Research Article

Design and Simulation of Lightweight Identity Authentication Mechanism in Body Area Network

Jianglong Yang ¹, Wanlin Yang ², Huwei Liu ¹ and Li Zhou ³

¹School of Management Engineering, Capital University of Economics and Business, Beijing, China

²School of Computer Science and Engineering, Northeastern University, Shenyang, China

³School of Information, Beijing Wuzi University, Beijing, China

Correspondence should be addressed to Huwei Liu; darion8@163.com

Received 5 January 2021; Revised 14 March 2021; Accepted 27 March 2021; Published 19 April 2021

Academic Editor: Zhe-Li Liu

Copyright © 2021 Jianglong Yang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wearable medical devices rely on the human body to form a small LAN around the human body, called body area network (BAN). Users can use these devices to monitor the changes of various body indicators in real time. The physiological data involved in this process belongs to personal privacy. Therefore, the security requirements of BAN are relatively high, and its current research focus is on authentication mechanisms. To meet the requirements of security and resource consumption of BAN, this paper proposes a lightweight identity authentication mechanism that meets the characteristics of BAN resource constraints. Based on the characteristics of BAN, a simple and mature star topology structure is applied to establish the network model of BAN. For the human body in normal situations and emergencies, the corresponding authentication mechanism and encryption and decryption method of physiological data are designed by using the physical unclonable function (PUF) and cloud database, physiological data, and cross-correlation algorithm. Furthermore, the formal and informal security analysis of the designed authentication mechanism proves that the authentication mechanism designed in this paper has certain security, and the lightweight authentication mechanism is simulated and evaluated. The experimental results show that compared with the benchmarking mechanism, the authentication mechanism designed in this paper solves more security problems and has certain advantages in terms of calculation cost, communication cost, and energy cost.

1. Introduction

In recent years, wearable devices are developing at an amazing speed, followed by intelligent and interconnected medical sensor devices and the popularization of medical sensor networks [1, 2]. With more and more medical sensor devices for monitoring and treatment on the human body, researchers have put forward the concept of personal local area network based on the human body [3], which is the predecessor of BAN. BAN refers to a kind of network attached to the human body, which is composed of medical sensor equipment implanted in the human body or worn on the human body surface. Data collected by nodes is transmitted to the remote server by external equipment for medical diagnosis [4, 5]. The existence of the BAN and wearable devices enables individuals to collect their own

physiological data in real time and monitor their physical activity and health status [6]. It is very convenient to know their own physical condition without going to the hospital regularly for examination, and its existence will not have any impact on people's life. With the aggravation of the aging of the social population, the number of chronic disease cases that need to consume a lot of human, material, and financial resources is also increasing. BAN has become the best choice to solve this problem [7]. The medical sensor equipment deployed in the BAN collects physiological data of different indicators of the human body. These data belong to personal privacy and cannot be accessed without permission. If we do not take any measures, then these data are easy to obtain, which may leak personal privacy and affect people's life, work, and other aspects, so the research on the security of BAN is urgent.

Therefore, based on the highly secure and limited resource requirements of the BAN, a lightweight authentication mechanism is constructed. (1) Under normal conditions, design the authentication mechanism and encryption and decryption method of physiological data using PUF and cloud database. (2) Design the authentication mechanism in emergencies using physiological data and cross-correlation algorithm. (3) Carry out formal and informal security analysis for the designed authentication mechanism. (4) Simulate and evaluate the lightweight authentication mechanism.

2. Related Works

The emergence of BAN brings new opportunities and challenges to human health care. The network connection of wearable devices and implantable medical devices has been quite advanced, but its system security problem has not been effectively solved, and its security mechanism is relatively weak, which has been attacked within the scope of the network, resulting in device security problems [8]. If we cannot solve all kinds of security problems existing in the BAN, then it is very difficult to be applied in the field of health care because the existence of various security problems will cause great harm to the human body. At present, research studies on the security of BAN are springing up. Among them, there are many research studies on authentication mechanisms in BAN.

Singla and Sachdeva [9] proposed a two-stage authentication mechanism. The first stage is the authentication between the medical sensor device and the receiver. Since the authentication resources are limited in this stage, it is necessary to design a lightweight authentication method; the second stage is the authentication between the receiver and the server, which is not limited by resources, so the traditional encryption method can be used. Based on the three-layer communication of the BAN, the mechanism is comprehensive, but it does not solve the problem of resource consumption reasonably. Under the premise of lightweight protocol and the requirement of physiological data sensitivity, Gritti et al. [10] limited the public information that could be obtained by the device. If more physiological data need to be obtained in some cases, such as an emergency, the access rights of personal information need to be realized based on device authentication. In reference [11], a device-to-device authentication scheme is proposed, that is, the authentication mechanism between two sensor nodes deployed on the human body. The key is always fresh and secure from the user's gait mode through the change of instantaneous acceleration. This method is only resistant to noise attacks (generated by sensor nodes when transmitting data) and active attacks. Anada [12] proposed a distributed multiauthority anonymous authentication scheme for the Internet of Things and blockchain, in which the verifiers were noninteractive. This scheme can dynamically increase/decrease the independent attribute permissions. When an entity wants the authority to issue attribute credentials, the authority only needs to generate a digital signature on its global identity to solve the problems of resource consumption and authentication

reliability. Based on the comprehensive consideration of data connectivity and user privacy and the joint scenario of eduGAIN, STORK, and eIDAS. Torroglosa-Garcia and Skarmeta-Gomez [13] proposed an interoperability mechanism for data connectivity to reduce the recurrence of identity authentication.

Some authentication mechanisms shield sensor nodes and ensure their security by adding proxy devices between sensor nodes and control nodes. Denning et al. [14] proposed a new method for the safety of the implantable medical device system from another angle, which added an additional external device (agent) to ensure the safety of the implantable medical device. The agent has no resource limitation. Some operations between the control node and the medical sensor device are completed by the agent. Only the agent exists outside, and the implantable medical device does not exist. The agent can solve some problems, but it also brings new and additional security risks to the system. In reference [15], a distance boundary method is proposed, in which a piezoelectric implantable device is implanted 1 cm or deeper into the human skin, and the random key is generated and sent out by means of sound emission, which can only be received by the control node at a certain distance. This method can resist remote attacks, but the addition of additional devices will bring new security problems, and the method of transmitting data by means of sound transmission itself will have security problems.

Other authentication mechanisms are designed using PUF. Lee et al. [16] proposed a mutual authentication mechanism between the control node and sensor node by using PUF. The challenge-response pairs generated by PUF were used, and each node was needed to complete the hash function operation and MAC operation. The mechanism designed in this paper can solve some security problems. However, resource consumption is not analyzed in this paper, and a good balance between resource consumption and security is not achieved. In reference [17], a mutual authentication mechanism between sensor nodes is designed by using PUF. In this method, the control node acts as the third party, and the key stored in the third-party control node is the shared key between two sensor nodes, which guarantees the reliability of data transmission when the sensor nodes authenticate with each other. The implementation of this method is based on the assumption that the control node is trusted, but the control node is not necessarily trusted.

Some use the characteristics of physiological signals to design authentication mechanisms. Steffen et al. [18] designed a secure authentication mechanism in BAN using ECG signals to identify whether sensor nodes are attached to the same body. The process of the mechanism is as follows: firstly, the sensor nodes including the analog filter and data preprocessor are deployed; then, the features of the data after preprocessing are extracted by technical means, and finally, the parameters of authentication protocol are determined by the extracted features. Hu et al. [19] designed a key protocol based on ordered physiological signals. The protocol authenticates control nodes and implantable medical devices by extracting and quantifying ECG signals. Rostami et al.

[20] designed a contact access mechanism, in which the control node contacts the human body, extracts the heart rate signal of the human body, analyses the pulse interval, and designs a new encryption pairing protocol to achieve good authentication between the control node and the implantable medical device. This method can be implemented in the existing devices without the need for additional devices. But when people are in a critical situation and need to receive treatment in time, the demand for speed is far higher than safety.

