3, T_1, T_2, ESID_j, M_4, M_5\}$, and then A computes:

$$K_i' = M_2 \oplus h(d_i' \| T_1) = M_2 \oplus h(h(ID_i' \| X_{GWN}) \| T_1)$$
$$= M_2 \oplus h(h((M_1 \oplus h(h(X_{GWN}) \| T_1)) \| X_{GWN}) \| T_1),$$
$$K_j' = M_4 \oplus h(x_j' \| T_1 \| T_2)$$
$$= M_4 \oplus h(h((ESID_j \oplus h(h(X_{GWN} \| 1) \| T_2)) \| X_{GWN}) \| T_1 \| T_2).$$

Step3: A computes $SK = h(K_i' \oplus K_j')$.

Once a privileged insider A calculates the session key SK, he/she can eavesdrop on the messages which are exchanged between the user and the sensor node even if these messages are encrypted by SK.

B. WEAKNESS 2: USER ANONYMITY PROBLEM

A secure identity authentication protocol requires complete confidentiality of the user's identity ID_i, hence all transmitted information that covers it should be highly encrypted so that no adversary can crack it in any way. However, Farash *et al.*'s scheme is not secure in terms of user anonymity. The user's identity ID_i can be extracted through the following steps:

Step1: Any authenticated user U_i has the capacity to retrieve the information $\{r_i, e_i, f_i, g_i\}$ from his/her smart card using the power consumption monitoring methods.

Step2: Assuming adversary A is an authenticated user, A can use his/her password PW_i to compute $MP_i = h(r_i \| PW_i)$, $d_i = f_i \oplus h(MP_i \| e_i)$, $h(X_{GWN}) = g_i \oplus h(MP_i \| d_i)$.

Step3: During the login and authentication phase of U_j, A can intercept the message $\{M_1, M_2, M_3, T_1\}$, where $M_1 = ID_j \oplus h(h(X_{GWN}) \| T_1)$, and then A computes $ID_j = M_1 \oplus h(h(X_{GWN}) \| T_1)$.

Therefore, any registered user can easily obtain the identity information of other users, which violates the user anonymity property that a security scheme should have.

C. WEAKNESS 3: STOLEN SMART CARD ATTACK

Sometimes the user's smart card SC would be lost, such as being picked up or stolen by an adversary A. Afterward, A can retrieve the information $\{r_i, e_i, f_i, g_i\}$ from the smart card. As stated in subsection B, if adversary A is an authenticated user, A can easily obtain the identity information ID_i of any other user U_i. Based on this information, A can launch the offline password guessing attack through the following steps:

Step1: A guesses a password PW_i^{guess}, and computes $MP_i^{guess} = h(r_i \| PW_i^{guess})$.

Step2: A checks whether $e_i = h(MP_i^{guess} \| ID_i)$. If it holds, A guesses the correct password PW_i.

Step3: Otherwise, A repeats from Step1 until he/she guesses the correct password PW_i.

After extracting the correct password PW_i, A can also launch the new smart card problem attack. In this situation, the attacker may use U_i's original identity ID_i and a new password (not equal to PW_i) to create a new smart card, and then use the new smart card to login to the network as ID_i and pass the verification. Further, he/she can access all the information which is transmitted by any registered S_j. We conclude the implementation process of this attack by the following steps:

Step1: A computes $MP_i = h(r_i \| PW_i), e_i = h(MP_i \| ID_i), d_i = f_i \oplus h(MP_i \| e_i)$.

Step2: A chooses a new password $\overline{PW_i}, \overline{d_i} = d_i$, and computes $\overline{MP_i} = h(r_i \| \overline{PW_i}), \overline{e_i} = h(\overline{MP_i} \| ID_i), \overline{f_i} = \overline{d_i} \oplus h(\overline{MP_i} \| \overline{e_i}), \overline{g_i} = h(X_{GWN}) \oplus h(\overline{MP_i} \| \overline{d_i})$.

U_i	S_j	GWN
knows its ID_i, PW_i	*stores* SID_j, x_j *and* $h(X_{GWN}\|1)$	*stores its master key* X_{GWN}
has a $SC = \{r_i, e_i, f_i, g_i\}$		

Inserts SC, *inputs* $< ID_i^{'}, PW_i^{'} >$

Calculates $MP_i^{'} = h(r_i \| PW_i^{'})$

Checks $e_i = ?\, h(MP_i^{'} \| ID_i^{'})$

Calculates $d_i = f_i \oplus h(MP_i^{'} \| e_i), h(X_{GWN}) = g_i \oplus h(MP_i^{'} \| d_i)$

$M_1 = ID_i^{'} \oplus h(h(X_{GWN}) \| T_1)$

Generates a nonce K_i

Calculates $M_2 = K_i \oplus h(d_i \| T_1), M_3 = h(M_1 \| M_2 \| K_i \| T_1)$

$\xrightarrow{\{M_1, M_2, M_3, T_1\}}$ *Checks* $|T_1 - T_c| < \Delta T$?

Calculates $ESID_j = SID_j \oplus h(h(X_{GWN} \| 1) \| T_2)$

Generates a nonce K_j

Calculates $M_4 = h(x_j \| T_1 \| T_2) \oplus K_j$, $M_5 = h(SID_j \| M_4 \| T_1 \| T_2 \| K_j)$

$\xrightarrow{\{M_1, M_2, M_3, T_1, T_2, ESID_j, M_4, M_5\}}$ *Checks* $|T_2 - T_c| < \Delta T$?

Calculates $SID_j^{'} = ESID_j \oplus h(h(X_{GWN} \| 1) \| T_2)$

$x_j^{'} = h(SID_j^{'} \| X_{GWN}), K_j^{'} = M_4 \oplus h(x_j^{'} \| T_1 \| T_2)$

Checks $M_5 = ?\, h(SID_j^{'} \| M_4 \| T_1 \| T_2 \| K_j^{'})$

Calculates $ID_i^{'} = M_1 \oplus h(h(X_{GWN}) \| T_1)$

$d_i^{'} = h(ID_i^{'} \| X_{GWN}), K_i^{'} = M_2 \oplus h(d_i^{'} \| T_1)$

Checks $M_3 = ?\, h(M_1 \| M_2 \| K_i^{'} \| T_1)$

Calculates $M_6 = K_j^{'} \oplus h(d_i^{'} \| T_3), M_7 = K_i^{'} \oplus h(x_j^{'} \| T_3)$

Checks $|T_3 - T_c| < \Delta T$?, $M_9 = ?\, h(M_7 \| x_j \| T_3) \xleftarrow{\{M_6, M_7, M_8, M_9, T_3\}}$ $M_8 = h(M_6 \| d_i^{'} \| T_3), M_9 = h(M_7 \| x_j^{'} \| T_3)$

Calculates $K_i^{'} = M_7 \oplus h(x_j \| T_3), SK = h(K_i^{'} \oplus K_j)$

$\xleftarrow{\{M_6, M_8, M_{10}, T_3, T_4\}}$ $M_{10} = h(SK \| M_6 \| M_8 \| T_3 \| T_4)$

Checks $|T_4 - T_c| < \Delta T$?, $M_8 = ?\, h(M_6 \| d_i \| T_3)$

Calculates $K_j^{'} = M_6 \oplus h(d_i \| T_3), SK = h(K_i \oplus K_j^{'})$

Checks $M_{10} = ?\, h(SK \| M_6 \| M_8 \| T_3 \| T_4)$

FIGURE 3. Login and authentication phase of Farash *et al.*'s scheme [19].

Step3: A chooses a new smart card and inserts $\{r_i, \overline{e_i}, \overline{f_i}, \overline{g_i}\}$ into it.

Obviously, the adversary can use this new smart card to pass *GWN*'s verification and successfully login to the system.

IV. PROPOSED PROTOCOL

In this section, we propose an enhanced protocol based on the CDH problem to overcome the shortcomings of Farash *et al.*'s scheme, and the architecture of the health monitor system is depicted in FIGURE 5. Medical sensor nodes are placed on the patient, collect relevant physiological data, and regularly upload it to a cloud service platform with sufficient storage and computing capabilities. Users (i.e., medical professionals) can obtain historical data of patients through the cloud service platform, analyze the transfer and development of the disease, and help guide patients' long-term health management. This aspect does not belong to the concern of our article (shown by the dashed line). More often, medical professionals want to obtain real-time patient data. In this scenario, the communication between doctors and medical sensors is carried out through insecure public channels. Therefore, before accessing the medical information of a patient, the mutual authentication between the user and the medical sensor must be completed to verify the legitimacy of both parties. In the proposed protocol, the mutual authentication process includes four steps, as shown by the solid line. The medical user first establishes a connection with a specific sensor node and sends an authentication request; then the sensor node sends its own information along with the information received from the user to the gateway node for authentication. After successfully verifying their identities, the gateway node sends a reply message to the sensor node and the user in turn to complete the authentication and key agreement process.

Inheriting the framework of Farash *et al.*'s scheme, the enhanced protocol still consists of the above five phases. The difference is that we will redesign some of the details of the previous process to improve the security features. TABLE 2 depicts all new notations in our protocol.

