Research Article

Wireless Sensor Acquisition of Human Motion Parameters Based on Blockchain

Daibin Peng[1] and Yonghong Liu [2]

[1]*Professional Tennis College of Wuhan City Polytechnic, Wuhan, Hubei 430064, China*
[2]*College of Physical Education, Hubei University, Wuhan, Hubei 430064, China*

Correspondence should be addressed to Yonghong Liu; 20040752@hubu.edu.cn

With the rapid development of intelligent technology, people's lives have gradually entered the era of information and intelligence. Traditional vision-based and sensor-based human motion detection methods have shortcomings such as high illumination requirements, difficulty in preserving privacy, and poor portability. The wireless sensor detection method based on a wireless network can overcome the shortcomings of these methods, so it has become a hot research direction. Human motion parameters are very important data. If leaked, it may cause unimaginable harm to individuals. Blockchain technology is an emerging technology in the field of information technology. Its decentralized nature, distributed storage, and data is not easy. The modification provides a feasible solution for us to realize the data upload. Combining the advantages of wireless sensing and blockchain technology, this paper proposes a method of wireless sensing collection of human motion parameters based on blockchain, and designs a human motion recognition system. The experiment found that under the experiments given in this article, the traditional accuracy rate of sensor data collection is 71.82%, and the accuracy rate of the wireless sensing collection method of human motion parameters based on the blockchain in this article has reached 95.31%, which verifies the effectiveness and superiority of the system designed in this article.

1. Introduction

With the rapid development of artificial intelligence technology, people's lives have gradually entered the era of informationization and intelligence. The emergence of more and more intelligent devices is convenient for people's lives, and at the same time, people's actual needs have spawned the continuous development of various emerging technologies. Human motion detection technology has always attracted much attention. This technology mainly refers to the use of some special equipment and related detection algorithms to identify the motion state of the target person. The current motion state of the target user can be judged by the obtained motion state information, and corresponding services can be provided based on it, which can be widely used in smart homes, health care, entertainment games, and other related fields. From the technical means of human motion detection, human motion detection technology is mainly divided into three categories. The first is the use special sensor equipment to collect information; wearable devices containing specific sensors are worn on human bodies to collect human motion data to judge the human motion state. The advantages of this detection method include the simplicity of the equipment needed and the high precision achieved; however, the disadvantages are that the target person needs to wear auxiliary equipment actively, which will increase the burden on the target person to a certain extent, and it is difficult to complete the detection of motion state without cooperation. Second, with the development of computer vision, human motion detection based on vision has become a hot research direction. However, this method relies on (1) high-resolution video or images under line-of-sight, (2) high-precision cameras that are often costly, and (3) recognition performance that is greatly reduced in dark or poor line-of-sight conditions. In addition, it is easy to reveal users' personal privacy in some scenes because the

camera shoots directly. The third kind of motion state detection method based on radio frequency has become a new detection technology because of the following advantages: (1) it is not affected by illumination conditions, (2) it has strong expansibility, and (3) it can overcome non-line-of-sight and passive sensing. The detection method based on radio frequency uses specific receiving and transmitting equipment to obtain the signal change information of human motion state change, and then realizes motion state detection through preprocessing, feature extraction, training, and classification. In recent years, wireless sensor networks have been widely used in various fields. With the rapid development of wireless communication technology, sensor technology, and microcontrol technology, wireless sensor networks have been widely used to build a robust Internet of Things system. A sensor network is composed of a large number of sensor nodes, which are composed of an energy supply unit, a data acquisition unit, a data processing unit, and a data transmission unit [1]. In this paper, the advantages of wireless sensors, combined with the decentralization and distribution of blockchain technology, ensure the reliability of data uploading and enable designing a wireless sensor acquisition system of human motion parameters based on blockchain. Through experiments, its accuracy is much higher than that of the traditional human motion parameter acquisition system.

These results show that the wristband based on a pressure sensor can classify gestures very well and can also control mouse interaction. A new pressure signal processing framework has been developed, and it is a prototype system for real-time, robust gesture recognition [2]. It can make the gestures of the worn device intersect with the computer. Through the wristband experiment of a pressure sensor, it shows that people with or without experience can complete interactive tasks. In practice, the motion recognition system based on radio frequency is widely used, but it can be disturbed and lead to low accuracy. Therefore, we propose a new wireless sensor system, the Motion-Fi +, which can perform some motions simultaneously by multiple users because of its noninterfering characteristics and it does not depend on the template or contour of the scene. We built a backscatter wireless platform, and after 6 months of different scene designs, we added different people and directions to verify the system [3]. Experiments show that this method has high accuracy. With the development of research, a wireless inertial sensor system applied to human motion capture is a decoding strategy of human node displacement and attitude data based on the advantages of the previous two filtering methods. Evaluated on a built platform, wireless inertial sensor systems accurately measure human movement in the joints [4]. Nowadays, people live at a fast pace, and there are great pressures in work and study. They basically do not exercise at ordinary times, which has a great impact on their health. People gradually realize this and pay attention to their own health. Mild jogging and walking are the first choice for everyone to exercise. Wearing equipment plays an increasingly important role in the field of health, and its research is also of great significance [5]. Researchers put forward a wearable human body monitoring system based on wireless acceleration sensor technology, which can monitor the amount of running performed by a human body in time. Aiming at the confusing parts in the process of motion, this paper proposes a recognition method of human motion state based on single fractal and multifractal methods. Experiments show that this method is effective and feasible for recognition. In recent years, the wide application of artificial intelligence has also made a breakthrough in wireless network monitoring. It can identify abnormal events and has the global operation and maintenance capability of analysis. The video is captured and transmitted by camera, and then it is displayed in a browser by ActiveX control. Then, the linkage coordinate system of wireless network remote monitoring is established by the DH parameter method to realize intelligent control of a wireless network [6]. The above methods applied to human body monitoring and data collection are sensor-based data collection and are not applied to blockchain technology. There are some problems in the design accuracy and accuracy of the above methods, and the prediction effect is not ideal when analyzing the data after collection. Therefore, the method of collecting data from the human body with blockchain sensors can obtain more accurate data than traditional ones.

2. Characteristics of Blockchain Technology and Introduction of Related Technologies

Blockchain is a way to organize data skillfully, while blockchain technology is a technology that integrates many outstanding achievements of human intelligence, including database technology and network technology related to distributed books, network technology related to consensus algorithm, and asymmetric encryption technology and software technology related to intelligent contracts. Blockchain technology, which integrates these cutting-edge technologies, has challenged and confronted the mechanism based on central node credit since it was put forward. With the development of time, this characteristic of blockchain technology is becoming more and more obvious, which makes it no longer limited to digital cryptocurrency, but widely used in many fields of social and economic life, such as supply chain finance, data authentication, asset management, election voting, and fair security traceability introduced in this paper. Nowadays, blockchain technology has become an important technology that cannot be ignored among many high-end cutting-edge technologies.

