Eavesdropping Interference in Wireless Communication Networks Based on Physical Layer Security

Mingming Chen*, Yuzhi Chen
College of Information and Smart Electromechanical, Engineering, Xiamen Huaxia University, Xiamen, 361024, China

***Abstract*—Effective communication security protection can protect people's privacy from being violated. To raise the communication security of wireless communication networks, a collaborative eavesdropping interference scheme with added artificial noise is proposed by combining physical layer security and clustering scenarios to protect the communication security of wireless sensor networks. This scheme adds artificial noise to the transmitted signal to interfere with the eavesdropping signal, making the main channel the dominant channel and achieving eavesdropping interference in wireless communication networks. The results show that after using artificial noise, as the signal-to-noise ratio of the main channel increases from 0 to 20dB, the confidentiality capacity can increase from 0.5 to over 4.0. When the transmission power is 0.4W, the confidentiality capacity reaches its maximum and does not depend on the signal-to-noise ratio. When the number of interfering nodes increases from 1 to 2, the confidentiality capacity increases from approximately 4.7 to around 5.8. The research designed a wireless communication network eavesdropping interference scheme that can effectively protect the information security of the wireless communication network, making the main channel an advantageous channel and achieving complete confidentiality. This scheme can be applied to wireless communication networks to improve the security level of the network.**

Keywords*—Wireless communication; sensors; network security; eavesdropping interference; clustering scenario

I. INTRODUCTION

With the quick development and popularization of technologies such as mobile networks, the Internet of Things, and smart cities, wireless communication technology is playing an increasingly important role in social life [1]. At the same time, its broadcasting and stacking characteristics pose greater challenges for wireless networks compared to wired networks when facing security issues. The broadcasting characteristics of wireless networks mean that all devices within the wireless range can receive the transmitted data packets. Attackers can deploy their devices near legitimate recipients and intercept transmitted data by listening to wireless signals. The superposition characteristic of wireless networks allows multiple signals to overlap and transmit on the same channel. Attackers can send interference signals, reducing the quality of legitimate signals, making it difficult for legitimate receivers to correctly decode the received data, while attackers attempt to obtain information in chaos. Attackers can set up a fake access point with the same SSID and password as a legitimate wireless access point, luring users to connect to this fake network. Once connected, the attacker can intercept all data transmitted through the access point. As attackers, they usually utilize these two characteristics to reduce decoding efficiency by pretending to be illegal recipients to steal information or sending interfering information as malicious disruptors [2-3]. Therefore, how to ensure information security and reliability in wireless networks has become particularly important. Traditional wireless networks mostly monitor network traffic by deploying wireless intrusion detection systems to detect abnormal behavior or potential attack patterns in a timely manner. Meanwhile, it implements a strong authentication mechanism to ensure that only authorized users can access network resources, to reduce the risk posed by attackers. In the past, wireless network communication security was mainly built on the security framework of wired networks. Physical layer security (PLS) technology involves multiple levels such as wireless signal processing, channel coding, modulation and demodulation, and requires a deep understanding of the physical characteristics of wireless communication. The technical threshold is high. Compared to traditional security technologies based on the application layer and transport layer, research on PLS started relatively late. Therefore, related research and discussion are not sufficient, leading to the neglect of PLS issues in wireless networks at times [4]. The communication security of traditional wireless networks completely depends on key protection. In the open environment, it is difficult to use key technology to encrypt communication information, and the encryption cost is high, which is difficult to apply on a large scale. In fact, PLS is crucial for wireless network security, especially in clustering scenarios of wireless sensor networks, it can provide a new direction of thinking [5]. Currently, PLS has been widely recognized as the most effective way to solve wireless network security issues and has been applied in many cutting-edge technologies [6]. The study combines the clustering scenario of wireless sensor networks with PLS and explores the PLS problem of wireless communication network eavesdropping interference in the clustering scenario. On the basis of not changing the original topology structure of the network, this study proposes to use idle ordinary nodes as collaborative nodes.

In the inter cluster communication process of the head node, to jointly send interference information and interfere with eavesdroppers in other directions.

The main innovation of the research lies in combining clustering scenarios with PLS and proposing a strategy of utilizing idle nodes for collaborative interference. This study not only provides new research directions and possible solutions for

*Corresponding Author.

PLS, but also provides important references for achieving secure communication in clustering scenarios of wireless sensor networks. This method fully utilizes the advantages of network topology without the need for additional equipment or hardware, thus ensuring the implementation of PLS. The research provides a new perspective and solution strategy for wireless communication network security issues at the physical layer. The primary contribution of this research is the utilization of idle nodes in wireless networks to create a synergistic interference effect on the signal information transmitted within the network. This increases the difficulty for attackers to steal network information and reduces the cost of information encryption in wireless network communication, thereby significantly enhancing the security of wireless network communication.

The research will be conducted in seven sections. Section II is an overview of the current status of wireless communication network security research. Section III is a study on wireless communication network eavesdropping interference based on clustering scenarios and PLS. Section IV is an experimental analysis of eavesdropping interference schemes based on clustering scenarios and PLS. Discussion and conclusion are given in Section V and Section VI respectively.

II. Related Works

The security issue of communication networks is one of the main challenges faced by wireless communication networks. Wei Z et al. proposed a new security technology to address the security issues in integrated sensing and communication transmission, to ensure information security (Table I). By embedding information signalling in the detection waveform, the security of transmission was ensured. Meanwhile, sensing capabilities were utilized to obtain target information, which further enhances security [7]. Wang C et al. systematically investigated node capture attacks to alleviate the security issues of user authentication in wireless sensor networks. Countermeasures were proposed for different types of attacks and 61 authentication schemes were evaluated. The results showed that understanding node capture attacks helped in designing more secure authentication schemes [8]. Naghibi M et al. proposed a secure data fusion method to reduce the energy consumption of wireless sensor networks. This method reduces the number of data packets through data aggregation and improves data security by using lightweight symmetric encryption. The simulation outcomes denoted that compared with traditional methods, this method had a higher level of data security [9]. Wu F et al. proposed a new three factor authentication scheme to address the security issues of data transmission in wireless sensor networks. This scheme provided session keys, maintained security through formal verification and informal analysis, and had better security and application value than similar schemes. The simulation results indicated that this scheme had practical prospects [10]. Jia XC analyzed the current resource efficiency and security technologies adopted to meet the strict requirements of wireless sensor networks in terms of resource budgeting and security. A resource efficient distributed state estimation method and a secure distributed state estimation strategy based on different scheduling were proposed. The results showed that these technologies could effectively improve the performance and security of wireless sensor networks [11]. Hu S et al. proposed a distributed machine learning-based communication data management method to address the issues of communication congestion and information leakage caused by data explosion in wireless communication networks. The results showed that this method could effectively prevent the leakage of communication data and improve the smoothness of communication networks [12].