A. PRE-DEPLOYMENT PHASE

This phase is the same as Farash *et al.*'s scheme which has been described above. In particular, the system administrator *SA* is to preset the identity information SID_j and the corre-

U_i

$knows\ its < ID_i, PW_i >, has\ a\ SC = \{r_i, e_i, f_i, g_i\}$

$Inserts\ SC, inputs < ID_i, PW_i >$

$Calculates\ \ MP_i = h(r_i \| PW_i)$

$Checks\ \ e_i = ?\ h(MP_i \| ID_i)$

$Calculates\ d_i = f_i \oplus h(MP_i \| e_i), h(X_{GWN}) = g_i \oplus h(MP_i \| d_i)$

$Chooses\ and\ inputs\ new\ password\ PW_i^{'}$

$Calculates\ \ MP_i^{'} = h(r_i \| PW_i^{'}), e_i^{'} = h(MP_i^{'} \| ID_i)$

$f_i^{'} = d_i \oplus h(MP_i^{'} \| e_i^{'}), g_i^{'} = h(X_{GWN}) \oplus h(MP_i^{'} \| d_i)$

$Changes\ \{e_i^{'}, f_i^{'}, g_i^{'}\}\ with\ \{e_i, f_i, g_i\}$

FIGURE 4. **Password change phase of Farash *et al.*'s scheme [19].**

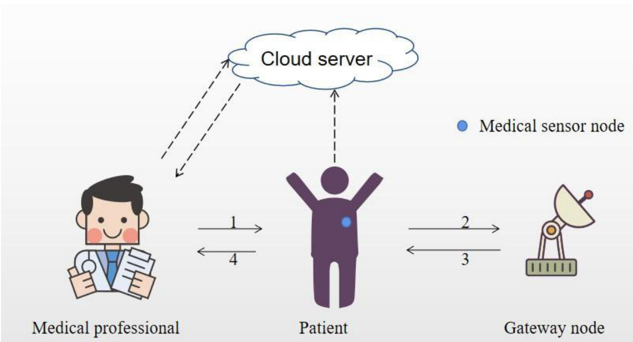


FIGURE 5. **Patient health monitor system model.**

TABLE 2. **Notations.**

Notation	Description
MIDi	masked identity of *Ui*
MID1	temporarily masked identity of *Ui* related to specific task
P	a point on the elliptic curve
a,b,c	random numbers

sponding security password X_{GWN-Sj} for each medical sensor that will be placed on the patient in our protocol.

B. REGISTRATION PHASE

The phase still contains two different parts: medical professional user registration and medical sensor node registration. For the user registration phase, a medical professional must first register in the system when he/she wants to obtain the medical data of a patient in order to protect the privacy of patients. Only authorized users (such as doctors and nurses) can access this sensitive information. We describe the process of user registration in detail:

U_i GWN

$Chooses < ID_i, PW_i >$

$Generates\ a\ nonce\ \ r_i$

$Calculates\ \ MID_i = h(r_i \| ID_i)$

$MP_i = h(r_i \| PW_i)$

$RSP_i = h(ID_i \| MP_i)\ \xrightarrow{\{MID_i, RSP_i\}}$

$Calculates\ \ e_i = h(RSP_i \| MID_i)$

$d_i = h(MID_i \| X_{GWN})$

$g_i = h(X_{GWN}) \oplus h(RSP_i \| d_i)$

$f_i = d_i \oplus h(RSP_i \| e_i)$

$\xleftarrow{\{SC\}}\ Stores\ \{e_i, f_i, g_i\}\ into\ \ a\ \ SC$

$Calculates\ \ r_i^* = h(ID_i \| PW_i) \oplus r_i$

$Insert\ \ r_i^*\ into\ SC$

$SC\ contains\ \ parameters\ \{r_i^*, e_i, f_i, g_i\}$

FIGURE 6. **User registration phase of the proposed protocol.**

Step1: The medical professional U_i, chooses an identity ID_i, a password PW_i, and a random number r_i, then computes $MID_i = h(r_i \| ID_i)$, $MP_i = h(r_i \| PW_i)$, $RSP_i = h(ID_i \| MP_i)$. Th-en it submits $\{MID_i, RSP_i\}$ to GWN.

Step2: Upon receiving the message $\{MID_i, RSP_i\}$, GWN computes $e_i = h(RSP_i \| MID_i)$, $d_i = h(MID_i \| X_{GWN})$, $g_i = h(X_{GWN}) \oplus h(RSP_i \| d_i)$, $f_i = d_i \oplus h(RSP_i \| e_i)$. Then GWN writes e_i, f_i, and g_i into a SC and issues it to U_i.

Step3: The medical professional U_i computes $r_i^* = h(ID_i \| PW_i) \oplus r_i$, and inserts r_i^* into SC.

The illustration of the process is depicted in FIGURE 6.

When a medical sensor node needs to be registered, there is no change and just following the steps of FIGURE 2:

Step1: S_j firstly selects a random number r_j, and computes $MP_j = h(X_{GWN-S_j} \| r_j \| SID_j \| T_1)$, $MN_j = r_j \oplus X_{GWN-S_j}$, where T_1 is current timestamp. Then S_j sends the registration message $\{SID_j, MP_j, MN_j, T_1\}$ to GWN.

Step2: After receiving the sensor registration message, GWN checks if $|T_1 - T_c| < \Delta T$ to avoid potential replay attack. If the condition holds, GWN uses its X_{GWN-S_j} and the received information MN_j to compute its own version $r_j' = MN_j \oplus X_{GWN-S_j}$. Then GWN checks if $MP_j = h(X_{GWN-S_j} \| r_j' \| SID_j \| T_1)$, if it holds, GWN trusts the S_j is legal. GWN chooses the new current timestamp T_2, and computes $x_j = h(SID_j \| X_{GWN})$, $e_j = x_j \oplus X_{GWN-S_j}$, $d_j = h(X_{GWN} \| 1) \oplus h(X_{GWN-S_j} \| T_2)$, $f_j = h(x_j \| d_j \| X_{GWN-S_j} \| T_2)$.

Finally, the message $\{e_j, f_j, d_j, T_2\}$ is sent to S_j as a response.

Step3: Similarly, S_j firstly checks if $|T_2 - T_c| < \Delta T$ to avoid potential replay attack. Afterwards, S_j computes its own version $x_j = e_j \oplus X_{GWN-S_j}$ and authenticates the identity of GWN by checking if $f_j = h(x_j \| d_j \| X_{GWN-S_j} \| T_2)$. S_j then computes $h(X_{GWN} \| 1) = d_j \oplus h(X_{GWN-S_j} \| T_2)$ and stores these information $\{x_j, h(X_{GWN} \| 1)\}$ to its memory. Finally, S_j

deletes the shared password X_{GWN-S_j} and sends a successful confirmation message to GWN.

Step4: After receiving the successful confirmation message, GWN deletes $\{SID_j, X_{GWN-S_j}\}$.

C. LOGIN AND AUTHENTICATION PHASE

Step1: U_i inserts the SC into a reader and inputs his/her ID'_i, PW'_i. SC computes $r'_i = r^*_i \oplus h(ID'_i \| PW'_i)$, $MID'_i = h(r'_i \| ID'_i)$, $MP'_i = h(r'_i \| PW'_i)$, $RSP'_i = h(ID'_i \| MP'_i)$. SC verifies the legitimacy of U_i by checking if $e_i = h(RSP'_i \| MID'_i)$. If this condition holds, U_i has a successful login.

Step2: SC computes $d_i = f_i \oplus h(RSP'_i \| e_i)$, $h(X_{GWN}) = g_i \oplus h(RSP'_i \| d_i)$. SC respectively chooses a to compute $R_1 = aP$ and c to mask the true identity with $MID_1 = h(c \| ID'_i)$.Then SC computes $x_i = h(MID_1 \| h(X_{GWN}))$, $M_1 = MID_1 \oplus h(h(X_{GWN}) \| T_1)$, $M_2 = h(M_1 \| x_i \| R_1 \| T_1)$, and sends the message $\{M_1, M_2, R_1, T_1\}$ to GWN for authentication.

Step3: After receiving U_i's authentication message, S_j will add its own information and send it to GWN for verification. But before that, S_j must first check if $|T_1 - T_c| < \Delta T$ to prevent replay attack. Then S_j chooses a random number b, computes $R_2 = bP$, $M_3 = h(SID_j \| x_j \| R_2 \| T_1 \| T_2)$, $R_3 = bR_1$, and sends $\{M_1, M_2, M_3, T_1, T_2, ESID_j, R_1, R_2\}$ to GWN.

Step4: Similarly, GWN first check if $|T_2 - T_c| < \Delta T$ to prevent replay attack. Then GWN computes its own version $SID'_j = ESID_j \oplus h(h(X_{GWN} \| 1) \| T_2)$, $x'_j = h(SID'_j \| X_{GWN})$, and verifies the legitimacy of S_j by checking if $M_3 = h(SID'_j \| x'_j \| R_2 \| T_1 \| T_2)$. GWN computes its own version $MID'_1 = M_1 \oplus h(h(X_{GWN}) \| T_1)$, $x'_i = h(MID'_1 \| h(X_{GWN}))$, and verifies the legitimacy of U_i by checking if $M_2 = h(M_1 \| x'_i \| R_1 \| T_1)$. After both U_i and S_j are verified successfully, GWN computes $M_4 = h(x'_i \| R_2 \| T_3)$, $M_5 = h(x'_j \| R_1 \| T_3)$, $M_6 = MID'_1 \oplus h(x'_j \| T_3)$,and sends $\{M_4, M_5, M_6, R_1, T_3\}$ to S_j.

Step5: When S_j receives the response message from GWN, this shows that U_i is a legitimate user. Hence, S_j starts to check if $|T_3 - T_c| < \Delta T$ to prevent replay attack. Then S_j authenticates GWN by comparing the received value M_5 with its own computed value $h(x_j \| R_1 \| T_3)$. If the two values are equal, then it proves that the received message is trustworthy. S_j continues to compute $MID'_1 = M_6 \oplus h(x_j \| T_3)$ and generates the session key $SK = h(MID'_1 \| SID_j \| R_3 \| T_3 \| T_4)$. Finally, S_j computes $M_7 = h(SK \| M_4 \| T_3 \| T_4)$ and sends $\{M_4, M_7, R_2, T_3, T_4\}$ to U_i.

Step6: When U_i receives the response message from S_j, U_i starts to check if $|T_4 - T_c| < \Delta T$ to prevent replay attack. Then U_i authenticates GWN by comparing the received value M_4 with its own computed value $h(x_i \| R_2 \| T_3)$. If the two values are equal, then S_j continues to compute $R_4 = aR_2$, and generates the session key$SK = h(MID_1 \| SID_j \| R_4 \| T_3 \| T_4)$. At the end of authentication phase, U_i needs to verify the legitimacy of S_j by comparing the received value M_7 with its own computed value $h(SK \| M_4 \| T_3 \| T_4)$. If this condition holds, U_i verifies the legitimacy of S_j and can use the SK for subsequent information transmission.

