A Secure and Reliable Data Transmission Scheme in Wireless Body Area Network

Huaijin Liu, Yonghong Chen, Hui Tian, Tian Wang, and Yiqiao Cai

(Corresponding author: Yonghong Chen)

College of Computer Science and Technology, Huaqiao University
Xiamen 361021, China
(Email: lhjhqdx@163.com)

(Received Jan. 5, 2018; Revised and Accepted Apr. 21, 2018; First Online Mar. 9, 2019)

Abstract

In view of the privacy protection and shadow effect of wireless body area network (WBAN), we propose a secure and reliable data transmission scheme. In the first place, on the basis of the characteristics of WBAN, we propose a reasonable relay transmission strategy, which uses the time-varying model to model the channel and select the relay node based on the principle of load balancing, to solve the problem of how reasonable and efficient use of relay nodes, thus improving the energy efficiency of relay transmission. In addition, in order to solve the problem of secure transmission of physical data in WBAN, a new authentication and key agreement protocol is proposed. Through in-depth analysis, it is verified that the proposed scheme conforms to the highest security level defined by IEEE 802.15.6 body area network standard, which can ensure the confidentiality and integrity of information while satisfying the demand of data reliability, and has high application value.

Keywords: Load Balancing; Privacy Protection; Reliability; Time-Varying Model; Wireless Body Area Network

1 Introduction

In recent years, with the rapid development of wireless communications, micro-sensor equipment and artificial intelligence, an emerging, human-centered wireless sensor network-wireless body area network (WBAN) came into being. WBAN is mainly composed of a variety of sensor nodes attached to the human body that continuously perceive human physiological data and a coordinator that collects and processes various perceived data.

Due to the asymmetry between the coordinator and the sensor nodes, a standard single-hop star topology is widely used in traditional WBAN. However, in the actual situation, the human body will cause the wireless link between the sensor node and the coordinator to be blocked, resulting in reduced data transmission reliability. In order to reduce the shadow effect of the human body on the channel, the use of relay transmission mechanism can greatly reduce the link outage probability.

However, the introduction of a relay transmission mechanism will bring additional energy overhead, which will further shorten the lifetime of WBAN. Therefore, how to use the relay node reasonably and efficiently is great importance to improve the energy efficiency of relay transmission. In addition, WBAN in the transmission of data, security is also very important. Since the data transmitted by WBAN are physiological parameters that are closely related to the human body, the confidentiality and integrity of the data are indispensable.

In order to ensure the reliability and security of data transmission in WBAN, we propose a secure and reliable data transmission scheme for WBAN. The main contributions of the scheme are the following:

1) Using the time-varying model to establish the wireless human body channel, according to the time-varying prediction model to determine whether the sensor node needs to allocate the relay node, to solve the problem of relay timing judgment.

2) A relay transmission strategy based on load balancing is proposed to solve the problem of relay node selection and improve the energy efficiency.

3) According to the transmission mode of different links, this paper proposes a new authentication and key agreement protocol, which solves the problem of data security transmission.

The rest of this article is organized as follows. Section 2 reviews the related work. Section 3 describes the system model and design goals. Section 4 presents this proposed safety and reliability scheme. Section 5 describes the safety analysis, and Section 6 describes the simulation results. Summarized in Section 7.

2 Related Work

A large number of personal data collected by WBAN are important information about the security and privacy of users, and it is of great significance to explore how to ensure that these data are transmitted securely to the relevant medical institutions. In the literature [3,19], the security requirements of WBAN are analyzed, and the security objectives of WBAN system are mainly to ensure the confidentiality, integrity, authenticity and freshness of the data. Because the sensor nodes have strict low power limits, it is challenging to meet these security requirements. If the use of complex security encryption measures, will inevitably lead to excessive energy consumption, and easy to affect the normal communication of the sensor nodes. IEEE 802.15.6 body area network standard defines a multi-level security level of communication, each of which corresponds to a different level of protection and frame format [15]:

1) Level 0: Unsafe communication, no data is authenticated during communication, and no integrity protection;

2) Level 1: Only authentication, data transmission in the security authentication mode, but the data is not encrypted;

3) Level 2: Authentication and encryption, which is the highest security level of communication mode. In order to ensure the safe transmission of data, the literature [28,30] through asymmetric encryption technology to encrypt the data, but these schemes have high computational complexity, not suitable for WABN. Literature [13,16] proposed a number of lightweight security encryption scheme, which can effectively ensure the safe transmission of private data, but these methods require a large storage space and does not meet the reliability of the data. In addition, in order to resist the presence of attacks in WBAN, the literature [9,20] proposed to use the time-varying human physiological signal to establish the symmetric key, reduces the key management of symmetric encryption algorithm, but this method is limited to the human body sensor symmetry of the network topology.

On the other hand, the traditional WBAN usually uses the standard star topology to transmit the data, but in the actual process, because of the shadow effect of the human body structure, in the signal transmission process will cause great path loss [2,23]. In order to optimize the topology of WBAN, the relay nodes can be introduced into the network to improve the reliability of data. Gorce *et al.* [10] conducted a theoretical study on the reliability of relay transmission mechanism in WBAN, and then compared the relay transmission mechanism with the single-link transmission mechanism and the two-hop transmission mechanism respectively. It is proved that WBAN adopts relay transmission mechanism can be more effective than the other two mechanisms to improve reliability. Errico *et al.* [6] proposed a performance evaluation method of relay transmission mechanism for WBAN, and based on the measured data of the wireless human body channel under the daily activities of the human body, it is proved that relay transmission mechanism can greatly reduce the link outage probability. However, the literature [6,10] does not give the specific implementation strategy of relay transmission in WBAN. Abbasi *et al.* [1] proposed a relay transmission strategy to improve the reliability of WBAN. The strategy uses a dynamic contention-based relay node selection mechanism, that is, the first relay node that makes feedback on the request from the source node is selected as the relay node of the source node. The results show that the strategy can effectively improve the reliability of transmission while reducing the delay. Hara *et al.* [12] also proposed a relay transmission strategy to improve the communication reliability of WBAN. This strategy is based on the principle of ?low interrupt correlation? to make a more reasonable choice of relay nodes. The results show that this kind of relay node selection method can improve the reliability in the weaker dynamic scenario. Although the research [1,12] proposed a specific relay transmission strategy for WBAN, they only verified the reliability of the strategy and did not examine the energy efficiency of the strategy. The study [18] evaluated the energy consumption of the proposed relay transmission strategy and found the high energy consumption problem of the relay node, but did not give the corresponding solution to the problem.

By analyzing and summarizing the above research results, we can see that only symmetric encryption technology is suitable for WBAN sensor nodes with low power consumption and limited storage resources. In addition, the main reason for the high energy consumption of relay nodes is that the relay nodes are not allocated reasonably in the relay transmission process. Therefore, in this paper, we propose a load balancing based relay transmission strategy to solve the problem of high energy consumption of relay nodes. At the same time, combined with the proposed authentication and key agreement mechanism, it provides the security guarantee for data transmission.

3 System Models and Design Goals

3.1 Network Model

WBAN mainly includes intra-body and extra-body two parts of the application structure, as shown in Figure 1. In this paper, we mainly study the safety and reliability of intra-body network. The intra-body part is mainly composed of a coordinator and each sensor node attached to the human body surface. Each sensor node continuously senses physiological information and periodically transmits the perceived data to the coordinator. The co-

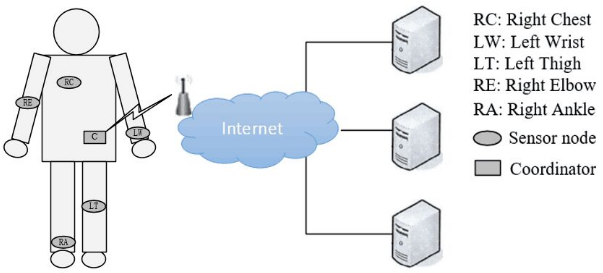


Figure 1: Wireless body area network application structure diagram

ordinator is responsible for collecting the data perceived by each sensor node and then processing and transmitting the data to the external network. The extra-body part mainly includes base stations, communication networks and remote servers. The coordinator sends the collected physiological information to the base station in extra-body, and the base station sends the information to the remote storage server through the external network.