TABLE I. List of Literature Surveys

Author	Method	Shortcoming
Wei Z [7]	Information signaling embedding	High technical costs
Wang C [8]	Attack capture auxiliary node authentication	Complex data processing
Naghibi M [9]	Lightweight symmetric encryption	High technical costs
Wu F [10]	Key encryption	High technical costs
Jia X C [11]	Distributed State Estimation Strategy	Poor timeliness
Hu S [12]	Distributed Machine Learning	Poor timeliness
Li X [13]	PLS Backscatter Communication Network Framework	Focus on improving signal quality, with weak signal protection
Yuan X [14]	Reconfigurable only on the surface	Unable to handle signal leakage issues
Pirayesh H [15]	Frequency hopping spread spectrum	Insufficient anti-interference ability
Yu X [16]	Intelligent reflective surface	High technical costs
Matthaiou M [17]	Intelligent reflective surface	Weak signal processing ability

PLS in wireless sensor networks is one of the effective ways to solve network security. Li X et al. proposed the PLS backward scattering communication network framework to solve the challenges faced by 6G wireless communication networks. This framework aimed to improve the reliability and security of communication. The results showed that the proposed framework could optimize the performance trade-off between reliability and security under a high signal-to-noise ratio (SNR) [13]. Yuan X et al. summarized the current channel state acquisition techniques for wireless communication networks to address the issues of channel state information acquisition, passive information transmission, and low complexity robust system design for reconfigurable intelligent surfaces in wireless network PLS. The results showed that reconfigurable smart surfaces had unique advantages in improving wireless channel capacity [14]. Pirayesh H et al. aimed to comprehensively

understand the interference attacks and anti-interference strategies of existing wireless networks. Various interference and anti-interference strategies for existing networks were proposed and analyzed in depth. The results showed that although some progress has been made, the design of anti-interference wireless network systems still faced challenges [15]. To enhance PLS performance, Yu X used intelligent reflective surfaces in challenging radio environments. The joint design of beamformer, covariance matrix, and phase shifter were studied to maximize system and rate while limiting information leakage. Effective algorithms were developed to solve non convex optimization problems. The results showed that intelligent reflective surfaces could significantly improve confidentiality performance, and evenly distributed reflective elements are better [16]. Matthaiou M et al. focused on the key physical layer enabling factors of 6G to meet the ubiquitous, reliable, and low latency connection needs of the future. The challenges related to intelligent reflective surfaces, large-scale multi-input and multi-output without honeycomb, and terahertz communication were proposed. The results showed that 6G would need to overcome challenges such as theoretical modeling, hardware implementation, and scalability, and signal processing played a critical role in the new era of wireless communication [17].

In summary, traditional communication anti-eavesdropping and interference technology is achieved through communication encryption. Although this method has a high communication encryption effect, it requires a large amount of computing resources and is suitable for specialized communication signal anti-eavesdropping and interference. It is not applicable in ordinary scenarios. PLS utilizes intelligent reflector surfaces to achieve anti-eavesdropping protection for communication signals, with low requirements for communication sending and receiving devices, and high applicability in IoT scenarios. However, PLS is unable to handle the attack behavior of eavesdroppers in communication data protection, and its protection capability is relatively weak. In the scenario of clustered routing, the same communication signal will be encrypted and transmitted multiple times, which can enhance the encryption strength of the communication signal. However, communication encryption will further increase the consumption of computing resources. Therefore, the study proposes to use cluster routing to improve PLS, combining the encryption enhancement effect of cluster routing with the low computational requirements of PLS encryption, to protect user communication data in the Internet of Things.

III. Eavesdropping Interference in Wireless Communication Networks Based on Clustering Scenarios and PLS

Clustering scenarios are widely used in wireless sensor networks, and PLS is a common way to protect data communication security. In Section III, the study analyzes the eavesdropping interference based on clustering scenarios and PLS wireless communication networks. Section III contains two sections: the first section is the analysis of artificial noise technology in the PLS field, and the second section is the analysis of collaborative interference based on clustering scenarios.

A. Analysis of Artificial Noise Technology in PLS Field

PLS is a new direction based on information theory, utilizing physical layer characteristics or using physical layer technology to achieve communication security? The existing communication encryption methods mostly rely on complex key encryption technology, which occupies a high amount of computing resources and requires extremely high device requirements, resulting in poor applicability in the Internet of Things. PLS technology is based on the randomness and uniqueness of wireless channels, utilizing their inherent characteristics to achieve secure transmission without relying on complex cryptographic algorithms or key distribution mechanisms [18]. PLS technology does not rely on computational complexity and can be implemented even on devices with weaker computing power. Although PLS based on the eavesdropping channel model has a necessary assumption that the quality of the main channel for legitimate communication is better than that of the eavesdropping channel, Maurer proposed a new method that used wireless channel characteristics to generate the key that information encryption relies on. At the same time, to weaken the premise assumption of eavesdropping channels, technologies such as beamforming, artificial noise, and collaborative interference were also adopted. Therefore, PLS is mainly divided into two directions: keyless security and wireless channel-based key generation. The eavesdropping channel model is shown in Fig. 1.

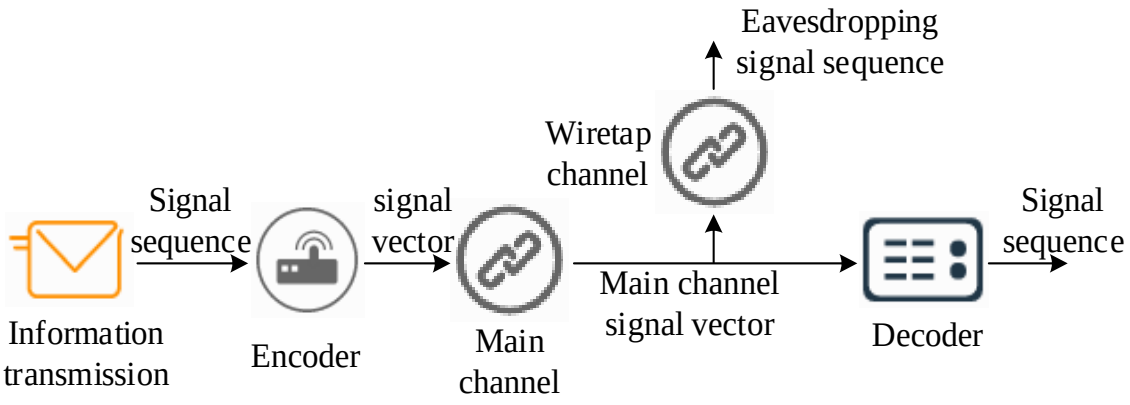


Fig. 1. The eavesdropping channel model.

The topic of the eavesdropping channel model is divided into four parts, namely encoder, main channel, eavesdropping channel, and decoder. In wireless communication systems, information transmission is a complex and constantly evolving process. There is a sequence S with a length of K, which contains communication raw data or information. Before sending, the sequence S is encoded as a vector X with a length of N, which is processed and modified by encoding before being sent through the main channel. After vector X is transmitted through the main channel, a vector Y with a length of N can be obtained. The task of the receiver is to decode the received vector Y to restore the original sequence S. Usually, decoding is a complex process that includes a series of steps such as denoising and demodulation, with the goal of restoring the sequence S as accurately as possible. However, there is a potential security risk involved in this process. In addition to legitimate recipients, there may also be a eavesdropping party attempting to intercept the information being transmitted. The eavesdropping party eavesdrops on the vector Y transmitted through the main channel through the eavesdropping channel, which is problematic and interferes with, just like the main channel. Therefore, the result that the eavesdropper overhears may be a vector Z with various noises and errors of length N. The confidentiality capacity is the main performance indicator of PLS, which is directly related to the channel capacity. In the eavesdropping channel model, when the eavesdropping channel is not considered, the channel capacity of the main channel is denoted in Eq. (1).

$$C_M = \max_{p(x)} I\left(X;Y\right) \tag{1}$$

In Eq. (1), $I\left(X;Y\right)$ means the mutual information between the information content X and Y. C_M means the channel capacity of the main channel. If considering eavesdropping channels, the capacity of the main channel can be defined as Eq. (2).

$$\hat{C}_M = \max_{p(x)} I\left(X;Y\middle|Z\right) \tag{2}$$

The eavesdropping channel can be regarded as obtaining Y through the main channel transmission, and then obtaining Z through the eavesdropping channel. The virtual channel is called, and at this point, a Markov chain is formed between the sequences X, Y, and Z. Based on the Markov chain, Eq. (3) can be obtained.

$$H\left(X\middle|Y,Z\right) = H\left(X\middle|Y\right) \tag{3}$$

In Eq. (3), $H\left(\cdot\middle|\cdot\right)$ represents conditional entropy, which represents the amount of information that X still contains, given all the information of Y. Through the basic properties of mutual information, equation (4) can be obtained.

$$I\left(X;Y\middle|Z\right) = H\left(X\middle|Z\right) - H\left(X\middle|Y,Z\right) = I\left(X;Y\right) - H\left(X;Z\right) \tag{4}$$

According to Eq. (4), Eq. (2) can be rewritten as Eq. (5).

$$\hat{C}_M = \max_{p(x)} \left[I\left(X;Y\right) - I\left(X;Z\right) \right] \tag{5}$$

In the eavesdropping channel model, it is assumed that the sender wants to send a message while also protecting the message from eavesdropping. To achieve this goal and obtain the maximum actual information transmission rate, the confidentiality capacity can be defined as Eq. (6).

$$C_s = \max_{R \in \Re} R \tag{6}$$

In Eq. (6), R represents the actual transmission rate. C_s represents confidential capacity. $\Re$ represents the reachable region of $\left(R, R_e\right)$, as shown in Fig. 2 [19].