The medical sensor equipment in the BAN collects the physiological data of the human body in real time, which leads to the existence of a large amount of data on the local side. The storage of these data needs to consume a lot of local resources. Therefore, some scholars propose that the BAN and cloud should be integrated. Wan et al. [21] pointed out that, with the support of mobile cloud computing, the implementation of deploying the wireless human local area network (WLAN) on a large scale in pervasive medicine can be enhanced, but there are some technical problems and challenges in the process of integrating wireless BAN and mobile cloud computing. This paper introduces the framework of the cloud-assisted human LAN, as well as the challenges of routing mechanism, cloud resource allocation mechanism, semantic attack, and data security. According to the characteristics of telemedicine, an efficient cloud-assisted message authentication scheme was proposed in reference [22]. In this scheme, the cloud server is responsible for storing and transmitting the encrypted data of patients to doctors for diagnosis and treatment, and then, the processing results are stored in the cloud server. Through the security analysis and performance evaluation of this scheme, it is concluded that the scheme not only ensures the privacy of stored human physiological data but also meets the purpose of saving local resources. Yu et al. [23] proposed a new solution to the security and privacy threats in the cloud-assisted wireless BAN, focusing on the confidentiality and integrity of data. The data confidentiality is guaranteed by the improved order-preserving symmetric encryption method, and the data integrity is guaranteed by using the virtual linear segmentation method. Although this method saves the resources at one end of the sensor node, it increases the cost of the remote control unit. The future research direction is to reduce the cost of both ends at the same time, instead of sacrificing one end to complete the other.

To sum up, at present, there are a lot of research studies on the authentication mechanism of BAN, but many designs do not meet the requirements of resource limitation and high security of BAN at the same time.

3. Lightweight Authentication Mechanism in BAN

3.1. Network Model. At present, two kinds of topology structure are widely used in BAN. One is two-layer star topology, that is, some sensor nodes need two hops to send data to the control node, and the other is star topology, that is, sensor nodes only need one hop to send data to control nodes. BAN is a network with very limited resources. If one

node interacts with the master node, it will consume a lot of resources. If it needs to interact with other nodes in the same network, it will consume resources faster. Moreover, even if the data of one node is transmitted to another node, the data is meaningless to this node at present because this node cannot process the data. This paper uses a mature, simple, and representative star topology. Figure 1 shows the star topology. As shown in the figure, there are N sensor nodes (medical sensor equipment) $\{S_1, S_2, S_3, \dots, S_n\}$ deployed on the guardians. Each node has an ID (unique and greater than 1), and there is no connection between these nodes. There is a control node whose ID value is equal to 0. It is used to collect the data collected by all sensor nodes deployed on the human body and is responsible for communicating with the outside world and sending the data to the medical staff so that the medical staff can make a correct and effective judgment on the health status of the guardians in time. The control node can communicate with all sensor nodes in one hop. Because different sensor nodes represent different types of medical sensor equipment and have different functions, there are many sensor nodes deployed in the human body in the BAN. It is mentioned in reference [2] that medical sensor equipment is divided into three security levels (I, II, and III). The greater the category number, the higher the risk level. Different security levels correspond to different medical sensor devices (sensor nodes).

3.2. Authentication Mechanism under Normal Circumstances

3.2.1. Authentication Protocol. In the design of normal authentication protocol, this paper uses the physical unclonable function and cloud database to achieve. Once the authentication mechanism is used on the device, it will last for a lifetime until the device is not available. It can be imagined that if the authentication mechanism is designed by using PUF, a large number of challenge-response pairs are needed, and the relationship between these challenge-response pairs is one-to-one. In order to avoid unnecessary waste of local resources due to the storage of a large number of challenge-response pairs, these challenge-response pairs are stored in the cloud database.

In authentication protocol, some data need to be transmitted between two entities, so the freshness, integrity, and nonrepudiation of data should be guaranteed in the process of transmission. Among them, freshness refers to the guarantee that the data used is up-to-date rather than has been used; integrity refers to ensuring that the messages in transmission are not partially missing due to malicious attacks by attackers; nonrepudiation means that if an entity has sent the message, it must ensure that the entity has no reason to deny this fact.

In order to authenticate both parties as trustworthy entities to each other, this paper designs a two-way authentication protocol, that is, the sensor node should prove to the control node *phone* that it is an honest entity, and the control node should also prove itself to the sensor node that it is an honest entity. Therefore, it is necessary to verify that the control node is trusted during authentication. It is not feasible for malicious sensor nodes to use the previous

FIGURE 1: Star topology.

challenge-response pairs to achieve the purpose of authentication because the principle of challenge-response pairs is to discard one by one. When the control node obtains the previously used incentive response pair, it will not find a matching response in the database, then the authentication will not succeed. Figure 2 shows the normal authentication protocol, mainly including the initialization phase and authentication phase. The symbols used in the protocol are illustrated in Table 1.

(1) *Initialization Phase*. In order to ensure the normal use of the protocol, we need to complete the following initialization work. Firstly, the challenge-response pairs required by the authentication process are stored in the cloud database. Secondly, the initial seed of the butterfly seed generation algorithm [24] is set. The key can then be generated using this method. The butterfly seed generation algorithm can get the required seed, and only a few bit changes can get random results. The method to get random seeds by using the variable function is to invert these bits bit by bit from the least significant bit to the j bit. j can be a value-added number or other to improve the unpredictability where $\sin it$ is the initial seed, Sj is the current seed, $Sj = \varphi(s)$ is the seed variation function, and $r = g(Sj)$ is the random number generation function.

(2) *Certification Phase*. In the authentication phase, both entities authenticate each other's trustworthiness. In the authentication process, sensor nodes and control nodes use the pseudorandom generation sequence to generate excitation Ci . The sensor node uses its own implanted PUF and Ci to execute PUF to generate response Ri , then uses the key Ks to encrypt the results of excitation Ci and response Ri XOR, and sends the encryption results α to the control node. The control node decrypts the received α to get Ri , then extracts its own stored Ri from the database, and records it as Ri' . If the error between the two is within an acceptable range, then the authentication is successful, that is, the other

FIGURE 2: Authentication protocol under normal circumstances.

TABLE 1: Symbol description.

Symbol	Description
Ci	Challenge
Ri	Response generated by sensor nodes
Ri'	Response when reading from cloud database
Ks	Key of sensor node
Kx	Key of phone
seed	Seed
t	Critical value

party is an honest and trustworthy entity. Similarly, the control node sends a message β to the sensor node to prove its identity. After receiving the message, the sensor node decrypts the message β by using the key Kx to obtain Ri' and compare it with its own Ri to verify whether the party sending the message is a trusted entity. If so, mutual authentication is successful. The algorithm pseudocode of authentication protocol is as follows. (Algorithm 1)

3.2.2. Information Encryption and Decryption Process. After the sensor node and the control node prove that they are honest and trustworthy entities through the authentication protocol, the sensor node sends the collected human physiological data to the control node. In this process, the transmitted information needs to be encrypted to ensure its security. Figure 3 is the process flow chart of encryption and decryption. The sensor node performs a pseudorandom generator to generate challenge, then uses the generated excitation and the human physiological signal collected by the sensor node for XOR, that is, encryption, and then sends the message to the control node; after receiving the message, the control node gets the excitation generated by its own end and decrypts the specific and correct human physiological data according to the excitation. The control node can also access the cloud database to obtain the physiological data


```

(1) //INPUT: The excitation response pairs generated by PUF
(2) //OUTPUT: Authentication success/failure message
(3) BEGIN
(4) Execute butterfly seed generation algorithm to generate seed and key Ks, Kx;
(5) phone and sensor nodes simultaneously execute pseudo-random sequence generator to generate Ci;
(6) The sensor node calculates the value of  $\alpha$  by  $\alpha = E_{Ks}(Ci \oplus Ri)$ , and then sends it to phone;
(7) phone reads the database to get  $Ri'$ , and calculates  $Ri$  by  $Ri = D_{Kx}(\alpha) \oplus Ci$ ;
(8) IF the error between  $Ri$  and  $Ri'$  is within the acceptable range, threshold  $(Ri, Ri') < t$ ;
(9) THEN phone authenticates the sensor node successfully, considers the sensor node to be a trusted entity, and sends authentication success message, Auth = accept;
(10) ELSE send authentication failure message, Auth = reject;
(11)   phone calculates  $\beta$  by  $\beta = E_{Kx}(Ci \oplus Ri')$  and sends it to sensor node;
(12) END IF
(13) IF the error between  $Ri$  and  $Ri'$  is within the acceptable range, threshold  $(Ri, Ri') < t$ ;
(14)   THEN the sensor node authenticates phone successfully and considers phone as a trusted entity, and sends an authentication success message, Auth = accept;
(15) ELSE send authentication failure message, Auth = reject;
(16) END IF
(17) END

```

ALGORITHM 1: Authentication protocol under normal circumstances.