3.2 Channel Model

In the study, based on the recommendation of the IEEE 802.15.6 Working Group [8], we use the time-varying model [5] to model the channel. The short-term average channel gain $\bar{G}(n)$ is a random variable that describes the slow fading characteristics of channel due to the human shadow effect. Based on the statistical analysis of a large number of measured channel gains, it is proved that the short-term average channel gain $\bar{G}(n)$ follows the normal distribution:

$$\bar{G}(n)\ |_{dB}\sim N(\mu_{\mathbb{S}},\sigma_{\mathbb{S}}^2). \quad (1)$$

Where $\mathbb{S}$ is a specific application scenario, $\mu_{\mathbb{S}}$ and $\sigma_{\mathbb{S}}^2$ are the mean and standard deviation for the specific scenario, respectively. Assume that the link between the sensor nodes S_i and S_j is denoted as S_{ij} and the short-term average channel gain of the link is represented by the random variable $\bar{G}_{ij}$. The random variables $\bar{G}_{ij}(m_i)$ and $\bar{G}_{ij}(m_i+k)$ represent the average channel gain of the link in slot m_i and slot m_i+k, respectively. According to Equation (1), the two random variables are Normal distribution:

$$\bar{G}_{ij}\ |_{dB}\sim N(\mu_{ij},\sigma_{ij}^2), \bar{G}_{ij}(m_i+k)\ |_{dB}\sim N(\mu_{ij},\sigma_{ij}^2). \quad (2)$$

Due to the temporal autocorrelation of the channel, there is a certain temporal correlation between the two variables, so their joint probability distributions can be expressed as follows:

$$\begin{aligned}(\bar{G}_{ij}(m_i),\bar{G}_{ij}(m_i+k))\ |_{dB}&\sim N(\mu_{ij},\mu_{ij},\sigma_{ij}^2,\sigma_{ij}^2,\rho_{ij}(k)),\\ \rho_{ij}(k)&=\frac{E\{[\bar{G}_i(m_i)-\mu_{ij}][\bar{G}_i(m_i+k)-\mu_i j]\}}{\sigma i j^2}\end{aligned} \quad (3)$$

We call Equation (3) denote the time-varying model, where $\rho_{ij}(k)$ represents the correlation coefficient between $\bar{G}_{ij}(m_i)$ and $\bar{G}_{ij}(m_i+k)$. Under the premise of known $\bar{G}_{ij}(m_i)$, the probability distribution of the random variable $\bar{G}_i(m_i+k)$ can be obtained by further derivation:

$$\begin{aligned}\bar{G}_i(m_i+k)\ |_{dB}\sim N((1-\rho_i(k))\cdot\mu_i+\rho_i(k)\cdot\bar{G}_i(m_i),\\ (1-\rho i^2(k))\sigma_i^2).\end{aligned} \quad (4)$$

Equation (4) shows that the outage probability $Pout_i(m_i+k)$ in the next transmission slot can be predicted based on the channel state $\bar{G}_i(m_i)$ in the current time slot:

$$\begin{aligned}Pout_i(m_i+k)&=Prob(\bar{P}_i(m_i+k)<\bar{P}^*)\\ &=Prob(\bar{G}_i(m_i+k)+P_t<\bar{P}^*)\\ &=Prob(\bar{G}_i(m_i+k)<\bar{G}^*)\\ &=\int_{-\infty}^{\bar{G}^*}f(\bar{G}_i(m_i+k))d\bar{G}_i\\ &=\phi(\frac{\bar{G}^*-(1-\rho_i(k))\cdot\mu_i-\rho i(k)\cdot\bar{G}_i(m_i)}{\sqrt{(1-\rho i^2(k))}\cdot\sigma i})\end{aligned} \quad (5)$$

We call Equation (5) denote the time-varying prediction model, where $\bar{P}_i(m_i+k)$ represents the average received signal power, $\bar{P}^*$ represents the predefined receive power threshold, $\bar{G}^*$ is expressed as the link interrupt threshold, and satisfies $\bar{G}^*=\bar{P}^*-P_t$, $f(\bar{G}_i(m_i+k)$ denotes the probability density function of $\bar{G}_i(m_i+k)$, and $\phi(\cdot)$ denotes the standard normal distribution function.

3.3 Threat Model

Because of the openness of wireless communication and the importance of transmitting information, WBAN is vulnerable to attack. These security threats are mainly from the following attacks.

Eavesdropping attacks: Since the openness of wireless channel transmission, so the attacker can eavesdrop any messages transmitted between nodes and obtains sensitive or valuable information by analysis.

Tampering attack: An attacker can remove or replace the eavesdropping message, and then send the tampered message to the original recipient to achieve some illegal purpose.

Camouflage attack: If the attacker eavesdropped to the legitimate sensor node or coordinator identity information, then he can be disguised as a legal node through the identity information to deceive.

Replay attack: The attacker to use network monitoring or other ways to steal data packets and resend a destination host has received packets, to achieve the purpose of deception system.

Man-in-the-middle attack: The attacker use a variety of technologies to intercept network data flow, and then to steal the information and illegal tampering, thus deceiving both ends of the authorized client.

Denial of service attack: An attacker sends a large number of packets to consume the network bandwidth and resources of the target server so that it can run out of power and can not continue to work.

3.4 Design Goals

In WBAN, because of the particularity of node structure, the particularity of function and the particularity of its application environment, WBAN not only to meet the basic security objectives of the network, but also to ensure the reliability of the data. A secure and reliable WBAN architecture should be able to provide the following services.

Data reliability: Due to the particularity of the wireless human channel, the human body's own blocking effect on the wireless channel will lead to a strong shadow effect, thus reducing the arrival rate of data packets, affecting the reliability of data.

Data confidentiality: Patient information in the transmission process should be encrypted, can not directly to the user's privacy information leaked to internal or external users.

Data integrity: If there is no relevant security mechanism to protect the integrity of the data, the attacker is easy to tamper with or forge the original data segment to destroy the integrity of the data.

Authentication: Since the coordinator collects the perceptual information from each sensor node in the body, the coordinator must have the ability to validate the data source.

4 The Proposed Scheme

In this section, we propose a secure and reliable data transmission scheme for WBAN. First of all, the scheme uses the time-varying prediction model to judge the relay timing, and then select the relay node according to the principle of load balancing to ensure the energy efficiency of relay transmission on the premise of reliability. At the same time, according to the different ways of link transmission, respectively, a two-party and three-party authentication and key agreement protocol are proposed to ensure the secure communication of data.

4.1 Judgment of Relay Timing

In the time-varying model, the coordinator C determines whether or not a relay node needs to be assigned to the sensor node in the next superframe according to the channel state. We use the typical TDMA superframe structure to allocate time slots, as shown in Figure 2, each superframe is divided into three parts, namely, the transmission period, the forwarding period and the sleep period. During the transmission period, the sensor node sends the perceptual data to the coordinator and the relay node in the allocated time slot. During the forwarding period, the relay node will forward the received packets to the coordinator C within the allocated forwarding time slot. During sleep, all nodes go to sleep.