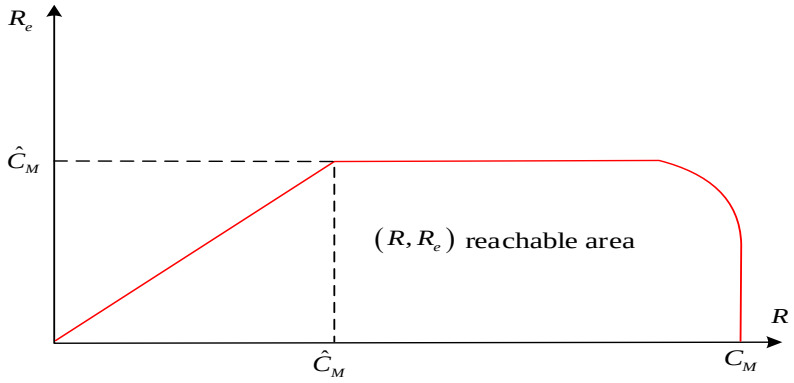


Fig. 2. $\left(R, R_e\right)$ range coverage.

In Fig. 2, the range of R is less than C_M, the range of R_e is less than $\hat{C}_M$, and in $R \le \hat{C}_M$, $R = R_e$ meets the requirements for complete confidentiality. Therefore, when the confidentiality capacity satisfies Eq. (7), communication at a rate of V with C_s as the upper bound can achieve complete confidentiality.

$$C_s = \hat{C}_M = \max_{p(x)} \left[I(X;Y) - I(X;Z) \right] \tag{7}$$

In the eavesdropping channel model, signal receiving channels are divided into legitimate receiving channels and illegal receiving channels. When the signal generator transmits a signal, it will add an error code to the transmitted signal. The frequency of the error code is different from the frequency of the legal channel. When the legal channel receives the signal, it will not receive the error code. The signal reception frequency of the eavesdropping channel is relatively wide, and it will receive a large number of signals when receiving signals. At the same time, it will also receive error codes in the signal, resulting in missing or incorrect received information. This makes the effective information in the signal received by the eavesdropper 0, which can achieve complete confidentiality of information. That is, in the eavesdropping channel model, when the quality of the main channel is higher than that of the eavesdropping channel, non-zero confidentiality ability can be obtained. To ensure that the quality of the main channel is higher than that of the eavesdropping channel, artificial noise can be added to the information to interfere with the eavesdropping channel and reduce its quality, thereby achieving complete confidentiality of the information. The artificial noise scheme design is shown in Fig. 3.

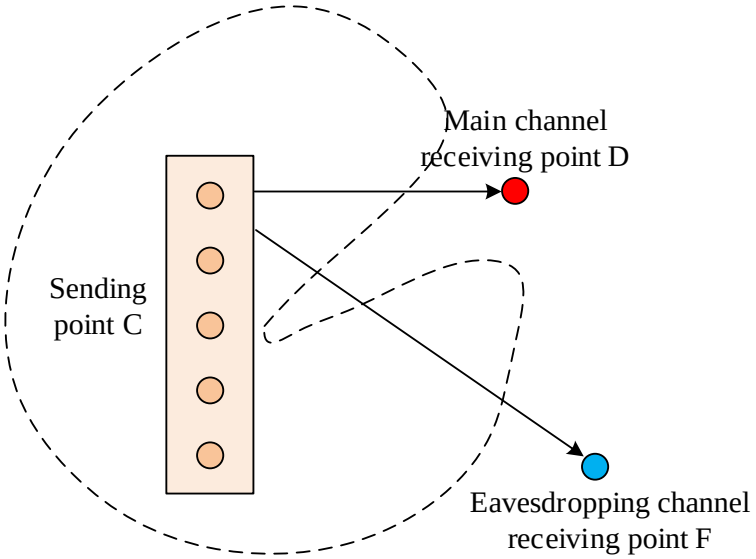


Fig. 3. Artificial noise confidentiality scheme.

In the research-designed artificial noise interference schemes, there is an artificially designed noise between the signal sender and receiver. When using this noise to interfere with eavesdroppers, it is necessary to use a legitimate channel to provide feedback on the channel status to the signal sender. After receiving channel status information, the signal sender sends zero space artificial noise to the legitimate channel based on the channel status. The legitimate receiving channel can process the received signal and extract information based on the zero space artificial noise. Due to the inability of illegal channels to provide feedback on channel status to the sender, zero space artificial noise cannot be obtained. Artificial noise between communication networks can interfere with the transmitted signal, organizing eavesdroppers to read signal information. In this scheme, the received signal z_k of the main channel can be represented as Eq. (8).

$$z_k = h_k x_k + n_k \tag{8}$$

In Eq. (8), h_k represents the main channel vector. x_k stands for sending signals. n_k represents the Gaussian white noise vector of the main channel. The received signal y_k of the eavesdropping channel can be expressed as Eq. (9).

$$y_k = g_k x_k + e_k \tag{9}$$

In Eq. (9), g_k represents the eavesdropping channel vector. e_k represents the Gaussian white noise vector of the eavesdropping channel. When the information sender is equipped with multiple antennas, the transmitted signal can be represented as Eq. (10).

$$x_k = p_k u_k + w_k \tag{10}$$

In Eq. (10), u_k represents the carrier signal. w_k represents artificial noise signal. p_k represents the beam wave vector. Artificial noise signals need to meet Eq. (11).

$$\begin{cases} h_k w_k = 0 \\ h_k p_k \neq 0 \end{cases} \tag{11}$$

At this point, the received signal at the main channel can be represented as Eq. (12).

$$z_k = h_k p_k u_k + n_k \tag{12}$$

The received signal at the eavesdropping channel can be expressed as Eq. (13).

$$y_k = g_k p_k u_k + g_k w_k + e_k \tag{13}$$

In order to make the impact of artificial noise on the eavesdropping channel equal in each direction, it can be designed as Eq. (14).

$$w_k = \Gamma_k v_k \tag{14}$$

In Eq. (14), Γ_k represents the zero space matrix of h_k, and v_k represents an independent and identically distributed Gaussian vector with a mean of 0.

B. *Collaborative Interference Analysis Based on Clustering Scenarios*

Clustering scenario is a commonly used network architecture model in wireless sensor networks. This scheme divides each node in the network into different clusters, with each cluster having a node called a cluster head responsible for managing and organizing communication within the cluster [20-21]. Within each cluster, cluster head nodes manage and control member nodes, collect and summarize data from nodes within the cluster, and then transmit this data to base stations or other cluster head nodes. Clustering can adapt to the dynamic joining and exiting of nodes, and cluster heads can reorganize the cluster structure based on changes in nodes within the cluster, maintaining network connectivity and stability. Moreover, each cluster can be independently managed, while the cluster head can be responsible for monitoring the status of nodes within the cluster and maintaining the stability of the cluster. If some nodes within a cluster fail, the cluster head can reorganize the remaining nodes or collaborate with other clusters to ensure the continuity of network services. In a clustered cluster, data transmission first occurs within the cluster and then communicates with other clusters or base stations through the cluster head. In a clustered cluster, the cluster head can aggregate data within the cluster, reduce redundant data transmission, and improve data transmission efficiency. This approach reduces the need for direct communication between each node and the base station and lowers the communication overhead of the entire network. During the communication process, the cluster head is responsible for collecting and transmitting data within the cluster, while other nodes reduce energy consumption due to reduced direct communication with base stations. The selection of cluster heads can be based on the energy level of nodes, thereby achieving balanced energy consumption and extending the service life of the network. This method can significantly reduce the number of communications between nodes, thereby significantly reducing energy consumption and improving the network's lifespan. In the process of dividing clusters, different goals and standards can be used, such as geographical location, energy consumption, network conditions, and so on. Due to the fact that the nodes in each cluster are usually located in similar areas, the communication distance between nodes is short, which is beneficial for energy conservation and improving network performance. Cluster routing is shown in Fig. 4.