FIGURE 3: Encryption and decryption process.

needed. The secure data transmission between the cloud database and the control node is realized by using the traditional encryption method.

Because the cloud database also has unsafe factors, two steps need to be done here. First, the challenge-response pairs generated by PUF are stored in the cloud database by the XOR encryption method. In order to prevent security problems in data transmission, the data in the transmission process is encrypted by the XOR method, and the cloud database also stores the data after XOR. Second, doctors obtain cloud database data through traditional encryption

methods (such as AES). Therefore, after obtaining XOR encrypted data, cloud database uses traditional encryption methods for stronger security. The details are shown in Figure 4.

3.2.3. Design of Safety Assurance. (1) Security guarantee of authentication protocol: freshness. A large number of challenge-response pairs are needed in the designed authentication mechanism. The use principle of these challenge-response pairs is to use up one and then discard it, and there will be no use of two duplicate challenge-response pairs. This method ensures that the challenge-response pairs used in each certification are fresh.

(2) Security guarantee of authentication protocol: nonrepudiation. When one entity sends data to another entity, the sending entity cannot deny that it has sent the data. In this paper, the unique ID number of each medical sensor device on the human body is used to ensure nonrepudiation. The ID number of the medical sensor equipment and the seed change function are combined into a function. The combination function is used as the parameter of the random number generation function as $r = g(f(\phi(Sj), ID))$, where f is a combination function.

(3) Security guarantee of authentication protocol: integrity. Because of the limited resources of the BAN, a critical value is used to judge whether the authentication is successful or not. In addition, the frequency and times of the implementation of the authentication mechanism should be considered. Therefore, in the authentication mechanism, it is necessary to design a method to check the integrity rather than to ensure the integrity [25]. The specific method is as follows: divide the message into n parts, each part has L - bit, and take the bit in the corresponding position out from each part; there are n bits in total, then XOR these bits to get a new bit block, so as to get L blocks, and then XOR L blocks to get a new message. Both entities need to perform this process. If

FIGURE 4: Data encryption and decryption in the cloud database.

the final result is the same, then it can be considered that the message has not been tampered within the transmission process, as shown in Figure 5.

(4) Security assurance of encryption and decryption: freshness. The challenges used in the encryption process are not like the challenge-response pairs used in the above authentication mechanism, which are discarded once, but need to be saved to the cloud database so that the collected physiological data can be decrypted. The challenge response here can be reused. Therefore, the freshness can be guaranteed by adding time variables into the formula as $r = g(f(\varphi(Sj), ti))$.

(5) Security assurance of encryption and decryption: nonrepudiation. The guarantee of nonrepudiation is realized by ID of the sensor node as $r = g(f(\varphi(Sj), ID, ti))$.

(6) Security assurance of encryption and decryption: confidentiality. The guarantee of confidentiality is to use the response generated by PUF as the key to encrypt the information. Because the response of PUF will be affected by temperature and environment, the response generated each time will be different. However, as a key, the response is required to be the same every time so that the encrypted message can be correctly decrypted. Because the instability of PUF is difficult to solve, it is not appropriate to use Ri encryption. At present, Ci encryption is considered. The guarantee of confidentiality is $E(Mi) = Ci \oplus Mi$, which utilizes the XOR operation on the challenge Ci and message Mi . The decryption process of the received message is to XOR the message, and Ci is obtained from the cloud database as $Mi = E(Mi) \oplus Ci$.

(7) Security assurance of encryption and decryption: integrity. Because the data encryption and decryption process require higher integrity, we cannot use the method of integrity checking to determine whether the message has been tampered with, but use the method to ensure the integrity of the message [26]. This paper uses the method of inserting parity bits into messages. The specific operation is as follows: first, add the check bit to the message, and then, encrypt the message with the check bit, and finally, get the Frame Check Sequence (FCS) and the encrypted message body. The check bit is selected by the control node and broadcast to all sensor nodes in the deployment phase. The message structure after adding check bits is shown in Figure 6.

FIGURE 5: Integrity test.

3.2.4. Safety Analysis. Formal and informal security analysis methods are mainly used to analyze the security of the designed authentication mechanism under normal conditions. The formal security analysis method is BAN logic. Through the analysis, it can be proved that the authentication mechanism has certain security.

(1) *Formal Security Analysis.* In this paper, BAN logic is used to analyze the formal security of authentication protocol under normal conditions. Assuming that the communication between external devices and the cloud database is secure, then the cloud database and control node can be regarded as a whole DP. The following is the formal security analysis of the authentication protocol designed in this paper.

The purpose of mutual authentication between the control node and sensor node is to ensure that both sides receive the data from the trusted entity. If the authentication purpose is expressed by expressions, the expressions are as follows:

$$\begin{aligned} \text{phone} &\equiv \{\text{if DP has } Ri \approx Ri' \text{ then phone} \equiv Ri\}, \\ \text{sensor} &\equiv \{\text{if sensor has } Ri' \approx Ri \text{ then sensor} \equiv Ri'\}. \end{aligned} \quad (1)$$

The initialization assumptions for the authentication protocol are as follows:

$$\begin{aligned} S1: \text{sensor} &\equiv \text{sensor} \xleftrightarrow{(Ks, Kx)} (Ks, Kx)DP, S2: DP \equiv \text{sensor} \xleftrightarrow{(Ks, Kx)} (Ks, Kx)DP, \\ S3: DP &\equiv \#(Ci), S4: \text{sensor} \equiv \#(Ci \oplus Ri), \\ S5: DP &\equiv \text{sensor} \Rightarrow Ri, S6: \text{sensor} \equiv DP \Rightarrow Ri'. \end{aligned} \quad (2)$$

FIGURE 6: Message structure.

The ideal model of the authentication protocol is shown as follows:

$$\begin{aligned}
 &DP \longrightarrow \text{sensor: Query,} \\
 &\text{sensor} \longrightarrow DP: \{Ci, (Ci \oplus Ri)_{Ks}\}(\alpha), \\
 &DP \longrightarrow \text{sensor: } \{(Ci \oplus Ri)_{Kx}\}(\beta).
 \end{aligned} \tag{3}$$

The analysis process of the authentication protocol is as follows.

According to the above initialization assumption and idealized model of the authentication protocol designed in this paper, the formal security analysis of the protocol is given below. First, DP will receive a message α from the sensor node, thus obtaining $DP \nabla \{(Ci \oplus Ri)_{Ks}\}$.

Combined with the hypothesis S2, according to the formal reasoning criterion of the BAN logic criterion, $DP \models \text{sensor} \sim (Ci \oplus Ri)$ is obtained, which shows that DP believes that α is sent by a sensor node with the same key as it. According to the message freshness criterion in S3 and BAN logic criteria, $DP \models \#(Ci \oplus Ri)$ is obtained. From $DP \models \text{sensor} \sim (Ci \oplus Ri)$ and $DP \models \#(Ci \oplus Ri)$, according to the random number verification criterion in the BAN logic criterion, $DP \models \text{sensor} \equiv (Ci \oplus Ri)$ can be obtained. From $DP \models \text{sensor} \equiv (Ci \oplus Ri)$ and belief union criterion in the BAN logic criterion, we can get $DP \models \text{sensor} \equiv Ri$. If the response is extracted from the cloud database according to the challenge, then according to $DP \models \text{sensor} \equiv Ri$ and protocol initialization hypothesis S5, it is concluded that $DP \models Ri$. If not, the message α is sent by the attacker, and the execution of the protocol is terminated.