2.1. Distributed Book of Accounts. Different from the traditional system network structure, the network architecture and data storage of a blockchain system choose distributed books with a decentralized architecture. The transmission of information in the network does not pass through the central node, and each member node retains complete data, which is embodied in the distribution of nodes in entity and the distribution of nonrelational databases on each node in logic. An account book is a storage form of data and a management unit of data. A nonrelational database is the logical carrier of data and an account book, and the physical carrier of data and the account book is a member node. Blockchain

is the underlying form of an account book, that is, the data form of a chain of blocks strung together. After the consensus process, consensus members will reach a consensus and write the same data into the blockchain system, so each member keeps a copy of the data. Because the data in each ledger cannot be deleted, the total amount of data will only increase, which is a great test for the ability of data storage; however, with the rapid development of technology, this problem will not be a problem. This is because the breeding nodes, slaughtering nodes, processing nodes, transportation nodes, and sales nodes in the livestock product supply chain are distributed in different places in the physical sense, in line with the distributed ledger technology in blockchain. In the ideal traceability model, the status of nodes where each link is located is expected to be equal, the information flow does not pass through the central node, and its network architecture naturally fits the characteristics of distributed books in blockchain technology; thus, it is reasonable and efficient for a livestock product traceability system to select the network architecture based on blockchain technology [7].

2.2. Cryptographic Algorithms.
Cryptography is the core of a blockchain data layer, which escorts the whole data transmission and access of blockchain. Cryptographic algorithms will be used in three places in the blockchain platform of cold chain drug traceability, including the hash algorithm and the asymmetric encryption algorithm. This section will discuss the principle and selection of these two algorithms [8].

2.2.1. Hash Algorithm.
The secure hash algorithm is an alias of the hash algorithm, which maps data of arbitrary length into hash strings of fixed length through certain rules. The more common ones are SHA-256, SHA-384, SHA-512, etc., which are widely used in various technologies requiring encryption including blockchain technology [9].

2.2.2. Asymmetric Encryption Algorithm.
The asymmetric encryption algorithm comes from the secret key method in the cryptographic algorithm; the key consists of a public key and a private key. The key is generated at the same time, in which the public key is public as its name implies, while the private key is private and needs to be saved by itself. When encryption is needed, one of the same pairs of keys is used to complete the encryption operation, and only the other key can complete the decryption of the message. The asymmetric encryption algorithm plays an important role in blockchain, which is the cornerstone of the security of the whole blockchain system. The asymmetric encryption algorithm is mainly used in encrypted communication and for generating a digital signature in blockchain [10].

2.3. SM2 Digital Signature Algorithm.
The SM2 algorithm is an improved national cryptographic algorithm based on ECC published in China in 2010, which includes the digital signature algorithm and the key exchange protocol and public key encryption algorithm. It has become the current public key algorithm standard GM/T 0003.2-2012 in China and entered the international standard ISO/IEC 14888-3.

2.3.1. Principle of the SM2 Digital Signature Algorithm.
The elliptic curve equation $E(a, b)$ selected by the SM2 algorithm is as follows:

$$y^2 = x^3 + ax + b. \tag{1}$$

The Abelian group $(G, +)$ is defined on $Ep(a, b)$, where the unit element O of the group is defined as an infinity point. Let the elliptic curve be $y^2 = x^3 - x$. Take two points P and Q on the elliptic curve $(G, +)$ as straight lines intersecting the other point R' of the elliptic curve, and make parallel lines of the y axis intersecting R through R', and define $P + Q = R$. In this way, the sum of the additions made by two points on the Abelian group will also be on the elliptic curve, and it also satisfies the properties of the Abelian group. When the same points P are added, that is, when the two points P and Q coincide, the tangent of the point P is made. Repeat the above operation, and when k points P are added, it is recorded as k_P.

Ordinary elliptic curves are continuous and not suitable for encryption. In the national standard, the elliptic curves with 256 bits in the prime number field are used to transform the elliptic curves into discrete points. Let the prime number be p, the prime number field formed by the elliptic curves be F_p, and the elliptic equation be $E_{rp}(a, b)$:

$$y^2 = x^3 + ax + b \,(\mathrm{mod}\ p), \tag{2}$$

where both a and b are elements in the prime field and satisfy $4a^3 + 27b^2 \neq 0 \,(\mathrm{mod}\ P)$. SM2 can be encrypted by assuming that in the elliptic curve $P = d_G$, where P and G are two points on $E_p(a, b)$, N is the order of G, and D is an integer and its value is not higher than order N. Given D and G, it is easy to compute P in the front direction but difficult to compute D in the reverse, according to the definition of the Abelian group addition rule. Let the set $\{O, G, 2G, 3G, (n-1)G\}$ be a cyclic subgroup generated by G on $d \in [1, n-1]$. If d is selected as the private key and $P = d_G$ as the public key, the problem of finding d from P is the discrete logarithm problem on the elliptic curve group, which is the mathematical basis of the elliptic curve encryption algorithm [11].

2.3.2. SM2 Digital Signature Scheme.
The digital signature scheme designed by the SM2 encryption principle is as follows: perform key generation with the input of SM2 elliptic curve parameter parms (elliptic curve equation E_p, large prime number p, base point G, and order n of base point), randomly generate private key $d \in [1, n-1]$ and keep it secretly, and use the public-private key relationship to generate the following public key:

$$P = [d]G. \tag{3}$$

In formula (3), P is the obtained SM2 public key, which is an important basis for SM2 to be used in encryption and signature. The SM2 signature process is as follows: input SM2 elliptic curve parameter parms, private key d and

message M to be signed, and calculate hash value Z_A at the same time:

$$Z_A = H_{256}(\text{IDL}_A \| \text{ID}_A \| a \| b \| x_G \| y_G \| x_A \| y_A). \qquad (4)$$

In formula (4), ID_A is the user's distinguishable identification, IDL_A is the length of ID_A, a and b are the coefficients of the elliptic curve, x_G and y_G are the horizontal and vertical coordinates of base point G, respectively, and x_G and y_G are the horizontal and vertical coordinates of the public key, respectively.

The hash value Z_A is obtained, and then the hash digest e with the message M to be signed is calculated:

$$e = H_{256}(Z_A \| M). \qquad (5)$$

Randomly generate $k \in [1, n-1]$ and calculate the elliptic curve point X_1 from it:

$$X_1 = (x_1, y_1) = [k]G. \qquad (6)$$

Calculate the signature parameters r and s to output the signature (r, s):

$$r = (e + x_1) \mod n, \qquad (7)$$

$$s = ((1+d)^{-1}(k - rd)) \mod n. \qquad (8)$$

The SM2 verification process is as follows: input parms, the public key P owned by the verifier, the message M to be verified, and the signature (r'', s') sent by the signer to obtain the hash digest e of the message M to be verified according to formula (8), and calculate the t value:

$$t = (r' + s') \mod n. \qquad (9)$$

Verify whether t is equal to equal, if it is equal to zero, the verification fails, otherwise calculate the elliptic curve point X_1'.

$$X_1' = (x_1, y_1) = [s']G + [r']P_A. \qquad (10)$$

Verify whether $r' = (e' + x_1') \mod n$ is true, and if it is true, the verification is successful.