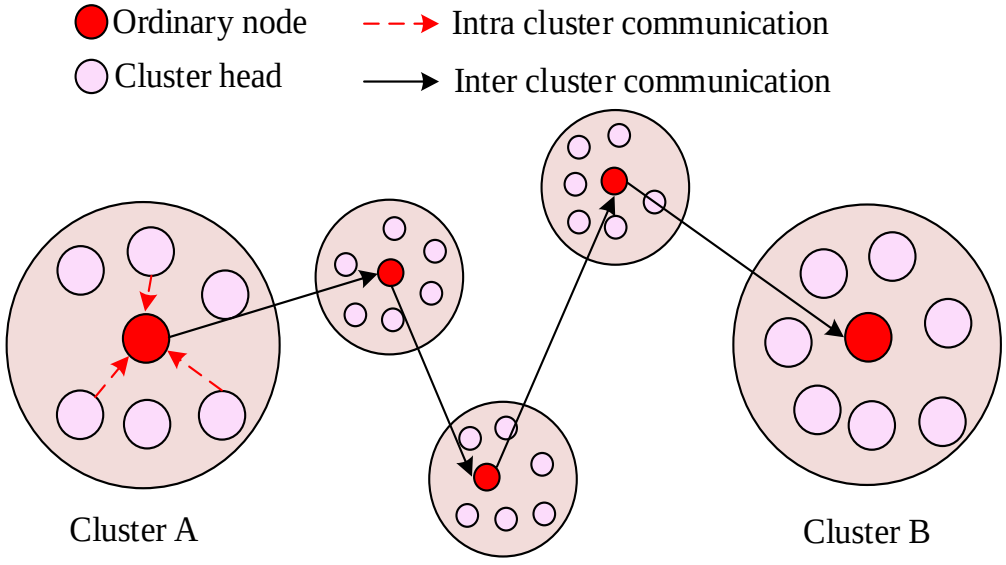


Fig. 4. Clustering routing.

Clustered wireless sensor networks provide a natural scenario for achieving collaborative interference. Firstly, in a clustering network, when cluster head nodes engage in inter cluster communication, ordinary nodes usually do not participate in intra cluster communication to avoid interference between intra cluster nodes. In this process, these temporarily idle ordinary nodes can be selected as interference nodes, jointly generating interference effects and obstructing potential eavesdroppers from obtaining information. Idle nodes within the cluster do not participate in intra cluster communication and can also accept artificial noise outside the cluster. After receiving artificial noise, idle nodes attach it to the communication space within the cluster, and attach it to the periphery of the communication nodes within the cluster, forming an interference protection layer for passing nodes. Secondly, the clustering scenario makes information exchange much more convenient. Cluster head nodes and regular nodes are relatively concentrated in physical locations and close in distance, making information exchange within a small area more convenient and efficient compared to the entire network. Cluster heads can better coordinate with ordinary nodes to generate collaborative interference, while monitoring the effectiveness of interference. In addition, the clustering scenario itself is a network management mechanism with good topology and organization. This structure provides convenience for designing and implementing collaborative interference strategies, making it easier to achieve collaborative actions between the sender and interference nodes. The two-stage collaborative interference scheme is a wireless communication strategy based on PLS. The core of this scheme is to use nodes in the network to collaborate in two stages to generate interference and improve communication security, as shown in Fig. 5.

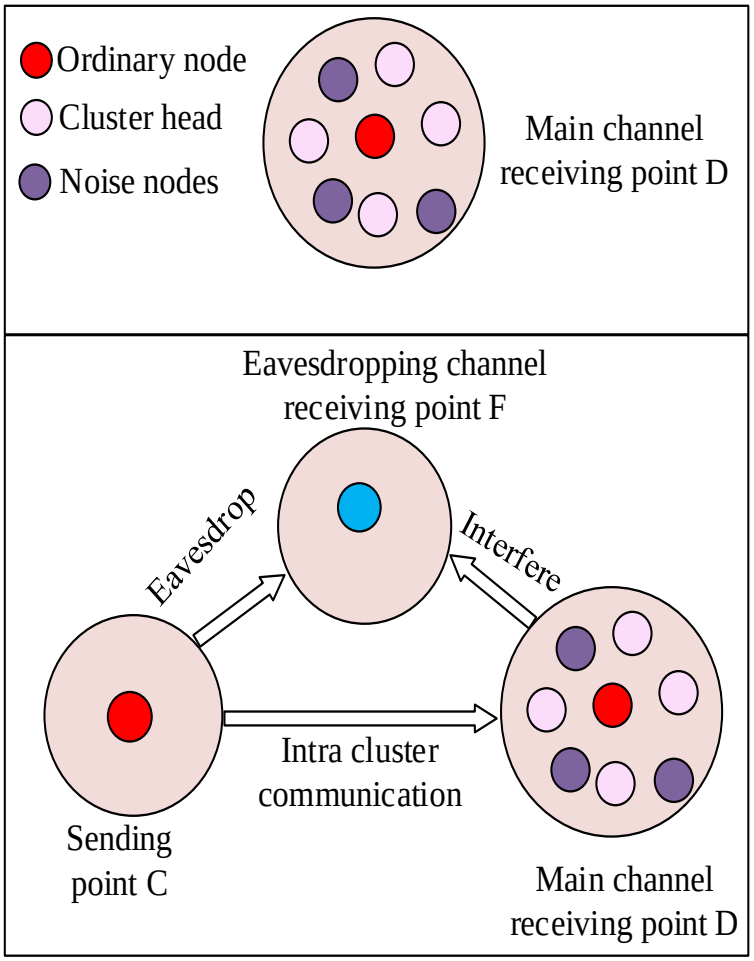


Fig. 5. Two-stage collaborative interference scheme.

The collaborative interference scheme based on clustering scenarios designed for research is based on this framework, which organizes sensor nodes in the network into multiple clusters based on specific algorithms or strategies. In each cluster, a cluster head node serves as the center to manage and command several child nodes to complete their respective tasks. The research assumes that the sender of inter cluster communication is C, the receiver is D, and the illegal eavesdropper is marked as F. C and D are cluster head nodes in two different clusters A and B. Their task is not only to collect data within their respective clusters, but also to transmit information between clusters. At the same time, illegal eavesdropper F is lurking in cluster E, attempting to intercept communication content between C and D through wireless eavesdropping channels. In order to address the potential threat of F, the plan proposes that D will select a portion of ordinary nodes belonging to cluster B under its management as interference nodes, as shown in Fig. 6.