If there is Ri' , the sensor node receives the message β from DP and gets $\text{sensor} \nabla \{(Ci \oplus Ri')_{Kx}\}$. Combined with the hypothesis S2, according to the message meaning criterion in the BAN logic criterion, $\text{sensor} \models DP \sim (Ci \oplus Ri')$ is obtained. In other words, the sensor node believes that β is sent by a DP, which has a shared key with it. From the hypothesis S4, it is concluded that $\text{sensor} \models \#(Ci \oplus Ri')$. According to $\text{sensor} \models DP \sim (Ci \oplus Ri')$ and $\text{sensor} \models \#(Ci \oplus Ri')$, combined with the random number verification criterion in the BAN logic criterion, $\text{sensor} \models DP \equiv (Ci \oplus Ri')$ is obtained. According to $\text{sensor} \models DP \equiv (Ci \oplus Ri')$ and belief union criterion in the BAN logic criterion, it is concluded that $\text{sensor} \models DP \equiv Ri'$. If there is $Ri' \approx Ri$ in the sensor node, it can be concluded from $\text{sensor} \models DP \equiv Ri'$ and S6 that $\text{sensor} \models Ri'$. It can be seen from the $DP \models Ri$ and $\text{sensor} \models Ri'$ that the authentication protocol under normal conditions can withstand the logical reasoning authentication of BAN. The message received by the sensor node or control

node is indeed sent by the trusted control node or sensor node, and the two are mutually trusted entities.

(2) *Informal Security Analysis*. Informal security analysis is the security analysis of the normal authentication protocol's resistance to attacks mainly including eavesdropping attack, replay attack, forward/backward security, and middleman attack.

(3) *Informal Security Analysis (Eavesdropping Attack)*. Attackers use the data overheard in the transmission process of sensor nodes and control nodes to conduct improper activities. Ks is used to encrypt the information transmitted between the sensor node and the control node, but the eavesdropping attacker does not know about Ks , so the messages between the sensor node and the control node cannot be eavesdropped and recorded.

(4) *Informal Security Analysis (Replay Attack)*. The data packet received by the sensor node or control node is sent again by attackers to get away with the other party's authentication, so as to cheat the sensor node or control node. Suppose the attacker sends the message α to the control node, which has been sent α before, but because the seed has changed at this time, Ks , Ci , and Ri' obtained after receiving α for the first time have changed, and finally, the authentication fails. Suppose the attacker sends the message β to the sensor node, which has been sent before. Because the sensor node performed a series of operations after receiving β last time, resulting in changes in Ks and Ci , so the final authentication will not succeed.

(5) *Informal Security Analysis (Forward/Backward Safety)*. Forward security means that the attacker cannot get the previous data from the known data. Backward security means that the attacker cannot use the current data to carry on the malicious attack to the later operation. There is no relationship between the challenge-response pairs generated by PUF, so attackers cannot infer the used or future challenge-response pairs according to the existing. There is no relationship between the former seed and the latter seed. It is difficult for attackers to analyze and infer useful information based on the existing seeds.

(6) *Informal Security Analysis (Middleman Attack)*. The attacker steals the transmitted data and masquerades as an aggressive sensor node or a control node to maliciously attack the authentication mechanism. Authentication protocol guarantees the integrity and freshness of the transmission message, and due to the nonclonality of PUF and the honesty of the control node, if the message changes in the transmission process, it can be detected.

3.3. Authentication Mechanism in Emergency. In the BAN, an urgent problem to be solved is that, in case of emergency, medical staff can access the medical equipment worn by patients, without authentication or simplified authentication, so as to know the patient's physical condition in time, reconfigure the equipment parameters, and timely treat the patients. At the same time, due to the sensitivity and complexity of patients' electronic health records and physiological data, the access rights of medical staff to patients' data should be limited in a specific range [27]. In this paper, the cross-correlation algorithm is used to calculate the correlation between the two signals, so as to know whether the patient is in a normal situation or an emergency and then take different measures. In case of emergency, the message is broadcast to the receiving device within a safe distance. In this way, in case of emergency, even if the doctor is not the commonly used treatment doctor of the patient, he can also obtain access right to the medical equipment of the patient in time so that the patient can be treated in time.

3.3.1. Selection of Physiological Signals. Now many heart patients have implanted the cardiac pacemaker, if the human body has a pacemaker, then the physiological signal will choose the ECG signal. If the human body does not wear a pacemaker, then the heart rate signal can be selected as the physiological signal. Now the bracelet, wristwatch, and so on can measure the human body's heart rate signal, this signal is related to the heart beat, easy to find the human body's health problems. The physiological signal used in this paper is the ECG signal. In an emergency, the reasons for choosing signals like this are as follows: first, most of the sensor nodes deployed on the human body will contact the blood vessels of the human body, and most sensor nodes can monitor the heart rate signal; second, in an emergency, the patient's pulse changes obviously, and using this signal will be easier and faster to detect human health problems than other signals.

The ECG signal of normal people is shown in Figure 7. Among them, the wave with the small waveform and similar shape to the sin function from 0 to π is the *P* wave. The wave with a flat shape and low amplitude (not less than 1/10 of the *R* wave) is the *T* wave. The most dramatic change of the waveform is the QRS wave group, which is composed of the *Q* wave with the downward waveform, *R* wave with the upward waveform, and *S* wave with the downward waveform. The interval between the starting point of the QRS wave group and the ending point of the *T* wave group is called the QT period. In a complete ECG signal diagram, the duration of the *P* wave is 0.08~0.11s, the duration of the PR interval is 0.120~0.200s, the duration of the QRS wave group is 0.06~0.10s, and the duration of the QT period is 0.340~0.430s. When the human atrium is excited, the *P* wave will be generated. The waveform generated by the right atrium is similar to the sin function from 0 to $(\pi/2)$, while that of the left atrium is from $(\pi/2)$ to π . If someone is older or has a slower heart rate, his PR interval will be longer than normal people. The *P* wave, QRS complex wave, and *T* wave all represent the potential change. The former two represent

FIGURE 7: Electrocardiogram signal.

the depolarization process, and the latter represents the ventricular repolarization process. The *P* wave and QRS complex wave are used to describe two atria and two ventricles, respectively.

3.3.2. Design of the Cross-Correlation Algorithm. According to the use environment and purpose, this paper improves the cross-correlation algorithm to determine whether the current human body is in an emergency. As shown in Figure 7, the waveform is divided into some segments or intervals by five special points. The waveform near each point represents different heart conditions, and the abnormal waveform represents different heart problems. The heart problems of each person are different, and the waveform changes around each point are also different when conditions occur. So, we divide an ECG waveform into three parts: PR interval, QRS wave group, ST segment and *T* wave. Then, set the weight values of the three parts according to the different disease conditions of each person. If the weight is 0.8, 0.2, and 0.2, it means that if the patient has an emergency, the PR section is easy to appear abnormal. This approach makes the method more targeted and more accurate.

In the process of execution, if the selected ECG signal cycle is as shown in Figure 7, the result may have a large error because it is impossible to accurately obtain the start time and end time of the cycle, so it is difficult to obtain the time cycle. Therefore, the cycle shown in Figure 8 is adopted in this paper.

According to the choice of segment and period of the ECG signal, we can assume that the duration of a cycle is 800 ms, then the PR interval accounts for 300 ms, ST segment and *T* wave part account for 300 ms, the first half QRS interval accounts for 100 ms, and the second half QRS interval accounts for 100 ms.

The control node is responsible for executing the cross-correlation algorithm to get the correlation number. The control node receives the ECG signal sent at T_i time and then performs the cross-correlation algorithm with the ECG signal stored at $T_i - 1$ time to judge the correlation degree. If x represents the signal sent at T_i time and y represents the signal sent at $T_i - 1$ time, the calculation formula of the cross-correlation function is as follows:

FIGURE 8: Time period.

$$R_{xy} = \frac{1}{n} \sum_{i=1}^n (w_1 x(\text{PR})y(\text{PR}) + w_2 x(\text{QRS})y(\text{QRS}) + w_3 x(T)y(T)). \quad (4)$$

Among them, $x(\text{PR})$ represents the data of the PR part at Ti time, $y(\text{PR})$ represents the data of the PR part at $Ti - 1$ time, and the other two represent data of the QRS and T part, respectively. $W1$, $W2$, and $W3$ represent three weight values, $W1 + W2 + W3 = 1$. n means averaging the data.