The illustration of the process is depicted in FIGURE 7.

D. PASSWORD CHANGE PHASE

Step1: U_i must first finish the successful login process through section IV-subsection C's Step1.

Step2: SC computes $d_i = f_i \oplus h(RSP'_i \| e_i)$, $h(X_{GWN}) = g_i \oplus h(RSP'_i \| d_i)$. Then U_i can input a new password PW_i^{new}.

Thus SC computes all the values that need to be changed due to the new password, including:

$$MP_i^{new} = h(r_i \| PW_i^{new}),$$
$$RSP_i^{new} = h(ID_i \| MP_i^{new}),$$
$$r_i^{*new} = r_i \oplus h(ID_i \| PW_i^{new}),$$
$$e_i^{new} = h(RSP_i^{new} \| MID_i),$$

$f_i^{new} = d_i \oplus h(RSP_i^{new} \| e_i^{new})$, $g_i^{new} = h(X_{GWN}) \oplus h(RSP_i^{new} \| d_i)$. Finally, SC replaces $\{r^*_i, e_i, f_i, g_i\}$ with $\{r_i^{*new}, e_i^{new}, f_i^{new}, g_i^{new}\}$.

The illustration of the process is depicted in FIGURE 8.

E. DYNAMIC NODE ADDITION PHASE

The main purpose of this phase is to meet the needs of system expansion and replacement of damaged nodes. During the operation of the system, there will be new patients who need to be monitored, then new medical sensors need to be added to ensure the system performance. In addition, medical sensor nodes in some patients maybe maliciously damaged or have reached the end of their useful lives, so new nodes need to be replaced at these patients to ensure the normal operation of the system. Suppose a new sensor node S_j^{new} needs to be replaced in a patient, the dynamic node addition will be performed by the following steps:

Step1: The system administrator SA selects an identity SID_j^{new} and shared key $X_{GWN-S_j^{new}}^{new}$ for the new medical sensor node. Then $\{SID_j^{new}, X_{GWN-S_j^{new}}^{new}\}$ are stored in the memory of SID_j^{new} and GWN;

Step2: SA replaces S_j^{new} to the patient of interests, and then S_j^{new} executes the sensor node registration phase expressed in section IV-subsection B;

Step3: SA informs the registered users (i.e., medical professionals) that they can communicate with S_j^{new}.

V. SECURITY ANALYSIS

A. PRIVILEGED INSIDER ATTACK

It is well known that many users may use the same identity and password in different systems. Therefore, even though the GWN is regarded as a trusted subject in our protocol, we should also avoid the possibility of privileged but malicious system administrators extracting the sensitive information (i.e., ID_i, PW_i) of registered users in various ways. Once this sensitive information is extracted, the adversary would impersonate a legitimate user and further initiate more attacks.

The proposed protocol resists this possible attack and eliminates it by providing more careful steps in user information protection. During user registration phase, the user U_i

U_i	S_j	GWN
knows its ID_i, PW_i	stores SID_j, x_j and $h(X_{GWN} \| 1)$	stores its master key X_{GWN}
has a $SC = \{r_i^*, e_i, f_i, g_i\}$		

U_i: Inserts SC, inputs $< ID_i^{'}, PW_i^{'} >$

Calculates $r_i^{'} = r_i^* \oplus h(ID_i^{'} \| PW_i^{'}), MID_i^{'} = h(r_i^{'} \| ID_i^{'})$

$MP_i^{'} = h(r_i^{'} \| PW_i^{'}), RSP_i^{'} = h(ID_i^{'} \| MP_i^{'})$

Checks $e_i = ?\, h(RSP_i^{'} \| MID_i^{'})$

Calculates $d_i = f_i \oplus h(RSP_i^{'} \| e_i), h(X_{GWN}) = g_i \oplus h(RSP_i^{'} \| d_i)$

Generates nonces a, c

Calculates $R_1 = aP, MID_1 = h(c \| ID_i^{'}), x_i = h(MID_1 \| h(X_{GWN}))$

$M_1 = MID_1 \oplus h(h(X_{GWN}) \| T_1), M_2 = h(M_1 \| x_i \| R_1 \| T_1)$

$\xrightarrow{\{M_1, M_2, R_1, T_1\}}$ (U_i to S_j)

S_j: Checks $|T_1 - T_c| < \Delta T$?

Calculates $ESID_j = SID_j \oplus h(h(X_{GWN} \| 1) \| T_2)$

Generates a nonce b

Calculates $R_2 = bP, R_3 = bR_1, M_3 = h(SID_j \| x_j \| R_2 \| T_1 \| T_2)$

$\xrightarrow{\{M_1, M_2, M_3, T_1, T_2, ESID_j, R_1, R_2\}}$ (S_j to GWN)

GWN: Checks $|T_2 - T_c| < \Delta T$?

Calculates $SID_j^{'} = ESID_j \oplus h(h(X_{GWN} \| 1) \| T_2), x_j^{'} = h(SID_j^{'} \| X_{GWN})$

Checks $M_3 = ?\, h(SID_j^{'} \| x_j^{'} \| R_2 \| T_1 \| T_2)$

Calculates $MID_1^{'} = M_1 \oplus h(h(X_{GWN}) \| T_1), x_i^{'} = h(MID_1^{'} \| h(X_{GWN}))$

Checks $M_2 = ?\, h(M_1 \| x_i^{'} \| R_1 \| T_1)$

Calculates $M_4 = h(x_i^{'} \| R_2 \| T_3), M_5 = h(x_j^{'} \| R_1 \| T_3)$

$M_6 = MID_1^{'} \oplus h(x_j^{'} \| T_3)$

$\xleftarrow{\{M_4, M_5, M_6, R_1, T_3\}}$ (GWN to S_j)

S_j: Checks $|T_3 - T_c| < \Delta T$?, $M_5 = ?\, h(x_j \| R_1 \| T_3)$

Calculates $MID_1^{'} = M_6 \oplus h(x_j \| T_3), SK = h(MID_1^{'} \| SID_j \| R_3 \| T_3 \| T_4)$

$M_7 = h(SK \| M_4 \| T_3 \| T_4)$

$\xleftarrow{\{M_4, M_7, R_2, T_3, T_4\}}$ (S_j to U_i)

U_i: Checks $|T_4 - T_c| < \Delta T$?

Calculates $M_4 = h(x_i \| R_2 \| T_3), R_4 = aR_2, SK = h(MID_1 \| SID_j \| R_4 \| T_3 \| T_4)$

Checks $M_7 = ?\, h(SK \| M_4 \| T_3 \| T_4)$

FIGURE 7. Login and authentication phase of the proposed protocol.

U_i

knows its ID_i, PW_i, has a $SC = \{r_i^*, e_i, f_i, g_i\}$

Inserts SC, inputs $< ID_i, PW_i >$

Calculates $r_i = r_i^* \oplus h(ID_i \| PW_i), MID_i = h(r_i \| ID_i)$

$MP_i = h(r_i \| PW_i), RSP_i = h(ID_i \| MP_i)$

Checks $e_i = ?\, h(RSP_i \| MID_i)$

Calculates $d_i = f_i \oplus h(RSP_i \| e_i)$

$h(X_{GWN}) = g_i \oplus h(RSP_i \| d_i)$

Chooses and inputs new password PW_i^{new}

Calculates $MP_i^{new} = h(r_i \| PW_i^{new}), RSP_i^{new} = h(ID_i \| MP_i^{new})$

$r_i^{*new} = r_i \oplus h(ID_i \| PW_i^{new}), e_i^{new} = h(RSP_i^{new} \| MID_i)$

$f_i^{new} = d_i \oplus h(RSP_i^{new} \| e_i^{new})$

$g_i^{new} = h(X_{GWN}) \oplus h(RSP_i^{new} \| d_i)$

Changes $\{r_i^{*new}, e_i^{new}, f_i^{new}, g_i^{new}\}$ with $\{r_i^*, e_i, f_i, g_i\}$

FIGURE 8. Password change phase of the proposed protocol.

only send $\{MID_i, RSP_i\}$ to the gateway node GWN, where $MID_i = h(r_i \| ID_i), RSP_i = h(ID_i \| MP_i) = h(ID_i \| h(r_i \| PW_i))$. To guess the correct information $\{ID_i, PW_i\}$, the privileged insider attacker needs to know r_i firstly. However, r_i is not stored in SC but r_i^*, where $r_i^* = h(ID_i \| PW_i) \oplus r_i$. In other words, there is no way for GWN to retrieve r_i. In addition, during the authentication phase, GWN can only retrieve MID_1 from $\{M_1, M_2, M_3, T_1, T_2, ESID_j, R_1, R_1\}$ which is different in each session and PW_i has never been transmitted over these insecure channels. As a result, it is impossible for any privileged insider to reveal these useful information in our protocol.

B. USER ANONYMITY

In the registration phase, only $\{MID_i, RSP_i\}$ is sent to the gateway node GWN via a secure channel, where $MID_i = h(r_i \| ID_i)$, $RSP_i = h(ID_i \| MP_i) = h(ID_i \| h(r_i \| PW_i))$.

Moreover, the user U_i communicates with S_j and GWN as MID_1, where $MID_1 = h(c \| ID_i)$ and c is generated freshly for each session. This means that the user U_i never reveals his/her true identity ID_i to transmit between channels and the adversary A cannot extract ID_i.

C. OFFLINE PASSWORD GUESSING ATTACK

Assuming that the adversary A retrieves the information $\{r_i^*, e_i, f_i, g_i\}$ from a stolen/lost smart card SC. However,

$e_i = h(RSP_i \| MID_i)$, $RSP_i = h(ID_i \| MP_i)$, $MID_i = h(r_i \| ID_i)$, $MP_i = h(r_i \| PW_i)$, the ID_i is anonymous and never revealed to others. Thus, the adversary A must first guess the correct identity ID_i before A can guess the password PW_i. This is almost impossible for the attacker.