2.4. Consensus Algorithm. At present, the consensus algorithms commonly used in blockchain are Pow, Pos, DPos, and PBFT. Pow uses the workload proof mechanism to determine the node accounting rights and ensures the consistency of data through a large number of calculations. Pos adds the concept of currency age to the workload proof mechanism and uses currency age instead of computing power to reduce the difficulty of acquiring a block solution. DPOS uses digital cash holders to generate node sets with bookkeeping rights through elections and adopts rotation bookkeeping to generate blocks. PBFT is a distributed consensus algorithm based on state machine replication. Consensus is completed through three-stage communication

between nodes. For the four consensus mechanisms in throughput, the performance of delay and scalability is compared. Details are as follows. The application of a consensus mechanism in blockchain is from PoW to PoS to DPOS to PBFT. In this process, computing power competition is gradually replaced by equity competition. The cost of obtaining node bookkeeping rights is gradually reduced. With the development of the blockchain application, the transaction speed gradually increases. At the same time, the consensus mechanism has gradually evolved from the initial decentralization to the current weak centralization. Each consensus mechanism has different advantages and disadvantages. PoW can realize decentralization to the greatest extent. It is safe, reliable, and has low consumption of network resources; however, it consumes too much computing resources. Computational attack can easily occur. Consensus time is longer. The emergence of PoS solves the problem of excessive waste of PoW computing power, but it makes the pressure of network traffic increase. The implementation is more complicated. DPOS has made appropriate compromises on centralization. The consumption of network resources is reduced. It has greatly shortened the consensus time. The throughput of the system is improved, but the security is reduced due to its weak centralization, which is prone to security loopholes. The PBFT algorithm solves the consistency problem of the distributed system with the Byzantine error nodes and improves the fault tolerance rate of the distributed system. However, due to the existence of a large number of point-to-point communications, it occupies a large amount of communication resources [12].

3. Wireless Sensor Network and Fingerprint Location Technology

When collecting human motion data, it is necessary to locate the human body accurately. This paper uses the characteristics of human heat source and chooses infrared sensors to identify the human body. In order to locate the human body more accurately, fingerprint positioning technology is selected to locate the human body. This section will briefly introduce these two technologies.

3.1. Wireless Sensor Networks. Typical wireless sensor networks are composed of a large number of low-cost and low-power sensor terminal nodes and gateway nodes, among which the structure of sensor terminal nodes is shown in Figure 1. As can be seen from Figure 1, the sensor terminal node not only has the function of data acquisition but also includes the functions of data processing and wireless data transmission. It ensures that each node can obtain the data of interest in the system in time, and accomplish specific supervision and control purposes by exchanging data or fusing the data of each sensor node. Usually, the sensor terminal nodes in the network are used as passive sensors. This type of sensor has the characteristics of low power consumption, low price, and convenient installation, which makes it meet the requirements of large-scale deployment and can be applied in large-scale sensor networks [13].
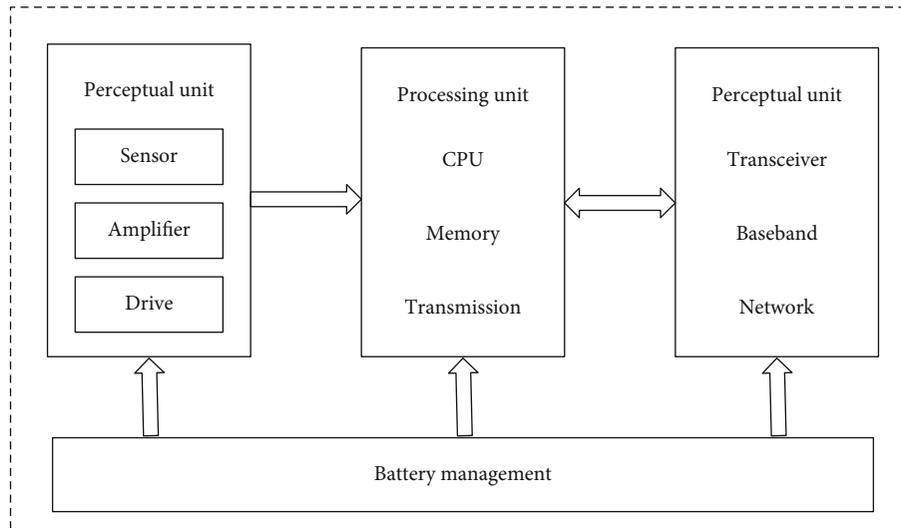
FIGURE 1: Wireless sensor network terminal node.

Because of the requirements of the deployment environment, sensor nodes often need to assemble batteries to supply power to the whole system, so that the whole network has the ability of data processing and transmission and node cooperation. The wireless sensor network structure is shown in Figure 2. In practical applications, wireless sensor networks not only need reliable communication channels but also need to prolong the life of network nodes as much as possible. Most of the energy consumption in WSNs comes from the wireless communication consumption in the network. However, considering the limited factors such as energy and economy, network nodes cannot be equipped with powerful communication and processing units, and sensor nodes are greatly limited in communication ability, computing ability, and data storage. These limitations will require further research on energy management, network topology optimization, node scheduling, distributed signal processing algorithms, and network communication protocols. The network topology and node scheduling guarantee the capacity of the network system and the real-time communication performance between nodes. The reliable communication protocol ensures that the data information can be transmitted in the network timely and accurately.

3.2. Fingerprint Location Technology

3.2.1. Principle of Fingerprint Location Technology. The location method based on position fingerprints firstly needs to collect infrared signals of a moving human body at each reference position in the off-line stage, then it needs to process these signals accordingly to build the PIR position fingerprint database, and then train these data through certain algorithms. Through training, a human body location model which can realize information matching is obtained. When positioning the position, firstly, the pyroelectric infrared signals generated when a human body walks on a certain path are collected online, then using the same data processing method as the off-line acquisition stage, the online acquisi-

tion signals are changed into position fingerprints. Finally, the trained model is matched with the fingerprints in the established PIR signal position fingerprint database, and the position positioning results are screened out.

3.2.2. Fingerprint Location Technology Algorithm

(1) Nearest Neighbor Algorithm (KNN). The NN algorithm is the most basic fingerprint-matching algorithm. It obtains the most similar reference point by calculating the Euclidean distance between the fingerprint data of the position to be measured and the fingerprint in the fingerprint database, and takes the reference point position as the approximate position of the target. The KNN algorithm is an improvement of the NN algorithm. Firstly, K similar reference points are selected as the initial measure of a position, and then the geometric centroid of K reference points is obtained as the final location result. Assume that there are N fingerprints in the off-line fingerprint database F_p, denoted $\{F_{p1}, F_{p2}, \cdots, F_{pN}\}$, and the reference point position corresponding to each fingerprint record is denoted $\{L_1, L_2, L_N\}$, where L_i is denoted (x_i, y_i). Assuming that the environment contains m PIR signal detection nodes, and the induced signal of each PIR node is denoted as a TSD vector, the fingerprint F_r is denoted $\{TSD_{i1}, TSD_{i2}, TSD_{im}\}$, where TSD_{im} represents the signal time series of the mth PIR node detected at the ith reference position. In the online stage, the signal amplitude vectors $\{TSD1, TSD2, \cdots, TSD_m\}$ generated when the human body moves are collected, and the similarity with the target reference point is calculated as follows [14]:

$$\text{dist}_i = \left\{ \sum_{j=1}^{m} \left| TSD_j - TSD_{ij} \right|^2 \right\}^{1/2}. \tag{11}$$

