Chinese Journal of Electronics
vol. 33, no. 3, pp. 833–846, May 2024
https://doi.org/10.23919/cje.2022.00.448

RESEARCH ARTICLE

A Secure Communicating While Jamming Approach for End-to-End Multi-Hop Wireless Communication Network

Xiao MA[1], Dan LI[1,2], Liang WANG[3], Weijia HAN[1], and Nan ZHAO[4]

1. *School of Physics and Information Technology, Shaanxi Normal University, Xi'an 710119, China*
2. *Beijing Aerospace Science and Industry Century Satellite Hi-tech Co., Ltd. Xi'an Branch, Xi'an 710111, China*
3. *School of Computer Science, Shaanxi Normal University, Xi'an 710119, China*
4. *School of Telecommunications Engineering, Xidian University, Xi'an 710071, China*

Corresponding author: Liang WANG, Email: wangliang@snnu.edu.cn

Manuscript Received December 26, 2022; Accepted February 14, 2023

Abstract — With the rapid development of wireless communications, cellular communication and distributed wireless network are fragile to eavesdropping due to distributed users and transparent communication. However, to adopt bigger transmit power at a given area to interfere potential eavesdroppers not only incurs huge energy waste but also may suppresses regular communication in this area. To this end, we focus on secure communication in multi-hop wireless communication network, and propose two communicating while jamming schemes for secure communication in presence of potential eavesdroppers for the narrow band and broad band point-to-point (P2P) systems respectively with the aid of artificial noise transmitted by a chosen cooperative interferer. Furthermore, to achieve the end-to-end (E2E) multi-hop secure communication, we devise the secure network topology discovering scheme via constructing a proper network topology with at least one proper node as the cooperative interferer in each hop, and then propose the secure transmission path planning scheme to find an E2E secure transmission route from source to destination, respectively. Experiments on the wireless open-access research platform demonstrate the feasibility of the proposed schemes. Besides, simulations results validate that the proposed schemes can achieve better performance compared with existing methods in both the P2P communication case and E2E multi-hop communication network scenario.

Keywords — Communication while jamming, Power division multiplexing, Orthogonal frequency division multiplexing, Multi-hop wireless communication network.

Citation — Xiao MA, Dan LI, Liang WANG, *et al.*, "A Secure Communicating While Jamming Approach for End-to-End Multi-Hop Wireless Communication Network," *Chinese Journal of Electronics*, vol. 33, no. 3, pp. 833–846, 2024. doi: 10.23919/cje.2022.00.448.

I. Introduction

With the rapid developing of wireless communication networks, various advanced communication standards and systems such as the fifth generation mobile communication technology (5G), the sixth generation mobile communication technology (6G) and non-terrestrial Internet of things (IoT) [1]–[3], are devised to satisfy all kinds of communication demands in people's daily life. At the same time, the electromagnetic interference inevitably occurs which may degrade the regular communication of legal users severely or can be eavesdropped to steal the traffic information of legal users illegally [4]. For example, the mobile phone jammers used in various examinations not only interfere with the potential illegal eavesdroppers, but also may damage people's legal communication around the given area. Thus, the effective electromagnetic interference control has become a key issue in people's daily life. In other words, how to ensure the secure communication while jamming the potential eavesdroppers has become a challenging problem in the civil wireless communication scenario.

To tackle this issue, existing approaches usually adopt the high transmit power, namely, barrage jamming schemes [5]–[7] to suppress the interference, which would degrade the communication performance of both eavesdroppers and legal users indiscriminately. Besides, the traditional effective electromagnetic interference control

Associate Editor: Prof. Liang ZHOU, Nanjing University of Posts and Telecommunications.

mainly focus on military scenario. In modern electronic warfare, the suppression jamming is mainly used to destroy or block the communication equipment of the enemy in a short time. These methods can not be applicable to the civil communication systems due to three main challenges. Firstly, users are usually scattered in urban area with high buildings, trees and other blocking things. Secondly, the communication standards of civil communication are usually various, such as the 5G, light fidelity (LiFi), and wireless fidelity (WiFi) [8]. Thirdly, the potential eavesdroppers and legal users may be highly overlapping in spatial distribution, staggered in complex urban environment, which is very challenging to balance quality of service (QoS) and security of legal users [9]. Thus, the pure suppression interference can not achieve the effective electromagnetic interference control in civil multi-hop wireless communication systems.