D. KNOWN SESSION SPECIFIC TEMPORARY INFORMATION ATTACK

In the authentication phase, we use the timestamp mechanism and CDH to prevent known session specific temporary information attack. Random numbers a, b are regenerated in each session to evaluate the session key $SK = h(MID_1 \| SID_j \| abP \| T_3 \| T_4)$. Based on CDH, it is a computationally difficult problem to guess abP even if the attacker gets the information aP and bP. Besides, it uses T_3 and T_4 to check whether the session message is the latest or not. If the condition does not hold, the protocol rejects the message and aborts the session.

E. PASSWORD CHANGE ATTACK

In the password change phase, user U_i inserts his/her SC into a terminal and inputs ID_i', PW_i'. Then SC computes $r_i' = r_i^* \oplus h(ID_i' \| PW_i')$, $e_i' = h(RSP_i' \| MID_i') = h(h(ID_i' \| MP_i') \| h(r_i' \| ID_i')) = h(h(ID_i' \| h(r_i' \| PW_i')) \| h(r_i' \| ID_i'))$ and checks whether $e_i' = e_i$ or not. If the condition holds, SC asks U_i for a new password PW_i^{new} to replace the old one. Otherwise, SC rejects the request. If an attacker wants to change the password, he/she must know the information $\{ID_i, PW_i\}$ in advance to pass the equation verification $e_i' = e_i$. As mentioned earlier, the attacker cannot obtain $\{ID_i, PW_i\}$ in any way. Therefore, the proposed protocol provides security against the password change attack.

F. TRACEABILITY ATTACK

In this attack, the attacker usually eavesdrops on two different session login and authentication messages and compares them. If the two messages have the same components, the attacker infers that they belong to the same user, so that the login activity of a single user can be tracked by the attacker. However, it is impossible for the attacker to track anyone in our protocol. In the login and authentication phase, the user sends the message $\{M_1, M_2, R_1, T_1\}$ to S_j where $M_1 = MID_1 \oplus h(h(X_{GWN}) \| T_1) = h(c \| ID_i') \oplus h(h(X_{GWN}) \| T_1)$, $M_2 = h(M_1 \| x_i \| R_1 \| T_1)$, $R_1 = aP$, and T_1 is the current timestamp. Note the random numbers (i.e., a, c) and timestamp are different in each session, so the message of each session differs from the other sessions. Similarly, other transmitted messages in this phase also depend on random numbers and timestamps. Hence, the protocol can resist the traceability attack.

VI. MUTUAL AUTHENTICATION PROOF USING BAN LOGIC

Through the security analysis using the widely-accepted BAN logic[34], it is shown that the proposed protocol provides the mutual authentication between a user U_i and a medical sensor node S_j.

A. GOALS

The proposed protocol must meet the following goals to prove that the protocol is secure:

Goal 1: $U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_j)$

Goal 2: $U_i \mid\equiv S_j \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_j)$

Goal 3: $S_j \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_j)$

Goal 4: $S_j \mid\equiv U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_j)$

B. IDEALIZED FORM

The ideal form of the messages exchanged in the protocol is expressed as follows:

Message 1:

$$U_i \overset{via\ S_j}{\longrightarrow} GWN :< MID_1, T_1, (U_i \overset{MID_1}{\longleftrightarrow} GWN) >_{h(X_{GWN})}$$

Message 2:

$$U_i \overset{via\ S_j}{\longrightarrow} GWN : (R_1, M_1, T_1, (U_i \overset{MID_1}{\longleftrightarrow} GWN), (U_i \overset{R_1}{\longleftrightarrow} GWN))_{x_i}$$

Message 3:

$$S_j \longrightarrow GWN :< SID_j, T_2, (S_j \overset{SID_j}{\longleftrightarrow} GWN) >_{h(X_{GWN} \| 1)}$$

Message 4:

$$S_j \longrightarrow GWN : (R_2, SID_j, T_1, T_2, (S_j \overset{SID_j}{\longleftrightarrow} GWN), (S_j \overset{R_2}{\longleftrightarrow} GWN))_{x_j}$$

Message 5:

$$GWN \longrightarrow S_j : (R_1, T_3, (S_j \overset{SID_j}{\longleftrightarrow} GWN))_{x_j'=x_j}$$

Message 6:

$$U_i \overset{via\ GWN}{\longrightarrow} S_j :< MID_1' = MID_1, T_3, (U_i \overset{SK}{\longleftrightarrow} S_j), (S_j \overset{SID_j}{\longleftrightarrow} GWN) >_{x_j'=x_j}$$

Message 7:

$$GWN \overset{via\ S_j}{\longrightarrow} U_i : (R_2, T_3, (U_i \overset{MID_1}{\longleftrightarrow} GWN))_{x_i'=x_i}$$

Message 8:

$$S_j \longrightarrow U_i : (M_4, T_3, T_4, (U_i \overset{MID_1}{\longleftrightarrow} GWN), (U_i \overset{R_1}{\longleftrightarrow} GWN), (U_i \overset{SK}{\longleftrightarrow} S_j))_{SK}$$

C. ASSUMPTIONS

The following assumptions about the initial state are used to analyze the proposed protocol:

A_1: $GWN \mid\equiv \#(T_1)$
A_2: $GWN \mid\equiv \#(T_2)$
A_3: $S_j \mid\equiv \#(T_3)$
A_4: $U_i \mid\equiv \#(T_4)$
A_5: $GWN \mid\equiv \#(R_1)$
A_6: $GWN \mid\equiv \#(R_2)$
A_7: $S_j \mid\equiv \#(R_1)$
A_8: $U_i \mid\equiv \#(R_2)$
A_9: $S_j \mid\equiv \#(MID_1' = MID_1)$
A_{10}: $U_i \mid\equiv (U_i \overset{x_i=h(MID_1\|h(X_{GWN}))}{\longleftrightarrow} GWN)$
A_{11}: $GWN \mid\equiv (U_i \overset{x_i=h(MID_1\|h(X_{GWN}))}{\longleftrightarrow} GWN)$
A_{12}: $S_j \mid\equiv (S_j \overset{x_j=h(SID_j\|X_{GWN})}{\longleftrightarrow} GWN)$
A_{13}: $GWN \mid\equiv (S_j \overset{x_j=h(SID_j\|X_{GWN})}{\longleftrightarrow} GWN)$
A_{14}: $GWN \mid\equiv (U_i \overset{h(X_{GWN})}{\longleftrightarrow} GWN)$
A_{15}: $GWN \mid\equiv (S_j \overset{h(X_{GWN}\|1)}{\longleftrightarrow} GWN)$
A_{16}: $GWN \mid\equiv U_i \Rightarrow (U_i \overset{R_1}{\longleftrightarrow} GWN)$
A_{17}: $GWN \mid\equiv U_i \Rightarrow (U_i \overset{MID_1}{\longleftrightarrow} GWN)$
A_{18}: $GWN \mid\equiv S_j \Rightarrow (S_j \overset{R_2}{\longleftrightarrow} GWN)$
A_{19}: $GWN \mid\equiv S_j \Rightarrow (S_j \overset{SID_j}{\longleftrightarrow} GWN)$
A_{20}: $S_j \mid\equiv U_i \Rightarrow (U_i \overset{SK}{\longleftrightarrow} S_j)$
A_{21}: $U_i \mid\equiv S_j \Rightarrow (U_i \overset{SK}{\longleftrightarrow} S_j)$

D. PROOF

Based on logical postulates in the BAN logic, the proof process is as follows:

From Message 1, we have,

$$GWN \triangleleft < MID_1, T_1, (U_i \overset{MID_1}{\longleftrightarrow} GWN) >_{h(X_{GWN})} \quad (1)$$

From (1), A_{14}, and message-meaning rule, we have,

$$GWN \mid\equiv U_i \mid\sim \; < MID_1, T_1, (U_i \overset{MID_1}{\longleftrightarrow} GWN) > \quad (2)$$

From A_1 and freshness rule, we have,

$$GWN \mid\equiv \# < MID_1, T_1, (U_i \overset{MID_1}{\longleftrightarrow} GWN) > \quad (3)$$

From (2), (3), and nonce-verification rule, we have,

$$GWN \mid\equiv U_i \mid\equiv \; < MID_1, T_1, (U_i \overset{MID_1}{\longleftrightarrow} GWN) > \quad (4)$$

From (4) and belief rule, we have,

$$GWN \mid\equiv U_i \mid\equiv (U_i \overset{MID_1}{\longleftrightarrow} GWN) \quad (5)$$

From (5), A_{17} and jurisdiction rule, we have,

$$GWN \mid\equiv (U_i \overset{MID_1}{\longleftrightarrow} GWN) \quad (6)$$

From Message 2, we have,

$$GWN \triangleleft (R_1, M_1, T_1, (U_i \overset{MID_1}{\longleftrightarrow} GWN), (U_i \overset{R_1}{\longleftrightarrow} GWN))_{x_i} \quad (7)$$

From (7), A_{11}, and message-meaning rule, we have,

$$GWN \mid\equiv U_i \mid\sim (R_1, M_1, T_1, (U_i \overset{MID_1}{\longleftrightarrow} GWN), (U_i \overset{R_1}{\longleftrightarrow} GWN)) \quad (8)$$

From A_1, A_5, and freshness rule, we have,

$$GWN \mid\equiv \#(R_1, M_1, T_1, (U_i \overset{MID_1}{\longleftrightarrow} GWN), (U_i \overset{R_1}{\longleftrightarrow} GWN)) \quad (9)$$

From (8), (9), and nonce-verification rule, we have,

$$GWN \mid\equiv U_i \mid\equiv (R_1, M_1, T_1, (U_i \overset{MID_1}{\longleftrightarrow} GWN), (U_i \overset{R_1}{\longleftrightarrow} GWN)) \quad (10)$$

From (10) and belief rule, we have,

$$GWN \mid\equiv U_i \mid\equiv (U_i \overset{R_1}{\longleftrightarrow} GWN) \quad (11)$$

From (11), A_{16}, and jurisdiction rule, we have,

$$GWN \mid\equiv (U_i \overset{R_1}{\longleftrightarrow} GWN) \quad (12)$$

From Message 3, we have,

$$GWN \triangleleft < SID_j, T_2, (S_j \overset{SID_j}{\longleftrightarrow} GWN) >_{h(X_{GWN}\|1)} \quad (13)$$