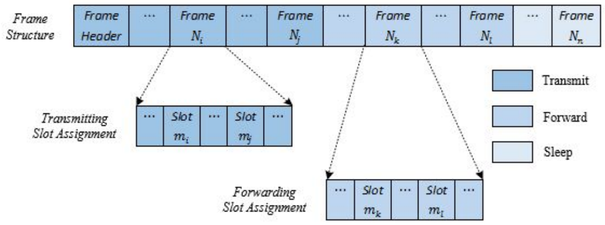


Figure 2: TDMA superframe structure

It is assumed that the sensor node S_i has transmitted the data to the coordinator C in the m_i-th time slot of the current superframe. The coordinator C obtains the average channel gain value of the link $S_i - C$ in the current transmission slot according to the RSSI (received signal strength indicator) value of the received packet, denoted $\bar{G}_i(m_i)$. If the coordinator C assigns the (m_i+k)-th time slots in the next superframe as the next transmission slot to S_i, the outage probability $Pout_i(m_i + k)$ in the next transmission slot can be predicted according to Equation (6):

$$\begin{aligned} Pout_i(m_i + k) &= \int_{-\infty}^{\bar{G}^*} f(\bar{G}_i(m_i + k))d\bar{G}_i \\ &= \phi(\frac{\bar{G}^* - (1 - \rho_i(k)) \cdot \mu_i - \rho i(k) \cdot \bar{G}_i(m_i)}{\sqrt{(1 - \rho i^2(k)) \cdot \sigma i}}) \end{aligned} \quad (6)$$

Where $f(\bar{G}_i(m_i + k_i))$ is the probability density function of the random variable $\bar{G}_i(m_i+k)$. When the coordinator C calculates the outage probability $Pout_i(m_i + k)$, it is possible to determine whether S_i needs to allocate the relay node in the next transmission slot according to Equation (7):

$$\begin{cases} Pout_i(m_i + k) > \sigma, & \text{allocate relay nodes} \\ Pout_i(m_i + k) \leq \sigma, & \text{do not allocate relay nodes} \end{cases} \quad (7)$$

Where δ is the predefined threshold for relay allocation.

4.2 Selection of Relay Node

Suppose there are N sensor nodes, denoted as $R = \{S_i \mid i = 1, 2, \cdots, N\}$. The coordinator C predicts the link quality of the next transmission slot of the sensor node set R according to Equation (7) to obtain the set $R_1 = \{S_i \mid Pout_{S_i} > \delta, S_i \in R\}$ that needs to allocate the relay node and the set $R_2 = \left\{S_j \mid Pout_{S_j} < \delta, S_j \in R\right\}$ that does not need to allocate the relay node. For each sensor node in the set R_1, we use load balancing principle to allocate the relay nodes to maximize the energy efficiency of the relay nodes. Assume that the coordinator

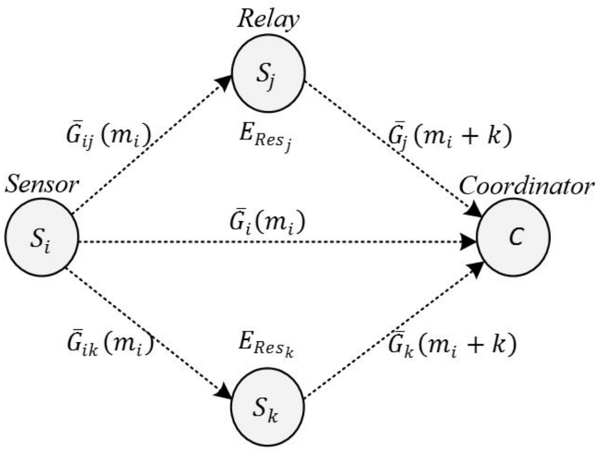


Figure 3: Relay transmission model based on load balancing

C needs to allocate a relay node for the sensor node S_i. First, the node S_i needs to broadcast a request so that the node who received the request will upload the unique identifier id and the remaining energy E_{Res} to the coordinator C. The coordinator C obtains the node set R_3 which makes the request feedback, and then performs the intersection operation with R_2 to get the candidate set of relay nodes R_4:

$$R_4 = R_2 \cap R_3 \tag{8}$$

Finally, the coordinator C allocates the lowest cost node as the optimal relay node to S_i according to the residual energy E_{Res} of the node in the candidate set R_4, thus extending the network lifetime. Figure 3 shows a simple diagram based on load balancing relay transmission model in which it is assumed that the residual energy E_{Res_j} the relay node S_j is greater than the residual energy E_{Res_k} the relay node S_k, so the coordinator C chooses S_j as the optimal relay node to allocate to S_i. When the link $S_i - C$ and the link $S_i - S_j - C$ are interrupted at the same time, the joint link of S_i is interrupted. Therefore, the outage probability $Pout_i(j)$ of S_i is:

$$\begin{aligned} &Pout_i(j) \\ &= Prob(\bar{G}_i(m_i) < \bar{G}^*) \times Prob(\bar{G}_{ij}(m_i) < \bar{G}^*) \\ &\quad + Prob(\bar{G}_i(m_i) < \bar{G}^*) \times Prob(\bar{G}_{ij}(m_i) \geq \bar{G}^*) \\ &\quad \times Prob(\bar{G}_j(m_i + k) < \bar{G}^*) \end{aligned} \tag{9}$$

4.3 Secure Transmission of Messages

After the coordinator C assigns the relay node to the sensor node S_i, S_i uploads the perceptual data to C. During data upload, the sensor node S_i and the coordinator C need to perform authentication and key agreement to ensure the security of data transmission. The system needs to be initialized before the key agreement. Therefore, we divide the data security transmission into system initialization phase, authentication and key agreement phase and data transmission phase.

4.3.1 System Initialization Phase

In the initialization phase, the system administrator (SA) needs to deploy some parameters for each sensor node S_i and coordinator C. The specific steps are as follows:

Step 1: SA assigns a unique identifier id_i and id_c to each sensor node S_i and coordinator C.

Step 2: SA selects a preshared key K_{ic} for each sensor node S_i and coordinator C.

Step 3: SA defines a one-way hash function $h(\cdot)$ and a keyed message authentication code $MAC_k(\cdot)$.

Step 4: SA selects a symmetric encryption algorithm $E_k(\cdot)$ and a pseudo-random function $f(\cdot)$.

Step 5: Finally, SA assigns the parameters $\{K_{ic}$, $H(\cdot)$, $MAC_k(\cdot), E_k(\cdot), f(\cdot)\}$ to S_i and C.

