Secure Transmission Algorithms for Multiplexing Information of Inter-Domain of Wireless Sensor Networks

Xiaopeng Yan* and Qiang Wang

Shandong Vocational College of Industry, Zibo 256414, China
E-mail: yanxp1325@163.com; wangq1325@163.com
**Corresponding Author*

Received 12 January 2026; Accepted 21 April 2026

Abstract

To enhance the anti-attack capability of inter-domain wireless sensor networks and ensure secure information transmission, a secure transmission algorithm for multiplexing inter- domain wireless sensor network information is proposed. This algorithm utilizes the inter- domain structure of wireless sensor networks to analyze channel transmission characteristics, integrating the network information transmission principles of multiplexing technology to construct a robust communication framework. The transmission model of inter-domain multiplexed information in wireless sensor networks is constructed. This model primarily relies on the HRC-MAC protocol, leveraging the characteristics of code division multiplexing to perform uplink spread spectrum and downlink modulation of information. It also incorporates the threshold method for information encryption and transmission control, which can improve the security of information transmission while reducing the fading loss of channel transmission. The experiment constructs a wireless sensor network environment and uses the algorithm for secure information transmission. The experimental results show that the channel transmission security

Journal of Cyber Security and Mobility, Vol. 15_4, 1023–1052.
doi: 10.13052/jcsm2245-1439.1549

capacity of the algorithm exceeds 1.5 bps/Hz, and the transmission security rate meets the standard. The transmission security factors of the channel within the domain exceed 0.917. The anti-attack performance of information encryption exceeds 90.2%. It can effectively disrupt the information sequence and significantly prevent tampering during information transmission.

Keywords: Wireless sensor networks, inter-domain, multiplexing, information security transmission, channel transmission characteristics, code division multiplexing.

1 Introduction

Wireless sensor networks (WSN) are mainly composed of micro sensor devices, which can realize the perception and monitoring of external targets or environments through wireless information transmission [1]. Such networks have the advantages of good networking flexibility, low cost, and adjustable deployment position, and it can be connected to the Internet through wired or wireless means to form a multi hop self-organized network [2]. However, in the application process, it also faces great security challenges. This type of network primarily forms a transmission domain through wireless sensor nodes [3]. Each inter-domain sensor node is exposed and relies on wireless transmission, which cannot guarantee network privacy and controllability [4]. As a result, during information transmission, sensor nodes are highly susceptible to external intrusion, leading to information leakage, damage, and even system compromise [5]. How to improve the security of information transmission in the WSN inter-domain and ensure the confidentiality, integrity, and availability of network information transmission has become the key research content of this network application [6].

Sureshkumar and Vimala [7] used technologies such as golden ant lion whale optimization (GALWO) and golden sea lion optimization (GTSLNO) to improve the information transmission security and reliability of wireless sensor networks. These methods are instrumental in selecting cluster heads and predicting the age of neighboring nodes, thereby ensuring the trustworthiness and robustness of the network structure. In application, this method effectively addresses transmission security within the network but performs poorly for exposed sensor nodes. Balamurugan et al. combined the enhanced Elman spike neural network and fractional discrete Chebyshev moment method [8] to encrypt the information to ensure transmission integrity. However, in the application process of this method, when multiple nodes in the

network domain are invaded at the same time, the encryption effect of this method will be reduced. Vijayakumar designed a secure transmission path for WSN routing, and used encryption technology to encrypt data along the selected path to ensure data transmission security [9]. However, this approach may compromise the real-time performance of information delivery in practical applications. Bethi and Moparthi used an energy-efficient routing protocol for network node selection, and determined the best transmission node by analyzing the residual energy of the node and its adjacent nodes, so as to ensure the safe transmission of information while reducing the transmission power [10]. However, in the application process of this method, if the amount of transmitted information is large and there are many types of information, its transmission efficiency is low.

Multiplexing technology can combine multiple low-speed channels into a high-speed channel to make more effective use of data link capacity [11], allowing high-speed backbone links to serve multiple low-speed access links, so that the network backbone can simultaneously carry a large number of voice and data transmissions. In addition, the technology can establish multiple communication channels on the physical line, and collect data from multiple users of the same domain [12]. Meanwhile, on the receiving end, the multiplexer separates and distributes the data to each user. Data from multiple users are collected together and then transmitted through physical lines. At the same time, on the receiving end, the multiplexer separates and distributes the data to each user. Therefore, this technology has been widely used in wireless networks. In order to realize the secure transmission of information between domains in wireless sensor networks, this paper designs a network information transmission framework, and constructs a task model based on reuse technology. In this paper, the encryption algorithm is added to the model to ensure the secure transmission of a large number of multi category information in wireless sensor networks. However, in cross domain scenarios of wireless sensor networks, the direct application of multiplexing technology and traditional encryption methods faces specific challenges. Multiplexing aims to aggregate multiple channels to improve transmission efficiency, but this may also expand the attack surface, making multiple concurrent information streams across domains more susceptible to collaborative interception and interference. However, traditional encryption methods are designed independently of the underlying physical channel characteristics, making it difficult to adaptively respond to security threats caused by multiplexing in dynamic and shared channel environments. Therefore, this paper proposes a cross domain multiplexing information security

transmission algorithm that deeply couples channel sensing and encryption control. This algorithm is not simply a combination of two techniques, but rather a unified transmission model based on HRC-MAC protocol and code division multiplexing. Its contribution is specifically reflected in utilizing the pseudo-random code characteristics of code division multiplexing to tightly integrate channel multiple access and information encryption and decryption at the physical layer. Furthermore, by using a threshold method based on channel attenuation loss and real-time signal-to-noise ratio evaluation, the encryption strength and transmission strategy are dynamically controlled to enable the security mechanism to respond to changes in cross domain multiplexed channels, thereby improving capacity and reliability while ensuring the confidentiality and integrity of information in the face of interception, interference, and other attacks.

2 Secure Transmission of Multiplexing Information of Inter-Domain of Wireless Sensor Networks

2.1 Inter-Domain Structure of Wireless Sensor Networks

WSN primarily refers to achieving area coverage via each sensor node [13], networking the nodes according to application requirements, forming a specific topology, and enabling information transmission within the domain through each node. The entire network comprises three parts: node inter-domain, the Internet, and the control center. When building a standard WSN, its network model has a direct impact on the role of sensor nodes and communication effects among base stations. When networking the sensor nodes, inter-domain coverage design should be carried out in combination with monitoring requirements so as to ensure the application effect of the network [14].

WSN inter-domain refers to the communication range formed between different wireless sensor nodes and forwarding nodes, as well as between them and external intrusion nodes, under the unified management of base stations in wireless sensor network architecture. It covers the transmission path and range that may include multiple relay nodes from the information sending node to the receiving node, and its core is to ensure the security and integrity of information transmission in this complex channel environment. WSN inter-domain primarily comprises the base station, sensor node, forwarding node, and intrusion node. The intrusion node is the biggest factor that affects the security of information transmission of the network inter-domain.