In equation (11), dist_i represents the Euclidean distance between the target position and the ith reference point in the fingerprint database. K reference points with the smallest
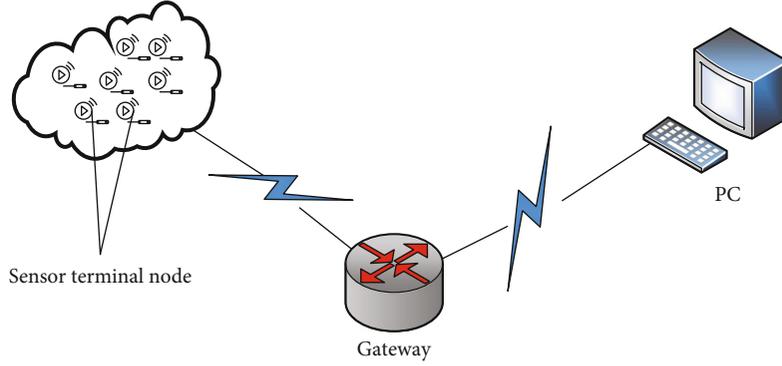
FIGURE 2: Structure diagram of a wireless sensor network.

distance are selected, and the position coordinates of the moving human body under K reference points are calculated as follows:

$$(x, y) = \frac{1}{k} \sum_{i=1}^{K} (x_i - y_i). \tag{12}$$

(2) Naive Bayesian Algorithm. The naive Bayesian algorithm is a learning algorithm based on statistical probability. In indoor location of PIR signals, conditional probability is used to establish the location fingerprint location model, and then the Bayesian law is used to calculate the position of the target. Suppose that there are N fingerprints in the off-line fingerprint database F_p, which are denoted as $\{F_{p1}, F_{p2}, F_{p3} \cdots F_{pN}\}$, and the reference point position corresponding to each fingerprint record is denoted as $\{L_1, L_2, L_3 \cdots L_N\}$, where L_i is denoted as (x_i, y_i). Assuming the existing fingerprint F_p, the posterior probability of the fingerprint appearing at each reference point is calculated by the naive Bayes algorithm, which is denoted as $P(L_i | F_p)$. The expansion formula is as follows [15]:

$$P(L_i | F_p) = \frac{P(F_p | L_i) * P(L_i)}{P(F_p)} = \frac{P(F_p | L_i) * P(L_i)}{\sum_{keL} P(F_p | L_K) * P(L_K)}. \tag{13}$$

In equation (13), $P(L_i)$ is a prior probability, which represents the probability that the real-time fingerprint appears at the reference point L_i; $P(F_p, L_i)$ is the conditional probability of the real-time target position at the reference fingerprint; $P(F_p, L_i)$ is the posterior probability obtained by the Bayesian algorithm. In the constructed system, it is assumed that the target can appear anywhere in the probe field of view. In the naive Bayesian algorithm, it is assumed that the output signals from different PIR nodes are independent of each other; that is, each fingerprint element is independent and irrelevant. On this basis, the conditional probability $P(F_p, L_i)$ can be decomposed into $P(DTS_1 | L_i) \cdots P(DTS_m | L_i)$. Assuming that the PIR signal detected at the reference point satisfies Gaussian distribution, the prior probability can be expressed as follows:

$$P\left(DST | L_i = \frac{1}{\sqrt{2\pi} * \delta_i} \exp\left\{ -\left(\frac{DTS - \mu_i}{2\delta_i^2} \right)^2 \right\} \right). \tag{14}$$

In equation (14), μ_i and δ_i are the mean and standard deviation of signal strength at reference point L, respectively. The calculated posterior probability is taken as the weight coefficient, and the actual position coordinates of the moving target are estimated in combination with the position of the reference point.

$$(x, y) = \sum_{i=1}^{N} P(L_i | F_p) * (x_i, y_i). \tag{15}$$

(3) Neural Network Algorithm. The neural network algorithm is widely used in function approximation, classification, and other fields. In indoor positioning based on a PIR signal, the BP neural network model is mainly used. The BP network is mature in theory and performance, and it has a strong nonlinear mapping ability and a flexible network structure [16]. In the training process of the BP network, the input vector is firstly propagated backward to the output layer through the forward propagation process to obtain the result vector. If the deviation between the output value of the output layer and the expected output value exceeds the given threshold, the weight and bias parameters of the neural network are modified continuously through the error signal back propagation process until the value of the loss function meets certain requirements. The fingerprint location model of the PIR signal position under the BP network is shown in Figure 3.

The steps of BP algorithm in the PIR location process are as follows:

Step 1. The neural network model shown in Figure 3 is established, and the input dimension is the length n of the PIR signal sequence collected for a period of time; the output dimension m represents the category of time series; the number of hidden layers is $l = 1$; and each network parameter is initialized.

Step 2. According to the size of the fingerprint database, the sample data is divided into a certain proportion of training
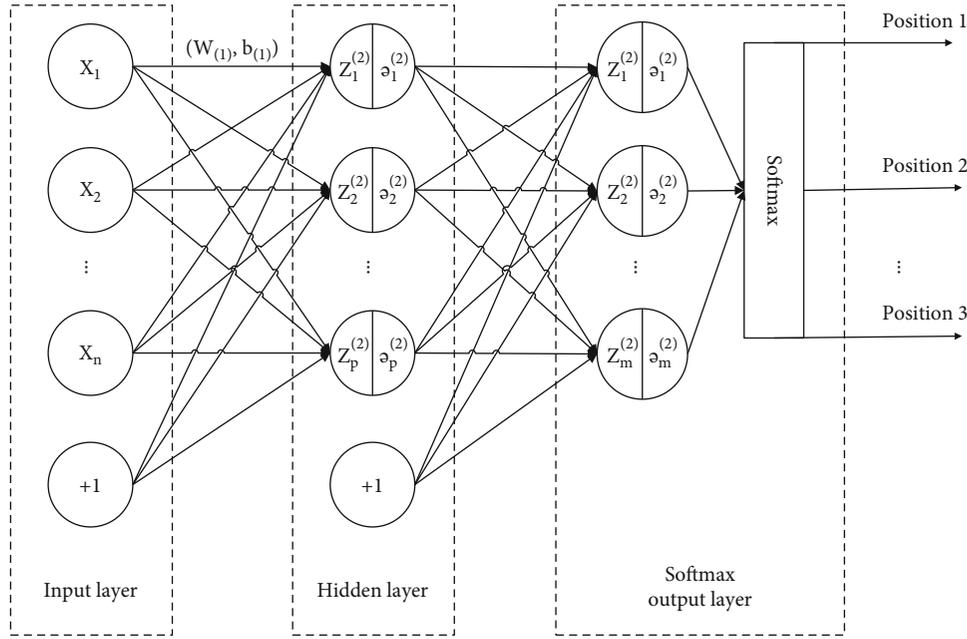
FIGURE 3: Fingerprint location model of the PIR signal position based on the BP neural network.

set and verification set, and the network model is trained by the training set.