4.3.2 Authentication and Key Agreement Phase

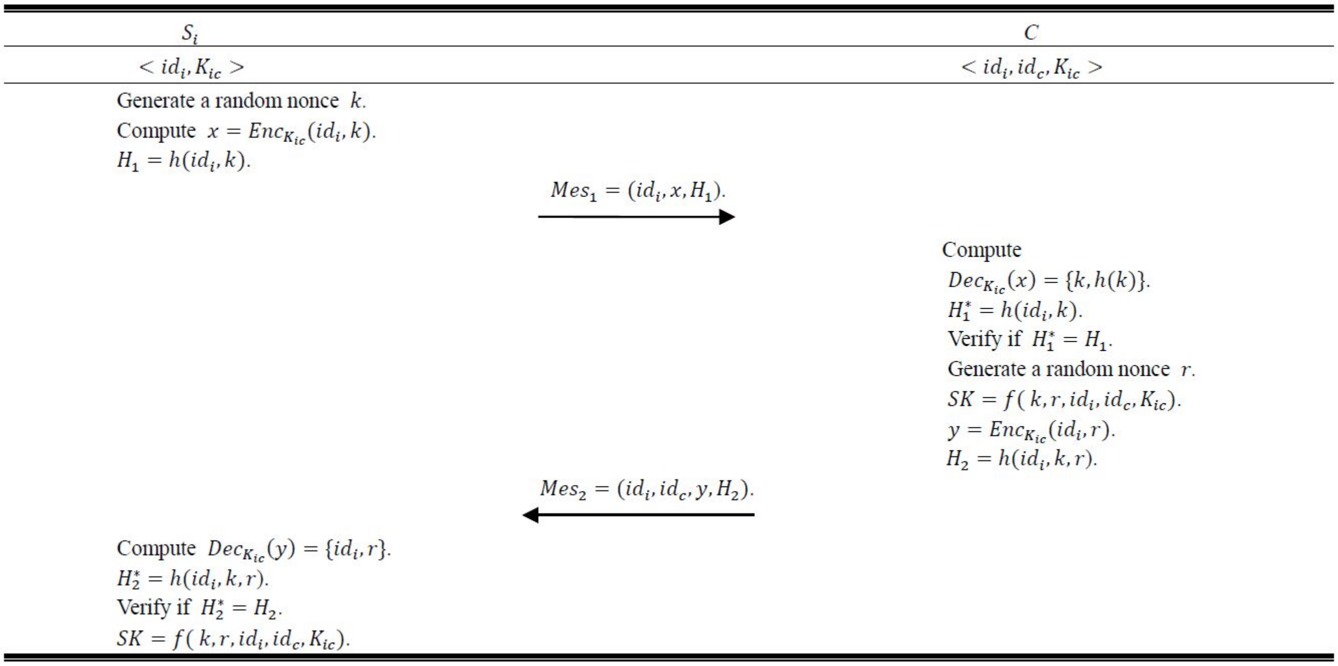
In the single link transmission process, we assume that the sensor node S_i communicates with the coordinator C. The proposed two-party authentication and key agreement protocol for single link transmission is shown in Figure 4. In the relay transmission process, it is assumed that the sensor node S_i communicates with the coordinator C through a relay node S_j. The proposed three-party authentication and key agreement protocol for relay link transmission is shown in Figure 5, described as follows:

Step 1: S_i Generate a random number k, calculate $x = Enc_{K_{ic}}(id_i, k)$ and $H_1 = h(id_i, k)$, then send the message $Mes_1 = (id_i, x, H_1)$ to S_j.

Step 2: S_j after receiving the message Mes_1, calculate $H_2 = MAC_{K_{jc}}(id_i, id_j, x, H_1)$ and send messages $Mes_2 = (id_i, id_j, x, H_1, H_2)$ to C.

Step 3: C after receiving the message Mes_2, calculate $H_2^* = MAC_{K_{jc}}(id_i, id_j, x, H_1)$ and verify that $H_2^* = H_2$ is equal. If the authentication fails, stop the session, otherwise C decrypt $Dec_{K_{ic}}(x) = id_i, k$, and then calculate $H_1^* = h(id_i, k)$ and verify that $H_1^* = H_1$ is equal. If the authentication fails, stop the session, otherwise C will generate a random number $r \in Z_p$, calculate $SK = f(k, r, id_i, id_c, K_{ic})$, $y = Enc_{K_{ic}}(id_i, r)$, $H_3 = h(id_i, k, r)$ and $H_4 = MAC_{K_{jc}}(id_i, id_j, id_c, y, H_3)$, and finally send the message $Mes_3 = (id_i, id_j, id_c, y, H_3, H_4)$ to S_j.

Step4: S_j after receiving the message Mes_3, calculate $H_4^* = MAC_{K_{jc}}(id_i, id_j, id_c, y, H_3)$ and verify that $H_4^* = H_4$ is equal. If equal, send the message $Mes_4 = (id_i, id_c, y, H_3)$ to S_i.



S_i

$< id_i, K_{ic} >$

Generate a random nonce k.

Compute $x = Enc_{K_{ic}}(id_i, k)$.

$H_1 = h(id_i, k)$.

$Mes_1 = (id_i, x, H_1)$. $\longrightarrow$

C

$< id_i, id_c, K_{ic} >$

Compute

$Dec_{K_{ic}}(x) = \{k, h(k)\}$.

$H_1^* = h(id_i, k)$.

Verify if $H_1^* = H_1$.

Generate a random nonce r.

$SK = f(\ k, r, id_i, id_c, K_{ic})$.

$y = Enc_{K_{ic}}(id_i, r)$.

$H_2 = h(id_i, k, r)$.

$\longleftarrow$ $Mes_2 = (id_i, id_c, y, H_2)$.

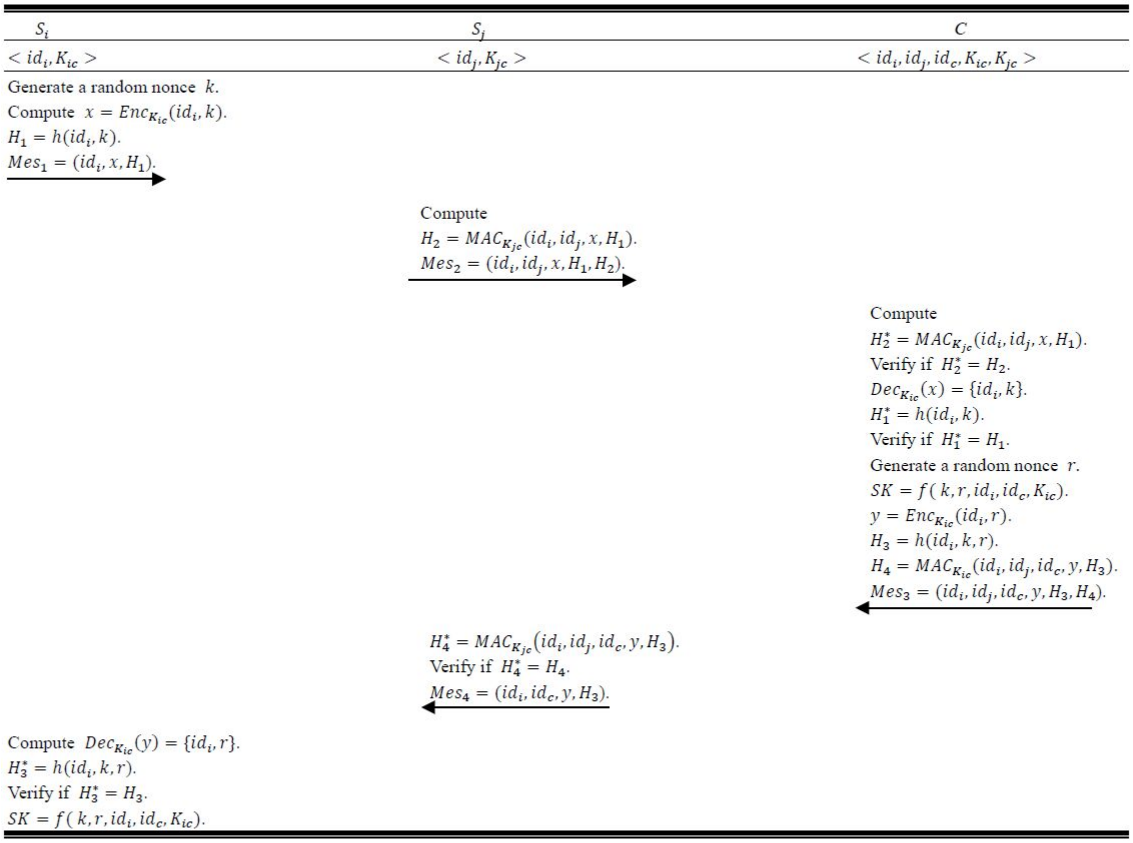
Compute $Dec_{K_{ic}}(y) = \{id_i, r\}$.

$H_2^* = h(id_i, k, r)$.

Verify if $H_2^* = H_2$.

$SK = f(\ k, r, id_i, id_c, K_{ic})$.

Figure 4: Two-party authentication and key agreement protocol for single link transmission



S_i

$< id_i, K_{ic} >$

Generate a random nonce k.

Compute $x = Enc_{K_{ic}}(id_i, k)$.

$H_1 = h(id_i, k)$.