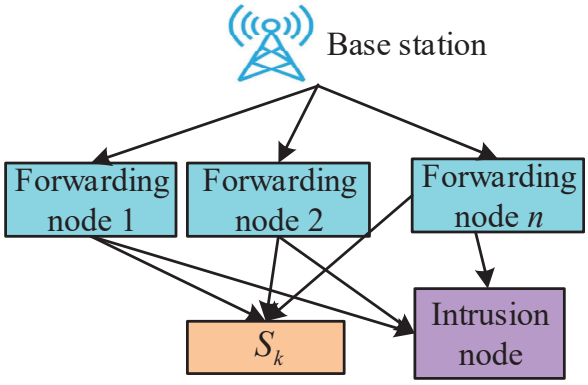


Figure 1 Information transmission structure in the WSN inter-domain.

The attack primarily targets the link between forwarding nodes and sensor nodes, aiming to intercept and steal the information being transmitted, as seen in selective forwarding attacks [15]. The information transmission structure of inter-domain is shown in Figure 1.

All devices in the WSN inter-domain are managed by the base station in a unified way. Each device is equipped with an antenna and operates in half duplex mode:

(1) If the forwarding node is represented by R_i, in which $i = 1, 2, \ldots, N$, the channel response parameter between the base stations and R_i is represented by h_{B,R_i}, the channel response between R_i and the intrusion node is represented by h_{E,R_i}.
(2) The channel response parameter of S_k between R_i and the sensor nodes is represented by h_{S_k,R_i}.
(3) If all the channels in the WSN inter-domain follow the Rayleigh fading principle, then the formulas of the cumulative distribution function $F_{gXY}(x)$ and the probability density function $f_{gXY}(x)$ of the channels are:

$$F_{gxy}(x) = 1 - exp\left(-\frac{x}{\Omega_{XY}}\right) \tag{1}$$

$$f_{gXY}(x) = \frac{1}{\Omega_{XY}} exp\left(-\frac{F_{gXY}(x)x}{\Omega_{XY}}\right) \tag{2}$$

$$g_{XY} = \frac{f_{gXY}(x)|h_{XY}|^2}{d_{XY}^{\sigma}} \tag{3}$$

where X and Y denote any two nodes in the domain; channel covariance and distance between two nodes are denoted by h_{XY} and d_{XY}^{σ}; σ indicates the path loss factor; Ω_{XY} denotes the average value of channel gain in the domain.

There are many types of nodes in the WSN inter-domain and, during information transmission, the intrusion node will invade the channel of the transmission process, affecting the security and integrity of network information transmission.

2.2 Secure Transmission of Multiplexing Information in the Inter-Domain of Wireless Sensor Networks

2.2.1 Network information transmission with multiplexing technology

In WSN inter-domain information transmission, each channel is limited to transmitting a single piece of information [16], leading to low network transmission efficiency. Multiplexing technology enables the aggregation of multiple terminals onto a single multiplexing device, which can then be connected to a computer via a dedicated set of lines for information transmission. The network information transmission with multiplexing technology is shown in Figure 2.

The multiplexer can collect all channel information in the WSN inter-domain and combine multiple channels to form a separate data stream, which is then transmitted through the network system. During the process of receiving transmission information, similar multiplexers [17] classify and process the information, which is then allocated to the designated channel to determine the channel location and ensure efficient information transmission.

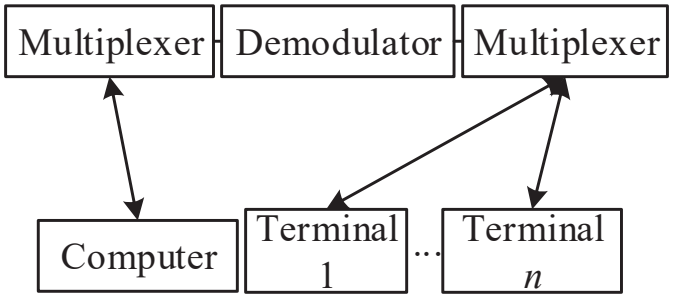


Figure 2 Network information transmission with multiplexing technology.

2.2.2 Construction of the transmission model of multiplexing information in the WSN inter-domain

Since nodes in the WSN inter-domain can transmit large amounts of multi-category information, an intrusion node can lead to significant information leakage or destruction. Therefore, to ensure secure information transmission in the WSN inter-domain, it is necessary to build an information transmission model using the sender as a reference and implement split transmission [18]. Combining with the characteristics and principles of multiplexing technology analyzed in the above sections, the information transmission model in the WSN inter-domain is constructed to ensure the secure transmission of information in the WSN inter-domain. The structure of the transmission model of multiplexing information in the WSN inter-domain is shown in Figure 3.

Based on the multiplexing information transmission model within the WSN inter-domain as depicted in Figure 3, the channel selection criteria for both information transmission ends are established. The specific criteria are outlined as follows:

(1) In the context of wireless sensor networks, where a single communication channel is often the only option for data transmission, this channel is selected and the information is transmitted using encryption to ensure security.
(2) In the context of secure communication between two parties, the selection of multiple channels must consider the efficiency and security

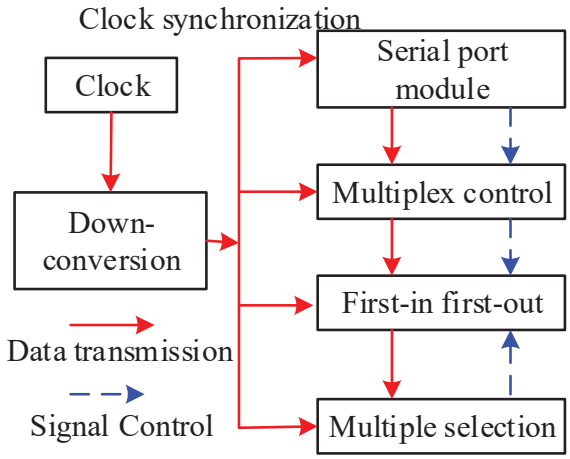


Figure 3 Structure of the transmission model of multiplexing information in the WSN inter-domain.

of information transmission. This involves comprehensive measurement [19] to determine the optimal transmission channel using a protocol and ensuring the encryption of the transmitted information.

2.2.3 Transmission protocols of multiplexing information

In the application process, the transmission model of multiplexing information in the WSN inter-domain is mainly based on the HRC-MAC protocol. It uses the characteristics of Code Division Multiplexing (CDMA) to ensure that multiple sensors requiring data transmission can share the channel simultaneously, meeting the requirements of real-time information synchronous transmission.