From (13), A_{15}, and message-meaning rule, we have,

$$GWN \mid\equiv S_j \mid\sim \; < SID_j, T_2, (S_j \overset{SID_j}{\longleftrightarrow} GWN) > \quad (14)$$

From A_2 and freshness rule, we have,

$$GWN \mid\equiv \# < SID_j, T_2, (S_j \overset{SID_j}{\longleftrightarrow} GWN) > \quad (15)$$

From (14), (15), and nonce-verification rule, we have,

$$GWN \mid\equiv S_j \mid\equiv \; < SID_j, T_2, (S_j \overset{SID_j}{\longleftrightarrow} GWN) > \quad (16)$$

From (16) and belief rule, we have,

$$GWN \mid\equiv S_j \mid\equiv (S_j \overset{SID_j}{\longleftrightarrow} GWN) \quad (17)$$

From (17), A_{19}, and jurisdiction rule, we have,

$$GWN \mid\equiv (S_j \overset{SID_j}{\longleftrightarrow} GWN) \quad (18)$$

From Message 4, we have,

$$GWN \triangleleft (R_2, SID_j, T_1, T_2, (S_j \overset{SID_j}{\longleftrightarrow} GWN), (S_j \overset{R_2}{\longleftrightarrow} GWN))_{x_j} \quad (19)$$

From (19), A_{13}, and message-meaning rule, we have,

$$GWN \mid\equiv S_j \mid\sim (R_2, SID_j, T_1, T_2, (S_j \overset{SID_j}{\longleftrightarrow} GWN), (S_j \overset{R_2}{\longleftrightarrow} GWN)) \quad (20)$$

From A_2, A_6, and freshness rule, we have,

$$GWN| \equiv \#(R_2, SID_j, T_1, T_2, (S_j \overset{SID_j}{\longleftrightarrow} GWN), (S_j \overset{R_2}{\longleftrightarrow} GWN)) \tag{21}$$

From (20), (21), and nonce-verification rule, we have,

$$GWN | \equiv S_j | \equiv (R_2, SID_j, T_1, T_2, (S_j \overset{SID_j}{\longleftrightarrow} GWN), (S_j \overset{R_2}{\longleftrightarrow} GWN)) \tag{22}$$

From (22) and belief rule, we have,

$$GWN | \equiv S_j | \equiv (S_j \overset{R_2}{\longleftrightarrow} GWN) \tag{23}$$

From (23), A_{18}, and jurisdiction rule, we have,

$$GWN | \equiv (S_j \overset{R_2}{\longleftrightarrow} GWN) \tag{24}$$

From Message 5, we have,

$$S_j \lhd (R_1, T_3, (S_j \overset{SID_j}{\longleftrightarrow} GWN))_{x'_j = x_j} \tag{25}$$

From (25), A_{12}, and message-meaning rule, we have,

$$S_j | \equiv GWN | \sim (R_1, T_3, (S_j \overset{SID_j}{\longleftrightarrow} GWN)) \tag{26}$$

From A_7 and freshness rule, we have,

$$S_j | \equiv \#(R_1, T_3, (S_j \overset{SID_j}{\longleftrightarrow} GWN)) \tag{27}$$

From (26), (27), and nonce-verification rule, we have,

$$S_j | \equiv GWN | \equiv (R_1, T_3, (S_j \overset{SID_j}{\longleftrightarrow} GWN)) \tag{28}$$

From (28) and belief rule, we have,

$$S_j | \equiv GWN | \equiv (S_j \overset{SID_j}{\longleftrightarrow} GWN) \tag{29}$$

From Message 6, we have,

$$S_j \lhd < MID'_1 = MID_1, T_3, (U_i \overset{SK}{\longleftrightarrow} S_j), (S_j \overset{SID_j}{\longleftrightarrow} GWN) >_{x'_j = x_j} \tag{30}$$

From (30), A_{12}, and message-meaning rule, we have,

$$S_j | \equiv U_i | \sim \; < MID'_1 = MID_1, T_3, (U_i \overset{SK}{\longleftrightarrow} S_j), (S_j \overset{SID_j}{\longleftrightarrow} GWN) > \tag{31}$$

From A_3, A_9, and freshness rule, we have,

$$S_j | \equiv \# < MID'_1 = MID_1, T_3, (U_i \overset{SK}{\longleftrightarrow} S_j), (S_j \overset{SID_j}{\longleftrightarrow} GWN) > \tag{32}$$

From (31), (32), and nonce-verification rule, we have,

$$S_j | \equiv U_i | \equiv \; < MID'_1 = MID_1, T_3, (U_i \overset{SK}{\longleftrightarrow} S_j), (S_j \overset{SID_j}{\longleftrightarrow} GWN) > \tag{33}$$

From (33) and belief rule, we have,

$$S_j | \equiv U_i | \equiv (U_i \overset{SK}{\longleftrightarrow} S_j) \tag{\textbf{Goal 4}}$$

From (Goal 4), A_{20}, and jurisdiction rule, we have,

$$S_j | \equiv (U_i \overset{SK}{\longleftrightarrow} S_j) \tag{\textbf{Goal 3}}$$

From Message 7, we have,

$$U_i \lhd (R_2, T_3, (U_i \overset{MID_1}{\longleftrightarrow} GWN))_{x'_i = x_i} \tag{34}$$

From (34), A_{10}, and message-meaning rule, we have,

$$U_i | \equiv GWN | \sim (R_2, T_3, (U_i \overset{MID_1}{\longleftrightarrow} GWN)) \tag{35}$$

From A_8 and freshness rule, we have,

$$U_i | \equiv \#(R_2, T_3, (U_i \overset{MID_1}{\longleftrightarrow} GWN)) \tag{36}$$

From (35), (36), and nonce-verification rule, we have,

$$U_i | \equiv GWN | \equiv (R_2, T_3, (U_i \overset{MID_1}{\longleftrightarrow} GWN)) \tag{37}$$

From (37) and belief rule, we have,

$$U_i | \equiv GWN | \equiv (U_i \overset{MID_1}{\longleftrightarrow} GWN) \tag{38}$$

From Message 8, we have,

$$U_i \lhd (M_4, T_3, T_4, (U_i \overset{MID_1}{\longleftrightarrow} GWN), (U_i \overset{R_1}{\longleftrightarrow} GWN), (U_i \overset{SK}{\longleftrightarrow} S_j))_{SK} \tag{39}$$

From (39), A_{10}, and message-meaning rule, we have,

$$U_i | \equiv S_j | \sim (M_4, T_3, T_4, (U_i \overset{MID_1}{\longleftrightarrow} GWN), (U_i \overset{R_1}{\longleftrightarrow} GWN), (U_i \overset{SK}{\longleftrightarrow} S_j)) \tag{40}$$

From A_4 and freshness rule, we have,

$$U_i | \equiv \#(M_4, T_3, T_4, (U_i \overset{MID_1}{\longleftrightarrow} GWN), (U_i \overset{R_1}{\longleftrightarrow} GWN), (U_i \overset{SK}{\longleftrightarrow} S_j)) \tag{41}$$

From (40), (41), and nonce-verification rule, we have,

$$U_i | \equiv S_j | \equiv (M_4, T_3, T_4, (U_i \overset{MID_1}{\longleftrightarrow} GWN), (U_i \overset{R_1}{\longleftrightarrow} GWN), (U_i \overset{SK}{\longleftrightarrow} S_j)) \tag{42}$$

From (42) and belief rule, we have,

$$U_i | \equiv S_j | \equiv (U_i \overset{SK}{\longleftrightarrow} S_j) \tag{\textbf{Goal 2}}$$

From (Goal 2), A_{21}, and jurisdiction rule, we have,

$$U_i | \equiv (U_i \overset{SK}{\longleftrightarrow} S_j) \tag{\textbf{Goal 1}}$$

According to Goal 1, Goal 2, Goal 3, and Goal4, it is obvious that the improved protocol makes it successful to provide a secure mutual authentication between a medical professional user U_i and a medical sensor node S_j.

VII. SIMULATION OF PROPOSED PROTOCOL USING AVISPA TOOL

There is a popular simulation tool called AVISPA which has the ability to automatically verify network security protocols and applications. In this section, we use the AVISPA tool to simulate the proposed protocol and verify whether the protocol is secure against an attacker.

Before the simulation, the protocol needs to be implemented in HLPSL (High Level Protocol Specification Language) that can be recognized by the AVISPA tool. In the implementation of HLSPL, the roles of all participating entities are specified, including the medical professional U_i, the medical sensor S_j, the gateway node *GWN*, as well as the session, the environment, and the goal. In FIGURE 9, we depict the role of the medical professional U_i. When the user wants to register in the system, U_i first computes and transmits the request message $\{MID_i, RSP_i\}$ to the gateway node *GWN* using *Snd*() operation via a secure channel. The statement *secret* ($\{ID_i, PW_i\}$, *sec_subs1*, U_i) indicates that only the U_i knows the information of ID_i and PW_i. Afterward, the U_i obtains a smart card with the information $\{E_i, F_i, G_i\}$ stored in it using *Rcv*() operation via a secure channel. When the professional wants to login the system, the U_i generates a fresh timestamp T_1 and random number *An*, *Cn* with the help of *new*() operation, and then forwards these message $\{M_1, M_2, R_1, T_1\}$ to the medical sensor S_j by *Snd*() operation via an insecure channel. The statements *secret* ({*An'*}, *sec_a*, U_i) and *secret* ({*Cn'*}, *sec_a*, U_i) indicate that *An'* and *Cn'* are U_i's secret and undisclosed to anyone else. The statements *witness* (U_i, S_j, *user_sensor_a, An'*) and *witness* (U_i, *G*, *user_gwn_a, An'*) indicate that the U_i generates the fresh value *An* for S_j and *GWN* respectively. Finally, when the U_i receives the message $\{M_4, M_7, R_2, T_3, T_4\}$ from the S_j using *Rcv*() via a insecure channel, the U_i computes *SK*. The statement *secret* ({*SK'*}, *sec_sk*, $\{U_i, S_j\}$) indicates that *SK* is a secret that only U_i and S_j know. The statement *request* (S_j, U_i, *sensor_user_b, Bn*) indicates that S_j authenticated the identity of U_i by its generated number *Bn*. The type statement *channel(dy)* indicates that the channels follow the Dolev-Yao threat model.

