Renewable Energy and Power Quality Journal
https://repqj.com/index.php/repqj/index
RE&PQJ, Vol. 23, No. 6, 2025

# Optimization Method of Unstable Over the Horizon Trunking Network Communication Between Microgrids Based on Long-distance Hybrid Networking Technology

Peng Yu[1], Rong Fu[1], Guanbao Yang[1], Yusheng Wu[2,*], Jiankang Ge[2]

[1]Sansha Electric Power Supply Company Limited, Sansha, Hainan, 573199, China
[2]Beijing Sifang Automation CO., LTD., Beijing, 100085, China
[*]Corresponding author email: yugai630572@163.com

**Abstract.** In the complex environment of tropical islands, affected by geography and climate, sensor nodes are unevenly distributed and microgrid clusters are far apart, resulting in extended signal transmission paths and compromising the communication quality between microgrid clusters. Consequently, a communication optimization method for non-stable long-range cluster networks between microgrid clusters based on long-distance hybrid networking technology is proposed. This method involves constructing a communication architecture for a beyond line of sight cluster network using long-distance easing networking technology, with physical layers including access nodes, and deploying sensors using wireless self-organizing network technology. Data is collected and transmitted to the network layer, employing multi-channel information fusion technology to integrate information from diverse networks by extracting bit soft values and implementing multi-channel decision level flexible information fusion. The data is subsequently transmitted to the perception layer, using cluster communication technology protocols and models to perceive signals and achieve communication management. Communication data encryption technology based on hyper-chaotic sequences is employed to optimize the communication process of microgrid clusters. Experimental results demonstrate that this method exhibits significant effects on channel equalization and noise suppression, with a minimum bit error rate of 0%, a character frequency statistical probability of about 0.0039, and an encrypted ciphertext sequence balance value approaching 0. These findings fully demonstrate the effectiveness and superiority of the method, indicating its ability to effectively resist various types of attacks.

**Key words.** Long-distance hybrid networking, Communication Architecture of Over the Horizon Cluster Network, Microgrid group communication, Multi channel information fusion, Sensor node layout

| symbol | meaning |
|---|---|
| $k$ | Gain coefficient |
| $s_i, s_j$ | Randomly select two nodes within a wireless sensor network |
| $d_{ij}$ | Distance between nodes $s_i$ and $s_j$ |
| $r_s$ | Optimal distance between nodes |
| $d_{th}$ | Distance threshold between nodes |
| $F_{xy}$ | Virtual resultant force of nodes |
| $d_m$ | Maximum movement distance of sensor nodes |
| $F_x, F_y$ | The components of $F_{xy}$ on the x-axis and y-axis |
| $w$ | Gain coefficient |
| $d_{ig}$ | Distance between nodes and grid points |
| $r$ | Perception radius |
| $R$ | Communication radius |
| $\varphi$ | Gain coefficient |
| $d_i$ | Distance from sensor node to boundary |
| $d_{bth}$ | Boundary distance threshold |
| $\xi_1, \xi_2, \xi_3$ | Maximum 3 related peak values |
| $v_1, v_2, v_3$ | Binary corresponding to the position of $\xi_1, \xi_2, \xi_3$ |
| $(\lambda_0, \lambda_1)$ | Specific single information bit soft value |
| $M_k$ | Basic trust allocation function |
| $d_1, d_2$ | Transformation coefficients in the nonlinear transformation process of $x_n$ and $y_n$ |
| $c_n$ | The signal obtained by nonlinear transformation |
| $c_i\ (i = 1, 2, \cdots, 52n)$ | subkey |
| $g_i$ | Wireless sensor network communication data plaintext |
| $u_i$ | Output wireless sensor network communication data ciphertext |
| $n_0$ | Number of degrees' 0 ' |
| $n_1$ | Number of degrees' 1 ' |
| $n$ | Total number of $n_0$ and $n_1$ degrees |
| $\phi$ | Balance of encrypted ciphertext sequence |

## 1. Introduction

China has many islands that are affected by typhoons, waves, storm surges, sea ice, and other disasters. It is one of the countries with the most serious marine disasters worldwide [1]. As an outpost of national coastal defense, the tropical island is the strategic fulcrum of national marine environment monitoring and marine traffic security to ensure a reliable energy supply, which plays an irreplaceable role in safeguarding national sovereignty and marine rights and interests [2]. However, for a long time, the power supply of these islands has mainly relied on the installation of submarine cables or traditional fossil fuel units such as diesel generators and gas turbines. This power supply mode has many drawbacks that are difficult to overcome. On the one hand, the construction cost of submarine cables is high, maintenance is extremely difficult in the later stages, and they are extremely vulnerable to marine natural disasters; On the other hand, fossil fuel units not only face challenges in fuel transportation and storage, but their carbon emissions during operation also exert significant pressure on the fragile ecological environment of islands. More importantly, the environment in which tropical island microgrids are located is extremely harsh [3]. The tropical island microgrid cluster spans multiple tropical kelp microgrids with long distances, multiple storms, and weak communication connections [4] and is subjected to extreme weather conditions of strong sunlight, strong typhoons, and heavy rainfall (the three strongest) for a long time [5]. The key to the observation and control of island microgrids is ensuring stable and reliable communication between microgrid groups owing to the influence of marine regions and the three strong environmental factors[6].

Naresh et al. [7] proposed a blockchain based communication method for the communication between micro grid groups. In this method, the content extraction signature based on elliptic curve is used to exclude sensitive information, reduce the probability of privacy information leakage in the process of communication data sharing, and at the same time, blockchain smart contracts are used to define user access rights, and cloud facilities are used to store actual communication data. The Ciphertext-Policy Attribute-Based Encryption (CP-ABE) access control policy based on the ciphertext policy attribute is used to authorize the data owner to protect the cloud storage and provide access rights to authorized users through the encrypted cloud storage link. The access control policy is blind. This method has high security of communication data, but the communication quality is not ideal owing to the influence of strong communication signal barriers in the actual application process. Guimaraes et al. [8] put forward an analysis model and method to support the optimization of network infrastructure design by considering the integration of communication and power infrastructure in the process of studying communication network optimization methods, and also considered technical and business oriented indicators, such as availability, reliability and total cost . In practical applications, this method ignores the problem of a large span of tropical island stations, resulting in poor communication. In the process of studying network communication optimization methods, Verma et al. [9] proposed an enhanced energy-saving clustering protocol that operates in three main stages of network setup: grid formation and grid head selection, clustering, and Cluster Head (CH) selection. Clustering is implemented using the naturally inspired Grey Wolf Optimization (GWO) algorithm, and CH selection is implemented using a system based on fuzzy reasoning. Simulate in MATLAB software and evaluate the protocol according to network life, First Node Death (FND), Half Node Death (HND), and Last Node Death (LND). This method is vulnerable to various external attacks during the communication process, resulting in communication information leakage.

Aiming at the problems existing in the above literature, a communication optimization method for unstable beyond line of sight cluster networks between microgrid groups based on long-distance hybrid networking technology is proposed. In response to the characteristics of large spans and strong communication signal obstacles of tropical island sites, this method integrates multi-domain technologies to construct a beyond line of sight cluster network communication architecture, including access nodes, coastal transmitters, and other multiple devices, and uses hyperchaotic sequence encryption to ensure security. The physical layer utilizes a virtual force algorithm to integrate grid points and boundary constraints to optimize the sensor layout; The network layer innovates multi-channel flexible data fusion algorithm based on D-S evidence theory, balancing transmission pressure and fusion capability; Design a dedicated data transmission protocol for the perception layer to improve transmission and parsing efficiency; The encryption process combines hyper chaotic sequences and IDEA algorithm to enhance security, overcome the communication difficulties of tropical island microgrid groups, ensure their reliable operation, and provide strong support for the national maritime strategy.