CDMA can assign values to the collected data of each sensor node, process the bandwidth by increasing the bandwidth, make it generate a high-speed pseudo-random code, then encrypt and send it. The receiving terminal of wireless sensor node can demodulate the unique pseudo-random code to form narrow bandwidth signal information. In addition, when variable rate information transmission of multiple types of information is done, multiplexing can be carried out in each dedicated physical data channel frame [20–22], and different information can be transmitted through channels with different frame total bit rates, so as to meet the transmission requirements of different types of information. The choice of HRC-MAC protocol as the core of this solution is mainly due to its deep integration with code division multiplexing technology, which can directly meet the requirements of the proposed secure multiplexing transmission architecture. The HRC-MAC protocol allocates and manages unique pseudo-random codes for each sensor node in the network by utilizing the core mechanism of code division multiplexing. This feature is the foundation for building a secure transmission model, which not only allows information streams from multiple sensors to be transmitted concurrently on the same frequency band, achieving efficient multiplexing of physical channels, but more importantly, these unique pseudo-random codes directly serve as the key basis for information encryption and decryption. At the transmitting end, information is spread and encrypted using pseudo-random codes. At the receiving end, it relies on the same pseudo-random code for despreading and decryption. This approach, which tightly combines multiple access with physical layer encryption, can more fundamentally combat channel interception and interference attacks compared to traditional MAC protocols based on time-division multiplexing or frequency division multiplexing. Without the correct pseudo-random code, intruders find it difficult to separate and crack specific node information from

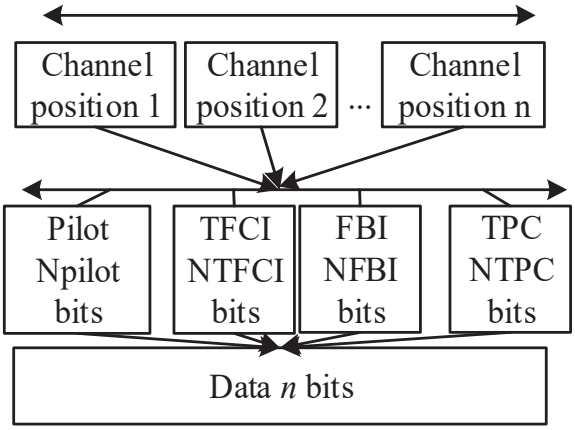


Figure 4 Uplink channel frame structure.

the mixed signal. Therefore, the code division based concurrent transmission and built-in encryption mechanism provided by the HRC-MAC protocol make it particularly suitable for cross domain information reuse scenarios in wireless sensor networks that require high transmission security and real-time performance.

When information transmission is carried out by wireless sensor networks based on the transmission protocols of multiplexing information, in the case of point-to-point transmission, it needs to be completed through the downlink channel frame structure and uplink channel frame structure shown in Figure 4.

In this model, each sensor node within the domain is allocated a unique physical channel, which is a common approach to ensure efficient communication and reduce interference in wireless sensor networks. When other standby channels and multiplexing channels complete the fixed rate allocation and mapping, the allocation of the same channel code is completed in the WSN inter-domain using the main public control channel. After the sensor network receives the unique scrambling code, it completes the matching and decrypts encrypted information.

2.2.4 Encryption transmission method of multiplexing information in the WSN inter-domain

The WSN inter-domain multiplexing information encryption transmission method designed in this paper is not simply a combination of multiplexing protocols and encryption techniques, but rather a complete process of deeply

coupled channel state perception and dynamic encryption control, which directly and quantitatively correlate the security of information transmission with the real-time quality of physical channels. Firstly, the initial transmission state is determined based on the channel cumulative distribution function and probability density function, and then an information distribution sequence formed by Gaussian distribution source signal and additional signal that satisfies the Laplace distribution condition is introduced. Based on this, the channel transmission attenuation loss is accurately calculated. This calculation result provides key input for subsequent dynamic control. Subsequently, the method dynamically determines the transmission process by comparing the node signal-to-noise ratio in real-time with an adaptive set value. By using derivative operations to generate out of order transmission sequences of information, the channel state is directly correlated, so that encryption scrambling behavior is no longer fixed, but dynamically triggered as channel conditions deteriorate. This method quantifies the interference caused by channel noise frequency and ultimately incorporates node energy consumption and out of order sequences into the probability calculation model for safety controllability. This series of steps, from perception, computation, decision-making to control, forms a continuous mapping from physical layer channel characteristics to upper layer security policies, achieving real-time response and adaptive adjustment of security transmission policies to changes in the underlying wireless environment, surpassing traditional static or layered combinations. The transmission model for multiplexing information in WSN inter-domain completes the matching of information transmission channels via the multiplexing information transmission protocol. To further ensure the security of information transmission, the model calculates the decay loss of the channel and judges the security degree of the channel according to the cumulative distribution function $F_{gXY}(x)$ of the channel and the probability density function $f_{gXY}(x)$, and calculates the controllable degree of the information transmission of the channel, so as to ensure that each sensor node is in a controllable state, to avoid the potential insecurity of the sensor node, and to ensure the safe transmission of information. The encryption transmission process of multiplexing information in the WSN inter-domain is shown in Figure 5.

The following information can be understood from Figure 5.

(1) When the information sender in the WSN inter-domain conducts the first information transmission, it needs to judge the channel transmission status of S_k between R_i in the WSN inter-domain and the sensor nodes, according to the cumulative distribution function $F_{gXY}(x)$ of the

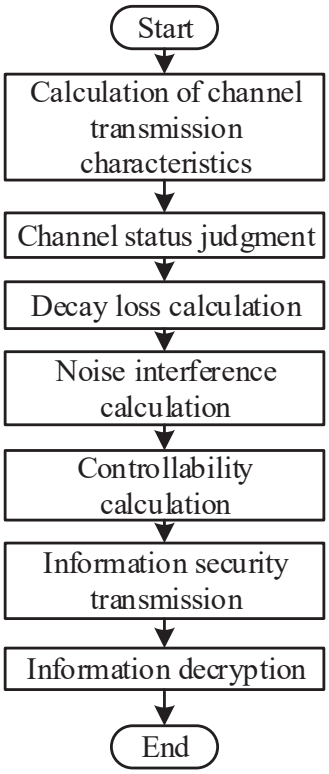


Figure 5 Encryption transmission process of multiplexing information in the WSN inter-domain.

channel and the probability density function $f_{gXY}(x)$, then the information transmission can be conducted. If a stagnation occurs during the information transmission, it is necessary to re-transmit the information.

(2) When multiplexing information in the WSN inter-domain is transmitted, a source signal and a channel additional signal will be formed. The two signals meet the Gaussian distribution. If the two signals are represented respectively by η and ξ, the sequence of information distribution received by neighboring nodes during the transfer process is represented by Ψ_i. Additionally, Ψ_i needs to satisfy the Laplace distribution condition, then the formula $f(\Psi_i)$ of the distribution function Ψ_i is:

$$f(\Psi_i) = F_{gXY}(x) g_{XY} \frac{1}{\pi\sigma^2} exp\left(-\frac{\bar{t}^2}{2\pi\sigma^2}\right) \Psi_i^2 f_{gXY}(x) \qquad (4)$$

where σ represents the standard deviation between the source signal and the channel additional signal; t indicates the average value of the transmission period of the channel additional signal.

