Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 259 (2025) 888–896

Procedia Computer Science

www.elsevier.com/locate/procedia

Sixth International Conference on Futuristic Trends in Networks and Computing Technologies (FTNCT06) held in Uttarakhand, India

Research on Feistel Encryption Algorithm Based On Wireless Medical Sensor Networks

Yichao Tao[a], Chenggui Wang[b], Huanlong Qin[a,*]

[a]*School of Medicine, Nantong University, Nantong 226001, China*
[b]*Department of General Surgery, Jianhu County People's Hospital, Yancheng 224001, China*

Abstract

Wireless Sensor Network (WSN) combines wireless communication and distributed processing technology, and is widely used in military, precision agriculture, medical, environmental monitoring, and intelligent transportation, especially in patient data collection, mobile monitoring, and real-time monitoring. However, WSN faces patient information security issues in medical applications. This article proposes a WSN group encryption algorithm based on chaos theory and performs data compression. The article briefly introduces the concept, characteristics, and security threats of WSN, and elaborates on the basic theory of chaotic encryption technology and its differences from traditional cryptography. In response to the problems of medical information leakage and insufficient existing encryption algorithms, we propose a chaotic block encryption algorithm using the Feistel structure. By using integer chaotic mapping and introducing long period random sequences for XOR operation, we solve the short period problem, improve security, and save energy. In addition, a data compression algorithm based on regression models was designed to address the characteristics of large data volume, high redundancy, and strong real-time performance in medical monitoring. By dynamically adjusting the sampling time and regression model parameters, the compressed data is closer to actual changes, significantly improving compression performance and extending network lifespan. Prioritize vital sign data based on its importance to ensure real-time data transmission. The chaotic encryption algorithm proposed in the experiment has good confusion and diffusion characteristics, which can effectively protect the security of patient data. The compression algorithm reduces data redundancy and WSN node energy consumption, achieving remote monitoring of patient vital signs, enabling doctors to timely grasp the condition and formulate treatment plans. Priority setting ensures rapid transmission of emergency data and earns valuable treatment time for patients.

Peer-review under responsibility of the scientific committee of the Sixth International Conference on Futuristic Trends in Networks and Computing Technologies (FTNCT06)

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: huanlongqin@yeah.net

Peer-review under responsibility of the scientific committee of the Sixth International Conference on Futuristic Trends in Networks and Computing Technologies (FTNCT06)
10.1016/j.procs.2025.04.041

Keywords: WSN, Shaotic Encryption Algorithm, Feistel Network Structure, Medical Information Protection, Security Improvement

1. Introduction

In today's era of rapid development of science and technology, sensor technology, as one of the most important means of information collection and monitoring, plays a key role. Sensor technology, originally developed for reliable transmission between endpoints, has evolved over time into powerful, targeted sensor nodes in wireless sensor networks (WSN) capable of sensing, collecting, and processing large amounts of information. This development continues to revolutionize the way information is analyzed and processed, especially in the fields of military, industrial process control, national security, environmental monitoring and health care, and has had a profound impact, and has been named as one of the top ten emerging network technologies in the future by authoritative magazines such as Technology Review.

With the expansion of wireless sensor network applications, security issues become more and more important and diversified, and different applications have different requirements for security. It is very important to solve the problems of data confidentiality, message authentication, security management, message freshness and authentication broadcast. However, due to the limitations of wireless sensor networks, many mature and effective security protocols and encryption algorithms cannot be applied smoothly. The introduction of chaos provides a new direction for the security research of wireless sensor networks, especially in recent years, a lot of achievements have been made in the research of chaotic encryption algorithms.

We conduct in-depth research on encryption algorithms and data compression techniques in wireless sensor networks to ensure the confidentiality and transmission efficiency of patient data. On this basis, we propose a group encryption algorithm based on chaotic thinking, which improves the chaotic mapping to solve the short period phenomenon and enhance the security and efficiency of the encryption algorithm. In response to the limited energy of wireless sensor network nodes, we have designed a data compression algorithm based on regression models to dynamically adjust sampling time and priority settings, effectively reducing energy consumption and ensuring real-time data transmission.