After getting the results of the cross-correlation algorithm, it is necessary to normalize the results in order to judge whether it is an emergency.

The average value of the signal $x(t)$ and $y(t)$ is calculated as follows:

$$\mu_x = \frac{1}{n} \sum_{i=1}^n (w_1 x(\text{PR}) + w_2 x(\text{QRS}) + w_3 x(T)), \quad (5)$$

$$\mu_y = \frac{1}{n} \sum_{i=1}^n (w_1 y(\text{PR}) + w_2 y(\text{QRS}) + w_3 y(T)). \quad (6)$$

The calculation of the variance value of the signal $x(t)$ and $y(t)$ is shown in the following equations:

$$\sigma_x^2 = \frac{1}{n} \sum_{i=1}^n \{(w_1 x(\text{PR}i) + w_2 x(\text{QRS}i) + w_3 x(Ti)) - \mu_x\}^2, \quad (7)$$

$$\sigma_y^2 = \frac{1}{n} \sum_{i=1}^n \{(w_1 y(\text{PR}i) + w_2 y(\text{QRS}i) + w_3 y(Ti)) - \mu_y\}^2. \quad (8)$$

The calculation of the correlation number is as follows:

$$\rho_{xy} = \frac{R_{xy} - \mu_x \mu_y}{\sqrt{\sigma_x^2} \sqrt{\sigma_y^2}}, \quad -1 \leq \rho_{xy} \leq 1. \quad (9)$$

The pseudocode of the cross-correlation algorithm is described as follows. (Algorithm 2)

3.3.3. Determination of the Correlation Coefficient. The correlation coefficient is determined according to each person's physical condition. Because each person's physical condition is different, the possible disease situation is not the same, and the correlation degree between normal ECG and

abnormal ECG is also different. For example, for patient A, when the similarity value is 0.8, it belongs to an abnormal condition, while for patient B, it may be normal. According to the different situations of each person, we plan to set the critical value of each person according to the characteristics of patients and get more accurate final results. According to the above description, it is necessary to set the unique critical value of the patient in each control node, judge whether the patient is in an emergency according to the critical value, and then perform the corresponding operation.

3.3.4. Safety Analysis. The formal security analysis of the mechanism's resistance to attack in an emergency mainly includes long-range attack, close attack, false signal attack, and misjudgment during movement.

(1) *Long-Range Attack.* For BAN, the protocol is sent by the sensor node to the control node within a safe distance by broadcasting. If the attacker is 2 meters away, there is no way to obtain the data, and the attack is invalid.

(2) *Close Attack.* Within 2 meters, the attacker can obtain the data and perform operations on the sensor node. When the patient is in an emergency, if the attacker is right beside him, there is a device that can collect data, and no doctor or witness, the attack is hard to be prevented. Otherwise, the attack is invalid.

(3) *False Signal Attack.* The attacker sends the wrong or tampered signal to the control node, and the control node requires the sensor node to broadcast the message within a safe distance. After the control node receives the message sent by the attacker, the alert function of the control node works after the operation, and the attack will not cause harm to the human body.

(4) *Misjudgment during Movement.* The cross-correlation algorithm compares the cross-correlation degree of the two ECG signal waveforms. No matter the frequency acceleration or the amplitude enhancement will not affect the waveform, so the judgment result is that the human body is still in the normal condition. When the human body is in a real emergency, the waveform of the ECG signal will change, and the waveform characteristics of five obvious points will disappear.

```

(1). //INPUT: ECG signals at  $Ti$  and  $Ti - 1$ 
(2). //OUTPUT: in normal/abnormal condition
(3). BEGIN
(4). IF the result of  $Ti$  executing the algorithm is emergency;
(5).   Select the ECG signal at  $Ti - 2$ ;
(6).   Use equation (4) to calculate the results of the cross-correlation algorithm of ECG signals at  $Ti - 2$  and  $Ti$ ;
(7).   Use equation (9) to calculate the cross-correlation coefficient;
(8). ELSE the result of  $Ti$  executing the algorithm is normal;
(9).   Select the ECG signal at  $Ti - 1$ ;
(10).  Use equation (4) to calculate the results of the cross-correlation algorithm of ECG signals at  $Ti - 2$  and  $Ti$  or  $Ti - 1$  and  $Ti$ ;
(11).  Use equation (9) to calculate the cross-correlation coefficient;
(12).  IF the error between  $\rho_{xy}$  and  $\rho_{xy}'$  is acceptable, threshold  $(\rho_{xy}, \rho_{xy}') > t'$ ;
(13).    The human body is in normal condition, the certification under normal condition shall be carried out;
(14).    ELSE the error between  $\rho_{xy}$  and  $\rho_{xy}'$  is not acceptable, threshold  $(\rho_{xy}, \rho_{xy}') > t'$  does not hold;
(15).    The human body is in an emergency, and the certification under emergency shall be carried out;
(16).  END IF
(17). END IF
(18). END

```

ALGORITHM 2: Judge whether it is an emergency.

3.4. Information Access Based on Node Security. The application of medical sensor equipment in the human body is more and more common. There may be several or even more than ten medical sensor equipment in a person's body, including heart beat measurement, blood pressure measurement, and blood glucose measurement; each medical sensor equipment has different requirements for safety. The risk level of medical sensor equipment is divided into three categories, and the greater the category number, the higher the risk [2, 28]. Because each doctor has his own department, it is impossible to obtain all the physiological data of patients, so it is necessary to set access rights for doctors. In the local area network of the human body, the data monitored by the medical sensor equipment is transmitted to the control node. Doctors can access the control node to obtain the required data. As long as it can authenticate with the control node successfully, the authentication of the two can be realized traditionally because they have no resource restriction, or the control node authorizes doctors to access the contents in the database. After the request message sent by the doctor reaches the control node, the control node queries the table stored by itself. If it is found that the doctor requests the data in the medical sensor device with a low-risk level, it will authenticate with the doctor. If the authentication is successful, the data stored by the control node will be sent to the doctor. If it is found that the doctor requests physiological information collected by the medical sensor device with a high-risk level, the control node finds that it has no right to make decisions and needs the medical sensor device to make its own decisions. The control node sends the data to the doctor with the consent of the medical sensor device. Because of the corresponding settings in the control node, the control node not only sends the data collected by the medical sensor device to the doctor but also transmits the data collected by other medical sensor devices with lower security level than the device, which the doctor has the right to access and helps make accurate medical decisions. The information access process is shown in Figure 9.

The pseudocode of the information access process based on the security level of the sensor node is given below. (Algorithm 3)

4. Simulation Implementation and Performance Evaluation

In order to evaluate and verify the authentication mechanism designed in this paper, the simulation is carried out based on OMNET++ in Windows [29]. Its underlying programming language is C++. The simulation results of OMNET++ have been gradually recognized, which provide an important basis for us to use OMNET++ for simulation. Among them, the ECG data set used in an emergency is processed by MATLAB.

4.1. Simulation Environment

4.1.1. Simulation of Functional Modules. In this paper, the network includes three roles: sensor node, phone, and doc. The sensor node is the medical sensor device worn by the human body. Different sensor nodes are used to collect different physiological data of the human body. In the process of authentication protocol implementation, it acts as an authenticated entity and authenticates whether the external receiving data device is an honest entity. phone, namely, control node, is used to send the physiological data of the human body sent by sensor nodes through the network. In the process of authentication protocol implementation, it is used as an authenticated entity and to authenticate whether the external receiving device is an honest entity. doc, that is, medical staff or other people who need physiological data. The information transmission mode between various sensor nodes and phone is wireless, while the information transmission mode between phone and doc is wired. The network model based on three roles is shown in Figure 10 (five sensor nodes).