Channel transmission decay loss occurs because, during information transmission, the sending end experiences multi-channel transmission in motion. Usually, multiple channels are available in the wireless sensing information transmission domain, and each channel generates crosstalk due to sensor node movement, leading to transmission signal decay in the network domain during information transmission. If the original power of the transmission signal formed during the transmission of information on the sending end is represented by P_0, and the receiving power of the next-hop sensor node is represented by P_e, then transmission decay loss x_g of the channel is:

$$x_g = \sum_{i=1} \frac{f(\Psi_i)P_0}{P_e(i)} \tag{5}$$

where $P_e(i)$ indicates the next-hop node of the channel in the transmission domain.

By introducing the power of any sensor node of the network inter-domain into Equation (5), the channel x_g result of multiplexing information transmission in the current WSN inter-domain can be obtained.

When performing encryption transmission of multiplexing information in WSN inter- domain scenarios, it is essential to fully consider both channel security and node security. During information transmission, sensor nodes may repeat the process among multiple nodes; if a sensor node moves during transmission, it will enter the coverage area of different transit nodes. Consequently, the transmission channels between nodes may be subject to invasion and attacks. Therefore, the transmission channel among the nodes will be invaded and attacked. Because sensor node information has the characteristics of relative continuity when it is transmitted in the domain, in order to ensure the security of multiplexing information transmission in the WSN inter-domain, the control of information encryption transmission is conducted by the threshold method, in the combination of the result of x_g in Equation (5).

Then the signal-to-noise ratio of the n-th sensor node in the WSN inter-domain is represented by y_n:

$$\gamma_n = \frac{x_g P_e(n)}{maxG(\omega)} \tag{6}$$

In the equation, $P_e(n)$ represents the current transmission power of the n-th sensor node in the WSN inter-domain; $G(w)$ represents the noise distribution function. The threshold of Equation (6) is not a fixed empirical value, but a dynamic adaptive value based on real-time channel state and transmission quality evaluation. The determination of this threshold is based on the calculation results of channel attenuation loss and the calculated signal-to-noise ratio of each sensor node. The system continuously calculates the channel attenuation loss during the transmission of multiplexed information using Equation (5), which reflects the severity of the current channel environment. Calculate the real-time signal-to-noise ratio of the nth sensor node using Equation (6), and combine it with a dynamically determined critical value based on historical transmission data, current network load, and preset security level. Adaptively adjust it based on the average channel gain, changes in noise distribution function, and detected intrusion attack intensity.

When multiplexing information is transmitted in the WSN inter-domain, the transmission decay loss of opposite end transmission signal and channel transmission exists at the same time. Compare the y_n calculated by Equation (6) with the set value, if the former is larger than the latter, the transmission of all the information to be transmitted is completed according to the transmission order determined by the transmission protocol.

However, under normal circumstances, the noise ratio received by the sensor node in Equation (6) is relatively high, so it can be set to obtain the corresponding critical value. Then the formula for calculating the signal-to-noise ratio q received by the current sensor node is:

$$q = \frac{\gamma_n P_e(n)}{maxG(\omega)} - u \tag{7}$$

In the equation, μ represents the overall decay loss result of information transmission in the WSN inter-domain.

When multiplexing information is transmitted across WSN domains, if the sensor node becomes active, it will generate random attributes, causing information transmission interference at the receiving end. At this time, the transmitted information can be scrambled and encrypted, to make the information appear disorderly distribution, and to generate the transmission order B_c of disordered information, thereby avoiding the disclosure of information after an attack. The formula for calculating B_c is:

$$B_c = \frac{d\Psi(q)}{dt} \tag{8}$$

In the equation, Ψ indicates a standard normal distribution.

When the WSN inter-domain is in a secure transmission state, B_c is positive and satisfies the conditions $\frac{d\psi(q)}{dt} > 0$, then the transmission power of sensor nodes is controlled according to the normal distribution characteristics of B_c, so as to reduce the blocking degree of multiplexing information transmission in the WSN inter-domain, and to improve the security of information transmission.

When the multiplexing information is transmitted in the WSN inter-domain, if the sensor node takes effect, it will generate random attributes, which will cause information transmission interference at the opposite end of the sending node. At this time, the channel will become unstable. The formula of the interference $R(w_k)$ is:

$$R(\omega_k) = \frac{1}{\sqrt{2\pi}} B_c {\omega_k}^2 \tag{9}$$

In the equation, w_k indicates the channel noise frequency.

In order to enhance the security of the information transmission process and to reduce the impact of $R(w_k)$ on information transmission, set the security controllability of multiplexing information transmission in the WSN inter-domain to grasp the probability of node failure during information transmission, then the formula of the energy consumption $E(n, t)$ for information transmission of the *n*-th sensor node is:

$$E(n, t) = \int_0^t P_0 R(\omega_k) dt \tag{10}$$

where t indicates the information transmission period of the node.

A metric constructed based on Equation (10) can quantify and minimize the relative energy consumption level of channel transmission during a random transmission period. Firstly, calculate the net excess energy consumption of the node during the cycle, which is the difference between the actual energy consumption and the basic energy consumption assumed to be continuously transmitted with initial power in an ideal state without attenuation. Secondly, normalize this difference. The normalized denominator contains two key factors: one is the information disorder transmission sequence defined by Equation (8), which characterizes the transmission uncertainty introduced by encryption scrambling. The second is the integral of basic energy consumption over time, used to measure the overall theoretical energy benchmark. Therefore, the energy consumption level of channel transmission is essentially the ratio of excess energy consumption to transmission uncertainty and

theoretical energy benchmark. The smaller the value, the higher the energy efficiency and the less affected by interference. The formula of λ is:

$$\lambda = \frac{E(n,t) - tP_0}{B_c \int_0^t tP_0 dt} \tag{11}$$

According to the calculation result of Equation (11), use the transmission sequence disorder degree to estimate the risk of information flow disorder caused by interference. Secondly, based on the simplified model of Poisson distribution, the probability of successful attack attempts occurring per unit time is calculated given the average transmission delay. Finally, by subtracting the sum of these risk items and summing them up to the order corresponding to the current energy consumption level, the probability estimate of the node being in a safe and controllable state for information transmission security controllability is obtained. When the controllability is less than 0, it indicates that the accumulated risk exceeds the safety threshold and the node is in an uncontrollable state. The formula for the calculation is:

$$K_u(n) = 1 - \sum_{0}^{\lambda} \sum_{n=0}^{N} (1 - B_c) \frac{q(t)^m}{m!} e^{-\lambda \Delta(t)} \tag{12}$$

where e indicates the control coefficient; $\Delta(t)$ indicates the transmission delay; N indicates the number of nodes.