2. Related Research

In the current era of technology, wireless sensor networks (WSN) and body area networks (BAN) play an important role in the medical and healthcare field. In order to improve the data acquisition effect of wireless sensor networks, C Xuan designed a data acquisition system based on symmetric encryption algorithm[1], and used the MapReduce programming model to achieve efficient and secure privacy protection functions. The experimental results show that the system has the advantages of high efficiency, large amount of data acquisition and high residual energy.PCMenon proposed a PBDM system based on Internet of Things (IoT) applications. Through intelligent recommendation system and wireless body area network sensor [2], it promoted dynamic data communication between doctors and patients, realized real-time update of patient status, and played a key role in disease treatment.

In order to optimize the energy consumption management of wireless sensor networks, Ali Kooshari proposed an optimal routing method, which uses the Water strider algorithm to cluster nodes and selects cluster heads for routing[3]. At the same time, ant colony optimization algorithm (ACO) is used to move short paths between cluster heads, thereby effectively reducing energy consumption and improving packet transmission rate, extending network life.H Sun designed a wireless sensor network monitoring system based on ZigBee technology, and adopted AODVJR multi-path optimization routing algorithm and regional compressed data technology to reduce network energy consumption and extend network life, while maintaining high energy of nodes and low data transmission cost [4]. The system has good stability, reliability and scalability, and can be widely used in other intelligent applications.

Zhao Geng proposed a high-speed block cipher algorithm CFE based on the dual-module structure design, which uses the spatio-temporal chaotic system of a unidirectional coupled map network to generate chaotic sequences and

divides the chaotic encryption process into two modules[5]. The algorithm has the characteristics of simple structure, high speed, flexibility and expansibility, and is suitable for data encryption and protection of wireless medical sensor networks.

Dezheng Zhang studied the effectiveness of using correlation power Analysis (CPA) to evaluate hardware security in Feistel chaotic block encryption algorithm[6]. The results show that CPA can successfully obtain the key and find the important sampling points in the power trajectory, laying the foundation for multi-sample correlation power analysis (MSCPA), which is of great significance for the security analysis of Feistel encryption algorithm in wireless medical sensor networks.INM Shah proposed a lightweight block cipher algorithm with an improved generalized Feistel network (GFN) structure[7], which optimizes the security of the cipher algorithm by reducing the number of encryption rounds, and is suitable for resource-constrained iot devices, especially wireless medical sensor networks.

K Zou proposed an attack method based on quantum algorithm, improved the attack technique on unbalanced Feistel structure[8], carried out quantum attack on Skipjack structure for the first time, and combined Grover algorithm to carry out quantum key recovery attack on six structures. Research on Feistel encryption algorithm for wireless medical sensor networks.Y Li proposed a new method of quantum cryptanalysis. By using the specific structure of Camellia round function [9], he proposed a quantum discriminator for the 5-round Feistel structure, and combined with the Grover-Simon algorithm, The quantum key recovery attack on 7 rounds of Camellia provides a new perspective for the research of Feistel encryption algorithm in wireless medical sensor networks.

S Mishra proposed an efficient, short and secure identity authentication algorithm ESS-IBAA for bilinear pairing computation, which is suitable for wireless medical sensor networks [10]. The algorithm eliminates the requirement and related cost of public key certificate, realizes low power consumption and fast authentication, and improves the communication and computing efficiency of the system.

N Tabassum proposed a new data aggregation algorithm[11], which aims to reduce the memory occupation, communication overhead and energy consumption in wireless medical sensor networks, while improving the security of data transmission.In the practical application of wireless medical sensor network, the efficiency and security of encryption algorithm are very important.

3. Wireless Medical Sensor Network

3.1 Key Technologies

As the core component of intelligent network information system, wireless sensor network has efficient information collection technology, real-time communication function and comprehensive data processing ability. It covers a wide range of monitoring areas, and realizes accurate perception and acquisition of monitoring target information through large-scale deployment of micro-sensor nodes, and applies the information to task processing.

Wireless sensor networks face significant security challenges. Because of its openness and wireless communication characteristics, it is vulnerable to eavesdropping, interception and attack. The physical layer of the network faces interference and destruction, including congestion attacks and physical damage, and measures must be taken to ensure the reliability of communication and the security of nodes. In the face of threats such as collision, unfair competition, and exhaustion attacks at the link layer, encoding, listening, and retransmission mechanisms must be used to ensure the integrity and reliability of data transmission.