Step 3. Calculate the sample output result through forward propagation, and calculate the error between the sample output result and the actual value. If the error does not meet the requirements or the iteration times are not reached, correct each network parameter through back propagation.

Step 4. Back propagation.

In view of the simple structure of the BP neural network and the strong generalization ability in signal sequence classification, the fingerprint location model of the PIR signal position based on the BP neural network will be adopted in the follow-up experiments of this paper.

4. Design and Implementation of Human Motion Recognition System

4.1. Design of Infrared Sensor Unit. A two-stage bandpass amplifier circuit is designed to filter, amplify, and resist interference from the weak infrared signal detected by the pyroelectric probe. The circuit realizes the accurate acquisition of infrared signals of the human body, and its signal processing flow is shown in Figure 4.

The infrared sensing unit is composed of a Fresnel lens array, a pyroelectric probe, and a signal-conditioning circuit. When human bodies with different temperatures from the ambient background pass through the sensing area of the pyroelectric sensor, the sensor will output a weak AC signal of about 1 mV, and this AC signal is superimposed on a variable DC bias signal. Because of the interference of the environment and circuit noise, the weak signal will be

annihilated in high-frequency noise, so a low-frequency bandpass filter circuit at $0.5 \sim 5$ Hz is designed. The signal-conditioning circuit can filter out the DC component of the sensor output signal, amplify the AC part, and filter out the environmental noise.

4.2. Design of Network Transmission Unit. The transmission network used in this design is a wireless network based on ZigBee technology. ZigBee technology is an area network protocol developed by ZigBee Alliance, which has excellent characteristics such as low power consumption and an ad hoc network; thus, it is widely used in wireless sensor networks. The ZigBee protocol stack is a specific implementation of the protocol, through which system developers can understand and use a certain part of the specific protocol. A complete ZigBee protocol stack includes a physical layer (PHY), a medium access control layer (MAC), a network layer (NWK), and an application layer (APL) from bottom to top. This is shown in Figure 5. Among them, the physical layer realizes the communication of the lowest level data, which will handle the receiving and sending of data from the physical end and is the basis of data communication between nodes. The medium access control layer completes the segmentation, recombination, and sequential transmission of the upper or lower layer data packets, thereby ensuring the reliability of data transmission, establishing network beacons, ensuring information synchronization, and establishing stable links between network nodes. The network layer function mainly realizes the establishment of an ad hoc network, configures the attributes and modes of nodes, and controls the transmission of data. The application layer develops the design of users' application requirements, and users can develop and design through the application layer to meet their own wireless sensor network needs.
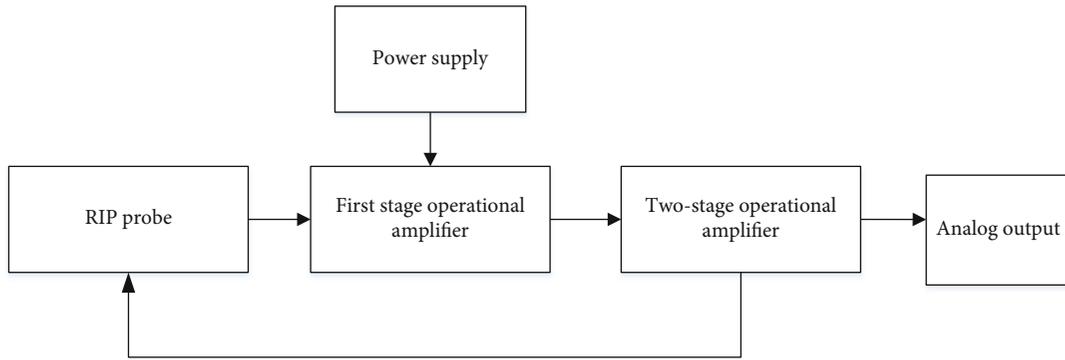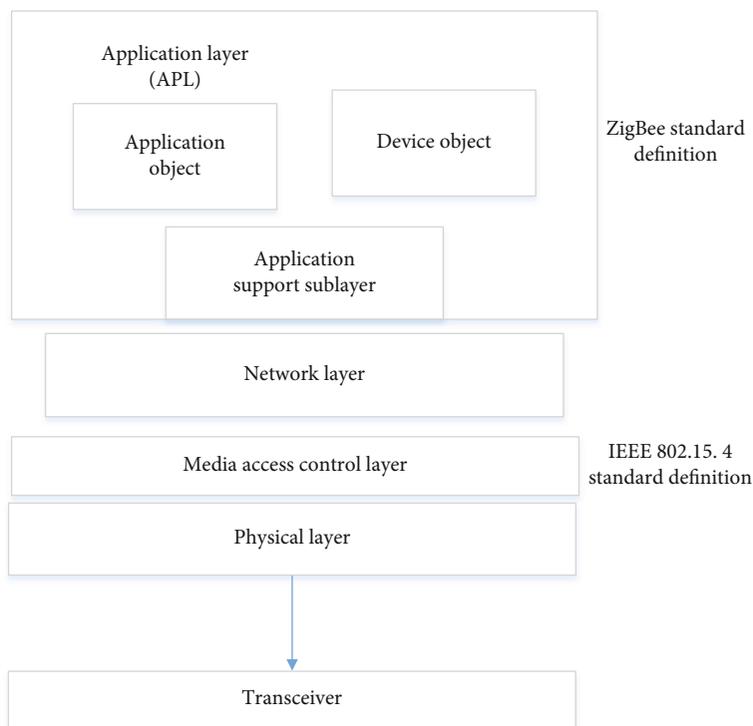
FIGURE 4: FIR signal processing flow.

FIGURE 5: Structure diagram of a ZigBee protocol stack.

According to the different roles of nodes in wireless sensor networks, ZigBee nodes can be divided into the following three types:

(1) Coordinator (Coordinator): the coordinator is responsible for the creation and deployment of the entire network. As a data sink node in the network, it can communicate with any node in the network after the network is deployed

(2) Routing node (Router): as a signal relay node in the network, routing nodes are responsible for forwarding network data. The terminal node can communicate with the coordinator node through the routing node, and the network coverage can be expanded through the routing node
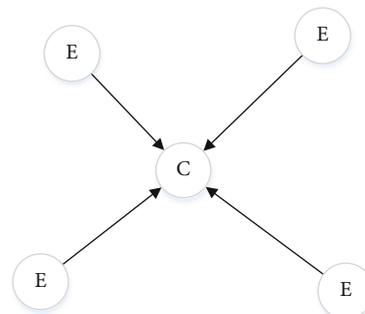

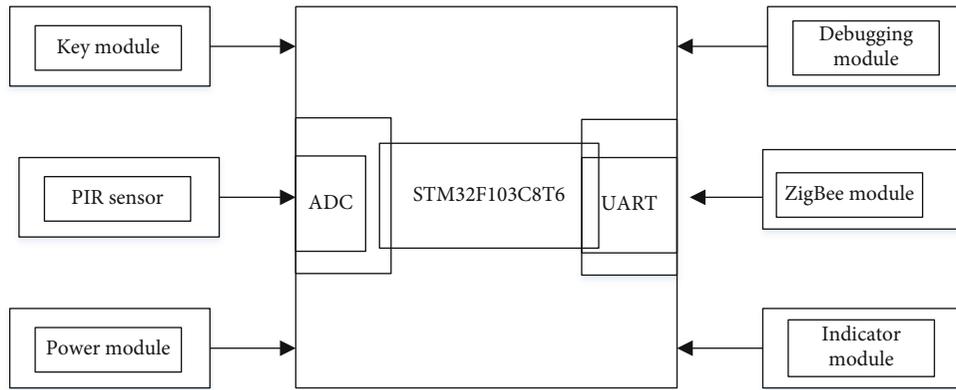
FIGURE 6: Star topology.