## 2. Optimization Method of Unstable Over the Horizon Trunking Network Communication Between Microgrids

### *A. Over the Horizon Trunking Network Communication Architecture*

The equipment composition of the unstable over the horizon trunking network communication architecture between microgrid clusters mainly includes six parts: access node, coastal transmitter, tropical island radio, IP bearer network, information fusion center, and frequency management system. The physical layer equipment mainly includes access nodes, coastal transmitters, tropical island radios, and sensors; Network layer equipment mainly includes IP bearer network and integration system; The perception layer equipment is mainly the frequency management system, and the

system composition is shown in Figure 1.

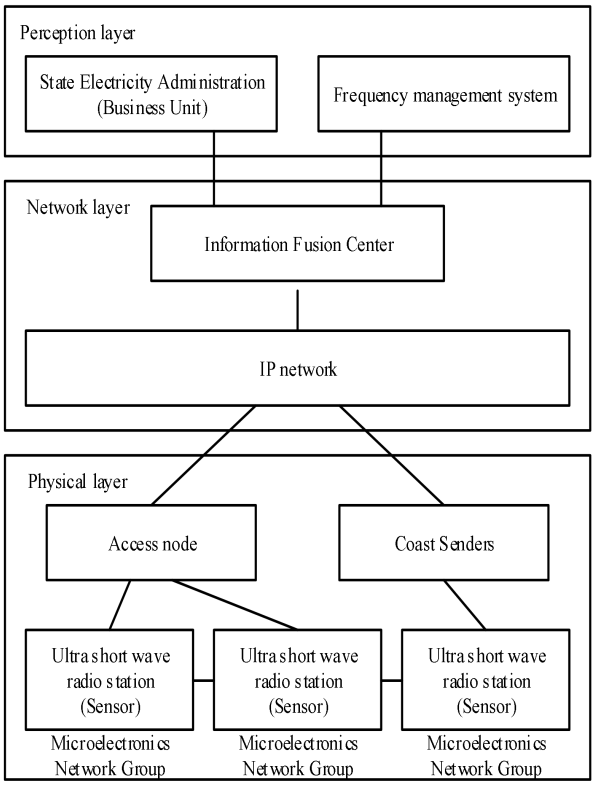



Figure 1. Unstable Beyond Line of Sight Cluster Network Communication Architecture between Microgrid Groups Based on Long Distance Hybrid Networking Technology

Access node: This includes ultrashort wave broadband receivers and ultrashort wave broadband receiving antennas. The receiver is configured in a mobile base station machine room and the antenna is configured on the tower base. The mobile base station can provide a good power supply and waterproof and moisture-proof guarantee for an ultrashort wave receiver. The access node only completes the signal reception, does not have a signal transmission function, and will not interfere with the existing communication system.

Coastal transmitter station: add network controller on the basis of the existing coastal radio station of the State Oceanic Administration to realize remote dispatching control, so as to facilitate the dispatching of tropical island users in different directions when communicating.In the process of the unstable hyper visual cluster network communication between the tropical island microgrids, the main purpose is to transmit the uplink data, and the downlink is to solve the wake-up and parameter configuration of island and reef radio stations. Coastal radio usually operates at the kilowatt level. By dispatching coastal radio in a specific direction, the downlink can effectively cover the islands and reefs in the relevant waters of China.

IP bearer network: relying on the widely distributed communication base stations and optical fiber communication facilities, it can realize the interconnection of the physical layer, network layer, and perception layer without any hardware cost and provide a reliable and secure data transmission infrastructure platform.

Information fusion center and spectrum management system: The information fusion system is responsible for fusing and processing the environmental monitoring information of islands and reefs uploaded by each access node to form complete and reliable environmental monitoring situation data for islands and reefs. The frequency perception system sends the working frequency of the islands and reefs planned for detection to each island and reef by dispatching corresponding coastal radio stations.

Tropical island radio station: A general maritime radio station can be used. The power consumption of meteorological and hydrological communication data acquisition is low, and the main power consumption is from ultrashort-wave radio stations. To ensure continuous operation under various weather conditions, the maximum transmitting power of the radio station is 100 W, and the antenna is a whip antenna that is easy to install and erect.

Physical layer sensor network nodes are responsible for data acquisition and preliminary processing and realize data integration and optimization through multi-channel information fusion technology at the network layer. In this process, the bit soft value extraction and multi-channel decision level flexible information fusion strategy effectively improve the accuracy and reliability of the data. The perception layer transmits the processed data according to the established protocol and communication model, encrypts the data based on the complex algorithm of the hyperchaotic sequence, and ensures data transmission security. The close cooperation among all layers constitutes an efficient and secure system of non-stable over-the-horizon trunking network communication between microgrid groups under the long-distance hybrid networking technology.

### *B. Physical Layer Sensor Network Node Layout Method*

The sensor node layout method in wireless ad hoc network technology is used to layout the micro grid sensors within the physical layer of the long-distance hybrid networks.

The virtual force algorithm demonstrates significant consistency with the node coverage technology, thus enabling its application in optimizing node layout within wireless sensor networks. The detailed process is as follows: $s_i$ and $s_j$ represents two random nodes in the wireless sensor network, node $s_i$ recipient node $s_j$ and the force relationship between them is shown in Formula (1) [10]:

$$F_{ij}=\begin{cases}k_1/d_{ij}^{\alpha 1},\ 0<d_{ij}<r_s\\ 0,\ d_{ij}=r_s\ or\ d_{ij}>d_{th}\\ k_2/d_{ij}^{\alpha 2},\ otherwise\end{cases}\quad(1)$$

In formula (1), $F_{ij}$ represents the force between nodes $s_i$ and $s_j$, which determines how nodes should be moved to improve network coverage and connectivity; $k_1$ and $k_2$ represent the gain coefficients, which are used to control the interaction force between nodes, so as to control the moving speed and distance of nodes, so as to achieve the expected network layout effect; $r_s$ represents the optimal distance between nodes; $d_{ij}$ indicates the distance between nodes $s_i$ and $s_j$; $d_{ij}^{\alpha 1}$ and $d_{ij}^{\alpha 2}$ represent the $\alpha 1$ power and $\alpha 2$ power of the distance of $d_{ij}$, respectively; $\alpha 1$ and $\alpha 2$ represent the exponential parameters of the influence decay rate; $d_{th}$ indicates the distance threshold between nodes, when the distance between nodes exceeds this threshold, the force between them will become zero, that is, they will no longer influence each other. As the basic units of perception and communication, nodes are strategically distributed in key positions within each microgrid, ensuring comprehensive network coverage and communication reliability through optimized layout strategies. Functioning as the logical center of data processing, grid points are responsible for collecting, integrating, and forwarding information from each node to establish an efficient information flow network. The communication protocol and encryption mechanism between nodes and grid points ensure secure and real-time data transmission, collectively supporting a stable communication architecture among microgrid groups.

Different sensor nodes will update the node position [11] according to the overall resultant force. The update process is as follows:

$$x_{new}=\begin{cases}x_{old},\ F_{xy}=0\\ x_{old}+\dfrac{F_x}{F_{xy}}\times d_m\times e^{\frac{-1}{F_{xy}}},\ F_{xy}\neq 0\end{cases}\quad(2)$$

$$y_{new}=\begin{cases}y_{old},\ F_{xy}=0\\ y_{old}+\dfrac{F_y}{F_{xy}}\times d_m\times e^{\frac{-1}{F_{xy}}},\ F_{xy}\neq 0\end{cases}\quad(3)$$

In the above formula, $F_{xy}$ and $d_m$ respectively represents the virtual force resultant acting on the node and the maximum movement distance of the sensor node; $F_x$ and $F_y$ respects $F_{xy}$'s components on the x and y axes.