In FIGURE 10, we give out the role of the medical sensor S_j in HLPSL. In the medical sensor registration phase, the S_j initially generates timestamp TS_1 and random number R_j, and then transmits the message $\{SID_j, MP_j, MN_j, TS_1\}$ to *GWN* by *Snd*() operation through an insecure open channel. The statement *witness* (S_j, *G*, *sensor_gwn_rj*, R_j') indicates that the S_j generates the fresh value R_j for *GWN*. In the login and authentication phase, when S_j gets the message $\{M_1, M_2, R_1, T_1\}$ from U_i using *Rcv*() operation, the S_j generates timestamp T_2 and random numbers *Bn* using *new*() operation, and forwards the message $\{M_1, M_2, M_3, T_1, T_2, ESID_j, R_1, R_2\}$ to *GWN*. The statement *secret* ({*Bn'*}, *sec_b*, S_j) indicates that *Bn'* is known to only S_j. The statements *witness* (S_j, U_i, *sensor_user_b, Bn'*) and *witness* (S_j, *G*, *sensor_gwn_b, Bn'*) indicate that the S_j generates the fresh value *Bn* for U_i and *GWN* respectively. Hereafter, S_j gets the message $\{M_4, M_5, M_6, R_1, T_3\}$ from *GWN*using *Rcv*() operation. Then the S_j generates timestamp T_4 using *new*() operation and computes *SK*. In the end, S_j transmits the message $\{M_4, M_7, R_2, T_3, T_4\}$ to U_i using *Snd*() operation. The statement *request* (U_i, S_j, *user_sensor_a, An*) indicates that U_i authenticated the identity of S_j by its generated number *An*.

```
role user (Ui,Sj,G:agent, SKgui:symmetric_key,
SKgsj:symmetric_key,
H,Mul:hash_func,
Snd,Rcv:channel(dy))
played_by Ui
def=
local State:nat,
IDi,PWi,Ri,MIDi,MPi,RSPi,Di,Ei,Fi,Gi,Xgwn,Xhgwn,Xg
wni,Rii,SIDj,Rj,MPj,MNj,TS1,Xj,Dj,Ej,Fj,TS2,An,Bn,Cn,P
,MID1,Xi,R3,R4,SK:text,
R1,R2,M1,M2,M3,M4,M5,M6,M7,T1,T2,T3,T4,ESIDj:me
ssage,
Inc:hash_func
const
sec_subs1,sec_a,sec_b,sec_c,sec_sk,sec_xgwn,user_sensor
_a,user_gwn_a,sensor_user_b,sensor_gwn_b,sensor_gwn_r
j:protocol_id
init State:=0
transition
%Registration phase
1. State = 0 /\ Rcv(start) =|> State':= 1 /\ Ri':= new()
/\ MIDi':= H(Ri'.IDi) /\ MPi':= H(Ri'.PWi)
/\ RSPi':= H(IDi.MPi')
/\ Snd({MIDi'.RSPi'}_SKgui)
/\ secret({IDi,PWi},sec_subs1,Ui)
2. State = 1 /\ Rcv({Ei.Fi.Gi}_SKgui) =|>
State':= 2
/\ Rii':= xor(H(IDi.PWi),Ri)
%Login and authentication phase
/\ An':= new() /\ Cn':= new() /\ T1':= new()
/\ Di':= xor(Fi,H(RSPi.Ei))
/\  Xhgwn':= xor(Gi,H(RSPi.Di')) /\R1':= Mul(An'.P)
/\ MID1':= H(Cn'.IDi) /\ Xi':= H(MID1'.Xhgwn')
/\ M1':= xor(MID1',H(Xhgwn'.T1'))
/\ M2':= H(M1'.Xi'.R1'.T1')
/\ Snd(M1'.M2'.R1'.T1')
/\ secret({An'},sec_a,Ui) /\ secret({Cn'},sec_c,Ui)
/\ witness(Ui,Sj,user_sensor_a,An')
/\ witness(Ui,G,user_gwn_a,An')
3. State = 2 /\ Rcv(M4.M7.R2.T3.T4) =|> State':= 3
/\ R4':= Mul(An.R2) /\ SK':= H(MID1.SIDj.R4'.T3.T4)
/\ secret({SK'},sec_sk,{Ui,Sj})
/\ request(Sj,Ui,sensor_user_b,Bn)
/\ witness(Ui,Sj,user_sensor_a,An)
end role
```

FIGURE 9. Role specification in HLPSL for U_i in our protocol.

In FIGURE 11, we summarize the implementation of gateway node *GWN* in HLPSL. In the user registration phase, *GWN* gets the request message {*MIDi, RSPi*} from the medical professional *Ui* using *Rcv*() operation. *GWN* sends the

```
role sensor (Ui,Sj,G:agent,SKgui:symmetric_key,SKgsj:symmetric_key,H,Mul:hash_func,
Snd,Rcv:channel(dy))
played_by Sj
def=
local State:nat,
IDi,PWi,Ri,MIDi,MPi,RSPi,Di,Ei,Fi,Gi,Xgwn,Xhgwn,Xgwni,Rii,SIDj,Rj,MPj,MNj,TS1,Xj,Dj,Ej,Fj,TS2,An,Bn,Cn,P,MID1
,Xi,R3,R4,SK:text,
R1,R2,M1,M2,M3,M4,M5,M6,M7,T1,T2,T3,T4,ESIDj:message,
Inc:hash_func
const
sec_subs1,sec_a,sec_b,sec_c,sec_sk,sec_xgwn,user_sensor_a,user_gwn_a,sensor_user_b,sensor_gwn_b,sensor_gwn_rj:prot
ocol_id
init State:=0
transition
%Registration phase
1. State = 0 /\ Rcv(start) =|> State':= 1 /\ Rj':= new() /\ TS1':= new() /\ MPj':= H(SKgsj.Rj'.SIDj.TS1')
/\ MNj':= xor(Rj',SKgsj) /\ Snd(SIDj.MPj'.MNj'.TS1') /\ witness(Sj,G,sensor_gwn_rj,Rj')
2. State = 1 /\ Rcv(Ej.Fj.Dj.TS2) =|> State':= 2 /\ Xj':= xor(Ej,SKgsj) /\ Xgwni':= xor(Dj,H(SKgsj.TS2))
%Login and authentication phase
3. State = 2 /\ Rcv(M1.M2.R1.T1) =|> State':= 3 /\ Bn':= new() /\ T2':= new() /\ ESIDj':= xor(SIDj,H(Xgwni.T2'))
/\ R2':= Mul(Bn'.P) /\ R3':= Mul(Bn'.R1) /\ M3':= H(SIDj.Xj.R2'.T1.T2') /\ Snd(M1.M2.M3'.T1.T2'.ESIDj'.R1.R2')
/\ secret({Bn'},sec_b,Sj) /\ witness(Sj,Ui,sensor_user_b,Bn') /\ witness(Sj,G,sensor_gwn_b,Bn')
4. State = 3 /\ Rcv(M4.M5.M6.R1.T3) =|> State':= 4 /\ T4':= new() /\ MID1':= xor(M6,H(Xj.T3))
/\ SK':= H(MID1'.SIDj.R3.T3.T4') /\ M7':= H(SK'.M4.T3.T4') /\ Snd(M4.M7'.R2.T3.T4')
/\ secret({SK'},sec_sk,{Ui,Sj}) /\ request(Ui,Sj,user_sensor_a,An) /\ witness(Sj,Ui,sensor_user_b,Bn)
end role
```

FIGURE 10. Role specification in HLPSL for S_j in our protocol.

TABLE 3. Security features comparison among the proposed protocol and other schemes.

Security features	Farash *et al.* 2016 [19]	Wu *et al.* 2017 [25]	Sureshkumar *et al.* 2019 [1]	Chandrakar *et al.* 2019 [9]	Li *et al.* 2020 [37]	Rangwani *et al.* 2021 [38]	Ours
SF1	No	No	Yes	Yes	No	Yes	Yes
SF2	No	No	No	No	No	No	Yes
SF3	No	Yes	Yes	No	Yes	Yes	Yes
SF4	No	No	Yes	No	Yes	Yes	Yes
SF5	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SF6	Yes	No	Yes	Yes	No	Yes	Yes
SF7	Yes	Yes	No	Yes	No	Yes	Yes
SF8	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SF9	No	No	No	No	Yes	No	Yes
SF10	No	Yes	/	No	/	/	Yes
SF11	No	No	No	Yes	Yes	Yes	Yes
SF12	Yes	Yes	Yes	Yes	Yes	No	Yes
SF13	Yes	Yes	Yes	Yes	Yes	/	Yes

SF1: user anonymity; SF2: resist privileged insider attack; SF3: resist offline password guessing attack; SF4: resist stolen smart card attack; SF5: resist denial-of-service attack; SF6: prevent replay attack; SF7: prevent man-in-the-middle attack; SF8: mutual authentication; SF9: session key security; SF10: dynamic ID; SF11: resist known session specific temporary information attack; SF12: untraceability property; SF13: server independent password update phase.