$Mes_1 = (id_i, x, H_1)$. $\longrightarrow$

S_j

$< id_j, K_{jc} >$

Compute

$H_2 = MAC_{K_{jc}}(id_i, id_j, x, H_1)$.

$Mes_2 = (id_i, id_j, x, H_1, H_2)$. $\longrightarrow$

C

$< id_i, id_j, id_c, K_{ic}, K_{jc} >$

Compute

$H_2^* = MAC_{K_{jc}}(id_i, id_j, x, H_1)$.

Verify if $H_2^* = H_2$.

$Dec_{K_{ic}}(x) = \{id_i, k\}$.

$H_1^* = h(id_i, k)$.

Verify if $H_1^* = H_1$.

Generate a random nonce r.

$SK = f(\ k, r, id_i, id_c, K_{ic})$.

$y = Enc_{K_{ic}}(id_i, r)$.

$H_3 = h(id_i, k, r)$.

$H_4 = MAC_{K_{ic}}(id_i, id_j, id_c, y, H_3)$.

$\longleftarrow$ $Mes_3 = (id_i, id_j, id_c, y, H_3, H_4)$.

$H_4^* = MAC_{K_{jc}}(id_i, id_j, id_c, y, H_3)$.

Verify if $H_4^* = H_4$.

$\longleftarrow$ $Mes_4 = (id_i, id_c, y, H_3)$.

Compute $Dec_{K_{ic}}(y) = \{id_i, r\}$.

$H_3^* = h(id_i, k, r)$.

Verify if $H_3^* = H_3$.

$SK = f(\ k, r, id_i, id_c, K_{ic})$.

Figure 5: Three-party authentication and key agreement protocol for relay link transmission

Step 5: S_i after receiving the message Mes_4, decrypt $Dec_{K_{ic}}(y) = id_i, r$ and calculate $H_3^* = h(id_i, k, r)$, and then verify that $H_3^* = H_3$ is equal. If equal, calculate the temporary session key $SK = f(k, r, id_i, id_c, K_{ic})$.

4.3.3 Data Transmission Phase

After the sensor node S_i, the relay node S_j and the coordinator C complete authentication and temporary session key establishment, the sensor node S_i uses SK to encrypt the perceptual data M to obtain $E_{SK}(M, h(M))$, and then through the relay node S_j transmitted to coordinator C. Coordinator C decrypts the data to get M.

5 Security Analysis and Proof

Theorem 1. *The proposed scheme can provide mutual authentication.*

Proof. In our scheme, the coordinator C can authenticate the sensor node S_i and the relay node S_j by the preshared key K_{ic} and K_{jc}, respectively. At the same time, S_i and S_j can also authenticate C through K_{ic} and K_{jc}. Therefore, our solutions are able to provide mutual authentication. □

Theorem 2. *The proposed scheme can resist denial of service attacks.*

Proof. Denial of service attack is the most common type of attack on the network. This kind of attack utilizes the asymmetry of information exchange resources and consumes a large amount of the limited resources of the victim, thus undermining the network usability. For example, an attacker could repeatedly send a forged Mes_1 to C, and in the absence of any protection measures, C will think that this is the retransmission message Mes_1 from S_i. Therefore, C will continue to repeat the calculation of temporary session key SK, and store all the calculated SK and the corresponding random number r. But in our proposed scheme, denial of service attack is invalid. Since C receives the forged Mes_1, it does not generate and store the random number r and the temporary session key SK after verifying H_1 failure. Similarly, S_i is the same. Therefore, our scheme can resist denial of service attacks. □

Theorem 3. *The proposed scheme can resist man-in-the-middle attacks.*

Proof. Man-in-the-middle attack means that the attacker can intercept, replace or tamper with the information in the interaction process. In the proposed scheme, it is impossible for an attacker to arbitrarily forge and tamper with the information, because it can not obtain a pre-shared key between the sender and the receiver. For example, suppose an attacker S_k intercepts the interaction between S_i and C and replaces the authentication request (x, H_i) with (y, H_k). However, this man-in-the-middle attack is still unsuccessful because the attacker does not have a pre-shared key K_{ic} and can not produce a correct $y = Enc_{K_{ic}}(id_i, k)$. Therefore, the proposed scheme can resist man-in-the-middle attacks. □

Theorem 4. *The proposed scheme can resist replay attacks.*

Proof. Replay attack is the attacker intercepts the message before the communication process, and then replays the intercepted message in the future interactive communication process. The solution proposed in this paper can resist the attack because of the addition of random numbers k and r to ensure the freshness of the message. If an attacker replays the previous interactive message, the interaction will be stopped because the failure of the random number verification. In addition, except the sender, only the receiver can obtain the random number by the preshared key decryption, and the attacker does not have a preshared key can not get the random number. Therefore, the proposed scheme can resist replay attacks. □

6 Performance Analysis

In the simulation experiment, we use a commonly WBAN settings, as shown in Figure 1. The human body wears five sensor nodes that transmit the perceived data to coordinator C in real time and have a relay forwarding function. At the same time, the indoor walk as the default body movement. Correspondingly, reasonable time-varying model parameters can be determined based on the measurement results of the wireless body channel in [5, 10, 21], as shown in Table 1 and Table 2. In addition, the predetermined reception power threshold $\bar{P}^*$ is set to -85dBm, and the transmission power P_t is set to -10dBm, which is the recommended transmission power level of the medical special node. Therefore, the link interrupt threshold $\bar{G}^*$ is -75dB. In the simulation, we use the superframe structure of the time slot length and superframe length were set to 5ms and 250ms. At the same time, the same time correlation coefficient ρ_i is considered for the link between all sensor nodes and coordinator C, and Table 1 gives the time correlation coefficient within 500ms. In order to examine the reliability of single link communication, the outage probability of all direct links are calculated, as shown in Table 1 and Table 2. It can be seen from Table 1 that the outage probability of link $S_{RA} - C$ and link $S_{LW} - C$ exceeds 5%, which means that it is necessary to assign the relay nodes to the two links to ensure the reliability of communication.

In order to prove the effectiveness of the proposed relay transmission strategy, we compare the load balancing relay transmission strategy with random selection relay transmission [6], optimal selective relay transmission [7] and maximum effort relay transmission [12]. At the same time, we compare the performance of the proposed authentication and key agreement protocol with some typical authentication and key agreement protocols. Two-party authentication and key agreement protocols including Guiying protocol [11], Saeed protocol [22], Yi protocol [27] and Xie protocol [25], three-party authentication and key agreement protocols including Lv protocol [17], Yang protocol [26], He protocol [14] and Chang protocol [4].

In the simulation experiment, we use the outage probability and the lifecycle of relay node to test the proposed relay transmission strategy, which represent the network reliability and energy efficiency. The lifecycle of the relay node selects the lifetime of the first relay node as the lifetime of the network, which reflects the starting time of network performance deterioration. At the same time, we use the two metrics of calculation overhead and energy consumption to evaluate the proposed authentication and key agreement protocol. The initial energy of each sensor node is set to 1000mJ/s.

6.1 Outage Probability

Figure 6 and Figure 7 shows the relationship between the outage probability of the link $S_{RA} - C$ and $S_{LW} - C$ using the relay transmission strategy and the next transmission time slot. As can be seen from Figure 6 and Figure 7, the outage probability increases with the increase of the next transmission time slot. This is because the time correlation coefficient decreases with the transmission time slot increases. In addition, we can find that the four relay transmission strategies significantly reduce the outage probability of link $S_{RA} - C$ and link $S_{LW} - C$, and prove the efficiency of the relay transmission strategy. It can be seen from Figure 6 and Figure 7 that the outage probability of best-effort relay transmission strategy is the lowest, but the energy consumption of the relay node is the largest. Figure 7 shows that the outage probability of our scheme is higher than that of the other three schemes, but the outage probability of our scheme is no more than 1%, and the link $S_{LW} - C$ still has high transmission efficiency.