The traditional virtual force algorithm solely considers the force of sensor nodes in the wireless sensor network and introduces the force of grid points on nodes to mitigate time loss during the position update process. The formula is described as follows [12]:

$$F_{grid}=\begin{cases}wd_{ig},\ r<d_{ig}<R\\ 0,\ other\end{cases}\quad(4)$$

In formula (4), $w$ and $d_{ig}$ respectively represents the gain coefficient and the distance between nodes and grid points, $r$ and $R$ represent perception radius and communication radius respectively.

In the actual sensor layout process, there is a certain probability that nodes will gather on the boundary. In view of this phenomenon, moving nodes according to the above process will cause the problem that nodes will be excluded from the boundary, leading to the decline of sensor node coverage.

Use $F_b$ indicates the constraint of the boundary of the region of interest on the node. Its main function is to make the node exist in the region of interest. Its formula is described as follows [13]:

$$F_b=\begin{cases}\dfrac{\varphi d_i}{d_i^3},\ d_i\geq d_{bth}\\ +\infty,\ d_i<d_{bth}\end{cases}\quad(5)$$

In formula (5), $\varphi$, $d_i$ and $d_{bth}$ respectively represent gain coefficient and sensor node $i$ distance to boundary and boundary distance threshold.

### *C. Network Layer Multi-Channel Information Fusion Technology*

The inner layer of the network adopts multi-channel information fusion technology to fuse information transmitted by different networks [14]. Multi-channel uplink information fusion is key to realizing wide-area cooperative reception. There are usually two implementation methods: detection-level fusion and decision-level fusion. During detection-level fusion, each receiving station does not carry out decision decoding, but directly transmits the received baseband information to the fusion center, and the central station makes fusion decisions. This fusion mode requires a high transmission capacity of the network and the receiver to have a strong ability to resist multipath interference. During decision level fusion, each station receives and decodes the data first and then transmits the data information to the fusion center for fusion judgment. This method reduces the pressure of network transmission, but requires the data center to have the fusion processing capability of fusing highly conflicting information.

In view of the problems of the tropical island microgrid group spanning long distances and weak communication connections to reduce the pressure of RF data network transmission faced by the detection level fusion and reduce the high rental cost of broadband data transmission, a new decision-level fusion algorithm based on multi-channel flexible data fusion is proposed under the D-S evidence theory framework to solve the problem of information fusion with high conflict between channels. The core content of the algorithm includes two parts: bit soft value extraction and multi-channel decision level fusion.

### *1) Bit Soft Value Extraction*

Starting with Walsh orthogonal decoding, soft value extraction is performed on the decoding result of DMFSK. The data output by DMFSK by frame is 64×5. Subsequent to the de-interleaving process, 64 data in each row corresponds to an ASCII code. The data in each row is sequentially traversed.

For the 64 data in a single row, a correlation is conducted with each column of the Hadamard matrix, yielding a correlation result with a length of 128. The largest correlation peak means the most likely result. Here, considering the influence of noise, the maximum three correlation peaks are selected, and the values of their correlation results are $\xi_1$, $\xi_2$, $\xi_3$, the binary value of the corresponding position can be represented as a vector $v_1$, $v_2$, $v_3$, any element can take 0 or 1, and the corresponding soft value can be expressed as [15]:

$$\begin{cases} \lambda_1 = \sum_{i=1}^{3} \xi_1 v_1 \\ \lambda_0 = \sum_{i=1}^{3} \xi_i v_i \end{cases} \tag{6}$$

In formula (6), $\lambda_i = \left[ \lambda_{i,1}, \lambda_{i,2}, \cdots, \lambda_{i,7} \right]$.

### *2) Multi Channel Decision Level Flexible Information Fusion*

In the traditional Viterbi decoding method, the comparison of cumulative distances across all states (branches) enables the decision to yield a unique optimal result. Howeer, in the process of receiving multiple uplink signals, the results of each channel's terby decoding are very different and contradictory, so it is difficult to directly obtain a reasonable final decision result. To address this issue, the decision-level information fusion method [14] based on the DSmT (degenerate smarandache theory) is introduced, employing a conflict information redistribution method is used for fusion decision-making. Using the obtained soft information, assume that the soft value of a specific single information bit is ( $\lambda_0$, $\lambda_1$ ), representing the soft information whose bit is 0 and 1 respectively. Through normalization, the Basic Belief Assignment (BBA) function of this information bit can be constructed [16]:

$$m_k = \begin{cases} \dfrac{\lambda_0}{\lambda_0 + \lambda_1}, X = 0 \\ \dfrac{\lambda_1}{\lambda_0 + \lambda_1}, X = 1 \end{cases} \tag{7}$$

In formula (7), $k = 1, 2, \cdots, s$ indicates that the current BBA is from the kth access point (channel), and a total of s access points simultaneously receive the information and participate in the integration. On this basis, the DSmT uncertainty information flexible fusion method and the Sixth Proportional Conflict Redistribution Rule (PCR6) are introduced to integrate the information from diverse stations.

## *D. Perception Layer Data Transmission Protocol and Communication Model*

During the design of the perception layer, the data transmission protocol and communication model in the trunking communication technology are used to sense the tropical island detection signals, dynamically plan the working frequency of offshore island and reef radio stations, and solve the problem that the success rate of the current maritime communication fixed channel communication chain building is low due to the dynamic change in the information transmission window with the alternation of day, night, and season [17].

The data stream of the unstable over the horizon cluster network between microgrid clusters is composed of continuous numerical matrix data [18,19], including a substantial number of floating points. For this type of data, common character stream file formats such as JSON and XML increase the overhead of data to be transmitted. The actual data content can only be obtained after additional parsing at the data receiving end, which is not the best transmission scheme. Consequently, according to the characteristics of unstable over the horizon cluster network data flow between microgrid groups, a message based data transmission protocol is designed to reduce the amount of data. At the same time, according to the protocol content, the receiver can directly obtain the data to be analyzed only once.

The protocol field includes the timestamp of each data packet, the serial number of the data packet (pkt_id), the data stream header information (s_head), and other relevant parameters. A packet can be uniquely identified according to its timestamp, serial number and stream number (id) in the stream header information. The cluster also requires regular information exchange for the task scheduling module to comprehensively analyze the load of nodes in the cluster and complete task allocation based on the analysis results. Short control messages are used for information exchange, including the maximum

computing power of computing nodes $V_8$ , current computing capacity $C_8$ and available bandwidth $anb_8$ etc.

Data receiving, sending, and task scheduling are shown in Figure 2. The configuration table is used to store the configuration information of the system, including the number of network card ports, port types, number of buffers, correspondence between forwarding cores and buffers, and the flow allocation table. The system uses multiple multiport network cards to send and receive data. Network card ports are divided into data-receiving and data-forwarding ports. The receiving core obtains the port number of the receiving port according to the information in the configuration table, and scans the port-receiving data circularly. A flow allocation table is used to allocate the AI data flows. The forwarding core queries the port number of the forwarding port in the configuration table and sends the data to the corresponding computing node to complete the task calculation based on the flow allocation table information.