If all transit nodes in the WSN inter-domain meet the condition of $K_u(n) < 0$, it indicates that all nodes in the WSN inter-domain are in a safe and controllable state and can complete the secure transmission of information without any security transmission risk.

If $K_u(n) = 0$, it can effectively ensure that the information transmission of adjacent nodes will not be blocked and can improve the security performance of multiplexing information transmission in the WSN inter-domain. The receiving terminal of the wireless sensor node can realize the decryption of the encrypted information according to the unique pseudo-random code after demodulating the received information.

3 Test Analysis

To verify the algorithm's application effect in secure transmission of multiplexing information across wireless sensor network domains, this paper constructs a wireless sensor network environment and tests the method

through secure information transmission using the algorithm. Node mobility can cause dynamic changes in channel state, including fluctuations in signal attenuation and exacerbation of multipath effects. Therefore, this paper explicitly introduces the scenario of sensor nodes moving into different coverage areas of intermediate nodes and uses this as the basis for analyzing the possibility of transmission channels being invaded and attacked. At the experimental verification level, the dynamic changes in the channel caused by mobility are mainly reflected and tested through two key designs: firstly, the basic channel model follows the Rayleigh fading principle described in Section 2.1, which is a classic method for characterizing the attenuation statistical characteristics of wireless signals in moving or rich scatterer environments. Its cumulative distribution function and probability density function are directly used to evaluate the channel state and calculate attenuation loss. Secondly, when testing the secure transmission capacity of the channel, a wide range of noise interference changes from 3 decibels to 30 decibels were introduced. This large-span signal-to-noise ratio testing scenario is designed to simulate the drastic fluctuations in channel quality caused by distance changes, obstacle occlusion, or entering multiple interference areas during the actual movement of nodes. Therefore, existing experiments have effectively evaluated the performance and robustness of the algorithm in the equivalent channel change environment caused by node movement through Rayleigh fading channel assumption and wide range dynamic noise interference testing. The built structure of the inter-domain of wireless sensor network mainly consists of wireless sensor network base station, sensor node, relay server, remote server, information decoding module and display center. The related parameters in the WSN inter-domain are shown in Table 1.

The details of intrusion and attack behaviors observed during the test, including the use of process data analysis and machine learning models, are detailed in Table 2. The overall structure is shown in Figure 6.

The testing environment constructed by this research institute is a simulation platform, but its parameter settings and scene construction strictly refer to and simulate the deployment conditions and physical constraints of real wireless sensor networks. The parameters listed in Table 1 are all derived from typical real hardware specifications and deployment scenarios. The setting of a node communication radius of 40 meters and an average node spacing of 20 meters simulates the common wireless communication distance and network topology under medium density deployment. The parameters of initial energy of 0.5 nanojoules, minimum transmission information consumption of 15 nanojoules, and maximum and minimum power

Table 1 Relevant parameters in the WSN inter-domain

Parameter	Numerical Value
Network inter-domain range/m	
Number of nodes/pieces	120
Node communication radius/m	40
Average distance between nodes/m	20
Node initial energy/J	0.5
Minimum energy consumption for node information transmission/J	15
Maximum power consumption of nodes/GJ	50
Minimum power consumption of nodes/GJ	0.05
Packet length/byte	200
Channel width/Mbps	2
Unit time slot length	0.00772
Frame Overhead/byte	512

Table 2 Details of intrusion and attack behaviors set up

Attack Code	Position	Attack Details
J1	Node	Intrusion node
J2	Channel	Transmission interception
J3	Channel	Interference transmission clock
J4	Node	Tampering position
J5	Channel	Information theft

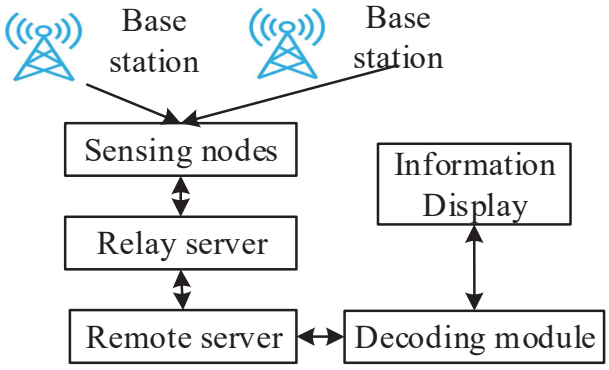


Figure 6 Inter-domain structure of wireless sensor network.

consumption of 50 picojoules and 0.05 picojoules, respectively, directly reflect the extremely limited energy budget and power consumption characteristics of real microsensor nodes. The setting of a channel width of 2 Mbps, a unit time slot length of 0.00772, and a frame overhead of 512 bytes

corresponds to the physical layer and data link layer specifications of the actual narrowband wireless communication module. In terms of interference modes, the experiment not only considered Rayleigh fading introduced by the channel model itself, but also actively injected various attack behaviors defined in Table 2, including node intrusion, transmission interception, and interference with transmission clocks. These attack modes simulate active threats such as malicious node access, eavesdropping, and interference in real environments. In addition, when testing the secure transmission capacity of the channel, a wide range of noise interference from 3 decibels to 30 decibels was introduced to simulate the changes in background noise and frequency interference from mild to severe in real wireless environments. The entire simulation aims to ensure that the algorithm performance validated in the experiment can be effectively mapped to real deployment scenarios facing energy, bandwidth limitations, and complex wireless interference through the aforementioned refined parameters and dynamic interference injection. Since the information of sensor nodes has relative continuity characteristics when transmitted in the domain, in order to verify the application performance of the algorithm in the paper, the channel transmission security capacity L_A is used as the evaluation metrics in the paper for the judgment of transmission performance of the algorithms in the paper. L_A is used to measure the security performance in the WSN inter-domain, that is, to ensure the secure transmission of information, and the intrusion node cannot obtain the transmission information content.

The larger the value, the better the security performance. The expected security capacity value in this paper is above 1.5 bps/Hz. The calculation formula of indicators is:

$$\begin{cases} L_A = \log_2(1+\gamma_1) - \log_2(1+\gamma_2) \\ L_1 = \log_2(1+\gamma_1) \\ L_2 = \log_2(1+\gamma_2) \end{cases} \tag{13}$$

where L_1 and L_2 indicate the legitimate channel capacity and the intrusion channel capacity respectively; Y_1 and Y_2 indicate the instantaneous signal-to-noise ratio of L_1 and L_2.

When there are noise interference of different sizes in the network domain, the information transmission of different sizes are carried out through the algorithm in the paper, and the results of the security capacity L_A of channel transmission during information transmission are obtained. The results are shown in Table 3.