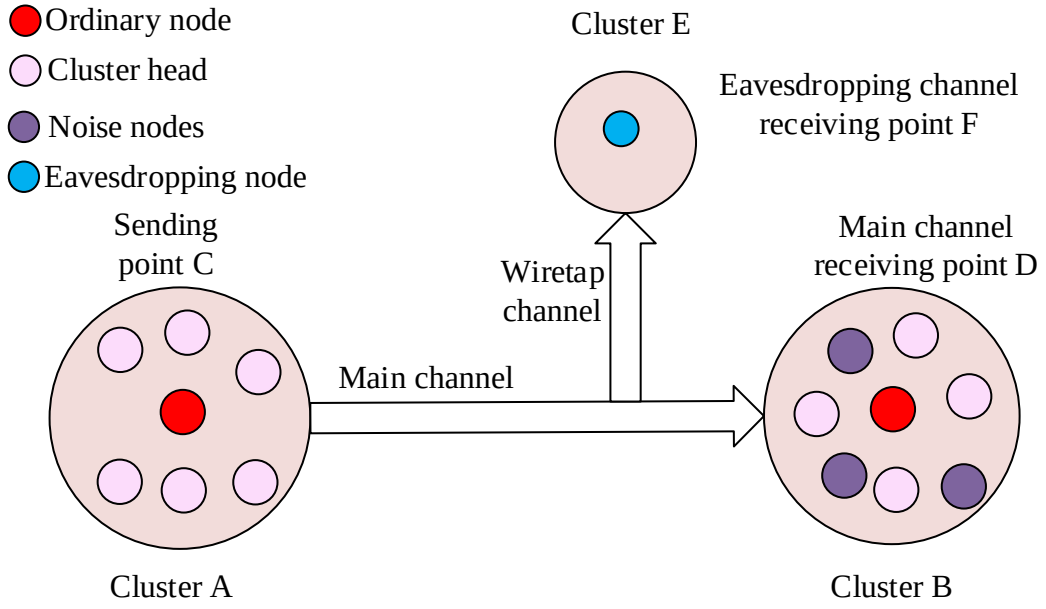


Fig. 6. Topology structure of collaborative interference network based on clustering scenarios.

Interference nodes are dynamically updated and can interfere with F's eavesdropping behavior, thereby protecting the security of information transmission. Due to the dynamic changes of nodes in clustering, it is not possible to select a constant node as the interfering node every time. Therefore, this study designs a strategy for selecting interfering nodes through the principle of reservoir sampling algorithm. Compared with traditional methods such as dynamic frequency hopping, the research-designed method not only protects wireless network communication security through PLS, but also considers the anti-interference ability of the communication channel. The study-designed wireless network communication security protection technology adopts cluster scenario design, which has good adaptability to network environment. Due to the use of PLS technology in the research-designed communication security protection methods, there may be compatibility issues with some systems or equipment. It is necessary to update or design supporting frameworks, develop compatibility layers, and improve the applicability of this technology.

IV. Analysis of Wireless Communication Eavesdropping Interference Schemes Based on Clustering Scenarios and PLS

In Section III, a wireless communication eavesdropping interference scheme based on clustering scenarios and PLS was proposed. To verify the feasibility of this scheme, simulation experiments were conducted in Section IV to analyze it. This part is divided into two sections. The first section is the setting of simulation experiment parameters and environment, and the second section is the analysis of the effectiveness of eavesdropping interference schemes.

A. Experimental Parameters and Environmental Settings

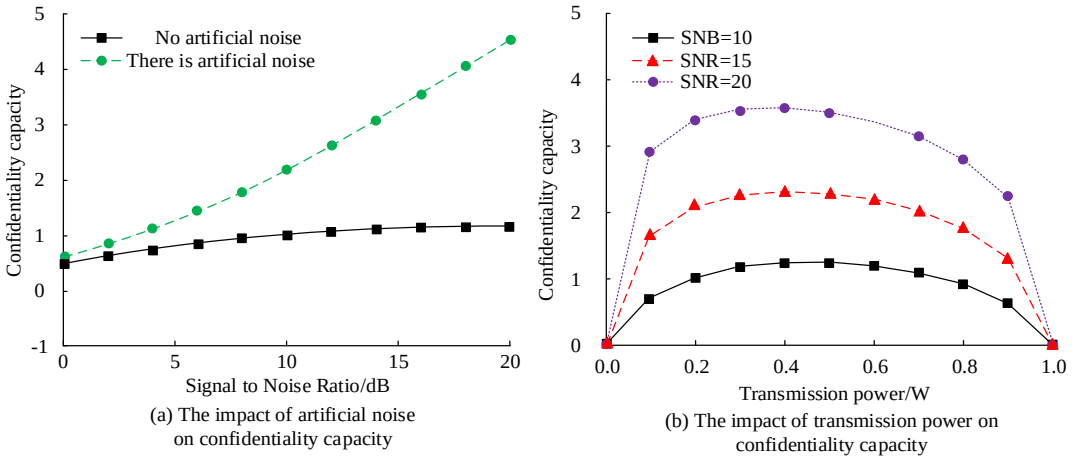
The system used in the study was Windows 10 64 bit, and the device processor was Inter (R) Core (TH) i5-12440. The device had 16GB of memory and the simulation experiment platform was MATLAB. The relevant parameters of the model are denoted in Table II.

TABLE II. Model Parameter

Parameter	Value	Unit	Parameter	Value	Unit
Total power	1	W	Cluster A radius	5	m
Antenna gain parameters	0.003	/	Cluster B radius	5	m
Main channel path loss index	2	/	Distance between the centers of cluster A and cluster B	15	m
Interference channel path loss index	2.5	/	Minimum node spacing	2	m
Communication bandwidth	5	MHz	Interference node density	0.05	Pieces/m2
Gaussian white noise unilateral spectral density	-174	dB	Eavesdropping node density	0.001	Pieces/m2

B. Analysis of the Effectiveness of Eavesdropping Interference Schemes

To evaluate the effectiveness of the proposed wireless communication network eavesdropping collaborative interference method, the study analyzed the variation of confidentiality capacity with the main channel SNR in the presence or absence of artificial noise, as well as the variation of confidentiality capacity with transmission power under different SNRs. The results are shown in Fig. 7.

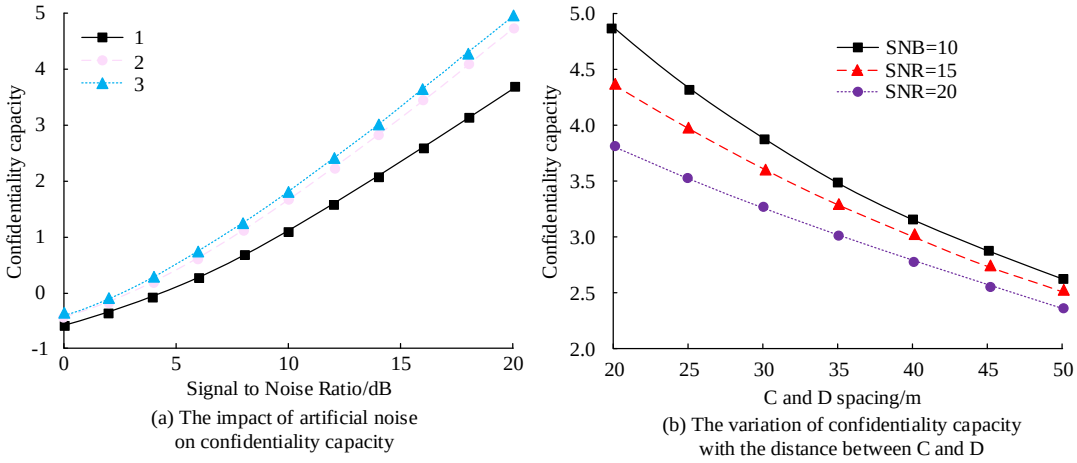


(a) The impact of artificial noise on confidentiality capacity

(b) The impact of transmission power on confidentiality capacity

Fig. 7. The recy capacity with the main channel parameter.

Fig. 7 (a) shows the change of confidentiality capacity with and without artificial noise as a function of the main channel SNR. The system confidentiality capacity remained between 0 and 1 without the addition of artificial noise. After adding artificial noise, the system's confidentiality capacity increased rapidly with the increase of the main channel SNR. When the main channel SNR was 0, the system's confidentiality capacity was about 0.5. When the main channel SNR increased to 20dB, the system's confidentiality capacity increased to above 4.0. Fig. 7 (b) shows the variation of system confidentiality capacity with transmission power under different SNRs. Regardless of the SNR, when the transmission power was 0.4W, the system's confidentiality capacity always reached its maximum value. The study analyzed the relationship between system confidentiality capacity and interfering nodes, as shown in Fig. 8.