At the network layer, false routing information, selective forwarding, and other attack forms may cause routing confusion and data security problems, so it is necessary to adopt policies such as multipath routing to deal with these threats. At the application and transport layer, it is necessary to pay attention to the limitations of energy and storage space, while strengthening the security of key management and data transmission.

As scientists continue to study chaos, its application fields involve physics, biology, ecology, mechanics, meteorology, economics and sociology, and has a wide range of application prospects. Firstly, chaos requires a certain degree of certainty, and secondly, it is a manifestation of nonlinear systems. Chaotic motion trajectories are complex and unpredictable, and even small adjustments can lead to huge changes. However, unlike other random changes, chaotic changes have a certain ordered structure and can maintain spatial regularity.

3.2 System requirement analysis and overall design

The key of wireless medical sensor network design is to ensure the security of patient data and efficiently process large amounts of data. The network faces the problem of patient information leakage and data transmission energy consumption. Traditional encryption algorithms have high complexity and are not suitable for resource-limited environments. Secondly, patient data acquisition results in a large volume of data, requiring simple and efficient compression processing methods. Security requirements include node security, defense capabilities, attack identification, and information transmission confidentiality. The compression requirement requires the algorithm to be simple in structure, high in computing efficiency and suitable for data characteristics. Functional requirements include diverse data collection, real-time transmission and management, as well as historical data analysis and research capabilities. These requirements are factors that must be optimally considered in the design.

Wireless medical sensor network monitoring system uses sensing technology and modern wireless communication technology to realize portable, low power consumption, real-time security monitoring of human health parameters. The system includes a medical sensor node, a gateway node, and a remote monitoring center, as shown in Figure 1. In the monitoring area, patients carry sensor nodes with encrypted modules to collect blood pressure, temperature and pulse data, and can move freely. The gateway node is responsible for centralized processing of the collected data, and transmits it to the local or remote monitoring center through the network to realize real-time monitoring, alarm and medical treatment of physiological signals.