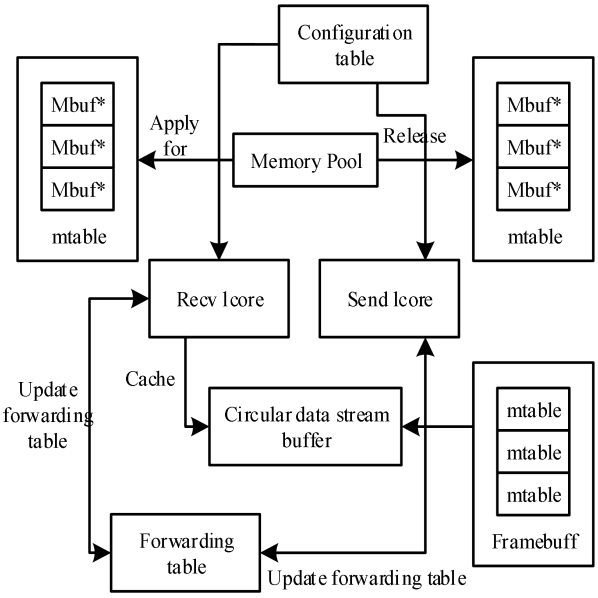



Figure 2. Schematic diagram of data transmission and task scheduling

The system maintains one or more unstable over the horizon trunking network data flow buffer zones between the microgrid groups. The number of buffer zones dynamically adjusts with the change in the unstable over the horizon trunking network dataflow between the microgrid groups. The unstable over the horizon trunking network data stream buffer between the circulating microgrid groups is used to cache the unstable over the horizon trunking network data stream between the microgrid groups according to the processing cycle, and the data of each line belongs to the same prime. DPDK uses a memory pool to manage the data. After receiving the data, the receiving core is first applied to the mbuf object from the memory pool. After the data are encapsulated, the data package is cached into the cache line corresponding to the write pointer pWrite according to the identifier and processing cycle of the data package, that is, each line corresponds to the unstable over the horizon cluster network data stream PAS between the concurrent microgrid groups with the same processing cycle. After the data cache is completed, the forwarding table is maintained. The forwarding table corresponds to the circular AI data stream buffer table one by one. When the corresponding buffer is full, the forwarding table marks the corresponding position as full, and records the number of data packets cached in each small block.

The forwarding core is bound to be unstable over the horizon trunking network data stream buffer between the circulating microgrid group, wakes up/sleeps with the change in data volume, and is responsible for data forwarding. The sending pointer pSend points to the unstable over the horizon trunking network data stream PAS between the concurrent microgrid groups that need to be sent in the buffer, forwards the core query forwarding table, forwards the prepared data according to the configuration table information, releases the memory space after the completion of data forwarding, and updates the forwarding table simultaneously.

### *E. Communication Data Encryption Based on Hyperchaotic Sequence*

To ensure the security of communication between microgrid groups, a communication data encryption method based on hyperchaos sequence is employed to encrypt the communication process, effectively preventing external attacks and ensuring the security of communication information.

#### *1) Communication Key Generation*

In the process of wireless sensor network communication data encryption, a binary key stream is generated based on two-dimensional discrete hyperchaotic sequence, and the communication data encryption of wireless sensor network is completed using this binary key stream [17]. But the actual encryption process does not use $x_n$ and $y_n$ directly cover the wireless sensor network communication data, but $x_n$ and $y_n$ carry out nonlinear transformation to obtain sequence $c_n$ , based on $c_n$ get the binary stream, and use this binary stream to encrypt the wireless sensor network communication data.

Utilize $x_n$ and $y_n$ sequence obtained by nonlinear transformation $c_n$ when encrypting the wireless sensor network communication data, even if the attacker obtains the data in a certain way $x_n$ and $y_n$ without obtaining the nonlinear transformation function, the key stream used for encryption of wireless sensor network communication data cannot be reconstructed, thus enhancing the confidentiality and anti cracking of

wireless sensor network communication data.

In parameter $\alpha$ , $\beta$ , $\delta$ , $\gamma$ under the conditions of 1.66, -1.4, -1.2 and 0.2 respectively, it can be obtained by mapping formula (1) $x_n$ and $y_n$ , use equation (8) to perform nonlinear transformation with both:

$$c_n = d_1 x_n^2 + d_2 y_n^2 \quad (8)$$

In formula (8), $d_1$ and $d_2$ respects $x_n$ and $y_n$ transformation coefficient in the process of nonlinear transformation.

As $d_1$ and $d_2$ at values of 0.4 and 0.5, respectively, $c_n$ as $x_n$ and $y_n$ the signal obtained by nonlinear transformation is the same as $x_n$ and $y_n$ . It is highly different. Utilize $c_n$ after the key stream is generated, the security of wireless sensor network communication data can be improved by encrypting the wireless sensor network communication data with the key stream [20,21].

For the purpose of obtaining binary key stream $c_n$ the sequence performs analog to digital conversion with limited precision. The computer double variable contains eight bytes in total, enabling computational precision to reach 10-15. To ensure the encryption effect of wireless sensor network communication data, the value obtained after the hyperchaotic map iteration at the corresponding time is taken as the initial value for analog-to-digital conversion. This approach ensures that the converted binary double values exhibit significant differences when the difference between the initial values reaches 10-15. At the same time, through the $c_n$ the analog-to-digital conversion of the key sequence can also effectively process the key sequence and improve the security of the key sequence. During calculation $c_n$ 's value of the sequence contains eight bytes. In the design of the conversion function, a double value is converted to 32 bits to prevent the deduction of subsequent keys when an attacker obtains one set of keys.

In general, the number of positive Lyapunov exponents in hyperchaos is not less than two. The greater the number of such exponents, the stronger the variability of the trajectory direction in the hyperchaotic system. This enhanced variability also improves the anti cracking ability of key streams generated by hyperchaos system.

### *2) IDEA Packet Encryption Algorithm*

IDEA packet encryption algorithm is to convert the clear text sequence of wireless sensor network communication data $g_1, g_2, \cdots, g_k, \cdots$ divided into equal length information groups $(g_1, g_2, \cdots, g_n)$ , $(g_{n+1}, g_{n+2}, \cdots, g_{2n})$ under the key control, encrypt the wireless sensor network communication data information group one by one according to the corresponding algorithm [22,23], and output the wireless sensor network communication data ciphertext group after encryption $(u_1, u_2, \cdots, u_n)$ , $(u_{n+1}, u_{n+2}, \cdots, u_{2n})$ , ..., and the length of the output ciphertext is the same as that of the plaintext.

### *3) Communication Data Encryption Process Design*

The primary advantages of using IDEA packet encryption algorithm for encrypting wireless sensor network communication data are its high efficiency and robust strength. The IDEA block cipher algorithm is improved based on the hyperchaotic sequence, and the key stream generated by the hyperchaotic sequence serves as the initial key for the IDEA block cipher algorithm [24-26]. Based on the IDEA block cipher algorithm, the anti-cracking ability of the key stream is improved, resulting in enhanced encryption efficacy for wireless sensor communication data.

The implementation process of the data encryption method for wireless sensor network communication based on improved block cipher algorithm of hyperchaotic sequence is as follows:

Enter the seed key of hyperchaotic map $(a, b, c, d, x_0, y_0, z_0)$ , generating hyperchaotic binary key stream via iterative process. Discard the previous N times of data and obtain the real value key stream.

The key stream C is derived from the nonlinear transformation of the hyperchaotic sequence.

The clear text of wireless sensor network communication data is divided into n groups according to 64bit, and the key stream C is divided into sub keys according to every 32bit $c_i (i = 1, 2, \cdots, 52n)$ , every 52 $c_i$ divide into groups.