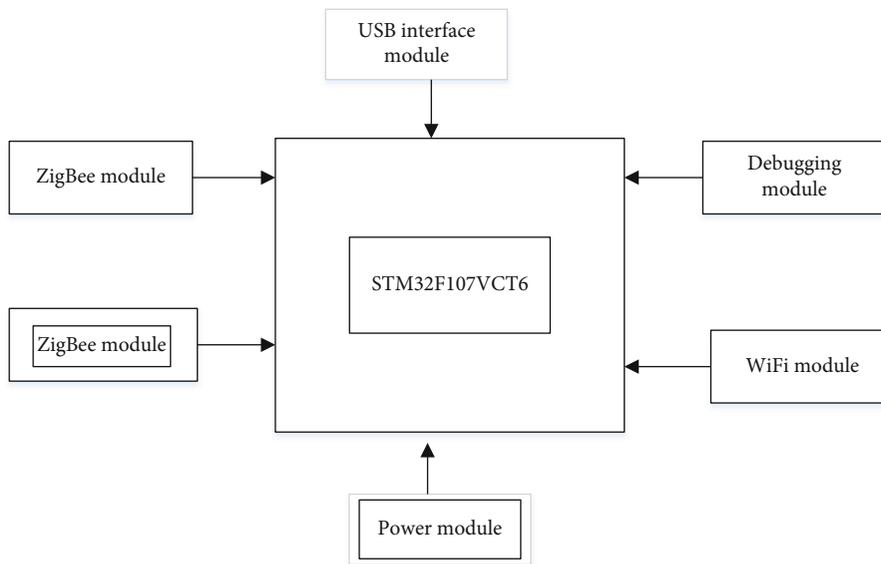FIGURE 7: Design block diagram of an acquisition unit.

FIGURE 8: Gateway design block diagram.

(3) End node (EndDevice): as the bottom equipment in the network, terminal nodes have the functions of signal control, data processing, and transmission, and they are an essential part of the whole network

ZigBee network supports three kinds of topology: star, tree, and mesh. In this design, the star topology structure is adopted, and its topology structure is shown in Figure 6.

At present, the mainstream chips conforming to the ZigBee protocol specification in the market include the CC253x of Texas Instruments and the MC13224 of Freescale. In this design, the CC2530F256 chip of Texas Instruments is selected as the transmission unit in the network. The CC2530F256 chip is packaged in QFN40, the chip size is 6 mm ∗ 6 mm, and the working voltage is 2.0~3.6 V. It is an enhanced C8051 microprocessor with 2 USART serial ports and 21 fast I/O ports. In this design, the E18-MS1PA1-IPX model produced by Chengdu Yibaite Company is selected as the network transmission module of this paper, which integrates CC2530 and CC2592 (PA). A built-in ZigBee pro-
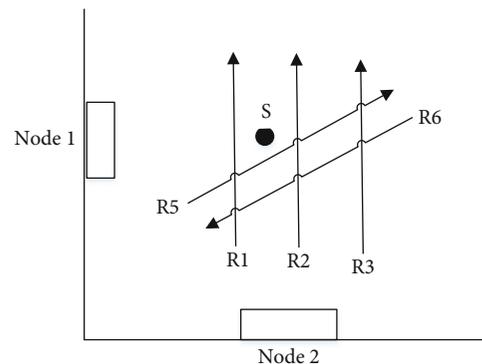

FIGURE 9: Some human movement paths in the experiment.

tocol stack, a 32.768 kHz clock crystal oscillator, a 256 kb flash, and an 8 kb RAM can realize the serial port transparent transmission function. This module is used in the signal acquisition terminal node and the network transmission unit in the coordinator gateway in this design system.
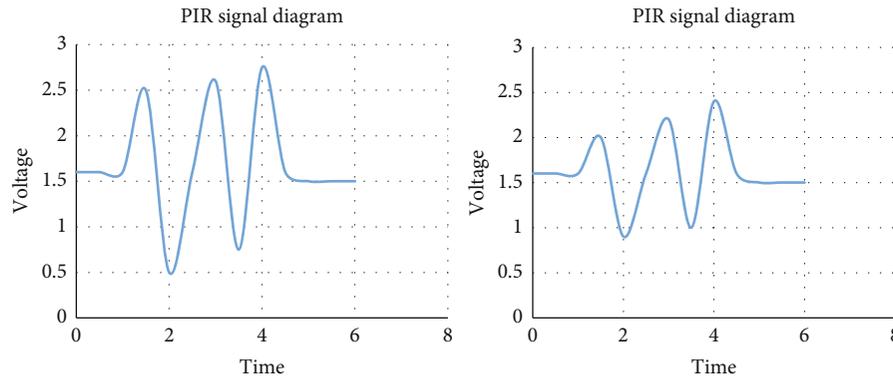
FIGURE 10: PIR signal diagram at different speeds.

4.3. Design of PIR Node Signal Acquisition Unit. The PIR node signal acquisition unit includes a power module and an MCU module, which can complete the data signal acquisition, filtering, packaging, transmission, and other functions. The design block diagram of the signal acquisition unit is shown in Figure 7.

4.3.1. MCU Module. The STM32F103C8T6 single-chip microcomputer used in this design has a 64 k flash and a 20 k SR AM, and the working voltage range is 2.0-3.6 V. It has two 12-bit A/D conversion modules, up to 16 conversion channels, conversion rates of up to 1 μs, a 7-channel DMA transfer controller, 26 fast I/O ports, an SWD debug interface, 7 timers, and 3 USART ports; these features are enough to meet the design requirements of this node and the expansion of future applications.

4.3.2. Power Module. Because the sensor node must be easy to deploy and install and its power consumption requirements are low, four 1.5 V dry batteries are selected for the external power supply, and the DC-DC voltage conversion module is selected for the internal power supply of the MCU and the peripheral sensor equipment. The AMS1117-33 V forward low-voltage regulator is selected as the voltage conversion module, which has 33 V stable output characteristics and supports overload and overheat protection.

4.4. Gateway Design. The gateway device includes a power module, an MCU module, a W-Fi module, a ZigBee module, and a USB serial port module. Through the gateway, the functions of the terminal nodes can be configured, and the network data can be received, unpacked, packaged, and sent. The design block diagram is shown in Figure 8.