Fortunately, the artificial noise (AN) can be transmitted with the traffic information of legal users together to ensure secure communication while jamming the illegal eavesdroppers in [10]. Thereafter, many works adopted the AN to tackle the eavesdropping attack. The authors in [11] proposed a decode-and-forward relay-assisted secure transmission scheme using AN in multi-antenna relay wiretap channels, and derived the secure transmission outage probability with an arbitrary number of antennas at source, relay and destination. The authors in [12] presented a novel cooperative jamming scheme in multiple access wiretap channel with non-collusion and collusion of eavesdroppers, and analyzed the secure sum rate performance. The authors in [13] developed an effective proactive eavesdropping scheme for short packet suspicious communication to maximize the monitoring success probability under average transmit power constraint of the monitor. The authors in [14] designed a new zero-forcing beamforming scheme in presence of active and passive eavesdroppers to maximize the achievable secrecy rate, where a multi-antenna jammer is considered to produce AN to confuse eavesdroppers. The authors in [15] proposed a clustering scheme for topological interference management based on the low-rank matrix completion approach including nuclear norm minimization and Frobenius norm minimization. The authors in [16] exploited the game theory to propose an anti-jamming power allocation method for health monitoring IoT network, and minimized the worst-case jamming effect under multi-channel fading. The authors in [17] established efficient privacy in a multiple-input multiple-output (MIMO) industrial IoT communication scenario with eavesdropping, derived the asymptotic regularized prompt privacy rate, and optimized the jamming parameters to tackle eavesdropping attack. The authors in [18] combined physical layer network coding and massive MIMO to tackle the barraging attack from a jammer equipped with any number of antennas, and demonstrated that the proposed scheme can improve the bite error rate and spectral efficiency. The authors in [19] exploited unmanned aerial vehicle (UAV) to send friendly jamming signal and protect against a full-duplex active eavesdropper for secure communication, and proposed an efficient algorithm to minimize the outage probability and intercept probability of legitimate users. The authors in [20] developed a two-stage Stackelberg game framework to stimulate the artificial jamming among selfish jammers, and proposed a novel incentive jamming-based secure routing scheme. The authors in [21] adopted a swarm of hovering UAVs to relay information, harvest wireless energy, and jam the eavesdropper, and proposed a collaborative time-switching relaying protocol for UAVs. Besides, they further derived the secrecy outage probability when the eavesdropper utilizes either the selection combining and maximum-ration combining scheme.

However, these existing artificial noise based schemes mostly considered the point-to-point (P2P) communication scenario. They usually focused on the outage probability and secure transmission capacity analysis, which cannot be applicable to the civil multi-hop wireless communication network scenario directly to ensure the regular end-to-end (E2E) communication between legal users while avoiding the eavesdropping. Besides, different communication modes for the communicating nodes, such as narrow band communication and broad band communication systems, are usually neglected. The detailed comparison of theses existing secure communication methods and our scheme is illustrated in Table 1.

Thus, in this paper, we propose a communicating while jamming scheme in E2E multi-hop wireless communication networks consisting of P2P communicating while jamming method and the E2E communication while jamming method respectively. To be specific, for P2P communicating while jamming method, we consider the narrow band communication system and broad band communication system respectively, which has been presented in our previous work [22]. Besides, we implement these schemes on the wireless open access research platform (WARP) and perform extensive simulations to evaluate the performance.

The contributions of this paper can be summarized as follows:

- For the narrow band P2P communication scenario, inspired by the idea of power division multiplexing (PDM), we design a jamming insertion for narrow band waveform (JI4Narrow) scheme where a chosen node acting as the cooperative interferer aids the legal transmitter to ensure secure communication while jamming the potential eavesdroppers.
- As for the broad band P2P communication case such as the orthogonal frequency division multiplexing (OFDM) system, we propose a jamming insertion for broadband waveform (JI4Broad) scheme based on the idea of OFDM time frequency resource blocks (RB) random mapping strategy to achieve communicating while jamming.
- Based on two P2P communicating while jamming

Table 1 Comparison of existing secure communication schemes

Work	Narrow band system	Broad band system	E2E multi-hop transmission	Commun. while jamming*	Hardware platform evaluation
Negi *et al.* [10]	√	×	×	×	×
Liu *et al.* [11]	√	×	×	×	×
He *et al.* [12]	√	×	×	√	×
Xu *et al.* [13]	√	×	×	×	×
Si *et al.* [14]	√	×	×	×	×
Jiang *et al.* [15]	√	×	√	×	×
Gouissem *et al.* [16]	×	√	×	×	×
Anajemba *et al.* [17]	√	×	×	√	×
Okyere *et al.* [18]	√	×	×	×	×
Zhou *et al.* [19]	×	√	×	√	×
Xu *et al.* [20]	√	×	√	×	×
Dang-Ngoc *et al.* [21]	√	×	×	×	×
Our scheme	√	√	√	√	√

Note: * "Commun. while jamming" stands for "Communicating while jamming", referring to the scenario where the transmitter can always send traffic information to its intended legal receiver securely while the jamming signal is transmitted at the same time even if the eavesdroppers are near or co-located with the legal receiver. Note that the beamforming based schemes may be not applicable here.

schemes mentioned above, we further prune the network topology to ensure there exists a legal node to send the jamming signal at each hop, and devise the secure network topology discovering method and secure transmission path planning method respectively to ensure the E2E multi-hop communication while jamming in the considered network scenario.