Clear text for a group of wireless sensor network communication data $g_i$ , based on IDEA packet encryption algorithm, using a set of keys $\left(c_{52(i-1)+1}, c_{52(i-1)+2}, \cdots, c_{52i}\right)$ encrypt the clear text of wireless sensor network communication data, and output the ciphertext of wireless sensor network communication data $u_i$ , until all clear text group encryption of wireless sensor network communication data is completed [27-30].

## 3. Experiment and Result Analysis

### *A. Experimental Environment Setup*

To verify the practical application effect of the method proposed in this paper, the research object of unstable over the horizon cluster network location between a

certain microgrid group was selected, and communication experiments were conducted using the method proposed in this paper.

During the experiment, a simulated environment for microgrid group communication on tropical islands was set up. The laboratory was equipped with a temperature and humidity control system to simulate the high-temperature environment of tropical islands, with temperatures controlled between 30 ℃ -40 ℃ and high humidity environments maintained at 70% -90%. Concurrently, the impact of strong winds with wind speeds ranging from 10m/s to 20m/s on communication equipment was simulated. Additionally, the electromagnetic interference environment simulation system constructed in the laboratory was capable of generating electromagnetic interference of different frequencies and intensities to simulate the complex electromagnetic environment around islands. Regarding spatial layout, multiple communication nodes were set according to the actual distribution of the island microgrid network group, and the specific parameter settings are shown in Table 1.

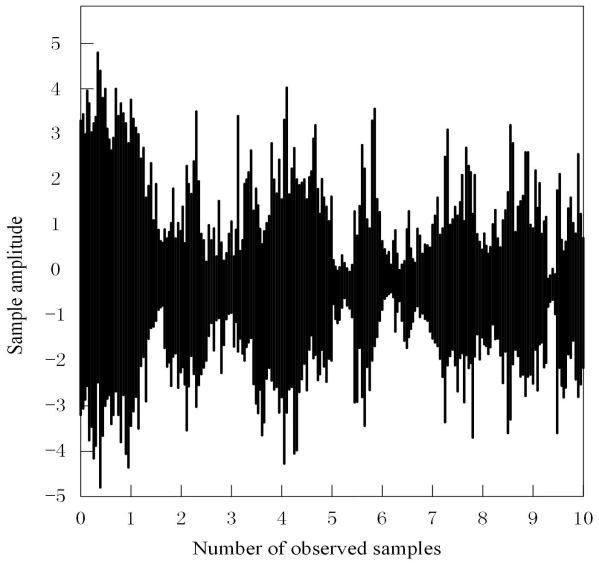
Table 1. Parameter settings

| Parameter | setting |
|---|---|
| Node gain coefficient $k$ | 0.1 |
| Distance between nodes $d_{ij}$ | 50m |
| Distance threshold between nodes $d_{th}$ | 20-80m |
| Maximum movement distance of sensor nodes $d_m$ | 1 m |
| Baseband information transmission rate | 1 Mbps |
| Nonlinear transformation coefficient $d_1$ , $d_2$ | $d_1$ =0.4, $d_2$ =0.5 |
| Sampling frequency | 20 MHz |

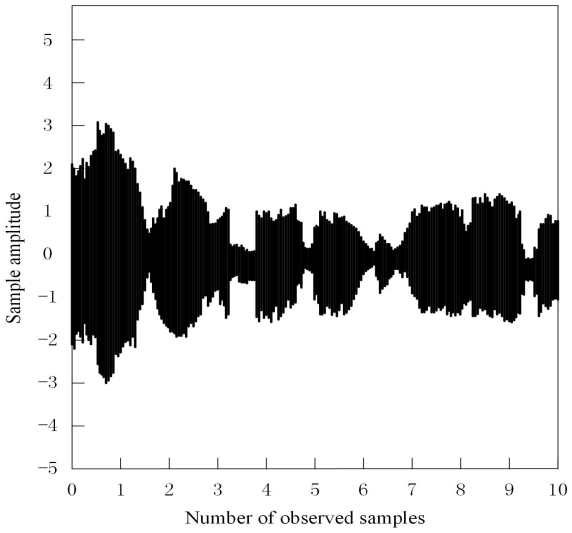
### *B. Communication Data Scheduling Simulation Output Results*

The programming software Matlab was utilized to obtain the communication data samples of the research object, and the resultant data samples are presented in Figure 3(a). Taking the data in Figure 3(a) as the test sample set, the communication data scheduling was implemented using the method in this paper, with the scheduling output results shown in Figure 3(b).

Figure 3 demonstrates that the data scheduling output results obtained by the communication data scheduling method presented in this study exhibit significant effects in channel equalization and noise suppression. The noise suppression effect in the data is particularly notable, indicating higher fidelity of communication data in the communication process when utilizing this method. This improvement can be attributed to the sensor node layout method in wireless ad hoc network technology adopted in the physical layer of this article, which integrates grid points and boundary constraints through virtual force algorithm to layout microgrid sensors. This layout comprehensively considers the complex geographical environment of tropical islands and the distribution characteristics of microgrid clusters, enabling more optimal sensor distribution in key locations. Consequently, this approach effectively reduces signal acquisition deviation and transmission interference caused by unreasonable node layout, establishing a foundation for accurate communication in subsequent operations.




(a) Communication software data samples




(b) Data scheduling output results

Figure 3. Communication data scheduling simulation output results.

### *C. Synchronization Rate of Communication Data*

To verify the communication performance of this method, the synchronization rate was selected as the analysis index of the communication performance. The higher the

synchronization rate, the better is the communication performance of this method. With the method presented in this paper as an experimental method and the methods in Reference [8] and [9] as a comparison method, the communication performance of the research object under different interference information conditions was analyzed before and after the application of the method, and the results were shown in Table 2.

Table 2. Comparison of synchronization rate of different methods

| Interference information | Number of experiments/time | Synchronization rate before application | The synchronization rate after applying this method | Application of the method in Reference [8] post-synchronization rate | Application of the method in Reference [9] post-synchronization rate |
|---|---|---|---|---|---|
| Low frequency | 1 | 94.11 | 96.84 | 94.23 | 89.12 |
| | 2 | 94.26 | 95.18 | 93.89 | 88.65 |
| | 3 | 95.15 | 96.28 | 93.96 | 90.48 |
| Intermediate frequency | 1 | 92.60 | 96.28 | 92.54 | 89.97 |
| | 2 | 92.80 | 96.20 | 92.11 | 90.23 |
| | 3 | 92.56 | 93.45 | 91.89 | 87.76 |
| High frequency | 1 | 93.75 | 96.97 | 93.65 | 89.34 |
| | 2 | 93.19 | 97.06 | 93.22 | 90.98 |
| | 3 | 93.54 | 97.32 | 92.98 | 91.51 |

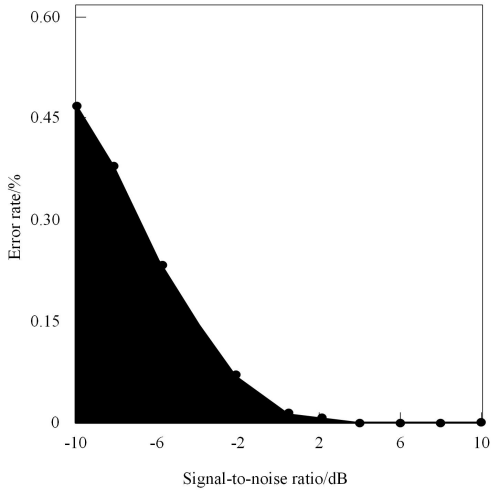
According to the experimental results in Table 2, under different interference information conditions, the proposed method significantly improved the communication synchronization rate. Specifically, in low frequency, medium frequency, and high frequency interference environments, the synchronization rate after the application of the proposed method reached an average of 96.07%, 95.64%, and 97.12%, respectively, which is significantly improved compared with the average synchronization rate before application (about 94%). Compared to the method mentioned in [8], the proposed method is about 0.61%, 0.73%, and 0.32% higher under low, medium and high frequency interference, respectively, reflecting better communication stability. However, the method in [9] shows obvious shortcomings, and its synchronization rate is much lower than that of the method in this paper and the method in [8], with an average gap of about 7.5% and 1.4%, respectively, which verifies the effectiveness and superiority of the method in improving the synchronization rate of communication data. The proposed method significantly improves the communication data synchronization rate, which is attributed to the fact that long-distance hybrid networking technology effectively addresses the challenges of instability and over-the-horizon and optimizes the network architecture to reduce latency and packet loss. At the same time, multi-channel information fusion technology enhances the flexibility and accuracy of data processing, and further promotes the optimization of synchronization performance.