Table 3 Channel transmission security capacity test results (bps/Hz)

	Information size/MB		
Noise/dB	300	600	900
3	1.74	1.68	2.25
6	2.58	1.96	2.76
9	3.77	2.84	2.21
12	3. 11	2.56	1.79
15	2.97	3.31	1.96
18	3.46	3.52	3.04
21	3.59	3.66	3.15
24	3.22	3.19	2.66
27	2.88	2.73	2.87
30	3.17	3.69	3.04

After analyzing the test results in Table 3, it is concluded that, with the gradual increase of the degree of noise interference in the network domain, the security capacity L_A of the channel transmission when transmitting information of different sizes is all above 1.5 bps/Hz by means of the algorithm in the paper, and the highest value is 3.77 bps/Hz. Thus, the algorithm proposed in this paper can ensure the stability and reliability of information transmission and meet the needs of various transmission scenarios.

To further evaluate the robustness of the algorithm in a more realistic and complex interference environment, three dynamic factors were introduced: burst pulse interference, multipath delay, and random node failure. Sudden pulse interference simulates instantaneous strong interference, which is periodically injected into the channel with a specific duty cycle and power peak. Multipath delay simulates the inter symbol interference generated by signals transmitted through multiple paths by setting delay extension parameters. The random failure of nodes simulates the random exit of nodes from the network due to energy depletion or physical damage. In the same network environment with 120 nodes, a node communication radius of 40 meters, and a basic noise of 12 dB, the algorithm proposed in this paper is compared with the methods in References [7–9] to test its average channel transmission security capacity and average anti interception attack performance under composite dynamic factors. The experimental results are shown in Tables 4 and 5.

According to the data analysis in Tables 4 and 5, it can be seen that the performance of all methods decreases after introducing various dynamic factors, but the algorithm in this paper always maintains an absolute advantage. Especially in composite dynamic scenarios, the average security capacity

Table 4 Performance comparison of average security capacity (bps/Hz)

Test Scenario Description	Proposed Method	Ref [7] Method	Ref [8] Method	Ref [9] Method
Baseline scenario (12dB Gaussian noise)	2.56	1.78	1.65	1.82
Baseline scenario + Burst pulse interference	2.31	1.52	1.41	1.48
Baseline scenario + Multipath delay spread	2.08	1.33	1.28	1.30
Baseline scenario + Random node failure (5%)	2.40	1.61	1.50	1.59
Composite dynamic scenario	1.86	1.05	0.98	1.02

Table 5 Performance comparison of average anti-interception performance (%)

Test Scenario Description	Proposed Method	Ref [7] Method	Ref [8] Method	Ref [9] Method
Baseline scenario (12dB Gaussian noise)	94.2	86.5	85.1	87.3
Baseline scenario + Burst pulse interference	92.7	81.4	80.2	82.5
Baseline scenario + Multipath delay spread	91.5	78.9	77.6	79.8
Baseline scenario + Random node failure (5%)	93.1	82.0	80.8	83.1
Composite dynamic scenario	90.3	72.5	71.2	73.6

and anti-interception attack performance of the algorithm proposed in this paper can still maintain above 1.86 bps/Hz and 90.3%, while the performance of the comparative method shows significant degradation. This proves that the encryption transmission mechanism adopted by the algorithm in this paper, based on real-time channel state perception and adaptive threshold control, can effectively combat complex dynamic degradation introduced by sudden interference, multipath effects, and node failures, thereby ensuring the security and reliability of cross domain multiplexed information transmission under simulation conditions approaching real wireless environments.

In order to verify the application effect of the algorithm in the paper, the security factor of network information transmission ℓ is used as an evaluation indicator in the paper. The value of ℓ is in the range of $0 \sim 1$, and the larger the value, the better the security of information transmission in the channel. The formula of calculating ℓ is:

$$\ell = \sum_{j \geq 1}^{j} W \times H_{\ell} \tag{14}$$

where j indicates a valid node in the network domain; W indicates channel stability; H indicates the transmission environment in the network domain.

Under different categories of information, with the gradual increase of the number of transmission terminals, the information is transmitted by the

Table 6 Network information transmission security factor test results

Number of Transmission Terminals/Piece	Information Categories/Number		
	2	4	6
2	0.944	0.933	0.925
4	0.958	0.951	0.933
6	0.939	0.966	0.948
8	0.942	0.947	0.956
10	0.957	0.932	0.917
12	0.963	0.985	0.966
14	0.977	0.919	0.982
16	0.984	0.925	0.973
18	0.964	0.966	0.988
20	0.925	0.955	0.946

algorithm in the paper, and the results of the transmission security coefficient ℓ of the channel are obtained. The test results are shown in Table 6.

After analyzing the test results in Table 6, it is concluded that, under different information categories, with the gradual increase of the number of transmission terminals, the security coefficients ℓ of channel transmission in the domain are all above 0.917 after information transmission through the algorithm in the paper, and the maximum value is 0.988. Therefore, in the process of information transmission, the algorithm in this paper introduces the multiplexing protocol to select the information transmission channel and masters the security controllability of multiplexing information transmission in the WSN inter-domain, so as to maximize the security of information transmission.

To clarify the necessity and superiority of the HRC-MAC protocol for the security reuse scheme proposed in this paper, a comparative experiment is designed. To quantitatively evaluate its advantages, the proposed scheme based on HRC-MAC was compared and tested with secure transmission schemes based on time-division multiple access protocol, carrier sense multiple access protocol, and low-power adaptive clustering and layering protocol in the same network environment and attack scenario. The experiment was conducted in a unified complex heterogeneous network environment, with key environmental variables including dynamic topology changes and mixed attack models. The testing indicators focus on security performance and communication efficiency. The comparative experimental results are shown in Table 7.

Table 7 Experimental results of protocol comparison

Contrast Protocol	Safety Margin (bps/Hz)	Anti-Jamming Capability (%)	Average End-to-End Delay (ms)	Average Energy Consumption (mJ/wrap)
HRC-MAC	1.6–1.9	92.3	45.2	18.7
TDMA based solution	1.1–1.4	85.1	38.5	16.2
Scheme based on CSMA/CA	0.8–1.2	79.6	62.3	22.4
LEACH based solution	1.0–1.3	81.5	51.8	14.9

Table 7 shows that the proposed scheme based on HRC-MAC is significantly better than other compared protocols in terms of core security indicators, and has the best latency and energy consumption, reflecting the necessity and superiority of the HRC-MAC protocol for the security reuse scheme proposed in this paper.