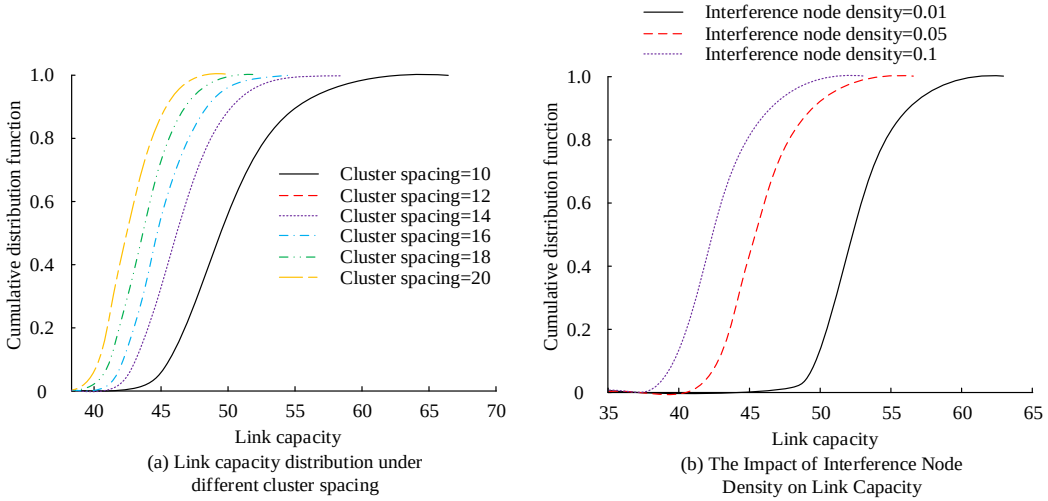


(a) The impact of artificial noise on confidentiality capacity

(b) The variation of confidentiality capacity with the distance between C and D

Fig. 8. Association between system confidentiality capacity and interference nodes.

Fig. 8 (a) shows the variation of system confidentiality capacity with SNR under different numbers of interfering nodes. When the number of interfering nodes was 1, the maximum confidentiality capacity of the system was about 4.7. After increasing the number of interfering nodes by one, the maximum confidentiality capacity of the system was about 5.8. Fig. 8 (b) shows the variation of system confidentiality capacity with the distance between C and D under different interfering nodes and F distances. When the distance between interfering nodes and F was fixed, the system's confidentiality capacity would increase with the increase of the distance between C and D. When the distance between nodes C and D was fixed, the system's confidentiality capacity would decrease as the distance between interfering nodes and F increased. Link capacity is a basic indicator for inter-cluster interference analysis. To assess the effectiveness of the proposed wireless communication eavesdropping interference scheme combining clustering scenarios and PLS, the variation of link capacity with cumulative distribution function was studied and analyzed under different cluster spacing and interference node density. The results are shown in Fig. 9.

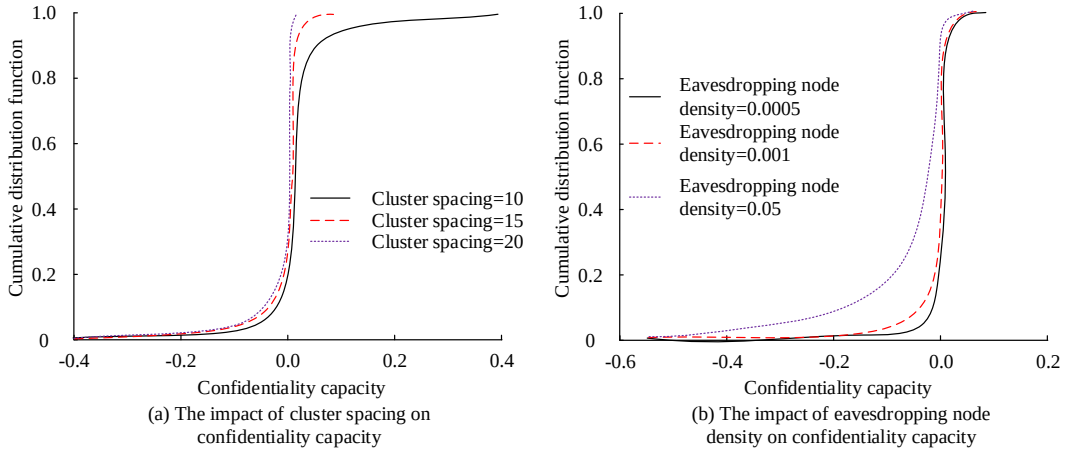


(a) Link capacity distribution under different cluster spacing

(b) The Impact of Interference Node Density on Link Capacity

Fig. 9. Effect of cluster spacing and interference node density on link capacity.

Fig. 9 (a) shows the distribution of link capacity under different cluster spacing. As can be seen, the cumulative distribution function value was 0.6, and when the cluster spacing was 10, the link capacity was about 50. When the cluster spacing was 20, the link capacity was about 30. As the cluster spacing increased, the overall link capacity decreased. As the distance between clusters increased, the loss of the signal during propagation also increased, resulting in a decrease in the energy received by the receiver, thereby reducing the overall communication performance. Fig. 9 (b) shows the distribution of link capacity under different interference node densities. As can be seen, when the cumulative distribution function value was 0.6 and the interference node density was 0.01Pieces/m2, the system link capacity was 54. When the interference node density was 0.1Pieces/m2, the system link capacity was 42. The link capacity would decrease as the density of interfering nodes increased, leading to a decrease in system communication performance. The study analyzed the variation of confidentiality capacity with the cumulative distribution function under different cluster spacing and eavesdropping node densities, as indicated in Fig. 10.



(a) The impact of cluster spacing on confidentiality capacity

(b) The impact of eavesdropping node density on confidentiality capacity

Fig. 10. Effect of cluster spacing and eavesdropping node density on confidentiality capacity.

Fig. 10 (a) shows the distribution of confidentiality capacity under different cluster spacing. As the distance between clusters increased, the signal from sender C to receiver D must be transmitted over a longer distance, which inevitably led to signal attenuation. Signal attenuation means a decrease in signal strength at receiver D, which requires a higher SNR to ensure the same communication quality. However, in actual wireless network environments, it is often difficult to compensate for signal attenuation caused by distance increase due to factors such as system transmission power and environmental noise. Fig. 10 (b) shows the distribution of confidentiality capacity under different eavesdropping node densities. As the density of eavesdropping nodes decreased, the confidentiality capacity of the system was also constantly increasing. The lower the density of eavesdropping nodes and the higher the confidentiality capacity, the better the communication performance of the system. Finally, the study also analyzed the impact of clustering radius, path loss index on the main channel, and confidentiality capacity, as denoted in Fig. 11.

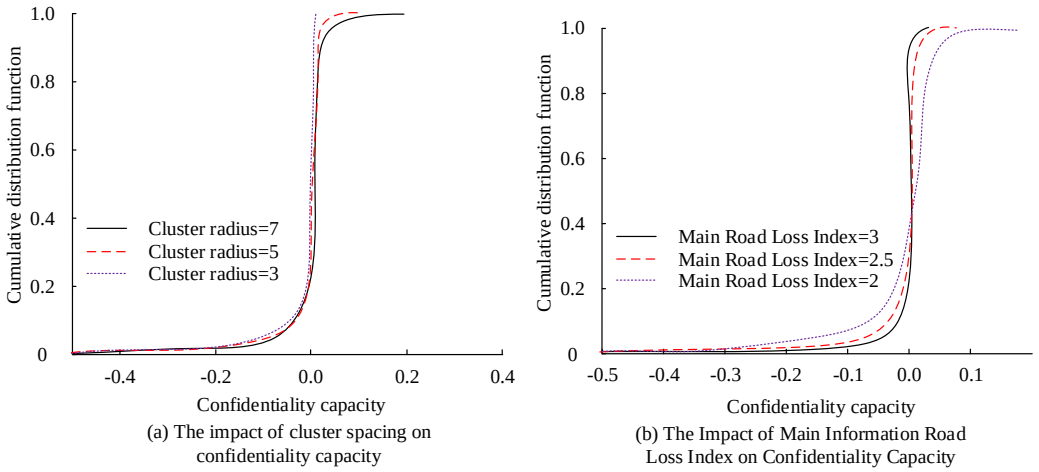


Fig. 11. Effect of branch cluster radius and main channel path loss index on secrecy capacity.