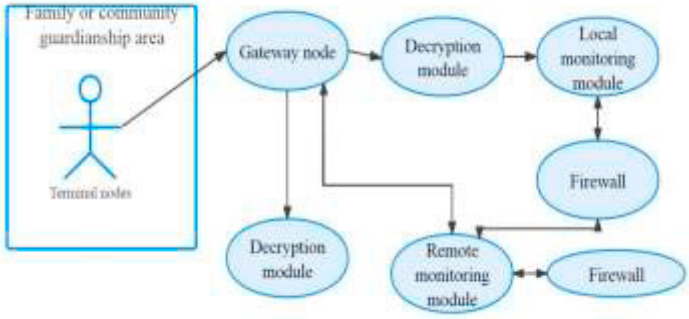

FIG.1 Monitoring process of wireless medical sensor network

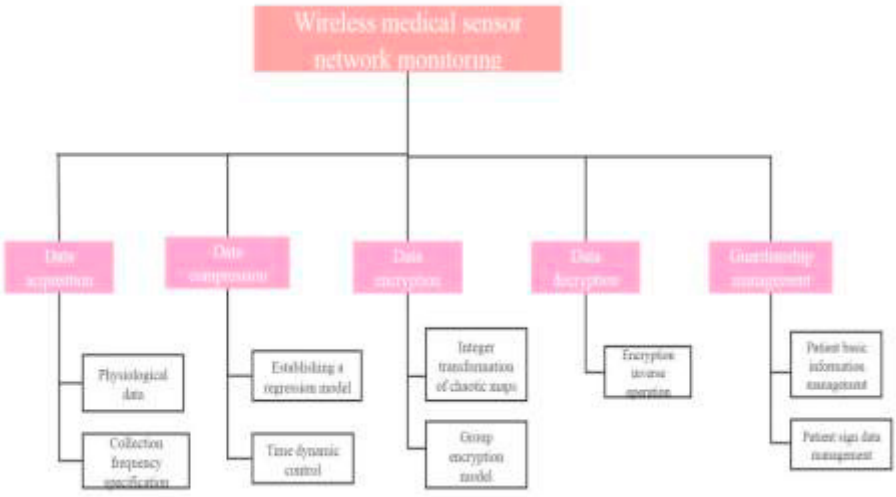

FIG.2 Monitoring function structure of wireless medical sensor network

The functional structure of wireless medical sensor network monitoring system is shown in Figure 2, which covers a number of important modules. These modules include data acquisition, data compression, data encryption, data transmission, data decryption and monitoring management. The main task of the data acquisition module is to obtain vital signs information from patients in the monitoring area through the medical sensor node. The frequency and time interval of collection can be adjusted as needed to ensure the accuracy and timeliness of information.

The data decryption module is used to decrypt the transmitted physiological parameter data. Due to the fact that the Feistel structure has the same architecture in the encryption and decryption processes, the decryption process iteratively uses keys in reverse order, thereby reducing the energy consumption of wireless sensor network nodes.

The monitoring and management module is to analyze and manage the patient's data by the medical staff of the medical monitoring center, including browsing the basic information of the patient and inquiring the vital signs data. When monitoring data exceeds the normal range, the system will issue alerts or provide corresponding care and treatment recommendations, thus realizing the informationization and modernization of medical services.

4. Test and verification

4.1 Chaotic encryption algorithm and data compression processing based on Feistel encryption algorithm

In the application of wireless sensor networks in medical field, a chaotic based packet encryption algorithm is proposed. We describe in detail several classical chaotic maps and their integer processing methods to solve the short-period problem caused by the resource limitation of wireless sensor networks, and optimize them by the method of composite chaotic sequences.

Logistic mapping is a typical one-dimensional chaotic mapping, and its mathematical formula (1) is as follows:

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

Where xn is the value of the NTH iteration and μ is the system parameter. When the value of μ is between (3.57,4), the system exhibits chaotic behavior. For example, μ =2 has a periodic variation, while μ =3.8 has no fixed period between 0.2 and 0.9. The equivalent form is formula (2) :

$$x_{n+1} = \lambda x_n(1 - x_n) \tag{2}$$

Where, when μ=4, λ=2. By using a formula on both ends of the multiplied by an integer a 2 available: $a^2 x_{n+1} = a^2 \lambda x_n(1 - x_n)setz_n = a x_n$， , then get a integer form: ： $z_{n+1} = a^2 z_n(a - z_n)$The value of zn is [0,2a]. For a computer with word length L, a=2^{L-1}, as shown in the following table, when L=32 时， a=2^{31}.

This integer form can avoid floating point operation, and is suitable for wireless sensor network nodes with limited resources and computing power. After processing, only shift and addition and subtraction operations are performed, which significantly reduces the complexity and energy consumption, and is very suitable for encryption applications in wireless sensor networks.

Aiming at the large amount of data generated in the process of medical monitoring, a compression algorithm based on regression model is proposed, which can effectively reduce the redundancy of data and reduce the amount of data transmission. Finally, prioritize data according to the importance of vital signs to ensure that key data can be transmitted to the monitoring center in time, so that doctors can understand the patient's dynamics and care or rescue.

The autocorrelation problem of the integer chaotic map can be evaluated by the autocorrelation function. The calculation formula (3) of the autocorrelation function is shown as follows, Where len is the length of the sequence, xi is the i th element of the sequence, x is the mean value of the sequence, and m is the parameter of the autocorrelation function. By calculating the autocorrelation function, the randomness and precision of the integer chaotic mapping can be evaluated.

$$R(m) = \frac{1}{len}\sum_{i=1}^{len-m}(x_i - \bar{x})(x_{i+m} - \bar{x}) \tag{3}$$

Table 1. Corresponding relationship of chaotic sequence period after integer change

a	Corresponding bit	Different disposal cycle period
2^7	8	4-24
2^{15}	16	7-46-79-119
2^{23}	24	272-716- 224-1
2^{31}	32	14448-33986-232-1
2^{39}	40	Minimum value:25538
2^{47}	48	Minimum value:532029

The number of binary bits in the calculation of integer chaotic mapping is an important criterion to measure randomness. The more bits, the better the binary properties, the better the autocorrelation, and the closer to the ideal randomness. The results in Table 1 show that the autocorrelation values of the integer Kent chaotic map vary greatly, and the randomness is not ideal. Therefore, it is necessary to solve the problem of dynamic degradation of chaotic mapping after integer, that is, the problem of short period, in order to ensure that the chaotic sequence in the encryption process has long periodicity and good pseudo-random performance.