message {*Ei, Fi, Gi*} in response by *Snd*() operation. The statement *secret* ({*Xgwn*}, *sec_xgwn, G*) indicates that *Xgwn* is undisclosed to anyone except *GWN*. In the medical sensor registration phase, the *GWN* obtains the message {*SIDj, MPj, MNj, TS1*} from *Sj* by *Rcv*() operation. Thence *GWN* generates timestamp TS_2 using *new*() operation and then sends

```
role gwn (Ui,Sj,G:agent,
SKgui:symmetric_key,
SKgsj:symmetric_key,
H,Mul:hash_func,
Snd,Rcv:channel(dy))
played_by G

def=
local State:nat,
IDi,PWi,Ri,MIDi,MPi,RSPi,Di,Ei,Fi,Gi,Xgwn,Xhgwn,Xg
wni,Rii,SIDj,Rj,MPj,MNj,TS1,Xj,Dj,Ej,Fj,TS2,An,Bn,Cn,
P,MID1,Xi,R3,R4,SK:text,
R1,R2,M1,M2,M3,M4,M5,M6,M7,T1,T2,T3,T4,ESIDj:me
ssage,
Inc:hash_func
const
sec_subs1,sec_a,sec_b,sec_c,sec_sk,sec_xgwn,user_sensor
_a,user_gwn_a,sensor_user_b,sensor_gwn_b,sensor_gwn_r
j:protocol_id
init State:=0
transition
%Registration phase
1. State = 0 /\ Rcv(MIDi.RSPi) =|>
State':= 1 /\ Ei':= H(RSPi.MIDi) /\ Di':= H(MIDi.Xgwn)
/\ Gi':= xor(H(Xgwn).H(RSPi.Di'))
/\ Fi':= xor(Di',H(RSPi.Ei'))
/\ Snd(Ei'.Fi'.Gi') /\ secret({Xgwn},sec_xgwn,G)
2. State = 1 /\ Rcv(SIDj.MPj.MNj.TS1) =|>
State':= 2 /\ TS2':= new() /\ Xj':= H(SIDj.Xgwn)
/\ Ej':= xor(Xj',SKgsj)
/\ Dj':= xor(H(Xgwn.1),H(SKgsj.TS2'))
/\ Fj':= H(Xj'.Dj'.SKgsj.TS2') /\ Snd(Ej'.Fj'.Dj'.TS2')
/\ request(Sj,G,sensor_gwn_rj,Rj)
/\ secret({Xgwn},sec_xgwn,G)
%Login and authentication phase
3. State = 2 /\ Rcv(M1.M2.M3.T1.T2.ESIDj.R1.R2) =|>
 State':= 3 /\ T3':= new()
/\ SIDj':= xor(ESIDj,H(H(Xgwn.1).T2))
/\ Xj':= H(SIDj'.Xgwn)
/\ MID1':= xor(M1,H(H(Xgwn).T1))
/\ Xi':= H(MID1'.H(Xgwn)) /\ M4':= H(Xi'.R2.T3')
/\ M5':= H(Xj'.R1.T3') /\ M6':= xor(MID1',H(Xj'.T3'))
/\ Snd(M4'.M5'.M6'.R1.T3')
/\ secret({Xgwn},sec_xgwn,G)
/\ request(Ui,G,user_gwn_a,An)
/\ request(Sj,G,sensor_gwn_b,Bn)
end role
```

FIGURE 11. Role specification in HLPSL for *GWN* in our protocol.

the message {*Ej, Fj, Dj, TS2*} to *Sj*. The statement *request* (*Sj, G, sensor_gwn_rj, Rj*) indicates that *Sj* authenticated the identity of *GWN* by its generated number *Rj*. In the login and authentication phase, *GWN* receives the message {*M1, M2, M3, T1, T2, ESIDj, R1, R2*} from *Sj*, and then generates timestamp T_3. Lastly, *GWN* sends the message {*M4, M5, M6, R1, T3*} to *Sj*. The statements *request* (*Ui, G, user_gwn_a, An*) and *request* (*Sj, G, sensor_gwn_b, Bn*) indicate that *GWN* is authenticated by the fresh number *An* generated by *Ui* and *Bn* generated by *Sj* respectively.

```
role session(Ui,Sj,G:agent,
SKgui:symmetric_key,
SKgsj:symmetric_key,
H,Mul:hash_func)

def=
local US,UR,SS,SR,GS,GR:channel (dy)
composition
user(Ui,Sj,G,SK,SKgui,SKgsj,H,Mul,US,UR)
/\ sensor(Ui,Sj,G,SK,SKgui,SKgsj,H,Mul,SS,SR)
/\ gwn(Ui,Sj,G,SK,SKgui,SKgsj,H,Mul,GS,GR)
end role

role environment()
def=
const ui,sj,g:agent,
skgui:symmetric_key,
skgsj:symmetric_key,
h,mul:hash_func,
idi,pwi,ri,midi,mpi,rspi,di,ei,fi,gi,xgwn,xhgwn,xgwni,rii,sid
j,rj,mpj,mnj,ts1,xj,dj,ej,fj,ts2,an,bn,cn,p,mid1,xi,r3,r4,sk:tex
t,
sec_subs1,sec_a,sec_b,sec_c,sec_sk,sec_xgwn,user_sensor
_a,user_gwn_a,sensor_user_b,sensor_gwn_b,sensor_gwn_r
j:protocol_id
intruder_knowledge={ui,sj,g,h,mul,ei,fi,gi,rii}
composition
session(ui,sj,g,sk,skgui,skgsj,h,mul)
/\ session(ui,sj,g,sk,skgui,skgsj,h,mul)
/\ session(ui,sj,g,sk,skgui,skgsj,h,mul)
end role

goal
secrecy_of sec_subs1
secrecy_of sec_a
secrecy_of sec_b
secrecy_of sec_c
secrecy_of sec_sk
 secrecy_of sec_xgwn
authentication_on user_sensor_a
authentication_on user_gwn_a
authentication_on sensor_user_b
authentication_on sensor_gwn_b,sensor_gwn_rj
end goal
environment()
```

FIGURE 12. Role specification in HLPSL for session, environment, and goal in our protocol.

We also describe the role of session, environment, and goal in FIGURE 12. There are 6 secrecy goals and 4 authentication goals as follows:

secrecy_of sec_subs1: It tells that only *Ui* is familiar with {*IDi, PWi*};

secrecy_of sec_a: It shows that only *Ui* is familiar with *An;*

secrecy_of sec_b: It indicates that *Bn* is undisclosed to everyone except *Sj*;

secrecy_of sec_c: It shows that only *Ui* is familiar with C*n*;

secrecy_of sec_sk: It shows that *SK* is kept secret for only *Ui* and *Sj*;

TABLE 4. Comparison of computational cost among the proposed protocol and other schemes.

	Farash *et al.* 2016 [19]	Wu *et al.* 2017 [25]	Sureshkumar *et al.* 2019 [1]	Chandrakar *et al.* 2019 [9]	Li *et al.* 2020 [37]	Rangwani *et al.* 2021 [38]	Ours
User	$11T_h$	$11T_h$	$8T_h+4T_{pm}$	$12T_h$	$9T_h+3T_{pm}$	$5T_h+2T_{pm}+3T_{pa}$	$14T_h+2T_{pm}$
Sensor node	$7T_h$	$6T_h$	$4T_h+6T_{pm}$	$5T_h$	$4T_h+2T_{pm}$	$8T_h+2T_{pm}+4T_{pa}$	$6T_h+2T_{pm}$
GWN	$14T_h$	$17T_h$	$6T_h+6T_{pm}$	$14T_h$	$8T_h+1T_{pm}$	$4T_h+2T_{pm}+3T_{pa}$	$11T_h$
Total	$32T_h$	$34T_h$	$18T_h+16T_{pm}$	$31T_h$	$21T_h+6T_{pm}$	$17T_h+6T_{pm}+10T_{pa}$	$31T_h+4T_{pm}$
Time	0.0736ms	0.0782ms	35.6574ms	0.0713ms	13.4043ms	13.6831ms	8.9753ms

T_h: time complexity of a one-way hash function; T_{pm}: time complexity of a point multiplication operation on an elliptic curve; T_{pa}: time complexity of a point addition operation on an elliptic curve.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/MWSN.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 1.54s
  visitedNodes: 392 nodes
  depth: 9 plies
```

FIGURE 13. Simulation output with OFMC backend.

secrecy_of sec_xgwn: It indicates that only *GWN* is familiar with *Xgwn*;

authentication_on user_sensor_a: It indicates that *Ui* generates a random number *An* to authenticate *Sj*;

authentication_on user_gwn_a: It indicates that *Ui* generates a random number *An* to authenticate *GWN*;

authentication_on sensor_user_b: It indicates that *Sj* generates a random number *Bn* to authenticate *Ui*;

authentication_on sensor_gwn_b, sensor_gwn_rj: It indicates that *Sj* generates random number *Bn* and *Rj* to authenticate *GWN* in the registration and authentication phase respectively.

FIGURE 13 and 14 represent the simulation results of our protocol in the OFMC and CL-AtSe backend respectively. The results show that the proposed protocol is secure against potential attacks.

VIII. SECURITY FEATURES COMPARISON AND EFFICIENCY ANALYSIS

TABLE 3 compares the security features of our protocol and other existing schemes. In order to better compare the computational cost of each scheme in the login and authentication phases, we use T_h ≈0.0023 ms, T_{pm} ≈2.226 ms,

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/MWSN.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed  : 15 states
  Reachable  : 15 states
  Translation: 0.07 seconds
  Computation: 0.00 seconds
```

FIGURE 14. Simulation output with CL-AtSe backend.

TABLE 5. Comparison of communication cost among the proposed protocol and other schemes.

	Communication Cost (bits)
Farash *et al.* 2016 [19]	9152
Wu *et al.* 2017 [25]	8704
Sureshkumar *et al.* 2019 [1]	5088
Chandrakar *et al.* 2019 [9]	7648
Li *et al.* 2020 [37]	6080
Rangwani *et al.* 2021 [38]	4608
Ours	8192

and T_{pa} ≈0.0288 ms as mentioned in [35], [36]. TABLE 4 shows the results. Through comparison, it is found that our proposed protocol has increased the computational cost compared with some other schemes [9], [19], [25]. This is because we use additional point multiplication operations to solve potential security problems. Besides, compared with those schemes [1], [37], [38] that also use point multiplication operations, the computational cost of our protocol is not high. Besides, we also compare the communication cost of our protocol with other existing schemes. We supposed that the lengths of identity, password, random number, and hash function output (SHA-512) are each 512 bits. The lengths of timestamp and ECC point are 160 bits and 320 bits, respectively. The analysis result is shown in TABLE 5. We can see that the protocol in [19] needs the most communication cost and our protocol is in the middle level. Even though the protocols in [1], [38] require less communication cost than ours, their schemes lack many of the security features shown in TABLE 3. Above all, our protocol provides a more complete security feature and a more robust authentication process whereas ensuring efficiency in terms of computational and communication costs.