Fig. 11 (a) shows the distribution of confidentiality capacity under different clustering radii. The clustering radius had a relatively small impact on the system's confidentiality capacity. Fig. 11 (b) shows the distribution of confidentiality capacity under different main channel path loss indices. As the main channel path loss index decreased, the confidentiality capacity showed a slight increase trend. To further verify the influence of different parameter settings on confidentiality capacity, the study performed ANOVA on main channel SNR, transmission power and number of interfering nodes, and the results are shown in Table III.

TABLE III. ANALYSIS OF VARIANCE OF MAIN CHANNEL SNR, TRANSMISSION POWER AND INTERFERENCE NODES

Factor	Df1	Df2	F	P
Main channel SNR	3	30	25.6	<0.001
Transmission power	2	20	13.4	<0.001
Number of interfering nodes	4	35	8.9	<0.001

ANO analysis of variance showed that the main channel SNR (F (3,30) =25.6, P <0.001), transmission power (F (2,20) =13.4, P <0.001) and the number of interfering nodes (F (4,35) =8.9, P <0.001) significantly influenced the confidentiality capacity. To further study the eavesdropping interference effect of the design method, the results was compared with the node camouflage eavesdropping scenario, and the results are shown in Fig. 12.

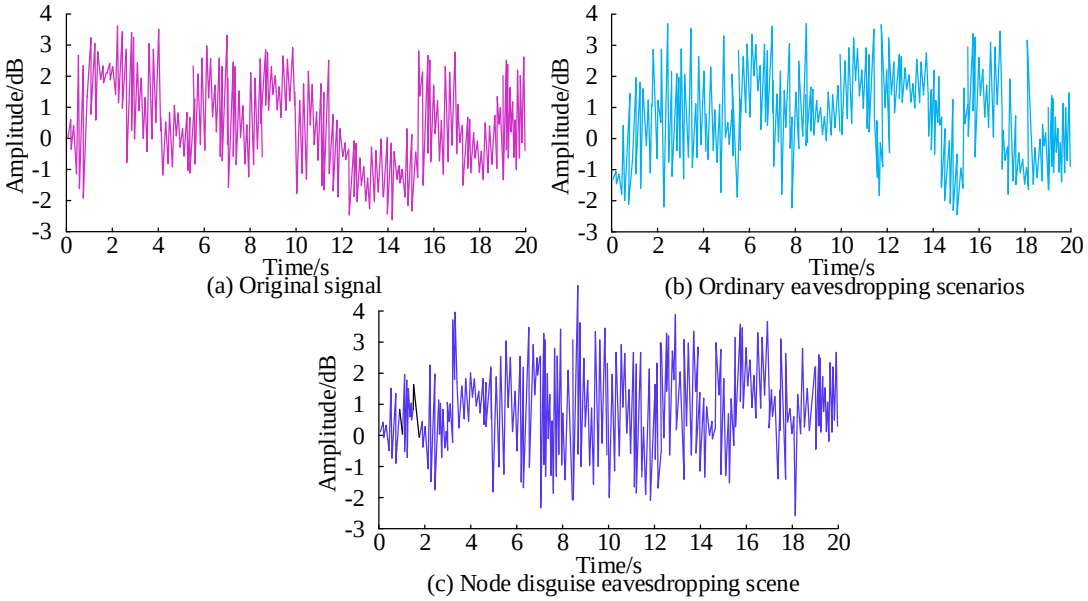


Fig. 12. The eavesdropping and interference effects in different scenarios.

Fig. 12 (a) shows the original signal at the transmitting end, Fig. 12 (b) shows the received signal of the eavesdropping channel in a normal eavesdropping scenario, and Fig. 12 (c) shows the received signal of the eavesdropping channel in a node disguised eavesdropping scenario. Regardless of the eavesdropping interference in any scenario, the designed eavesdropping interference scheme could always effectively conceal the true information of the transmitting signal. To further verify the practical application of the wireless communication network, the quality of the signal received by the receiver and the effective information in the eavesdropping information were compared. The results are shown in Fig. 13.

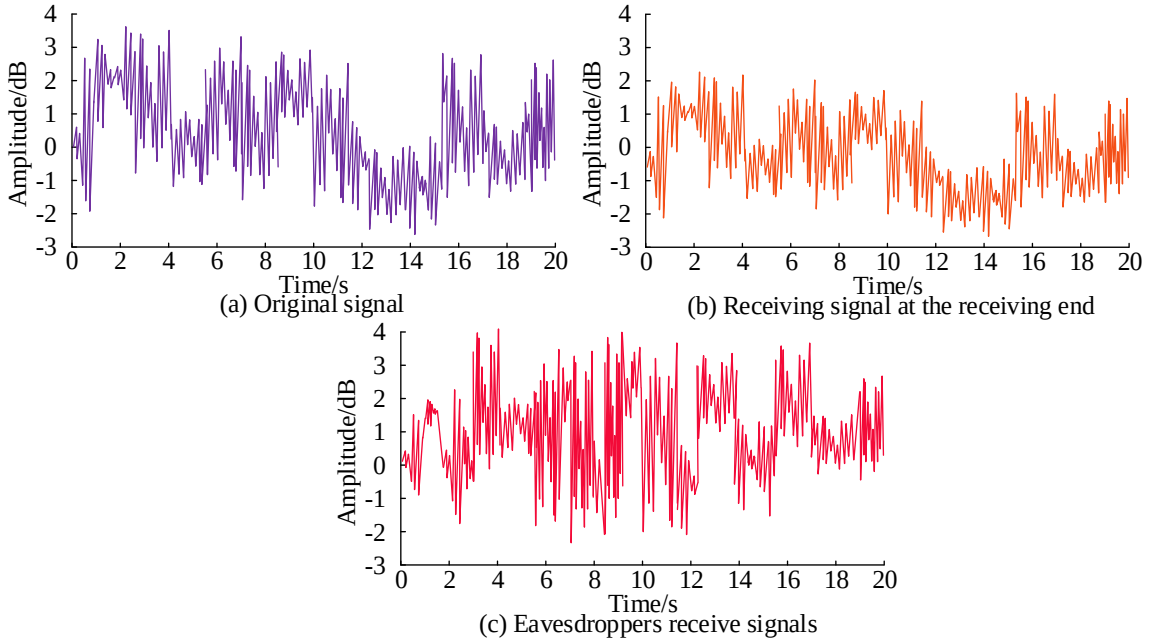


Fig. 13. The of interference under artificial noise.

Fig. 13 (a) is the original signal, Fig. 13 (b) is the receiving signal of the receiver, and Fig. 13 (c) is the receiving signal of the eavesdropping party. It can be seen that the waveform of the received signal at the receiving end was basically the same as the original signal waveform, but the signal amplitude was weakened, and the overall information was kept intact. The waveform of the signal received by the eavesdropper was quite different from the original signal, and only the individual bands overlapped somewhat, and the original signal information was basically not reserved. Under the interference of artificial noise, the receiving end could still receive the original signal well, and effectively avoid the risk of information leakage. When deploying the artificial noise, if the noise signal characteristics were similar to the emission signal characteristics, the eavesdropping interference effect would be poor. The artificial noise remained unchanged for a long time, which would also lead to the poor eavesdropping interference effect. Therefore, when deploying artificial noise, it is necessary to adjust the artificial noise signal at different time to improve the eavesdropping interference effect of artificial noise. To further verify the effectiveness of network eavesdropping and interference technology based on clustering scenarios and PLS, an experiment was designed to compare the anti-eavesdropping effect of this method with the artificial noise assisted secure wireless communication technology proposed in study [19]. The results are shown in Table IV.

In Table IV, when using the research-designed anti-eavesdropping method, the effective signal proportion in the signal received by the eavesdropper did not exceed 1%. However, when using the method proposed in study [19], the effective signal proportion in the signal received by the eavesdropper could reach up to 2.67%. Research on anti-eavesdropping technology can better protect privacy and security.