Feistel structure and SP structure are common block cipher structures. The SP structure enhances the diffusion and confusion in the process of encryption through multiple S-layer functions and P permutation, which improves the security, but the encryption and decryption methods are different and consume more energy. While Feistel structure encrypts and decrypts in the same way, the security depends on the design of wheel function F, which needs to be complex and irreversible.

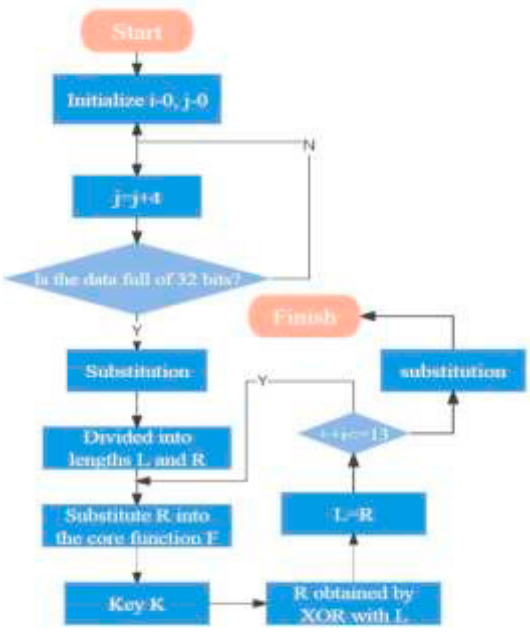

FIG.3 Flow chart of WSN encryption algorithm based on chaos

The number of iterations of the core function F is chosen as half of the cycle, taking into account the algorithm confusion and security, as well as encryption speed and storage capacity. The plaintext unit of the algorithm is 32 bits, but the basic unit of 8 bits is used for storage and calculation, and the simple operations such as XOR, shift, addition and subtraction are used to adapt to the limited node resources. Compared with SP structure, Feistel structure saves node energy consumption, and the decryption and encryption processes are inverse operations, as

shown in Figure 3. Although the design of the core function F is complex and irreversible, it does not affect the reversibility of the encryption algorithm.

4.2 System implementation test and result analysis

We use JAVA as programming language in our research, and combine MyEclipse development platform, which makes the system has good portability and flexibility. The first task is to design the wireless medical sensor network monitoring system, including user login, vital signs data display and medical personnel management and other core functions. In the aspect of data encryption, we adopt the chaotic group encryption algorithm, which has low computational complexity and is very suitable for the resource-limited environment of wireless sensor networks. In addition, in the data compression module, we adopt the method of dynamically adjusting the sampling time and rebuilding the regression model, which effectively reduces the amount of medical data transmission, thus saving the energy overhead. Finally, we optimized the data transmission module, especially prioritizing the vital signs data to ensure real-time transmission and accuracy of the data.

We collected vital signs data, including pulse, temperature and blood pressure, from eight patients in a hospital. Figure 4 and Table 2 record the sampling values of the eight patients at the same time point, while Figure 5 and Table 3 record the ten sampling values of the seventh patient at different time points.