FIGURE 9: Process of information access.

```

(1). //INPUT: request access to information.
(2). //OUTPUT: physiological information collected by nodes.
(3). BEGIN
(4). Doctors send request message  $M1$  to phone;
(5). phone certifies doctors according to DoctorID in the message;
(6). IF the certification is successful, judge the safety level of medical sensor equipment according to SensorID;
(7).   IF SensorID  $\in$  LowSecurity;
(8).     phone sends physiological messages collected by phone to doctors;
(9).   ELSE SensorID  $\in$  HighSecurity;
(10).    phone sends unable to process message Not Message to doctors;
(11).    After receiving the Not Message, the doctor sends the request message  $M2$  to phone again;
(12).  END IF
(13).  phone judges the state of the human body according to Algorithm 2;
(14).  IF the human body is in the normal state, execute Algorithm 1 for authentication;
(15).    IF the authentication is successful, phone looks up the authority table and sends the information;
(16).    ELSE Authentication failed;
(17).  END IF
(18).  ELSE the human body is in an emergency;
(19).    Send physiological information to phone within safe distance;
(20).  END IF
(21).  ELSE Authentication failed. No message will be sent.
(22).  END IF
(23). END

```

ALGORITHM 3: Information access process based on the security level of sensor node.

FIGURE 10: Network model.

4.1.2. Message Design. In OMNET++, messages are represented by the `cMessage` class and `cPacket` class, where `cPacket` is a subclass of `cMessage`. In this experiment, messages are mainly used for data transmission. Table 2 shows the message files used in the simulation process.

4.1.3. Statistical Analysis of Results. Table 3 shows the various statistical signals involved in the simulation process. After the simulation, we can get the statistical results of these signals, and we can evaluate the network performance according to these results.

4.2. Simulation Results and Analysis

4.2.1. Topology Use Case. Table 4 shows the settings of simulation parameters. In OMNET++, simulation parameters are set by the configuration file `omnetpp.ini`, including CPU running time, simulation time, and network topology usage type. When only the parameters set in the configuration file are changed without modifying other files in the project, new simulation results can be obtained without deploying the project. Among them, there are three kinds of network scenarios, including 5 sensor nodes, 10 sensor nodes, and 15 sensor nodes in the network.

4.2.2. Performance Evaluation

(1) Normal Performance Evaluation. Because the design of this paper is an authentication mechanism and the design goal is lightweight, then how to prove security and lightweight is the focus of our performance evaluation, which conforms to the characteristics of the integrated domain network resource constraints and high security requirements of BAN, and the performance evaluation of the authentication mechanism in the BAN should focus on resource overhead and security. For the evaluation of network performance, the end-to-end delay and packet loss rate are selected to verify the correctness of the parameter setting.

(2) Normal Performance Evaluation (End-to-End Delay). End-to-end delay refers to the average time of packets from the source node to destination node in BAN, which is calculated as $EED = (\sum_{i=1}^n (T_{receive_i} - T_{send_i})/n)$. Among them, T_{send_i} and $T_{receive_i}$ represent the sending time and receiving time of the packet i , respectively, and n represents the number of i packets. The delay time increases with the number of nodes. The delay time is 0.0168 ms when 5 sensor nodes, 0.0183 ms when 10 sensor nodes, and 0.0196 ms when 15 sensor nodes are set in BAN. The reason for this situation is that when the number of nodes increases, the number of information exchange in the network increases. Too much information exchange leads to network congestion, and the blocked network will naturally lead to the increase of information exchange time, that is, the end-to-end delay time.

(3) Normal Performance Evaluation (Packet Loss Rate). Packet loss rate refers to the ratio between the number of

packets lost and the number of packets sent during the operation of the BAN, which is calculated as $PLR = 1 - (N_{receivepkt}/N_{totalpkt}) \times 100\%$. $N_{receivepkt}$ and $N_{totalpkt}$ represent the number of received and sent packets, respectively. The packet loss rate increases with the number of nodes. When the number of sensor nodes in the BAN is 5, the packet loss rate is 2%. When the number of sensor nodes in the BAN is 10, the packet loss rate is 9%. When the number of sensor nodes in the BAN is 15, the packet loss rate is 14%. The reason for the above situation is that, with the increase of the number of nodes, the number of information exchange and transmission between nodes increases. A large quantity of information is transmitted in the network, and the delay time increases, resulting in the packet loss due to the long time of transmission to the receiving end or not to the receiving end. At the receiving end, when a large number of data packets are transmitted, the receiving end may not be able to process these data packets in time due to some restrictions or other reasons and may also have the phenomenon of packet loss.

(4) Normal Performance Evaluation (Storage Overhead). In the authentication protocol, in order to get different random numbers by using a pseudorandom generation sequence, we set up the initial seed and butterfly seed generation algorithm. In the butterfly seed generation algorithm, in order to get different seeds, a parameter is set, and the value of j needs to be saved in real time. Its type can be an integer, and the size of the integer is generally 2 byte, that is, 16 bits. In addition, it is necessary to save an initial seed and then transform the seed randomly, which is unpredictable. The size of the initial seed and control nodes is 640 bits. Both the receiver and the sender need to store this initial seed. The receiver has only one device, while the sender is multiple sensor nodes in the network. This value can be set to n . In this paper, the values of n are 5, 10, and 15, respectively. So, the storage overhead can be expressed as $640(n + 1) + 16$.

(5) Normal Performance Evaluation (Communication Overhead). Communication overhead refers to the size of messages transmitted between two entities. Both sender and receiver need to send encryption and acknowledgment messages to the receiver. The size of the encrypted message is 640 bits, and the confirmation message is a string of authentication success or failure, with the size of 96 bits. In conclusion, the communication overhead is 1472 bits, in which both the communication overheads of control nodes and sensor nodes are $640 + 96$ bits.

(6) Normal Performance Evaluation (Computational Overhead). In the authentication protocol, the computation of sensor nodes includes the execution of hardware PUF, XOR operation, encryption, Hamming distance, seed generation, and pseudorandom sequence generator. The total calculation time of these operations is about 0.28 ms. The calculation of the receiver includes XOR operation, decryption, seed generation algorithm, Hamming distance, and reading data from the cloud and pseudorandom sequence generator. The total calculation time of these operations is about 2.91 ms.

TABLE 2: Message files in the simulation.

Message files	Description
α .msg	Authentication message
β .msg	Authentication message
endRxEvent	Self-information
MessagePhysical.msg	Physiological information
MessageEmergency.msg	Emergency information
MessageAuth.msg	Confirmation message
MessageMerger.msg	Merged message

TABLE 3: Statistical signal.

Statistical signal	Function
endToEndDelaySignal	End-to-end delay
packetLossRate	Packet loss rate
pkCount	Packets received
pkNumber	Packets sent
pkTime	Packet transfer time
compTime	Computing time

TABLE 4: The setting simulation parameters.

Parameters	Values
Simulation time	300 s
Scene size	3 m*3 m
Network scenarios	I:5 sensor nodes
	II:10 sensor nodes
	III:15 sensor nodes
Transmission speed	40 kbps
Interval time	Exponential 2 s
Packet size	640 bits
Delay time	10 ms

(7) *Normal Performance Evaluation (Energy Cost)*. Ideally, the longer a medical sensor device is worn on or implanted into the human body, the better, so the lower the energy consumption, the better. When a 32-bit Cortex-M3, 72 MHz microcontroller is active at 27°C, it requires 36 mA current and 36 V voltage, and the electric power is about 118.8 mW [30]. According to the above situation, the corresponding energy consumption can be calculated by reusing the calculation cost. Assuming that the computation cost is t (ms), the energy consumption is $118.8 t/1000$. The calculation cost of this paper is about 3.19 ms, so the energy cost is 0.379 mJ. The energy cost of control nodes is 0.346 mJ, and the energy cost of sensor nodes is 0.033 mJ.

(8) *Performance Evaluation in Emergency (ECG Signal Data Set)*. The ECG signal data set used in this experiment is from the PhysioBank database, which is a large scientific research resource database mainly based on ECG signals and supplemented by other data such as magnetic resonance imaging (MRI) [31]. The ECG database in PhysioBank records the physiological signals of healthy people and patients. Each person's record consists of three files, which are data file (also known as binary file, suffix is .dat), annotation file (suffix is .atr), and header file (suffix is .hea). PhysioNet

FIGURE 11: ECG signal of wfdbdemo.m.

provides a toolkit WFDB for developers to use in the development process. With WFDB, we can connect the data on PhysioNet with MATLAB development software so that we can get the data we want in MATLAB. Figure 11 is the ECG signal diagram obtained by executing the demo file after WFDB is configured successfully in MATLAB. It is the ECG signal diagram with the number 105.