- Experiments on the wireless open-access research platform and simulation results demonstrate that the proposed JI4Narrow and JI4Broad schemes can achieve better performance compared with existing schemes in P2P communication situation. Besides, the E2E communicating while jamming scheme can obtain higher packet successful delivery ratio compared with traditional shortest path scheme in multi-hop wireless network scenario.

The remainder of this paper is organized as follows. The system model is described in Section II. The JI4Broad and JI4Narrow schemes for P2P communication scenario are proposed in Section III and IV, respectively. Then, we propose the communicating while jamming scheme in E2E multi-hop wireless communication network in Section V, and evaluate the performance of the proposed schemes in Section VI. Finally, Section VII concludes this paper.

II. System Model

In this section, we first describe the multi-hop ad hoc wireless communication network scenario, and then provide the problem formulation for the secure communication while jamming in the scenario of interest.

1. Network scenario

We consider a multi-hop ad hoc wireless communication network with M communication nodes consisting of multiple legal users and potential eavesdroppers as shown in Figure 1. All these communication nodes are equipped with single antenna. Here, let $\mathcal{U}=\{U_1,U_2,\ldots,U_i,\ldots,U_N\}$ denote the set of legal users, where N refers to the total number of legal users. $\mathcal{E}=\{E_1,E_2,\ldots,E_k,\ldots,E_K\}$ refers to the set of eavesdroppers, where K means the number of eavesdroppers. Then, we have $M=N+K$. The legal users communicate with each other while the eavesdroppers try to decode the regular traffic information sent by the legal users. The source legal user s sends data traffic to its corresponding legal destination d via multi-hop transmission. Here, for one hop transmission, that is, P2P communication, the legal transmitter may adopt the narrow band waveform or the broad band waveform such as OFDM to send traffic information to its intending legal receiver. The data traffic transmission may be eavesdropped at every transmission hop in the whole multi-hop transmission path due to the potentially eavesdroppers. In order to ensure secure communication between s and d in presence of eavesdroppers, some legal users are chosen to transmit AN cooperatively with the legal transmitter together aiming at jamming the potential eavesdroppers, which is known as the cooperative interferer as shown in Figure 1.

Let d_k^e and d_i^c denote the communication ranges of the k-th eavesdropper and the i-th legal user, respectively. Besides, $d_{k,j}$ refers to the distance between communication nodes k and j. To calculate the distance between two nodes, these communication nodes can acquire its own localization with the aid of existing global navigation satellite systems (GNSSs), e.g., BeiDou navigation satellite system (BDS) and global positioning system (GPS), or utilize the methods in [23] once the GNSS is limited by the complexity of these nodes or intentionally disabled. Besides, these nodes can also estimate the dis-

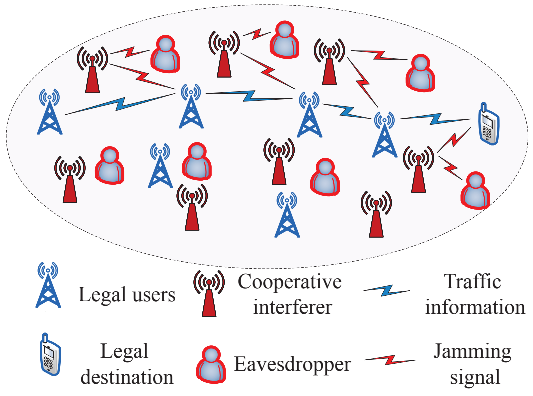


Figure 1 Communicating while jamming network scenario.

tance directly, such as using the method in [24]. Meanwhile, existing work for multi-hop wireless communication networks usually leverages the distance information to improve the network performance, such as [25]. Let c_{ij} denote the weight between the communication node i and j. Here, we have $c_{i,j}=1$ if $d_{i,j}\le d_i^c, \forall i\in\mathcal{U}\cup d_{i,j}\le d_i^e$, $\forall i\in\mathcal{E}$; otherwise, $c_{i,j}=\infty$. Then, we can express the network topology matrix as $C=(c_{i,j})_{M\times M}$.