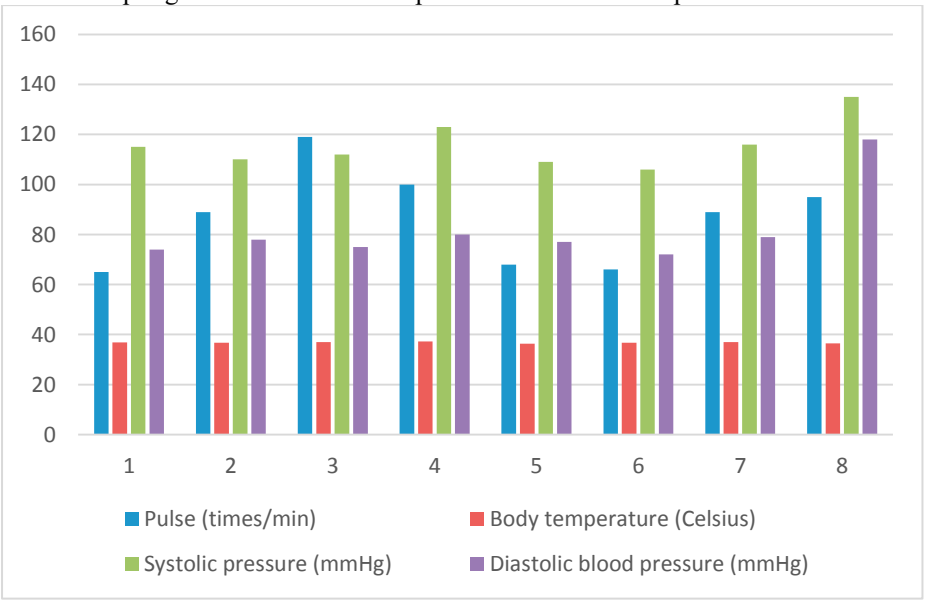

FIG.4 Patient simultaneous sampling data

Table 2. Sampling data of different patients at the same time

Patient	Pulse (times/min)	Body temperature (Celsius)	Systolic pressure (mmHg)	Diastolic blood pressure (mmHg)
1	65	36.8	115	74
2	89	36.7	110	78
3	119	37	112	75
4	100	37.2	123	80
5	68	36.4	109	77
6	66	36.7	106	72
7	89	37	116	79
8	95	36.5	135	118

Table 3. Sampling data of the same patient at different times

Frequency	Pulse (times/min)	Body temperature (Celsius)	Systolic pressure (mmHg)	Diastolic blood pressure (mmHg)
1	109	37.5	140	110
2	100	37	132	97
3	96	37	127	82
4	99	36.9	123	88
5	79	37	116	79
6	94	36.5	120	86
7	65	36.8	119	82
8	73	36.7	128	96

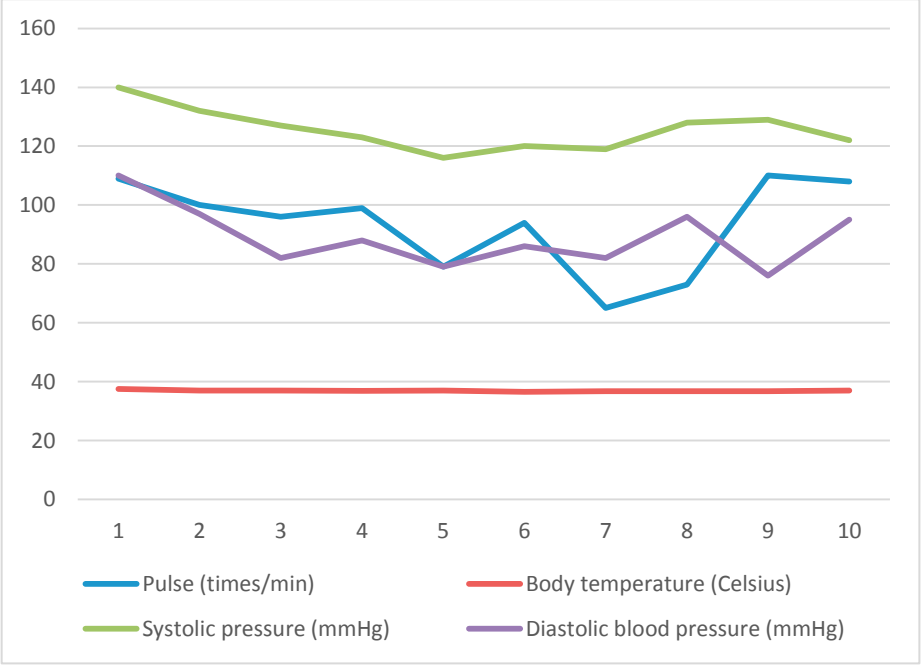

FIG.5 Comparison of sampling data of the same patient in different time periods

In this study, JAVA programming language is used and MyEclipse development platform is adopted, which makes the system have good portability and development flexibility. The system design covers the login interface, patient vital signs data display and medical personnel management and other functional modules. In order to ensure patient privacy, the block encryption algorithm based on chaos theory is adopted in the data encryption module, which has low computational complexity and is very suitable for resource-limited wireless sensor networks.