(9) *Performance Evaluation in Emergency (Performance Analysis)*. In this paper, the improved cross-correlation algorithm is implemented in MATLAB; there are two methods to use, one is to use the function expression of the data set, the other is to use the specific value of the data set, and then form the vector sequence according to the specific value. Since there is no fixed function expression for the ECG signal of the human body, this paper chooses the second method. Through the calculation of the cross-correlation algorithm and normalization operation, we hope to get the required cross-correlation coefficient, that is, the value of ordinate in the graph, and the maximum ordinate value in the graph is the result we want. The results obtained by the cross-correlation algorithm are shown in Figures 12–14.

The ECG signals selected in Figure 12 are the data from the subject 100 on the website, which shows the correlation number of the subject 100 in two different periods. It can be seen from the figure that the cross-correlation coefficient is closer to 1 after the weighted processing of the ECG signal, and the result is the same as expected, which also achieves the purpose of improving the cross-correlation algorithm and improving the accuracy of identification.

The ECG signals selected in Figure 13 are normal and abnormal data from the subject 100 on the website. It can be seen from the figure that there is a certain distance between the maximum value of the normal ECG signal and the abnormal ECG signal obtained by the improved cross-correlation algorithm, so this method can easily identify the abnormal ECG signal. When people's body is suddenly abnormal, it can be relatively easy and accurate to judge the abnormal situation and make the correct response to the abnormal situation so that the human body can be treated in time.

FIGURE 12: Comparison figure of weighted 100 and 100 and unweighted 100 and 100.

FIGURE 13: Comparison figure of weighted 100 and 100 and weighted 100 and exception 100.

FIGURE 14: Comparison figure of weighted 100 and 100 and weighted 100 and 105.

The selected ECG signals in Figure 14 are ECG data from subjects 100 and 105 on the website. It can be seen from the figure that if an attacker uses another person's ECG signal to impersonate the party's ECG signal and attempts to muddle through and destroy the normal operation of the authentication mechanism, it is obviously not feasible because it is easy to be found.

4.2.3. Benchmark Mechanism. One of the benchmark mechanisms selected in this paper is the effective anonymous authentication mechanism based on the elliptic encryption algorithm (ECC-based) [32]. This mechanism ensures the security of BAN by improving the traditional security methods. It is a classic scheme to solve the security problems of BAN by using the traditional security methods and has certain representativeness in solving the security problems of BAN.

In this mechanism, there are three roles: control node (client), third-party entity (nm), and sensor node (AP). The sensor node collects and sends the physiological data of the human body; the control node can obtain the collected physiological data and send it to the doctor for treatment; the main task of the third-party entity is to generate the required private key.

The mechanism is divided into three phases: initialization phase, registration phase, and authentication phase. In the initialization phase, the third party is responsible for generating the required system parameters. In the registration stage, the control node and the third party establish a legal relationship through certain measures so that the control node becomes a legal node. When the control node operates again next time, it can be known that it is a legal node that has passed the authentication. In the authentication stage, the control node can obtain the service it needs from the common node after passing the authentication. The running process of the ECC mechanism is shown in Figure 15.

Another benchmark mechanism selected in this paper is based on simple cryptographic primitives (HASH-BASED) [30]. The mechanism is divided into three stages: initialization stage, authentication and key sharing stage, and joining sensor node stage. In the initialization stage, before the deployment of sensor nodes and control nodes, the third party will perform some operations, which include generating a master key that can be used by the control node for a long time and assigning a unique identification number to the sensor node. In the stage of authentication and key sharing, the sensor node and the control node can judge whether the other party is a trusted entity by using the designed mechanism, and the public session key established in this process is saved by both parties for safe use in future communication. In the dynamic joining stage, the third-party entity assigns a unique identification number to the new sensor node, calculates its key, checks the vector value, stores tuples, and then deploys it to the corresponding location and notifies the control node.

4.2.4. Performance Comparison. Through the performance analysis of the authentication mechanism in an emergency,

FIGURE 15: The operation process of the ECC mechanism.

we can see that the authentication mechanism designed in this paper can make a good response when the emergency needs to be handled. The performance of the improved cross-correlation algorithm is better, the cross-correlation coefficient calculated by the improved algorithm is more accurate, and the probability of misjudgment is reduced. Most of the previous studies do not consider the emergency, but the design of this paper comprehensively considers each situation so that it can make different responses to different situations so that the BAN can play a better role.

By comparing the performance of PUF-BASED in terms of resource consumption and security with the benchmark mechanisms, Table 5 shows the communication overhead, computational overhead, and energy consumption of PUF-BASED, HASH-BASED, and ECC-BASED.

Table 6 shows the different security categories that can be guaranteed by the design scheme and comparison mechanism. It can be seen from the table that although the design schemes are different, they can resist certain security attacks. However, the security categories guaranteed by different schemes are different. It cannot simply indicate which scheme has better security performance. It can only be said that the scheme in this paper can resist a certain degree of attacks, and the security performance is guaranteed. It can be seen from the table that the scheme in this paper can resist eavesdropping tampering attack, replay attack, middleman attack, and simulation attack and has forward/backward security. The ECC-BASED authentication scheme can resist eavesdropping tampering attack, replay attack, and middleman attack and has elastic recovery ability. The HASH-BASED authentication scheme can resist eavesdropping tampering attack, replay attack, middleman attack, and simulation attack and has forward/backward security and elastic recovery ability.

From the above analysis, it can be seen that the mechanism of this paper has certain advantages over the improved traditional security methods in terms of both resource consumption and security performance. In this paper, the design does not use symmetric encryption or asymmetric encryption method; nor does it make use of the characteristics of large numerical value, large quantity, and difficult calculation to ensure security, such as the elliptic curve encryption algorithm takes advantage of the difficulty of numerical calculation; and, there is no particularly tedious calculation, so the effect of resource consumption is better. In addition, the authentication mechanism designed in this paper comprehensively considers the security problems in various situations, so it has good security performance.

TABLE 5: Resource consumption of different authentication mechanisms.

		Communication overhead (bits)	Computational overhead (ms)	Energy consumption (mJ)
PUF-BASED	Control nodes	1472	2.91	0.379
	Sensor nodes		0.28	
HASH-BASED	Control nodes	1120	0.48	0.093
	Sensor nodes		0.3	
ECC-BASED	Control nodes	1856	26.46	4.73
	Sensor nodes		13.35	

TABLE 6: Safety performance of different authentication mechanisms.

	Eavesdropping tampering attack	Replay attack	Forward/ backward security	Nonclonability	Middleman attack	Simulation attack	Elastic recovery ability
PUF-BASED	✓	✓	✓	✓	✓	✓	—
HASH-BASED	✓	✓	✓	—	✓	✓	✓
ECC-BASED	✓	✓	—	—	✓	—	✓

However, the mechanism designed in this paper is not as good as the mechanism designed with simple cryptographic primitives in terms of total computing cost and energy consumption. This is because this paper introduces the cloud database to store a large amount of data, so as to reduce the consumption of local resources. Therefore, there are operations of reading and writing data, which will increase the computing cost of the control node and then increase the energy consumption. However, the computational cost of the mechanism designed in this paper is slightly lower than that of the authentication mechanism designed with cryptographic primitives, so it can reduce the resource consumption of the sensor node and prolong its service life. In terms of security performance, the mechanism designed in this paper is similar to that designed with cryptographic primitives.

In the process of its implementation, there may be the following challenges and limitations. In terms of possible challenges, firstly, this paper mentions that, in an emergency, a certain characteristic signal of each individual is used as a way to judge whether it is safe. Because there is no personal data in the early stage or there may be a lack of data due to various reasons such as the network, the use in the early stage and when the network is poor may not reach the ideal state. Second, it is mentioned in the article that the cloud database is used to store a large amount of data, and the data should be kept confidential. At present, this kind of cloud database needs to pay, so how to effectively reduce the cost is a certain challenge. In terms of possible limitations, one is that the network topology of this scheme is limited to star topology, and other topologies have not been considered. Although star topology is widely used at present, other topologies have been studied in some papers. Second, the current emergency use of the ECG signal as a method of using instructions; in real cases, there will be other physiological characteristics of data; for different physiological characteristics of data, we can further select its data feature points as function parameters.