4.4.1. MCU Module. The STM32F107VCT6 single-chip microcomputer in this design has a 256 K flash, a 64 K SRAM, a working voltage range of 2.0-3.6 V, a 12-channel DMA transfer controller, 5 USART ports, and an SWD debugging interface. These characteristics are enough to meet the design of this node and the expansion of future applications. The functions of the five serial ports in the gateway are as follows: one USB debugging interface, one

W-Fi communication interface, and up to three ZigBee communication interfaces.

4.4.2. WiFi Module. The W-Fi module model selected is the Shanghai Hanfeng HF-LPB100, which has three working modes of STAIAP/STA + AP coexistence. The STA (station) mode is a site mode, which is equivalent to the terminal node in the network. The AP (access point) mode is the central node in the W1-Fi network. Other terminal nodes in the STA mode can communicate with each other through nodes in the AP mode. Usually, a wireless router is an AP node. In this design, the W-Fi module has the STA + AP mode, that is, the module supports an AP interface and an STA interface at the same time. Through the STA + AP coexistence mode, it is convenient for users to use mobile phones and other devices to monitor the terminal equipment in the network and realize the mode setting of the W-Fi module conveniently without changing its original network position. In the system, the mode configuration of the gateway and the acquisition of network data can be carried out through mobile phone equipment.

4.4.3. USB Adapter Module. The USB to serial port module adopts the CP2102 chip, which can realize data transmission with a PC through a USB cable.

4.4.4. Power Module. Externally, the gateway equipment adopts a general-purpose power adapter with 5 V-1 A and DC5 5 ∗ 2.1 mm interfaces; internally, the AMS1117-3.3 V LDO conversion module is adopted to supply power to the MCU, ZigBee, WiFi, etc.

5. Experiment

5.1. Experimental Environment and Data Processing. In the experiment, each sensor node is fixed at a height of 1.4 m. The MCU collects data at a sampling rate of 100 Hz and transmits it through the ZigBee sensor network in real time. The characteristics of sensor output signals in different motion states are analyzed through a MATLAB real-time interface. Part of the moving path in the experiment is shown in Figure 9, where Node 1 and Node 2 are two sensor nodes in the experimental environment. S is a static position point; R1, R2, and R3 are three paths parallel to Node 1; and
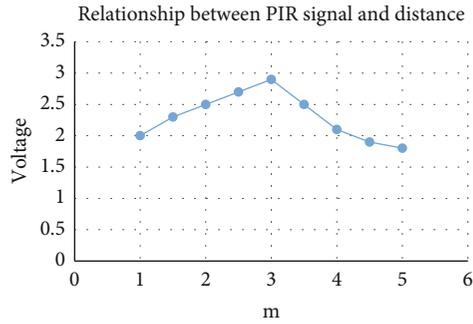
Relationship between PIR signal and distance

FIGURE 11: PIR signal and distance relationship.

Peak time and distance relationship

FIGURE 12: Relationship between peak time and distance.

their distances are D1 = 2 m, D2 = 3 m, and D3 = 4 m, respectively. R5 and R6 are the paths with 135 and -45 angles with Node 1, respectively.

Because different people move at different speeds, in order to eliminate the influence of speed on wireless sensor acquisition parameters, the same person walks along the R2 route at different speeds, and the results are shown in Figure 10.

According to the PIR1 output signal, when the human moving path is the same, different moving speeds will have an impact on the sensor output signal. In this experiment, when the speed is faster, the average amplitude of the sensor output signal is smaller; with the increase of the speed, the average peak time difference gradually decreases.

Because it is an infrared sensing unit, the distance between the equipment and the human body will also affect the collection of human motion parameters. Therefore, we let the experimenter walk parallel to different paths of Node 1 at the same speed and observe PIR signals. The results are shown in Figures 11 and 12.

According to the PIR1 output signal, when the human body moves at the same speed, different moving distances will have an impact on the sensor output signal. In this experiment, when the distance $D = 3$ m, the output signal amplitude of the sensor reaches the maximum value, and the average peak time difference increases with the increase of the distance. The relationship between the peak value and the peak time difference of the sensor output signal and the horizontal moving distance is shown in Figure 12.

From the above experiments, it can be seen that the infrared signal of a human body obtained by the system is a nonstationary random signal due to the tiny movements of the human body in the process of movement and the noise interference of the external environment. However, in this experiment, it is assumed that the human body walks along a fixed path, that is, the sensor will obtain the infrared waveform signal sampled for a period of time every time. By
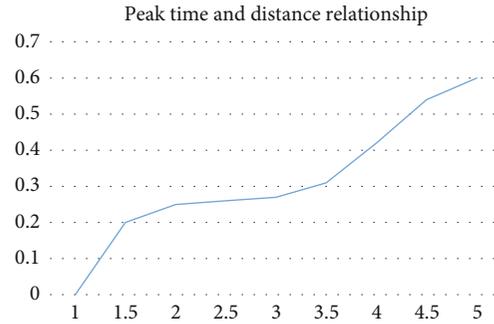
TABLE 1: Classification and recognition results.

Dataset category	Node 1	Node 2	Node 1 and Node 2
Raw dataset	66.41%	64.06%	77.34%
Simplified feature data set	81.25%	82.81%	95.31%

processing the infrared signal of this moving human body, the effective eigenvalue can be extracted, which can help this paper to make further judgment on the position of the human body.

In the experiment, this paper mainly considers the peak value of the signal waveform, the time when the peak value is located, and the number of the peak value. MATLAB firstly saves the collected data in frames and tags them. Then, the original infrared signal sequence is preprocessed, and the extracted effective eigenvalue vector is used as the input of the neural network. The valid eigenvalue data X is as follows:

$$x_i = \left[v_{p1}, \cdots, v_{pi}, \cdots, v_{pm}, t_{pp1}, \cdots, t_{ppj}, \cdots, t_{ppn} \right], \qquad (16)$$

wherein I represents the index of the Ith peak element in the peak time series, and M is the number of peaks in the peak time series, including all peaks of the PIR1 output signal and the first two peaks of the PIR2 output signal; J represents the Jth peak element subscript in the peak time series, and n is the number of peaks in the peak time series, including all peak-to-peak pairs of the PIR1 output signal and the first peak-to-peak pair of the PIR2 output signal. V_{pi} represents the ith peak voltage in the peak time series in volts (V); t_{ppj} represents the Jth peak-to-peak time difference in the peak time series in seconds (s).

According to equation (16), for a group of real-time waveform signals collected by Node 1 in normal travel time at $D = 2$ m and $D = 3$ m, signal peak time series characteristics $x1$ and $x2$ can be extracted, respectively:

$$x1 : [2.48, 0.61, 2.29, 1.11, 1.89, 1.37, 2.48, 0.98, 1.87, 2.24, 1.01, 0.24, 0.20, 0.19, 0.23, 0.30], \qquad (17)$$

$$x2 : [2.44, 0.52, 2.74, 0.80, 2.60, 0.77, 2.74, 0.69, 2.05, 1.85, 1.50, 0.30, 0.25, 0.24, 0.25, 0.33]. \qquad (18)$$

TABLE 2: Accuracy rate of human motion recognition system.