TABLE IV. COMPARISON OF THE ANTI-EAVESDROPPING EFFECT

Signal number	Proportion of effective information (%)	
	Proposed method	Reference [19]
1	0.56	1.35
2	0.48	2.67
3	0.95	1.94
4	0.67	2.54
5	0.89	2.13

V. DISCUSSION

A collaborative eavesdropping interference scheme based on PLS and clustering scenarios was proposed to improve the communication security of wireless communication networks. By adding artificial noise to the transmitted signal, eavesdropping signals could be successfully interfered with, enhancing the advantages of the main channel and achieving eavesdropping interference in wireless communication networks. The research results indicated that as the SNR of the main channel increased, the confidentiality capacity of the system significantly improved, increasing from 0.5 to over 4.0. In addition, as the number of interfering nodes increased, the

confidentiality capacity also increased, similar to the research results of Pang X et al. [21]. The proposed method not only provided new research directions and possible solutions for PLS, but also provided important reference value for clustering scenarios in wireless sensor networks. By fully utilizing the advantages of network topology without the need for additional equipment or hardware, PLS implementation was ensured, providing a new perspective and solution strategy for wireless communication network security issues. The different channel models and environmental noise considered in the experiment may not cover all the complex details in practical scenarios, and future research needs to be further deepened. For example, it is possible to explore universal interference strategies that can adapt to various channel conditions and noisy environments, and optimize the deployment methods of interfering nodes. In the future, further research and optimization will be conducted on the generation mechanism of artificial noise to adapt to the dynamically changing network environment. Secondly, it should explore interference strategies under different channel conditions to improve the adaptability and robustness of the system. Finally, considering the compatibility issues in actual deployment, it will investigate how to seamlessly integrate PLS technology with existing wireless communication networks.

VI. Conclusion

To improve the communication security of wireless sensor networks, a research proposal was proposed to combine PLS with cluster routing. A collaborative eavesdropping interference scheme combining PLS and cluster scenarios was designed to protect the communication security of wireless sensor networks. This scheme added artificial noise to the transmitted information to achieve eavesdropping interference. The results showed that in an environment without artificial noise, the confidentiality capacity ranged from 0 to 1. After using artificial noise, as the SNR of the main channel increased from 0 to 20dB, the confidentiality capacity could increase from 0.5 to over 4.0. When the cumulative distribution function value was 0.6, the cluster spacing increased from 10 to 20, and the link capacity decreased from 50 to 30. The density of interfering nodes was increased from 0.01Pieces/m² to 0.1Pieces/m². At that time, the link capacity decreased from 54 to 42. When the path loss index decreased, the confidentiality capacity slightly increased, while the clustering radius had little effect on the confidentiality capacity. The addition of artificial noise effectively improved the confidentiality capacity of the system, which was highly sensitive to the SNR of the main channel and achieved the optimal confidentiality capacity at a certain transmission power level. The increase in the number of interfering nodes could significantly affect the confidentiality capacity of the system, but this effect tended to saturate after the number of nodes reached a certain threshold. In terms of spatial distribution, an increase in cluster spacing and interference node density could lead to a decrease in link capacity, thereby affecting communication performance. When conducting simulation analysis on eavesdropping interference schemes, the consideration of different channel models and environmental noise was insufficient to cover all the complex details in actual scenarios, and further deepening is needed. In the future, it can explore universal interference strategies that can adapt to various channel conditions and noisy environments, and optimize the deployment methods of interference nodes. The use of PLS and cluster routing to achieve eavesdropping interference in communication signals greatly protects user personal privacy and improves wireless network communication security, which can effectively promote the development of the Internet of Things.

Acknowledgment

The research is supported by Education Science 14th Five-Year Plan Project of Fujian Province, Research on the construction of training system of digital literacy education for college students (No. Fjxczx23-302).

References

[1] Huang C, Hu S, Alexandropoulos G C, Zappone A, Yuen C, Zhang R, Debbah M. Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends. IEEE Wireless Communications, 2020, 27(5): 118-125.

[2] Arfaoui M A, Soltani M D, Tavakkolnia I, Ghrayeb A, Safari M, Assi C M, Haas H. Physical layer security for visible light communication systems: A survey. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1887-1908.

[3] Pirayesh H, Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2022, 24(2): 767-809.

[4] Fang S, Chen G, Li Y. Joint optimization for secure intelligent reflecting surface assisted UAV networks. IEEE Wireless Communications Letters, 2020, 10(2): 276-280.

[5] Wang C X, Di Renzo M, Stanczak S, Wang S, Larsson E G. Artificial intelligence enabled wireless networking for 5G and beyond: Recent advances and future challenges. IEEE Wireless Communications, 2020, 27(1): 16-23.

[6] Du J, Jiang C, Wang J, Ren Y, Debbah M. Machine learning for 6G wireless networks: Carrying forward enhanced bandwidth, massive access, and ultrareliable/low-latency service. IEEE Vehicular Technology Magazine, 2020, 15(4): 122-134.

[7] Wei Z, Liu F, Masouros C, Su N, Petropulu A P. Toward multi-functional 6G wireless networks: Integrating sensing, communication, and security. IEEE Communications Magazine, 2022, 60(4): 65-71.

[8] Wang C, Wang D, Tu Y, Xu G, Wang H. Understanding node capture attacks in user authentication schemes for wireless sensor networks. IEEE Transactions on Dependable and Secure Computing, 2020, 19(1): 507-523.

[9] Naghibi M, Barati H. SHSDA: secure hybrid structure data aggregation method in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(12): 10769-10788.

[10] Wu F, Li X, Xu L, Vijayakumar P, Kumar N. A novel three-factor authentication protocol for wireless sensor networks with IoT notion. IEEE Systems Journal, 2020, 15(1): 1120-1129.

[11] Jia X C. Resource-efficient and secure distributed state estimation over wireless sensor networks: A survey. International Journal of Systems Science, 2021, 52(16): 3368-3389.

[12] Hu S, Chen X, Ni W, Hossain E, Wang X. Distributed machine learning for wireless communication networks: Techniques, architectures, and applications. IEEE Communications Surveys & Tutorials, 2021, 23(3): 1458-1493.

[13] Li X, Zheng Y, Khan W U, Zeng M, Li D, Ragesh G K, Li L. Physical layer security of cognitive ambient backscatter communications for green Internet-of-Things. IEEE Transactions on Green Communications and Networking, 2021, 5(3): 1066-1076.

[14] Yuan X, Zhang Y J A, Shi Y, Yan W, Liu H. Reconfigurable-intelligent-surface empowered wireless communications: Challenges and opportunities. IEEE Wireless Communications, 2021, 28(2): 136-143.

[15] Pirayesh H, Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2022, 24(2): 767-809.

[16] Yu X, Xu D, Sun Y, Ng D W K, Schober R. Robust and secure wireless communications via intelligent reflecting surfaces. IEEE Journal on Selected Areas in Communications, 2020, 38(11): 2637-2652.

[17] Matthaiou M, Yurduseven O, Ngo H Q, Morales-Jimenez D, Cotton S L, Fusco V F. The road to 6G: Ten physical layer challenges for communications engineers. IEEE Communications Magazine, 2021, 59(1): 64-69.

[18] Polese M, Jornet J M, Melodia T, Zorzi M. Toward end-to-end, full-stack 6G terahertz networks. IEEE Communications Magazine, 2020, 58(11): 48-54.

[19] Hong S, Pan C, Ren H, Wang K, Nallanathan A. Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. IEEE Transactions on Communications, 2020, 68(12): 7851-7866.

[20] Bandewad G, Datta K P, Gawali B W, Pawar S N. Review on Discrimination of Hazardous Gases by Smart Sensing Technology. Artificial Intelligence and Applications, 2023, 1(2): 86-97.

[21] Pang X, Sheng M, Zhao N, Tang J, Niyato D, Wong K K. When UAV meets IRS: Expanding air-ground networks via passive reflection. IEEE Wireless Communications, 2021, 28(5): 164-170.