To further validate the efficacy of the algorithm presented in this paper, we have employed the methodologies outlined in References [7–9] as comparative benchmarks. These references encompass a comprehensive analysis of encryption algorithms, one-way hash functions, and the Twofish algorithm, which are tested for their resistance to various types of attacks during the transmission of information of varying sizes. This comparative approach allows us to rigorously evaluate the anti-attack performance of our algorithm alongside these well-established methods. The test results are shown in Table 6. Due to the limited space in this paper, the results present the anti-attack performance of the four methods under two kinds of attacks. The anti-attack performance metric used in this experiment is defined as the ratio at which the algorithm can successfully protect information from being intercepted or tampered with by enemy nodes in a simulated attack environment. The specific calculation method is as follows: in each experiment, a specific type and intensity of attack is applied to the transmission channel, and the number of times the information is not correctly decrypted by the enemy under this attack is counted as a percentage of the total number of transmissions. This indicator directly measures the algorithm's ability to maintain information confidentiality and integrity in the face of active attacks. During testing, sufficient independent transmission experiments are conducted for each attack category and level, and the final anti-attack performance value is the ratio of successful defense times to the total number of experiments. Therefore, the performance values shown in Table 8 are a statistically significant success rate, with higher values indicating more reliable protection effectiveness of the algorithm under corresponding attack intensities.

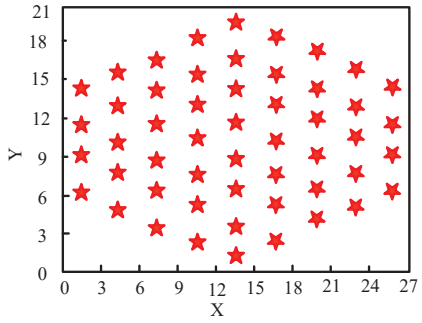
Table 8 Anti-attack performance of four methods

Attack Category	Attack Level/%	Ref [7] Method	Ref [8] Method	Ref [9] Method	Proposed Method
Intercept attack	5	87.3	85.6	86.6	97.6
	10	86.2	82.5	83.7	95.5
	15	81.4	80.3	80. 1	93.6
	20	78.9	78.2	79.4	92.2
Tampering	5	86.9	86.6	87. 1	97.8
	10	85.5	83.3	85.5	95.5
	15	83. 1	81.2	82.4	92.4
	20	78.3	77.6	79.3	92.3

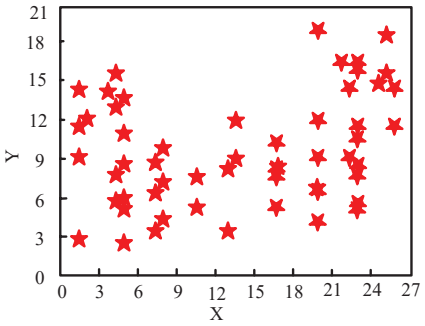
After analyzing the test results in Table 8, it is concluded that, after different degrees of attacks occur in the process of information transmission, information transmission conducted using the methods of References [7–9], the anti-attack performance of the three methods in the process reduces with the gradual increase of the degree of the attack. When the degree of the attack reaches 20%, the anti-attack performance reduces to the lowest 77.6%. The anti-attack performance of information encryption is above 90.3% when the information transmission is conducted under different attacks using the algorithms in the paper. Even when the attack degree reaches 20%, the anti-attack performance of different attack categories is still above 92.2%, which is a stable anti-attack performance and can better guarantee the secure transmission of information.

The superior performance of the method presented in this paper stems from its transmission model, which is based on multiplexing technology and tightly integrates the HRC-MAC protocol with code division multiplexing characteristics. Utilizing distinct pseudo-random codes for each sensor node in uplink spreading and downlink modulation ensures robust encryption, even when transmissions are compromised by multiple node intrusions, as pseudo-random codes enhance the security and anti-interference capabilities of spread spectrum communication. At the same time, the introduction of threshold methods dynamically evaluates the channel security status, ensures that nodes are under safe and controllable conditions through signal-to-noise ratio comparison and energy consumption control, and can maintain high anti-attack performance even when the attack level intensifies, avoiding the vulnerability caused by static encryption or path dependence in traditional methods.

In order to verify the applicability of the encrypted transmission of the algorithm in the paper, the transmission of the packet is conducted using



(a) Distribution of the original information packet to be transmitted



(b) Distribution of the information packet after encrypted transmission

Figure 7 Test results of the effect of encrypted transmission of information.

the algorithm in the paper, the original information in the packet presents an orderly arrangement. The encrypted transmission of the packet is conducted through the algorithm in the paper, the packet is transmitted from the transmitting end to the receiving end, to obtain the presented results of the undecrypted information received by the receiving end, as shown in Figure 7.

After analyzing the test results in Figure 7, it is concluded that, after the information is encrypted transmitted using the algorithm in the paper, the method is able to complete the scrambling of the information sequence, so that the information sequence is transformed from an orderly arrangement into a non-sequential, irregular arrangement, and the data shows a random distribution, which can greatly avoid the tampering of information in the process of information transmission, and therefore the algorithm in the paper is able to enhance the security of the inter-domain transmission of information in the wireless sensor network. This method utilizes the distribution

characteristics of information sequences, such as Laplace distribution and normal distribution, through an encrypted transmission mechanism to perturb the transmission order, transforming the original ordered information into a random and disordered arrangement. By combining channel attenuation loss and interference control, the transmission power can be dynamically adjusted to reduce the cross effects of multiple channels, effectively avoiding information tampering and enhancing transmission security. This is due to the optimization of channel selection by multiplexing protocols and the integrated application of encryption algorithms. The core security significance of the sequence permutation change caused by the encryption disruption operation lies in completely changing the statistical characteristics and predictability of information presented in the channel. Before being disrupted, ordered packets have clear temporal or logical associations, which allows eavesdroppers to infer information content, transmission patterns, and even carry out replay attacks by analyzing their inherent patterns, entropy values, or protocol fields after intercepting consecutive packets. After disturbance, the surface correlations between information packets are stripped away, and the data stream observed by the receiving end approaches random noise in statistical properties. This change directly leads to two transmission outcomes: firstly, attackers can no longer correct their attempt to crack a single packet by observing the order of adjacent packets, and cracking each packet becomes an independent event, increasing the cost and difficulty of obtaining complete and valid information. Secondly, active tampering attacks targeting the transmission process will become highly susceptible to detection, as any attempt to insert, delete, or modify specific data packets in an unordered stream to maintain semantic coherence will disrupt the deep verification relationships controlled by encryption algorithms that appear random but are actually controlled by legitimate recipients, leading to decryption failures or integrity verification errors. Therefore, the transition from ordered to unordered sequences not only changes the appearance but fundamentally alters the form of information existence and adversarial interaction in non-secure channels, enabling the transmission process to effectively resist deep attacks based on traffic analysis and correlation reasoning.

4 Conclusion

(1) In order to enhance the security of information transmission between domains in wireless sensor networks, this paper proposes a secure transmission algorithm for information reuse in cross domain wireless

sensor networks. The algorithm uses the cross domain structure of wireless sensor networks to analyze channel transmission characteristics and constructs the communication framework. Based on the HRC-MAC protocol, the transmission model of information multiplexing in cross domain wireless sensor networks is constructed, and the information uplink spread spectrum and downlink modulation are realized based on the characteristics of code division multiplexing. The threshold method of information encryption and transmission control is adopted to achieve secure transmission.