6.2 Relay Node Energy Consumption

Figure 8 shows the relationship between the energy consumption of relay nodes and the lifecycle of four relay transmission strategies. From the figure we can see that the lifecycle of best-effort relay transmission strategy is the shortest, this is because the best-effort relay transmission strategy assigns all candidate nodes as relay nodes to the sensor node, thus greatly reducing the service life of the relay nodes. In addition, it can be seen from the figure that the lifecycle of load balancing relay transmission strategy is the longest, which means that the proposed relay transmission strategy is superior to the other three strategies in terms of energy efficiency. This is because in our relay transmission strategy, the coordinator to select the optimal relay node according to the residual energy of nodes, thus significantly improving the energy efficiency of relay transmission while ensuring the reliability of transmission.

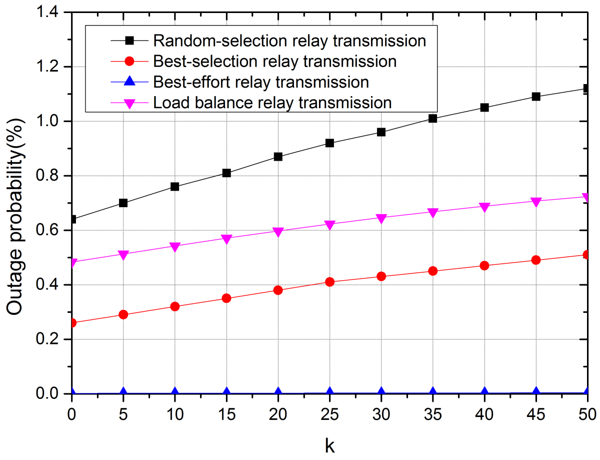


Figure 6: The change curve of the outage probability of link RA-C with the time slot

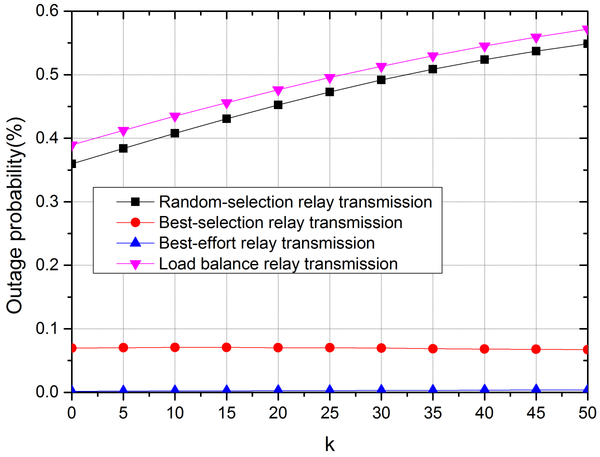


Figure 7: The change curve of the outage probability of link LW-C with the time slot k

6.3 Computation Overhead

Before simulating the running time of the protocol, the running time of the various algorithms used in the protocol is simulated on the single chip. The simulation environment is 512KB memory, clocked at 72MHz 32-bit Cortex-M3 single chip [24]. As shown in Table 3, we run the simulation time for each operation 100 times to get the average result.

In this paper, we use AES-128 algorithm for encryption and decryption, pseudo-random function using HMAC-SHA256 algorithm to calculate the temporary session key, hash function using SHA-256 algorithm, message authentication code using HSHA-256 algorithm, random number

Table 1: Single link parameters for time-varying model in indoor walking scenarios

Link	(μ_i, σ_i)	$Prob(\bar{G}_i < -75dB)$	$\rho_i(5), \rho_i(10), \cdots, \rho_i(100)$
$S_{RA} - C$	(-69.6,6.3)	6.59%	0.95,0.90,0.85,0.80,
$S_{RE} - C$	(-68.0,6.2)	4.74%	0.75,0.70,0.65,0.60,
$S_{LT} - C$	(-66.5,5.5)	2.12%	0.55,0.50,0.45,0.40,
$S_{LW} - C$	(-63.4,7.9)	5.21%	0.35,0.30,0.25,0.20,
$S_{RC} - C$	(-57.7,5.2)	0.11%	0.15,0.10,0.05,0.00.

Table 2: Relay link parameters for time-varying model in indoor walking scenarios

Source node	**Relay node**	(μ_{ij}, σ_{ij})	$Prob(\bar{G}_i < -75dB)$
S_{RA}	S_{RE}	(-64.4,7.6)	5.28%
	S_{LT}	(-59.7,7.1)	1.84%
	S_{RC}	(-71.2,6.2)	8.19%
S_{LW}	S_{RE}	(-68.6,7.8)	9.92%
	S_{LT}	(-65.4,7.1)	4.89%
	S_{RC}	(-59.7,6.6)	1.23%

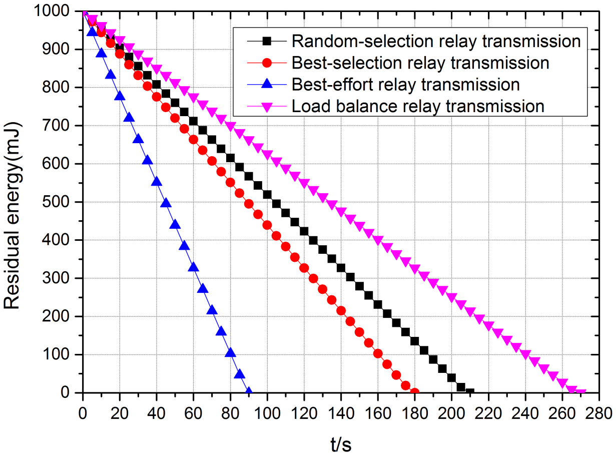


Figure 8: The change curve of the energy of relay node with time t

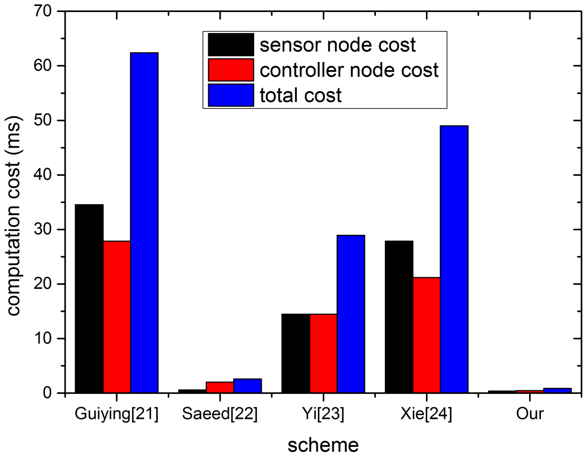


Figure 9: The computational cost of two-party authentication and key agreement protocol

generation contains three AES-128 encryption and two XOR operations. When simulating the running time of the protocol, the intermediate transmission time of the message is ignored, taking into account only the time at which it is calculated at both ends. In the process of single link transmission, we compare the proposed two-party authentication and key agreement protocol with some classical two-party authentication and key agreement protocol. The operation time of each two-party protocol is shown in Table 4, and the corresponding histogram result is shown in Figure 9. In the process of relay transmission, we compare the proposed three-party authentication and key agreement protocol with some classic three-party authentication and key agreement protocol. The operation time of each three-party protocol as shown in Table 5, the corresponding histogram results shown in Figure 10.

It can be seen from Figure 9 that the calculation overhead of Guiying protocol, Yi protocol and Xie protocol is relatively large. We propose that two-party authentication and key agreement protocol have the shortest running time in the five protocols, compared to other protocols is more superior. From Figure 10 we can see that the proposed three-party authentication and key agreement protocol is less time-consuming in this comparison of four protocols. In the other three schemes, the computation of relay nodes is relatively large, which greatly shortens the lifetime of nodes, and is not suitable for WBAN.