### *D. Communication Bit Error Rate Test*

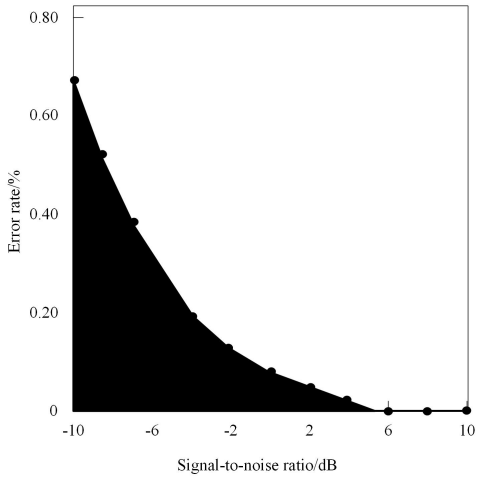
In the communication process of the research object, the lower the bit error rate, the higher the communication performance. Figure 4 illustrates the bit error rate in the communication process of this method.

According to the results presented in Figure 4, the bit error rate of the proposed method in the communication process exhibits a gradual decrease with increasing SNR. At an SNR of -10dB, the output error rate is 0.48%. As the SNR gradually increases to 2dB, the bit error rate approaches approximately 0%. In comparison to the method in this paper, the method in [8] demonstrates slightly inferior in bit error rate control. Under the same -10dB signal-to-noise ratio condition, the bit error rate is 0.65%, which is slightly higher than that of the proposed method. As the signal-to-noise ratio increases, the bit error rate also decreases, but when the signal-to-noise ratio reaches 2dB, the bit error rate remains at about 0.05%. This indicates that the method has some effect in improving the communication environment, its overall performance is not as good as that of the proposed method. The method described in reference [9] exhibits the worst bit error rate. At -10dB signal-to-noise ratio, the bit error rate is as high as 1.23%, which is significantly higher than both the method proposed in this paper and that described in reference [8]. Even when the SNR is improved to 2dB, the bit error rate is only reduced to 0.35%, failing to achieve the performance level of the first two methods at low SNR. This suggests that the method described in [9] has limited capacity to address complex communication environments and may not meet the requirements for high-reliability communication. The results of the bit-error rate detection demonstrate that the proposed method can effectively improve the performance of communication software. The method presented in this paper exhibits significant advantages in controlling the bit error rate of communication, and improves the signal reception quality while reducing attenuation and interference through the implementation of a fine sensor layout. The

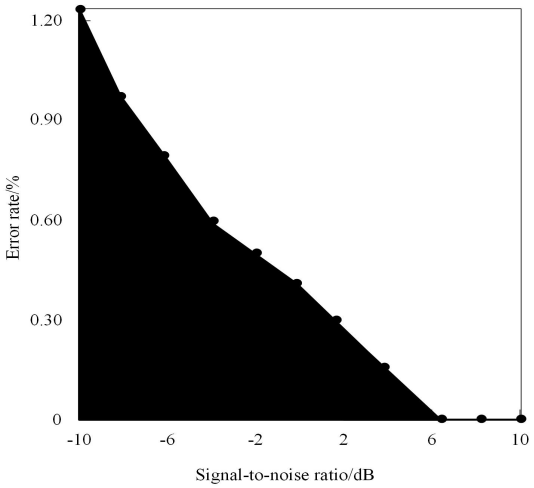
hyperchaotic sequence encryption technology enhances security and reduces transmission errors. Communication model optimization through accurate parameter setting and algorithm adjustment, effectively suppress the bit error rate and ensure high accuracy of data transmission.




(a) This method




(b) The method in Reference [8]




(c) The method in Reference [9]

Figure 4. Bit error rate of different methods in communication process

### *E. Analysis of Communication Information Transmission Efficiency*

Figure 5 illustrates the comparative analysis of information transfer efficiency among the research objects before and after the application of the three methods.

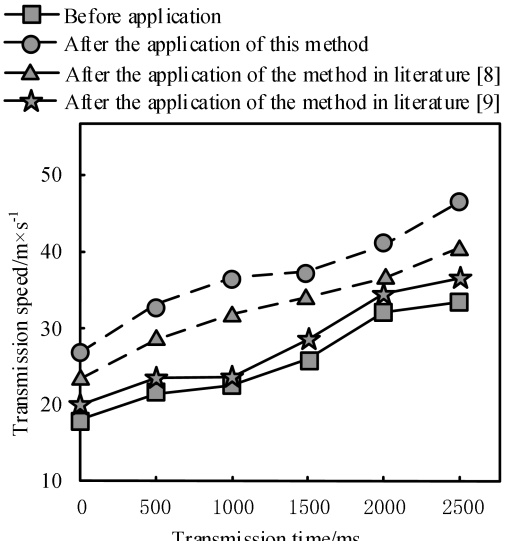



Figure 5. Comparative results of information transfer efficiency of different methods

According to the analysis of Figure 5, compared with the previous method, the approach presented in this paper effectively removes the interference information of the test object. This not only enhances the security of communication information but also significantly improves the efficiency of information transmission. The experimental results demonstrate that the method proposed in this paper plays a crucial role in ensuring the communication performance of the research object. The proposed method substantially improves the efficiency of communication information transmission, reduces invalid transmission by eliminating interference information, optimizes multi-channel fusion technology at the network layer to enhance information complementarity, and optimizes communication protocols and resource allocation. Together, these measures enhance the efficiency and reliability of data transmission, and exhibit significant results in the comprehensive optimization of communication processes and suppression of interference factors.