(2) After verification, the channel transmission security capacity of the algorithm is more than 1.5 bps/Hz, the transmission security rate meets the standard, the channel transmission security coefficient in the domain is more than 0.917, and the anti-attack performance of information encryption is more than 90.2%. This method can effectively prevent the tampering behavior in the process of information transmission and ensure the secure transmission of information reuse in cross domain wireless sensor networks.

(3) However, this method needs higher software and hardware environment conditions to achieve real-time transmission when constructing the transmission model, which has certain limitations. Therefore, future research will lightweight design the transmission model and improve the application and hardware dependency of the algorithm.

References

[1] Rani, K. P., Sreedevi, P., Poornima, E., and Sri, T. S. (2023). FTOR-Mod PSO: A fault tolerance and an optimal relay node selection algorithm for wireless sensor networks using modified PSO. Knowledge-Based Systems, 272(July 19): 110583.1–110583.12.

[2] Chenthil, T. R., and Jayarin, P. J. (2022). An energy aware multi slot scheduling with two-layer hexagonal based integrated aggregation approach for underwater wireless sensor networks (UWSN). Journal of Interconnection Networks, 22(4): 44–71.

[3] Pang, F., and Dou L. J. (2023). Research on end-to-end secure rerouting protocol between multi domains in WLAN. Computer Simulation,40(06): 444–448.

[4] Rajasoundaran, S., Prabu, A. V., Routray, S., Malla, P. P., Kumar, G. S., and Mukherjee, A., et al. (2022). Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based

5G wireless sensor networks. Computer Communications, 187(Apr.): 71–82.

[5] Anselme, R. A. M., and Satori, H. (2024). Machine learning attack detection based-on stochastic classifier methods for enhancing of routing security in wireless sensor networks. Ad Hoc Networks, 163(c):103581.1-103581.9.

[6] Nguyen, T. T., Dao, T. K., Nguyen, T. D., and Nguyen, V. T. (2023). An improved honey badger algorithm for coverage optimization in wireless sensor network. Journal of Internet Technology, 24(2): 363–377.

[7] Sureshkumar, K., and Vimala, P. (2023). Simultaneous wireless information and power transmission-based power transfer and energy prediction for efficient communication with golden Taylor sea lion optimization in wireless sensor network. International Journal of Communication Systems, 36(13): e5544.1–e5544.28.

[8] Balamurugan, V., Karthikeyan, R., Sundaravadivazhagan, B., and Cyriac, R. (2023). Enhanced Elman spike neural network based fractional order discrete Tchebyshev encryption fostered big data analytical method for enhancing cloud data security. Wireless Networks, 29(2): 523–537.

[9] Vijayakumar, M. (2022). Network statistics-based routing and path orient data encryption scheme for efficient healthcare monitoring with IoT in WSN. International Journal of Communication Systems, 36(1): e5361.1–e5361.12.

[10] Bethi, S., and Moparthi, N. R. (2022). Adaptive secure energy efficiency routing protocol for wireless sensor network. Journal of Mobile Multimedia, 18(4): 1009–1034.

[11] Wang, X., Liang, X., Yang, C., Yuan, Y., Liu, G., Wang, J., and Wang, J. (2024). Performance analysis of pre-distorted layered asymmetrically clipped optical orthogonal frequency division multiplexing. In 2024 IEEE 30th International Conference on Telecommunications (ICT), 106(6): 24–27.

[12] Lang, O., Hofbauer, C., Feger, R., and Huemer, M. (2023). Range-division multiplexing for MIMO OFDM joint radar and communications. IEEE Transactions on Vehicular Technology, 72(1): 52–65.

[13] Bhat, S. J., and Santhosh, K. V. (2022). An artificial hummingbird algorithm-based localization with reduced number of reference nodes for wireless sensor networks. Physical Communication, 55(Dec.): 101921.1–101921.8.

[14] Mozaffari, M., Mazinani, S. M., and Khazaei, A. A. (2025). An energy efficient grid-based clustering algorithm using type-3 fuzzy system in wireless sensor networks. Wireless Networks, 31(1): 109–125.

[15] Ghosh, T., Roy, A., Misra, S., and Raghuwanshi, N. S. (2022). CASE: A context- aware security scheme for preserving data privacy in IoT-enabled society 5.0. IEEE Internet of Things Journal, 9(4): 2497–2504.

[16] Ayyadurai, M., Seetha, J., Haque, S. M. F. U., Juliana, R., and Karthikeyan, C. (2023). Routing algorithm for underwater acoustic sensor network. Neural Processing Letters, 55(1): 441–457.

[17] Raut, G., Biasizzo, A., Dhakad, N., Gupta, N., Papa, G., and Vishvakarma, S. K. (2022). Data multiplexed and hardware reused architecture for deep neural network accelerator. Neurocomputing, 486(May 14): 147–159.

[18] Chakraborty, D., Mukherjee, P., Sarkar, S., and Das, N. R. (2025). Intelligent detection threshold optimization in WDM systems: A machine learning approach for crosstalk mitigation. Optical and Quantum Electronics, 57(11): 618–624.

[19] Kotb, M. M. E., Abdel-Haleem, M. R., Hassan, A. Y., Plawiak, P., and Mohra, A. S. (2025). Hybrid time synchronization and ANN-based M-QAM demodulation for enhanced performance in OFDM and MIMO-OFDM systems. Neural Computing & Applications, 37(31): 26249–26279.

[20] Priyadharsini, N. A., Kumar, J. A., and Baby, S. R. (2024). A hybrid multicarrier modulation and multiplexing scheme for beyond 5G systems. Wireless Personal Communications: An International Journal, 138(1): 369–385.

[21] Pan, P., Su, Y., Pan, G., et al. (2024). A secure transmission scheme with efficient and lightweight group key generation for underwater acoustic sensor networks. IEEE Internet of Things Journal, 11(23): 37916–37927.

[22] Zarei, M., Dindarlou, M. H. F., Taghizadeh, M., et al. (2025). Enhancing the LEACH protocol and lightweight chaotic cryptography for secure data transmission in wireless sensor networks. Scientific Reports, 15(1): 42323–42328.

Biographies

Xiaopeng Yan obtained the Master of Software Engineering degree from Jiangxi Normal University, China, in 2016. She is currently a teacher at the School of Architecture and Information Engineering, Shandong Vocational College of Industry, with research interests including mobile data collection and network security.

Qiang Wang obtained his doctoral degree from Busan Silla University, China, in 2024. He is currently the Dean of the School of Architecture and Information Engineering, Shandong Vocational College of Industry, with research interests including multiplexing technology and radio security.