6.4 Energy Consumption

The energy consumption of encryption operation is used to evaluate our protocol. For 32-bit Cortex-M3 microcontroller with 72MHz, the current consumption of active mode is 36mA [29] at an ambient temperature

Table 3: Computational time

Notations	Operations	Computation time (ms)
T_{sym}	Symmetric en/decryption	0.031/0.067
T_{Asym}	Asymmetric en/decryption	0.146/1.584
T_{Hash}	One-way hash function	0.032
T_{Ran}	Random number	0.117
T_{HMAC}	Keyed message authentication code	0.043
T_{Pse}	Pseudorandom function	0.156
T_{Exp}	Modular exponentiation	5.542
T_{Bp}	Bilinear pairing	14.316
T_{Ecsm}	Elliptic curve scalar point multiplication	6.697

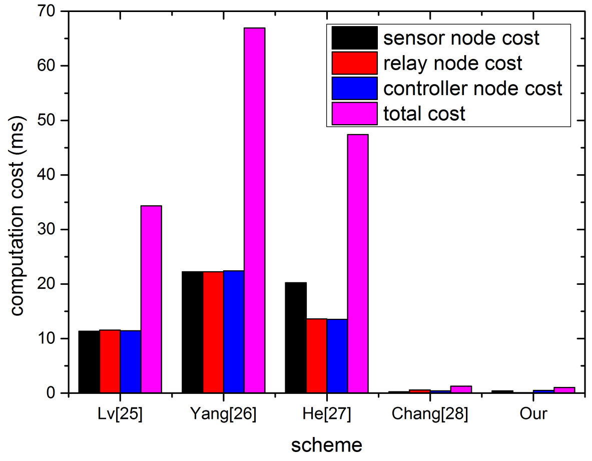


Figure 10: The computational cost of three-party authentication and key agreement protocol

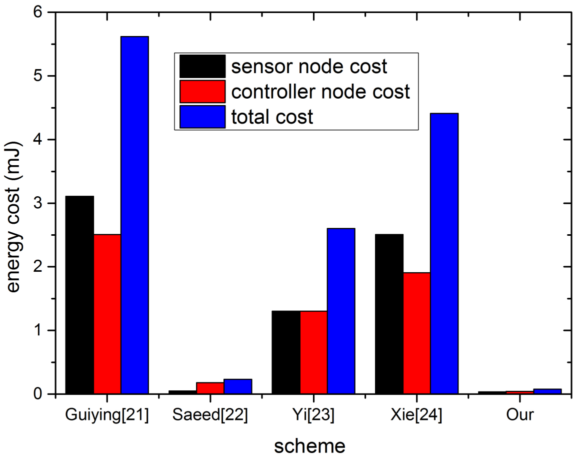


Figure 11: The energy consumption of two-party authentication and key agreement protocol

of 27, and the power consumption of active mode is approximately 90mW at a voltage of 2.2V. Therefore, according to Table 4 and Table 5 running time, we can calculate the corresponding energy loss. For example, a sensor node takes 0.031ms to complete the AES-126 encryption operation, the energy consumption is about $0.031ms \times 90/1000 = 0.003mJ$. The energy consumption of all schemes is shown in Figure 11 and Figure 12. From Figure 10 we can see that the total energy consumption of the proposed two-party authentication and key agreement protocol is the smallest, and the calculated energy consumption of the sensor node is also the smallest, and can meet the limited computing ability of WBAN demand. From Figure 12 we can see that the proposed three-party authentication and key agreement protocol of the sensor nodes, relay nodes and control node are the smallest energy consumption. In WBAN, the relay node needs to be used frequently, so the proposed scheme can meet its needs.

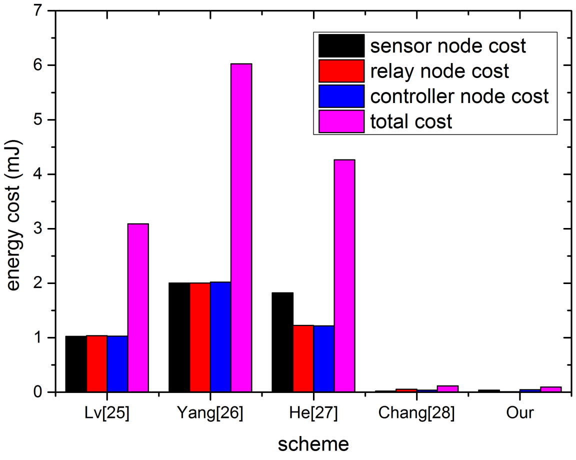


Figure 12: The energy consumption of three-party authentication and key agreement protocol

Table 4: Simulation results of two-party authentication and key agreement protocol

Protocols	Computation cost $[T_{Ran}, T_{Asym}, T_{Sym}, T_{Pse}, T_{Hash}, T_{HMAC}, T_{Bp}, T_{Ecsm}]$			
	Sensor node (ms)	Controller node (ms)	Tatal computation cost (ms)	Total energy cost (mJ)
Guiying [21]	[1,0,0,0,2,0,1,3]	[1,0,0,0,2,0,1,2]	62.413	5.617
Saeed [22]	[1,1,0,1,2,1,0,0]	[1,1,0,1,2,1,0,0]	2.577	0.232
Yi [23]	[1,0,0,0,1,0,1,0]	[1,0,0,0,1,0,1,0]	28.93	2.603
Xie [24]	[1,0,0,0,2,0,1,2]	[1,0,0,0,2,0,1,1]	49.019	4.412
Our	[1,0,2,1,2,0,0,0]	[1,0,2,1,2,0,0,0]	0.87	0.078

Table 5: Simulation results of three-party authentication and key agreement protocol

Protocols	Computation cost $[T_{Ran}, T_{Asym}, T_{Sym}, T_{Pse}, T_{Hash}, T_{HMAC}, T_{Exp}, T_{Ecsm}]$				
	Sensor node (ms)	Relay node (ms)	Controller node (ms)	Tatal computation cost (ms)	Total energy cost (mJ)
Lv [25]	[1,0,3,0,1,0,2,0]	[2,0,4,0,1,0,2,0]	[1,0,3,0,2,0,2,0]	34.338	3.090
Yang [26]	[0,0,0,0,3,0,4,0]	[0,0,0,0,3,0,4,0]	[0,0,0,0,8,0,4,0]	66.952	6.026
He [27]	[0,0,2,0,2,0,0,3]	[0,0,4,0,1,0,0,1]	[0,0,2,0,1,0,0,2]	47.399	4.266
Chang [28]	[1,0,0,0,4,0,0,0]	[2,0,0,0,11,0,0,0]	[1,0,0,0,10,0,0,0]	1.268	0.114
Our	[1,0,2,1,2,0,0,0]	[0,0,0,0,0,2,0,0,]	[1,0,2,1,2,2,0,0]	1.042	0.094

7 Conclusion

In this paper, a new security and reliability scheme is proposed based on the channel characteristics of WBAN. Through the use of time slot allocation and load balancing relay transmission strategy to realize the reliability transmission of data. Then, in the process of data transmission, a new authentication and key agreement protocol is proposed for single-link transmission and relay link transmission mode respectively, which ensures the security transmission of data. Through the security analysis, we prove that the proposed scheme meets the high security level requirements of communication. The simulation results show that our transmission strategy can improve the reliability of data transmission with low computational cost and energy consumption.

Acknowledgments

Above work is supported by National Natural Science Foundation (NSF) of China under grant Nos. 61370007, 61572206, U1405254, Huaqiao University graduate research innovation ability cultivation project of China under grant No. 1511314006, Fujian Provincial Natural Science Foundation of China under grant No. 2013J01241, and Program for New Century Excellent Talents of Fujian Provincial under grant No. 2014FJ-NCET-ZR06.