Method	Parallel Node 1	Parallel Node 2	Slant line
Traditional human motion recognition system	72.31%	73.41%	71.82%
Wireless sensor human body recognition system based on blockchain	81.25%	82.81%	95.31%

According to equation (16), for a group of real-time waveform signals collected by Node 1, signal peak time series characteristics $x3$ and $x4$ can be extracted, respectively, when walking normally and fast at $D = 3$ m:

$$x3 : [2.44, 0.52, 2.74, 0.80, 2.60, 0.77, 2.74, 0.69, 2.05, 1.85, 1.50, 0.30, 0.25, 0.24, 0.25, 0.33], \tag{19}$$

$$x4 : [2.45, 0.56, 2.45, 0.94, 2.31, 0.93, 2.51, 0.87, 1.98, 1.76, 1.68, 0.26, 0.20, 0.21, 0.20, 0.10]. \tag{20}$$

From the characteristics of the waveform signal sequence, it can be seen that the distance between a moving human body and the sensor and the speed of the moving human body are related to the peak voltage, peak-peak time difference, and time series length of the sensor output signal.

5.2. Motion Recognition Analysis Process and Results. The task of this experiment is to verify the accuracy of the classification results of a PIR signal time series under the human infrared signal data set constructed in this paper. The experimental requirement is to collect infrared signals of a single human motion state. In this experiment, we mainly classify the position of a moving human body. At the horizontal distance $D_n = 1, 2, 3, 4$ m and the vertical distance $D_v = 1, 2, 3, 4$ m, the infrared signal of the human body is collected by normal walking and fast walking, respectively. In the experiment, a single person did 40 groups of experimental data at the above 8 paths with fast walking and slow walking; that is, a total of 640 groups of experimental data were generated.

In the design of the BP neural network, the number of hidden layers is 1. The conjugate gradient momentum algorithm (trainscg) is selected as the training algorithm, the tansig function is selected as the hidden layer transfer function, the softmax function is selected as the output layer transfer function, the learning rate is set to 0.1, and the mean square error is 1e-3. The number of hidden layer nodes is constantly revised, and a relatively stable neural network is obtained through multiple trainings.

The experimental results are analyzed as follows.

As shown in Table 1, the recognition results of the original data set and the peak time series feature (simplified feature) data set are analyzed, and the recognition results of a single node and a double node are analyzed, respectively. The original data dimension is 600, and the simplified feature dimension is 16. The experimental results show that Node 1 and Node 2 are similar in recognition rate, because each node has a higher recognition rate when moving horizontally with itself, but a lower recognition rate when moving perpendicularly with itself. When two nodes act at the same time, the recognition rate of the whole network is higher due to the data fusion between nodes. When the orig-inal data set is used, the time series obtained on the same path are quite different due to the difference of the intercepting position of the starting point of the time series, but the peak time series feature does not have these problems, and the accuracy rate of a moving human body position recognition is 95.31%.

In order to verify the superiority of this system, the accuracy of the wireless sensor human motion recognition system based on blockchain designed by us is compared with that of the traditional human motion recognition system. We mainly compared three kinds of motion routes: parallel to Node 1, parallel to Node 2, and diagonal line. The mean value of the five experimental results are shown in Table 2.

It can be seen from the experimental results that the system designed in this paper has high accuracy.

6. Conclusion

Traditional vision-based and sensor-based human motion detection methods have some disadvantages, such as high illumination requirements, difficulty in preserving privacy, and poor portability. To solve this problem, combining the advantages of wireless sensing and blockchain technology, a wireless sensor acquisition method of human motion parameters based on blockchain is proposed, and a human motion recognition system is designed. Experiments show that the accuracy of the wireless sensor acquisition method of human motion parameters based on blockchain in this paper reaches 95.31%, which verifies the effectiveness and superiority of the system designed in this paper.

Data Availability

The experimental data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declared that they have no conflicts of interest regarding this work.

References

[1] J. Huang, Y. Hao, M. Zhao et al., "Biomass-based wearable and self-powered pressure sensor for human motion detection," *Composites Part An Applied Science and Manufacturing*, vol. 146, no. 5, p. 106412, 2021.

[2] Y. Zhang, B. Liu, and Z. Liu, "Recognizing hand gestures with pressure-sensor-based motion sensing," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 13, no. 6, pp. 1425–1436, 2019.

[3] N. Xiao, P. Yang, Y. Yan, H. Zhou, and X.-Y. Li, "Motion-Fi+: recognizing and counting repetitive motions with wireless backscattering," *IEEE Transactions on Mobile Computing*, vol. 20, no. 5, pp. 1862–1876, 2021.

[4] H. Kim, S.-H. Shin, J.-K. Kim, Y.-J. Park, H.-S. Oh, and Y.-B. Park, "Cervical coupling motion characteristics in healthy people using a wireless inertial measurement unit," *Evidence-Based Complementray and Alternative Medicine*, vol. 2013, article 570428, 2013.

[5] J. Ren, F. Guan, M. Pang, and S. Li, "Monitoring of human body running training with wireless sensor based wearable devices," *Computer Communications*, vol. 157, pp. 343–350, 2020.

[6] J. Zhou, "Artificial intelligence driven wireless network remote monitoring based on Diffie-Hellman parameter method," *Computer Communications*, vol. 160, pp. 132–138, 2020.

[7] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234–246, 2017.

[8] H. Bai, G. Zhou, Y. Hu et al., "Traceability technologies for farm animals and their products in China," *Food Control*, vol. 79, pp. 35–43, 2017.

[9] D. Ding, "From Ant Financial to Alibaba's Rural Taobao Strategy—how Fintech is transforming social inclusion," *Handbook of Blockchain, Digital Finance, and Inclusion*, vol. 1, pp. 19–35, 2018.

[10] K. W. Lye and J. M. Wing, "Game strategies in network security," *International Journal of Information Security*, vol. 4, no. 1-2, pp. 71–86, 2005.

[11] W. Gan, L. Chen, and Y. Liu, "Research on optical encryption system based on unequal modulus decomposition and polarized vortex optical holography," *Optics Communications*, vol. 482, p. 126609, 2021.

[12] M. Du, Q. Chen, and X. Ma, "MBFT: a new consensus algorithm for consortium blockchain," *IEEE Access*, vol. 8, pp. 87665–87675, 2020.

[13] P. Lorenz, "New path centrality based on operator calculus approach for wireless sensor network deployment," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 1, pp. 162–173, 2019.

[14] B. Jia, B. Huang, H. Gao, W. Li, and L. Hao, "Selecting critical WiFi APs for indoor localization based on a theoretical error analysis," *IEEE Access*, vol. 7, pp. 36312–36321, 2019.

[15] M. Hazas and A. Hopper, "Broadband ultrasonic location systems for improved indoor positioning," *IEEE Transactions on Mobile Computing*, vol. 5, no. 5, pp. 536–547, 2006.

[16] E. S. Tselishchev, A. G. Salin, I. S. Kudryashov, and S. V. Strakhov, "Application of new design automation in the development of the Pregolskaya TPP automated process control system," *Thermal Engineering*, vol. 66, no. 9, pp. 672–680, 2019.