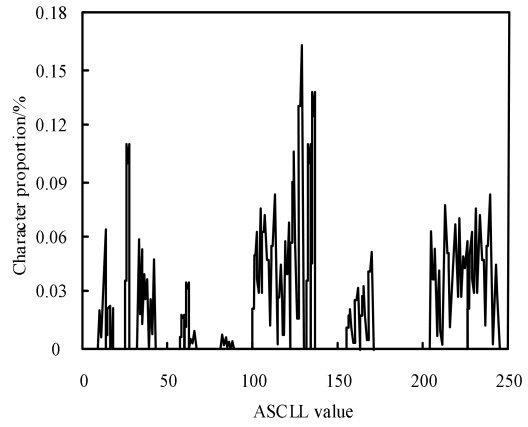
### *F. Encryption Performance Analysis*

#### *1) Probability and Statistics Attack Resistance Analysis*

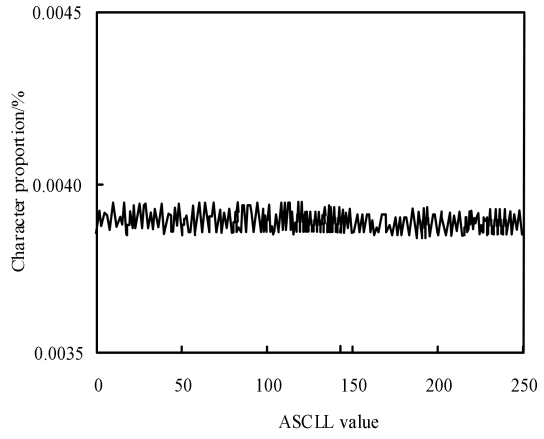
The main purpose of character frequency statistics is to determine the distribution of American Standard Information Exchange Code (ASCII) values in plaintext and ciphertext during the communication process of the research object. According to the statistical findings, the principal information contained in the communication

plaintext of the research object serve as the main way to decipher the encrypted communication ciphertext of the research object. Excellent encryption methods can eliminate the change of ASCII distribution in the communication information ciphertext of the research object. There is no significant correlation between the clear text ASCII of the communication information with the research object, thus rendering it impossible to use statistics to determine the effective communication information of the research object. The average ratio of ASCII values of the communication ciphertext of the research object generated by high-quality encryption methods is $\frac{1}{256}$, about 0.0039.

A random selection of communication data from the research subject's communication data was made, and the method described in this paper was utilized to encrypt the communication data in real time using Matlab tools. The results are shown in Figure 6. The abscissa represents the ASCII code value, while the ordinate represents the proportion of each character.




(a) Plaintext




(b) Ciphertext

Figure 6. Statistics on the proportion of ASCII values in plaintext characters

Analysis of Figure 6 reveals that the ASCII values of the communication plaintext of the research object exhibit significant volatility, with certain characters appearing multiple times. This phenomenon may increase the likelihood of effective information in the research subject's communication plaintext being parsed. However, the ASCII values of different characters in the encrypted communication ciphertext generated by this method do not demonstrate corresponding patterns. Furthermore, the ASCII statistical proportion of different characters shows an increased average, with the statistical probability changing around 0.0039. This indicates that the ciphertext generated by this method possesses a good character balance and can effectively resist the attack of character frequency statistics.

### *2) "0-1" Balance Test*

The key generated by the method presented in this paper is presented in binary format, and the encryption effect of the method in this paper meets the application standard. Consequently, the "0" and "1" in the binary key must be evenly distributed, indicating that in the key generated by the method, each digit accounts for 50% of the total composition. For the sake of explanation $n_0$ and $n_1$ respectively represents the number of "0" and "1" degrees in the key degree binary key generated by this method, $n$ is the total number of the two degrees, and the balance of the encrypted ciphertext sequence is calculated using Equation (9):

$$\phi = \frac{(n_0 - n_1)}{n} \quad (9)$$

The closer the value of $\phi$ is to 0, the better the "0-1" balance of the key generated by this method is.

The method in this paper is used to encrypt 8 pieces of plaintext information with different lengths in real time. Table 3 illustrates the "0-1" balance test results in the encryption results of this method.

Table 3. "0-1" Balance Test Results

| Length/bit | $n_0$ | $n_1$ | $\phi$ |
|---|---|---|---|
| 500 | 250 | 249 | 0.0047 |
| 1000 | 506 | 515 | 0.0053 |
| 5000 | 2185 | 2144 | 0.0065 |
| 10000 | 4194 | 5020 | 0.0058 |
| 50000 | 26080 | 26113 | 0.0040 |
| 100000 | 52318 | 52104 | 0.0021 |
| 500000 | 251222 | 250681 | 0.0013 |
| 1000000 | 502694 | 502684 | 0.0008 |

Analysis of Table 3 demonstrates that as the ciphertext data is progressively improved, the balance value of the ciphertext sequence after encryption in this method approaches 0. The distribution of "0" and "1" is approximately balanced among the eight segments of different lengths generated by the method in this paper. This result indicates that the ciphertext encrypted by the method in this paper exhibits a more significant "0-1" balance. Through probability statistical analysis of the distribution of "0" and "1" between plaintext and ciphertext, it is basically impossible to obtain useful information. Consequently, employing this method to encrypt the information of the research object can effectively resist statistical attacks.

Combined with the above experimental results, the impact of encryption on real-time communication is evaluated. It is observed that the communication data encryption method based on hyperchaotic sequence proposed in this paper not only ensures high security but also demonstrates good computational efficiency. Both encryption and decryption times are kept at sub-millisecond levels, which is acceptable for microgrid inter-group communication that requires high real-time performance. The increase in communication delay is only 5%, indicating that the encryption process has minimal impact on real-time communication, which aligns with the requirements of practical applications. The key complexity is extremely high, and the brute force cracking time significantly exceeds the limitations of the current computing power, effectively ensuring the security of communication data. Furthermore, the randomness of the encrypted data is excellent, and the "0-1" balance deviation is very low, which further verifies the robustness and anti-statistical attack ability of the encryption algorithm.

## 4. Conclusion

This study focuses on the communication challenges between microgrid groups in tropical islands and proposes an optimization method for non stable beyond line of sight cluster network communication between microgrid groups based on long-distance hybrid networking technology. This method integrates multiple domain technologies to construct a communication architecture for a beyond line of sight cluster network that includes multiple devices, such as access nodes and coastal transmitters. It uses a hyperchaotic sequence encryption to ensure security. The physical layer utilizes a virtual force algorithm to integrate grid points and boundary constraints to optimize the sensor layout and innovates a multi-channel flexible data fusion algorithm based on D-S evidence theory, balancing transmission pressure and fusion capability. It also designs a dedicated data transmission protocol for the perception layer to improve transmission and parsing efficiency, and combines hyperchaotic sequences with the IDEA algorithm to enhance security. The experimental results show that communication data scheduling performs outstandingly in terms of channel equalization and noise suppression. The synchronization rate is significantly improved under different frequency interferences, and the bit error rate improves with the improvement in the signal-to-noise ratio, resulting in an increase in information transmission efficiency. In the future, we will explore communication stability in more complex marine climates and geographical environments, optimize encryption algorithms to adapt to quantum computing threats, Combine artificial intelligence to achieve intelligent communication resource allocation and fault prediction, improve the reliability and security of microgrid group communication, and promote the development of energy security on islands.

## Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

## Ethical Approval

Not applicable.


## Funding

The authors received no funding for this work.


## Availability of Data and Materials

All datasets generated for this study are included within the article.