References

[1] U. F. Abbasi, A. Awang, and N. H. Hamid, "Performance investigation of using direct transmission and opportunistic routing in wireless body area networks," in *IEEE Symposium on Computers and Informatics (ISCI'13)*, pp. 60–65, Apr. 2013.

[2] A. Boulis, D. Smith, D. Miniutti, L. Libman, and Y. Tselishchev, "Challenges in body area networks for healthcare: The mac," *IEEE Communications Magazine*, vol. 50, no. 5, pp. 100–106, 2012.

[3] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1635–1657, 2014.

[4] C. C. Chang, W. Y. Hsueh, and T. F. Cheng, "A dynamic user authentication and key agreement scheme for heterogeneous wireless sensor networks," *Wireless Personal Communications*, vol. 89, no. 2, pp. 447–465, 2016.

[5] R. D'Errico and L. Ouvry, "Time-variant ban channel characterization," in *IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 3000–3004, Sep. 2009.

[6] R. D'Errico, R. Rosini, and M. A. Maman, "performance evaluation of cooperative schemes for on-body area networks based on measured time-variant channels," in *IEEE International Conference on Communications (ICC'11)*, pp. 1–5, June 2011.

[7] H. Feng, B. Liu, Z. Yan, C. Zhang, and C. W. Chen, "Prediction-based dynamic relay transmission scheme for wireless body area networks," in *IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'13)*, pp. 2539–2544, Sep. 2013.

[8] E. Forrister, G. Lee, D. Xue, B. Garner, and Y. Li, "Characterization of narrowband on-body wireless channels using motion capture experimentation," in

Texas Symposium on Wiireless and Microwave Circuits and Systems (WMCS'16), pp. 1–4, Mar. 2016.

[9] L. C. Fourati N. Jamali, "Skep: A secret key exchange protocol using physiological signals in wireless body area networks," in *International Conference on Wireless Networks and Mobile Communications (WINCOM'15)*, pp. 1–7, Oct. 2015.

[10] J. M. Gorce, C. Goursaud, G. Villemaud, R. D'Errico, and L. Ouvry, "Opportunistic relaying protocols for human monitoring in ban," in *IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 732–736, Sep. 2009.

[11] L. Guiying, H. Mengbo, Z. Chuan, and X. Qiuliang, "A two-party certificateless authenticated key agreement protocol with provable security," in *9th International Conference on Computational Intelligence and Security (CIS'13)*, pp. 559–563, Dec. 2013.

[12] S. Hara, D. Anzai, K. Yanagihara, K. Takizawa, and K. Hamaguchi, "A cooperative transmission scheme for real-time data gathering in a wireless body area network," in *IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'11)*, pp. 2254–2258, Sep. 2011.

[13] D. He, S. Chan, Y. Zhang, and H. Yang, "Lightweight and confidential data discovery and dissemination for wireless body area networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 2, pp. 440–448, 2014.

[14] D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 71–77, 2015.

[15] B. E. Ieee, "Ieee standard for local and metropolitan area networks - part 15.6: Wireless body area networks," *IEEE Standard for Information Technology*, vol. 802, no. 6, pp. 1–271, 2012.

[16] J. Iqbal, N. ul Amin, A. I. Umar, N. Din, and A. Waheed, "Secure lightweight authentication and key agreement for wireless body area networks," *International Journal of Computer Science and Information Security*, vol. 14, no. 5, p. 196, 2016.

[17] C. Lv, M. Ma, H. Li, J. Ma, and Y. Zhang, "An novel three-party authenticated key exchange protocol using one-time key," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 498–503, 2013.

[18] M. Maman and L. Ouvry, "Batmac: An adaptive tdma mac for body area networks performed with a space-time dependent channel model," in *5th International Symposium on Medical Information and Communication Technology (ISMICT'11)*, pp. 1–5, Mar. 2011.

[19] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[20] S. C. Mukhopadhyay, "Wearable sensors for human activity monitoring: A review," *IEEE Sensors Journal*, vol. 15, no. 3, pp. 1321–1330, 2015.

[21] H. Ren, M. Meng, and C. Cheung, "Experimental evaluation of on-body transmission characteristics for wireless biosensors," in *IEEE International Conference on Integration Technology (ICIT'07)*, pp. 745–750, Mar. 2007.

[22] M. Saeed, H. S. Shahhoseini, A. Mackvandi, M. R. Rezaeinezhad, M. Naddafiun, and M. Z. Bidoki, "A secure two-party password-authenticated key exchange protocol," in *IEEE 15th International Conference on Information Reuse and Integration (IRI'14)*, pp. 466–474, Aug. 2014.

[23] D. B. Smith, D. Miniutti, and L. W. Hanlen, "Characterization of the body-area propagation channel for monitoring a subject sleeping," *IEEE Transactions on Antennas and Propagation*, vol. 59, no. 11, pp. 4388–4392, 2011.

[24] S. Wang, Z. H. Wu, P. Hu, and Z. LI, "Design and implement of bootloader based on pxa270 processor," *Journal-Sichuan university natural science edition*, vol. 44, no. 3, p. 578, 2007.

[25] Y. Xie, L. Wu, Y. Zhang, and Z. Xu, "Strongly secure two-party certificateless key agreement protocol with short message," in *International Conference on Provable Security*, pp. 244–254, Nov. 2016.

[26] H. Yang, Y. Zhang, Y. Zhou, X. Fu, H. Liu, and A. V. Vasilakos, "Provably secure three-party authenticated key agreement protocol using smart cards," *Computer Networks*, vol. 58, pp. 29–33, 2014.

[27] T. Yi, M. Shi, and W. Shang, "Personalized two party key exchange protocol," in *IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS'15)*, pp. 575–579, June 2015.

[28] X. Yi, A. Bouguettaya, D. Georgakopoulos, A. Song, and J. Willemson, "Privacy protection for wireless medical sensor data," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 3, pp. 369–380, 2016.

[29] D. Zhao, Y. Wang, J. Tan, "Design and experiment on a biomimetic robotic fish inspired by freshwater stingray," *Journal of Bionic Engineering*, vol. 12, no. 2, pp. 204–216, 2015.

[30] J. Zhou, Z. Cao, X. Dong, N. Xiong, and A. V. Vasilakos, "4s: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," *Information Sciences*, vol. 314, pp. 255–276, 2015.

Biography

Huaijin Liu received the B.S. degree from Huaqiao University, China, in 2015, where he is currently pursuing the master's degree. His current research interest includes wireless sensor network security, wireless body area network security and privacy protection, wireless vehicle network security.

Yonghong Chen received the B.S. degrees from Hubei National University, and M.Eng. and Ph.D. degree degrees from Chognqing University, Chongqing, China, in 2000 and 2005 respectively. He is currently the professor of of College of Computer Science and Technology, Huaqiao University, Xiamen, China. His research interests include network security, watermarking and nonlinear processing.

Hui Tian received his BSc and MSc degrees in Wuhan Institute of Technology,Wuhan, China in 2004 and 2007, respectively. He received his PhD degree in Huazhong University of Science and Technology, Wuhan, China. He is now an associate professor in the National Huaqiao University of China. His research interests include network and multimedia information security, digital forensics and information hiding.

Tian Wang received his BSc and MSc degrees in Computer Science from the Central South University in 2004 and 2007, respectively. He received his PhD degree in City University of Hong Kong in 2011. Currently, he is a professor in the Huaqiao University of China. His research interests include wireless sensor networks, fog computing and mobile computing.

Yiqiao Cai received the B.S. degree from Hunan University, Changsha, China, in 2007, and the Ph.D. degree from Sun Yat-sen University, Guangzhou, China, in 2012. In 2012, he joined Huaqiao University, Xiamen, China, where he is currently a lecturer with the College of Computer Science and Technology. He is interested in differential evolution, multiobjective optimization, and other evolutionary computation techniques.