IX. CONCLUSION

In this research, we first reviewed and analyzed the scheme of Farash *et al.* and found that there are many security problems, such as privileged insider attacks, user anonymity problems, stolen smart card attacks, and offline password guessing attacks. In order to solve these security flaws, the authors proposed an improved ECC-based anonymous authentication protocol for smart healthcare systems using WMSN. The formal analysis using BAN logic and informal security analysis ensured that our protocol can provide secure mutual authentication and the ability to resist various security attacks. In addition, simulation outputs using AVISPA showed the scheme is secure to guard against intruders. Finally, security features comparison and efficiency analysis of our protocol with other existing schemes could prove that the improved protocol can provide more robust security features and less communication cost whereas increasing a small amount of computational cost. Therefore, our protocol is suitable for use in the smart healthcare environment.

However, we must point out that the protocol still has some shortcomings. There is still room for improvement in the communication cost of our protocol. Besides, the storage and computational capacity of a single gateway node are always limited, which makes the authentication tasks it can undertake is also limited. Therefore, in practical use, multiple gateways would be used to coordinately manage a huge medical monitoring network. Hence how to enable users registered in one GWN to pass the authentication of another GWN and access the medical sensor information managed by the latter GWN becomes a question worth considering. In the future, we need to think how to solve this problem in an authentication protocol for multi-gateway WMSN. In addition, how to achieve cross-hospital information transmission is also what the protocol needs to settle.

REFERENCES

[1] V. Sureshkumar, R. Amin, V. R. Vijaykumar, and S. R. Sekar, "Robust secure communication protocol for smart healthcare system with FPGA implementation," *Future Gener. Comput. Syst.*, vol. 100, pp. 938–951, Nov. 2019.

[2] W.-L. Tai, Y.-F. Chang, and Y.-L. Lo, "An anonymity, availability and security-ensured authentication model of the IoT control system for reliable and anonymous eHealth services," *J. Med. Biol. Eng.*, vol. 39, no. 4, pp. 443–455, Aug. 2019.

[3] J. J. Rodrigues, D. B. D. R. Segundo, H. A. Junqueira, M. H. Sabino, R. M. Prince, J. Al-Muhtadi, and V. H. C. De Albuquerque, "Enabling technologies for the internet of health things," *IEEE Access*, vol. 6, pp. 13129–13141, 2018.

[4] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015.

[5] B. D. Deebak, F. Al-Turjman, and A. Nayyar, "Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care," *Multimedia Tools Appl.*, vol. 80, no. 11, pp. 17103–17128, Nov. 2020, doi: 10.1007/s11042-020-10134-x.

[6] Y. K. Ever, "Secure-anonymous user authentication scheme for e-Healthcare application using wireless medical sensor networks," *IEEE Syst. J.*, vol. 13, no. 1, pp. 456–467, Mar. 2019.

[7] S. F. Aghili, H. Mala, and P. Peris-Lopez, "Securing heterogeneous wireless sensor networks: Breaking and fixing a three-factor authentication protocol," *Sensors*, vol. 18, no. 11, p. 3663, 2018.

[8] P. Chandrakar and H. Om, "An extended ECC-based anonymity-preserving 3-factor remote authentication scheme usable in TMIS," *Int. J. Commun. Syst.*, vol. 31, no. 8, May 2018, Art. no. e3540.

[9] P. Chandrakar, "A secure remote user authentication protocol for healthcare monitoring using wireless medical sensor networks," *Int. J. Ambient Comput. Intell.*, vol. 10, no. 1, pp. 96–116, Jan. 2019.

[10] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[11] T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, N. B. A. Juma'at, I. Ahmedy, N. A. Ghani, and S. Bhattacharyya, "Review on security of Internet of Things authentication mechanism," *IEEE Access*, vol. 7, pp. 1–36, 2019.

[12] P. Kumar, S. G. Lee, and H. J. Lee, "E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," *Sensors*, vol. 12, no. 2, pp. 1625–1647, 2012.

[13] M. K. Khan and S. Kumari, "An improved user authentication protocol for healthcare services via wireless medical sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 4, Apr. 2014, Art. no. 347169.

[14] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Syst.*, vol. 21, no. 1, pp. 49–60, Feb. 2015.

[15] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks," *Multimedia Syst.*, vol. 23, no. 2, pp. 195–205, Mar. 2017.

[16] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 2643–2655, Oct. 2016.

[17] A. K. Das, A. K. Sutrala, V. Odelu, and A. Goswami, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks," *Wireless Pers. Commun.*, vol. 94, no. 3, pp. 1899–1933, 2017.

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

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

[20] R. Amin and G. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Netw.*, vol. 36, pp. 58–80, Jan. 2016.

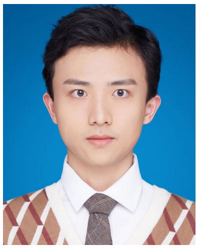
[21] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," *Comput. Netw.*, vol. 101, pp. 42–62, Jun. 2016.

[22] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K. R. Choo, M. Wazid, and A. K. Das, "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment," *J. Netw. Comput. Appl.*, vol. 89, pp. 72–85, Jul. 2017.

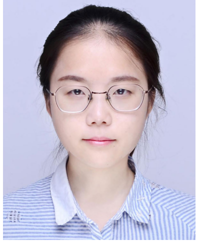
[23] R. Amin, S. K. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 80, pp. 483–495, Mar. 2018.

[24] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and A. C. Shehzad, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Comput. Elect. Eng.*, vol. 63, pp. 182–195, Oct. 2017.

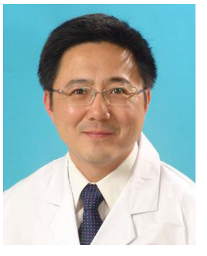
[25] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu, and J. Shen, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 82, pp. 727–737, May 2018.
[26] R. Ali, A. K. Pal, S. Kumari, A. K. Sangaiah, X. Li, and F. Wu, "An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring," *J. Ambient Intell. Humanized Comput.*, pp. 1–22, Sep. 2018, doi: 10.1007/s12652-018-1015-9.
[27] W. Li, B. Li, Y. Zhao, P. Wang, and F. Wei, "Cryptanalysis and security enhancement of three authentication schemes in wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–11, Jul. 2018.
[28] M. Shuai, B. Liu, N. Yu, and L. Xiong, "Lightweight and secure three-factor authentication scheme for remote patient monitoring using on-body wireless networks," *Secur. Commun. Netw.*, vol. 2019, pp. 1–14, Jun. 2019.
[29] J. Mo, Z. Hu, and Y. Lin, "Cryptanalysis and security improvement of two authentication schemes for healthcare systems using wireless medical sensor networks," *Secur. Commun. Netw.*, vol. 2020, pp. 1–11, Feb. 2020.
[30] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Elect. Eng.*, vol. 69, pp. 534–554, Jul. 2018.
[31] P. Soni, A. K. Pal, and S. H. Islam, "An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system," *Comput. Methods Programs Biomed.*, vol. 182, Dec. 2019, Art. no. 105054.
[32] G. Xu, F. Wang, M. Zhang, and J. Peng, "Efficient and provably secure anonymous user authentication scheme for patient monitoring using wireless medical sensor networks," *IEEE Access*, vol. 8, pp. 47282–47294, 2020.
[33] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K.-R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 8, pp. 2146–2156, Aug. 2020.
[34] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.
[35] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1005–1023, 2nd Quart., 2014.
[36] A. Ostad-Sharif, A. Babamohammadi, D. Abbasinezhad-Mood, and M. Nikooghadam, "Efficient privacy-preserving authentication scheme for roaming consumer in global mobility networks," *Int. J. Commun. Syst.*, vol. 32, no. 5, Mar. 2019, Art. no. e3904.
[37] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," *IEEE Syst. J.*, vol. 14, no. 1, pp. 39–50, Mar. 2020.
[38] D. Rangwani and H. Om, "A secure user authentication protocol based on ECC for cloud computing environment," *Arabian J. Sci. Eng.*, vol. 46, no. 4, pp. 3865–3888, Apr. 2021.



WANG YUANBING received the bachelor's degree in biomedical engineering from Xi'an Jiaotong University, in 2019. He is currently a Student with the College of Biomedical Engineering, Shanghai Jiao Tong University. His main research interests include communication security of medical information management and the Internet of Things Technology.



LIU WANRONG received the bachelor's degree from Luoyang Institute of Technology, in 2018, and the master's degree from Shanghai Ocean University, in 2021. She is currently working with Shanghai Jiao Tong University Affiliated Sixth People's Hospital. Her main research interests include communication security and the Internet of Things Technology.



LI BIN received the master's degree from the NMR Analysis Center, East China Normal University, in 1990.

From 1990 to 1996, he worked in hospital and global medical equipment manufacture. He has been trained on MRI and CT technology four times in Japan and USA. Since 1997, he has been in charge of device management and quality control of medical equipment with Shanghai Sixth People's Hospital for 20 years. He is currently the Vice-Director of Shanghai Sixth People's Hospital Affiliated to Shanghai Jiao Tong University (East-Campus). He authorized and coauthorized six books and published over 60 articles in national statistical source journal. His research interests include regional medical equipment management and quality control, assessment and management of medical equipment suppliers, management of service and rating of customer satisfaction, evaluation of medical imaging equipment performance and service system, the IoT, and communication safety in medical technology management.

Mr. Li is the Director of Shanghai Quality Control Centre of Management of Medical Equipment, the Council Member of Chinese Society of Biomedical Engineering, a Committee Member of medical device classification technology of China SFDA, a Coopted Member of Clinical Engineering Division of IFMBE, the Chairman of Clinical Engineering Society of Chinese Medical Association, and the Vice Chairman of Clinical Engineers Branch of Chinese Medical Doctor Association,.