5. Conclusion and Prospect

The rapid development of wireless sensor network technology in the medical field has not only promoted the informatization transformation of modern medical models, but also effectively solved many problems in traditional medical methods, better adapting to the needs of modern life. This method successfully solves the problems of high redundancy, large volume, and low fault tolerance in vital sign data. On the premise of ensuring data security, by designing a complex and irreversible core function F and utilizing the sensitive characteristics of chaotic initial values for key updates, the system's anti attack ability and data protection effect have been greatly improved.

Meanwhile, by dynamically adjusting the data collection time and reconstructing the univariate linear regression model, the compression algorithm not only effectively reduces the amount of data transmission and node energy consumption, but also maintains the accuracy of data changes. With the continuous advancement of technology, further research and optimization of the integer performance of chaotic encryption algorithms, exploration of new chaotic mapping methods, and improvement of optimization strategies for data collection time will help to further enhance the security and efficiency of wireless medical sensor networks. Establishing a security performance evaluation model for chaotic encryption algorithms to meet the special needs of wireless medical monitoring will make it more adaptable and practical, providing stronger support for the secure transmission and efficient management of medical information.

References

[1] Xuan C. Design of Wireless Sensor Network Data Acquisition System via Health Sensor Based on Symmetric Encryption Algorithm[J]. Journal of Testing and Evaluation: A Multidisciplinary Forum for Applied Sciences and Engineering, 2023.

[2] Menon P C, Bipin P R, Ragesh G K ,et al.Smart Critical Patient Care System with Doctor and Bystander Support with Wireless Sensor Network Using IoT and Intelligent Recommender Algorithm[J]. 2021.DOI:10.1007/978-981-16-1056-1_2.

[3] Kooshari A, Fartash M, Mihannezhad P ,et al.An optimization method in wireless sensor network routing and IoT with water strider algorithm and ant colony optimization algorithm[J]. Evolutionary Intelligence, 2024, 17(3):1527-1545.DOI:10.1007/s12065-023-00847-x.

[4] Sun H, Hu J .Study on the Wireless Sensor Network Monitoring System Based on ZigBee Technology and Optimization Algorithm Simulation[C]//International Wireless Communications and Mobile Computing Conference.2021.

[5] Zhao Geng. Chaotic based Two-module Feistel structure local speed block cipher algorithm design [J]. Journal of Beijing Institute of Electronic Science and Technology, 2021(003):029.

[6] Zhang D, Zhang S, Luo Y ,et al. Cryptanalyzing a Feistel Chaotic Block Cryptosystem Based on Correlation Power Analysis[J].International Journal of Bifurcation and Chaos, 2022.DOI:10.1142/S0218127422501279.

[7] Shah I N M, Ismail E S, Samat F ,et al. Modified Generalized Feistel Network Block Cipher for the Internet of Things[J]. 2023.

[8] Kun Z, Xinfeng D, Fuzhong Z .Improved quantum attack on several generalized unbalanced Feistel structures[J]. 2022 International Conference on Networks, Communications and Information Technology (CNCIT), 2022:113-121.DOI:10.1109/CNCIT56797.2022.00026.

[9] Li Y, Lin H, Liang M ,et al. A new quantum cryptanalysis method on block cipher Camellia[J]. IET Information Security, 2021.DOI:10.1049/ise2.12037.

[10] Mishra S, Yaduvanshi R, Dubey K ,et al. ESS‐IBAA: Efficient, short, and secure ID‐based authentication algorithm for wireless sensor network[J].International Journal of Communication Systems, 2021.DOI:10.1002/dac.4764.

[11] Tabassum N, Deshpande D A, Singh S P .SECURE DATA AGGREGATION ALGORITHM IN HETEROGENEOUS WIRELESS SENSOR NETWORK[J]. 2021.