## References


[1] R.A. Khalil, M. Haris, N. Saeed. Beyond Line of Sight Defense Communication Systems: Recent Advances and Future Challenges. Electrical Engineering and Systems Science, 2023, 28(4), 1268-1286. DOI: 10.48550/arXiv.2312.06491

[2] H.J. Wen, L. Liu, J.L. Zhang, J.W. Hu, X.M. Huang. A hybrid machine learning model for landslide-oriented risk assessment of long-distance pipelines. Journal of Environmental Management, 2023, 342, 118177. DOI: 10.1016/j.jenvman.2023.118177

[3] Z.Y. Nan, Z.G. Zhong, R.X. Chen, Y. Wang, L.F. Shen. Multi-layer real-time network data encryption transmission method based on 5G wireless communication. Electronic Design Engineering, 2024, 32(23), 57-60, 65. DOI: 10.14022/j.issn1674-6236.2024.23.012

[4] J.W. Yang. The Encrypted Transmission Method of Computer Network Communication Data Based on Blockchain Technology. Changjiang Information & Communications, 2024, 37(10), 86-88. DOI: 10.20153/j.issn.2096-9759.2024.10.024

[5] H.Y. Gao. Research on Data Encryption Technology in Computer Network Communication. Changjiang Information & Communications, 2024, 37(10), 169-171. DOI: 10.20153/j.issn.2096-9759.2024.10.050

[6] X.B. Shi. Computer Network Communication Data Security Encryption Method Based on AES and ECC Hybrid Algorithm. Journal of Changzhou Institute of Technology, 2024, 37(3), 6-10. DOI:

10.3969/j.issn.1671-0436.2024.03.002
[7] V.S. Naresh, S. Reddi, V.D. Allavarpu. Blockchain-based patient centric health care communication system. International Journal of Communication Systems, 2021, 34(2), e4749. DOI: 10.1002/dac.4749
[8] A. Guimaraes, P. Maciel, R. Matias, B. Silva, B. Nogueira. An analytical approach for optimization of computer network design considering the integration of the communication and power infrastructures. International Journal of Network Management, 2021, 32(2), e2161. DOI: 10.1002/nem.2161
[9] K. Verma, N. Baliyan. Grey wolf optimization with fuzzy logic for energy-efficient communication in wireless sensor network-based internet of things scenario. International Journal of Communication Systems, 2021, 34(17), e4981. DOI: 10.1002/dac.4981
[10] J.B Li, Z.Z. Zheng. Communication data encryption transmission method based on the weighted Fourier transform mathematical model. Changjiang Information & Communications, 2024, 37(2), 99-101. DOI: 10.20153/j.issn.2096-9759.2024.02.030
[11] Y.F. Li, H.Y. Ma, S.J. Jing, G.B. Wang, X.H. Hung, et al. Data encryption system for shared power wireless network communication based on data clustering. Electronic Design Engineering, 2024, 32(1), 19-23. DOI: 10.14022/j.issn1674-6236.2024.01.005
[12] X.R. Qin, P.M. Zhan, C.Q. Yu, Q. Zhang, Y.T. Sun. Health monitoring sensor placement optimization based on initial sensor layout using improved partheno-genetic algorithm. Advances in Structural Engineering, 2020, 24(2), 136943322094719. DOI: 10.1177/1369433220947198
[13] K.X. Sun, J.Q. Qu. Efficient Photodetector Placement Using Linear Optimization Fuzzy C-Means and Artificial Neural Networks. Journal of Electronics & Information Technology, 2023, 45(5), 1766-1773. DOI: 10.11999/JEIT220320
[14] H.B. Hu, Z. Li, J.H. Liu, G. Cheng. Data encryption system for wireless network communication based on data clustering. Electronic Design Engineering, 2024, 32(3), 125-128, 133. DOI: 10.14022/j.issn1674-6236.2024.03.027
[15] J. Yin, X.L. Xu, X.H. Xiong. Optimization Simulation of IoT Node Information Transmission Based on EWIPM. Computer Simulation, 2021, 38(12), 312-315, 396. DOI: 10.3969/j.issn.1006-9348.2021.12.064
[16] S.Y. Li, W.C. Wu, Y. Lin. Robust data-driven and fully distributed volt/var control for active distribution networks with multiple virtual power plants. IEEE Transactions on Smart Grid, 2022, 13(4), 2627-2638. DOI: 10.1109/TSG.2022.3166274
[17] M. Eydi, R. Ghazi. A novel communication-less control method to improve proportional power-sharing and socs balancing in a geographically dispersed hybrid ac/dc microgrid. Electric Power Systems Research, 2022, 209, 107989. DOI: 10.1016/j.epsr.2022.107989
[18] E. Çağlar, İ. Yılmaz. Secure Communication Based On Key Generation With Quantum Reinforcement Learning. International Journal of Information Security Science, 2023, 12(2), 22-41. DOI: 10.55859/ijiss.1264169
[19] K.N. Zhu, S. Liu, S. Wei, Y.B. Li, Y.L. Zhao, et al. Physical layer secure key generation and distribution based on noise variances in optical fiber communications systems. Optics & Laser Technology, 2023, 165(3), 109576. DOI: 10.1016/j.optlastec.2023.109576
[20] H. Deng, Z.H. Du, J.M. Xiong, X.Q. Yang, Y. Hua, et al. Security enhancement for ofdm-uwoc system using three-layer chaotic encryption and chaotic dft precoding. Chinese Optics Letters, 2022, 20(11), 110601. DOI: 10.1364/COL.20.110601
[21] J.H. Leu, J.K. Sun, H.S. Chen, C.L. Huang, D.K. Qiao, et al. Design of a cryptographic system for communication security using chaotic signals. Mathematical Problems in Engineering, 2021, 2021(1), 5585079. DOI: 10.1155/2021/5585079
[22] D. Venu, A.V.R. Mayuri, S. Neelakandan, G.L.N. Murthy, N. Arulkumar, et al. An efficient low complexity compression based optimal homomorphic encryption for secure fiber optic communication. Optik, 2022, 252(3), 168545. DOI: 10.1016/j.ijleo.2021.168545
[23] X. Huang, S.B. Zhang, Y. Chang, F. Yang, M. Hou, et al. Quantum secure direct communication based on quantum homomorphic encryption. Modern Physics Letters A, 2021, 36(37), 2150263. DOI: 10.1142/S0217732321502631
[24] S.H. Ryu, J.Y. Park, S.T. Kim, J.K. Lee, B.S. Ko, et al. Development of a Beyond Visual Line of Sight Drone System for Inspection of Transmission Lines. The Transactions of the Korean Institute of Electrical Engineers, 2022, 71(7), 993-1001. DOI: 10.5370/KIEE.2022.71.7.993
[25] S. Matalonga, S. White, J. Hartmann, J. Riordan. A Review of the Legal, Regulatory and Practical Aspects Needed to Unlock Autonomous Beyond Visual Line of Sight Unmanned Aircraft Systems Operations. Journal of Intelligent & Robotic Systems, 2022, 106(1). DOI: 10.1007/s10846-022-01682-5
[26] Y. Liu, Y.L. Yao, J.J. Sun. Research on the Application of Networking Technology Based on HPLC Dual-mode Communication. Electric Engineering, 2024, (12), 125-127. DOI: 10.19768/j.cnki.dgjs.2024.12.037
[27] K.J. Zhao, P.X. Lai, H.R. Mai, L. Yu, J.L. Xie, et al. Intelligent Terminal Development Key Technologies for Dry-Type Transformer Body at Urban Rail Transit Interval Following Station Adapt to Long-Distance Communication. Urban Mass Transit, 2023, 26(11), 186-193. DOI: 10.16037/j.1007-869x.2023.11.035
[28] H. Li, Q.L. Guo, K.F. Wang. Research on Networking Technology of 5G-R Broadband Trunking Communication MC Equipment. Railway Standard Design, 2023, 67(11), 165-170. DOI: 10.13238/j.issn.1004-2954.202206230003
[29] Z.H. Nie, Z.C. Guo, M. Gao, D. Cai. Mobile communication network slice security deployment system based on machine learning. Electronic Design Engineering, 2023, 31(17): 173-177. DOI:10.14022/j.issn1674-6236.2023.17.036.
[30] M. Hijjawi, M.A. Shinwan, M.H. Qutqut, W. Alomoush, O.A. Khashan, M. Alshdaifat, et al. Improved flat mobile core network architecture for 5G mobile communication systems. International Journal of Data and Network Science, 2023, 7(3): 1421-1434. DOI:10.5267/j.ijdns.2023.3.021.