5. Conclusions

By analyzing the communication model, security and performance requirements, as well as various existing authentication methods, this paper explains the importance of a lightweight authentication mechanism for BAN. As for the design of the authentication mechanism under normal conditions, according to the characteristics of PUF, the mutual authentication mechanism between the sensor node and control node is designed by using the challenge response generated by the function. In case of emergency, patients need timely treatment, and the demand for timely treatment is much higher than safety. Given this situation, the improved cross-correlation algorithm is used to judge whether the human body is in an emergency; if so, broadcast the data to get timely and effective treatment. Different data access methods are designed according to the security level of medical sensor devices, and the designed authentication mechanism is simulated by using the OMNET++ simulation platform, and the results are compared and analyzed with the comparison mechanism. The experimental results show that the authentication mechanism designed in this paper has good effects in four aspects: computing cost, communication cost, energy consumption, and security.

The lightweight identity authentication mechanism proposed in this paper mainly includes two parts: one is to design the authentication mechanism under normal circumstances; the other is to design the authentication mechanism in an emergency, and according to the authentication, the information access method based on the node level is designed, but there are still some shortcomings. This paper uses the mature and representative star topology. This topology can be further studied in the future. In the aspect of simulation, the simulation of BAN should use real sensors with a simulation platform to achieve so that the simulation results will be more accurate. In the evaluation of security and resource consumption, this paper analyses these two aspects separately and then

compares them with other methods. BAN requires high security performance and low resource consumption, so as to achieve a balance between them. In the future, we will further consider the comprehensive analysis of security and resource consumption.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This study was supported by the Beijing Social Science Foundation Key Project (18GLA009), Beijing The Great Wall Scholars' Program (no. CIT & TCD20170317), and Beijing Intelligent Logistics System Collaborative Innovation Center Open Topic (no. BILSCIC-2019KF-03) and funded by the Graduate Science and Technology Innovation Project of Capital University of Economics and Business.

References

- [1] P. Kumar and H. J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: a survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.
- [2] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security challenges for medical devices," *Communications of the ACM*, vol. 58, no. 4, pp. 74–82, 2015.
- [3] E. Jovanov, D. Raskovic, J. Price et al., "Patient monitoring using personal area networks of wireless intelligent sensor," *Biomedical Sciences Instrumentation*, vol. 37, pp. 373–378, 2001.
- [4] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. M. Leung, "Body area networks: a survey," *Mobile Networks and Applications*, vol. 16, no. 2, pp. 171–193, 2011.
- [5] M. Rushanan, A. D. Rubin, D. F. Kune et al., "SoK: security and privacy in implantable medical devices and body area networks," in *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, pp. 524–539, Berkeley, CA, USA, May 2014.
- [6] S. Faye, N. Louveton, G. Gheorghe et al., "A two-level approach to characterizing human activities from wearable sensor data," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 7, no. 3, pp. 1–21, 2016.
- [7] M. Kumar, "Security issues and privacy concerns in the implementation of wireless body area network," *Food Policy*, vol. 34, no. 3, pp. 245–251, 2015.
- [8] S. Aram, R. A. Shirvani, E. G. Pasero et al., "Implantable medical devices; networking security survey," *Journal of Internet Services and Information Security*, vol. 6, no. 3, pp. 40–60, 2016.
- [9] A. Singla and R. Sachdeva, "Review on security issues and attacks in wireless sensor networks," *International Journal of Future Generation Communication & Networking*, vol. 8, no. 4, pp. 81–88, 2015.
- [10] C. Gritti, M. Onen, R. Molva et al., "Device identification and personal data attestation in networks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 9, no. 4, pp. 1–25, 2018.
- [11] N. Nguyen, C. A. Y. Kaya, A. Bru"Sch et al., "Demo of BANDANA-body area network device-to-device authentication using natural gAit," in *Proceedings of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 421–423, San Jose, CA, USA, July 2018.
- [12] H. Anada, "Decentralized multi-authority anonymous authentication for global identities with non-interactive proofs," *Journal of Internet Services and Information Security*, vol. 10, no. 4, pp. 23–27, 2020.
- [13] E. M. Torroglosa-Garcia and A. F. Skarmeta-Gomez, "Towards interoperability in identity federation systems," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 8, no. 2, pp. 19–43, 2017.
- [14] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: new directions for implantable medical device security," in *Proceedings of the USENIX Workshop on Hot Topics in Security*, San Jose, CA, USA, July 2008.
- [15] D. Halperin, T. S. Heydt-Benjamin, B. Ransford et al., "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses," in *Proceedings of the 2008 IEEE Symposium on Security and Privacy (Sp 2008)*, pp. 129–142, Oakland, CA, USA, May 2008.
- [16] Y. S. Lee, H. J. Lee, and E. Alasaarela, "Mutual authentication in wireless body sensor networks (WBSN) based on physical unclonable function (PUF)," in *Proceedings of the 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1314–1318, 2013.
- [17] B. Ovilla-Martinez, A. Díaz-Pérez, and J. J. Garza-Saldaña, "Lightweight mutual authentication among sensors in body area networks through physical unclonable functions," in *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, Paris, France, May 2017.
- [18] P. Steffen, P. R. Bhanu, M. Farshad et al., "Design of secure ECG-based biometric authentication in body area sensor networks," *Sensors*, vol. 16, no. 4, p. 570, 2016.
- [19] C. Hu, X. Cheng, F. Zhang et al., "OPFKA: secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," *2013 Proceedings IEEE INFOCOM*, pp. 2274–2282, 2013.
- [20] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): authentication for implanted medical devices," in *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 1099–1112, Berlin, Germany, November 2013.
- [21] J. Wan, C. Zou, S. Ullah, C.-F. Lai, M. Zhou, and X. Wang, "Cloud-enabled wireless body area networks for pervasive healthcare," *IEEE Network*, vol. 27, no. 5, pp. 56–61, 2013.
- [22] H. Liu, Y. Chen, H. Liu et al., "An efficient cloud-assisted message authentication scheme in wireless body area network," *International Journal of Security and Its Applications*, vol. 11, no. 3, pp. 71–80, 2017.
- [23] C.-M. Yu, C.-Y. Chen, and H.-C. Chao, "Verifiable, privacy-assured, and accurate signal collection for cloud-assisted wireless sensor networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 48–53, 2015.
- [24] R. Sampangi and S. Sampalli, "Butterfly encryption scheme for resource-constrained wireless networks," *Sensors*, vol. 15, no. 9, pp. 23145–23167, 2015.
- [25] E. Nigussie, T. Xu, and M. Potkonjak, "Securing wireless body sensor networks using bijective function-based hardware

- primitive,” *IEEE Tenth International Conference on Intelligent Sensors*, pp. 1–6, 2015.
- [26] C. Liu, P. Cronin, and C. Yang, “A mutual auditing framework to protect IoT against hardware Trojans,” in *Proceedings of the Asia & South Pacific Design Automation Conference*, pp. 69–74, Macao, Macao, January 2016.
 - [27] C. Gritti, W. Susilo, and T. Plantard, “Certificate-based encryption with keyword search: enabling secure authorization in electronic health record,” *Journal of Internet Services and Information Security*, vol. 6, no. 4, pp. 1–34, 2016.
 - [28] “Medical device-Classify your medical device,” *Food and Drug Administration*, <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/default.htm>, 2020.
 - [29] J. Y. Wang, Y. H. Wei, H. B. Qiu et al., *Network Simulator OMNeT++*, Xidian University Press, Xi’an, China, 2014.
 - [30] M. H. Ibrahim, S. Kumari, A. K. Das et al., “Secure anonymous mutual authentication for star two-tier wireless body area networks,” *Computer Methods & Programs in Biomedicine*, vol. 135, p. 37, C, 2016.
 - [31] A. L. Goldberger, L. A. N. Amaral, L. Glass et al., “PhysioBank, PhysioToolkit, and PhysioNet,” *Circulation*, vol. 101, no. 23, pp. e215–e220, 2000.
 - [32] Z. Zhao, “An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem,” *Journal of Medical Systems*, vol. 38, no. 2, pp. 1–7, 2014.