2. Problem formulation

How to ensure the secure transmission for legal users in presence of eavesdropping, where the pure suppressing interference is not applicable due to the severe interference to the legal users. Thus, we need design an efficient approach to achieve the secure communication between legal users while jamming the potential eavesdropper which is termed as communication while jamming in this paper. In order to ensure the secure transmission from s to d in the multi-hop wireless communication network, we propose a secure communication and jamming scheme in an E2E manner. Then, we formulate this problem as below:

$$\begin{aligned} P0:\ &\underset{\{n_i,n_j,p_i\}}{\text{find}}\quad r_s=\{s,\dots,n_i,\dots,n_j,\dots,d\}\\ \text{s.t. } &C1: R_{s,d}^s\ge R_{\min}^c,\\ &C2: R_{n_i,n_i^e}^e\le R_{\max}^e,\ \forall n_i^e\in\mathcal{E},\\ &C3: \forall n_i,n_j\in\mathcal{U},\\ &C4: c_{n_i,n_{i+1}}=1,\\ &C5: p_i\le P_{\max} \end{aligned}\tag{1}$$

where $r_s=\{s,\dots,n_i,\dots,n_j,\dots,d\}$ denote the secure transmission path $s\rightarrow\cdots\rightarrow n_i\rightarrow\cdots\rightarrow n_j\rightarrow\cdots\rightarrow d$ from s to d. Here, $n_i\in\mathcal{U}$ denote the i-th communication node on this path. $R_{s,d}^s$ denote the secure transmission rate from s to d in an E2E manner, and $R_{\min}^c$ is the minimal date rate requirement for the legal users to communicate from source to its destination in the multi-hop wireless communication network. Similarly, $R_{n_i,n_i^e}^e$ is the data rate obtained by the eavesdroppers within the communication range of the i-th legal transmitter n_i, and $R_{\max}^e$ is maximal allowed data rate perceived by the eavesdroppers at the i-th hop transmission for secure transmission. In $P0$, constraint $C1$ ensure the efficient communication between source and its destination in an E2E manner, while constraint $C2$ limits the data rate received by the eavesdroppers to prevent eavesdropping. Constraint $C3$ requires all the intermediate communication nodes are legal users. Constraint $C4$ requires that two neighboring legal communication node are within each other's communication range. Constraint $C5$ is the maximal transmit power requirement for n_i. Thus, we can see that $P0$ is a non-convex mixed integer optimization problem, which is very challenging to solve.

To tackle $P0$ mentioned above efficiently, we firstly need locate the eavesdroppers on multi-hop ad hoc wireless communication network. Our previous work [26] has exploited the wide cover range of UAV and handled this issue by the deep reinforcement learning method. Provided that the locations of eavesdroppers are known in this work, we further decompose $P0$ into two sub-problems, namely the one-hop P2P secure communication problem $P1$ and E2E multi-hop secure transmission problem $P2$.

Then, for each hop secure transmission in $P1$, the transmitter of legal user sends traffic information to its next hop receiver with the aid of a cooperative interferer. Here, the cooperative interferer will transmit specific designed interference known as AN to interfere with the potential eavesdropper while ensuring the secure receiving at the next hop receiver, which can be expressed as

$$\begin{aligned} P1:\ &\max_{\{p_i,p_i^c,w_i,w_i^c\}}\ R_{n_i,n_i^r}^s\\ \text{s.t. } &C1: p_i\le P_{\max},\\ &C2: p_i^c\le P_{\max}^c,\\ &C3: w_i+w_i^c=W,\\ &C4: R_{n_i,n_i^e}^e\le R_{\max}^e,\ \forall n_i^e\in\mathcal{E}\cap c_{n_i,n_i^e}=1 \end{aligned}\tag{2}$$

where n_i^r denote the legal receiver of the i-th legal transmitter n_i, which can also be expressed as n_{i+1}. n_i^e refers to the eavesdroppers which are with the communication range of i-th legal transmitter n_i. p_i and p_i^c refer to the transmit power of the i-th legal transmitter n_i and its corresponding cooperative interferer n_i^c, respectively. w_i and w_i^c denote the channel bandwidth of n_i and n_i^c respectively. Besides, $R_{n_i,n_i^r}^s$ denotes the efficient communication data rate between the legal transmitter and legal receiver. Constraints $C1$ and $C2$ mean the maximal transmit power limit for the legal transmitter and cooperative interferer respectively. Constraint $C3$ refers to the maximal channel bandwidth occupied by the legal transmitter and cooperative interferer.

In $P1$, we further consider two kinds of P2P communication modes: namely P2P narrow band communication system and P2P broadband communication system. We need to design the proper transmission strategy of traffic information of legal transmitter and the effective jamming interference for the cooperative interferer in both narrow band waveform and broadband waveform P2P communication situations respectively. Here, the narrow waveform refers to the narrow band transmission system where the channel fading is frequency-flat. Meanwhile, the broadband waveform denotes the wide band transmission system where the channel fading is frequency-selective, such as OFDM technique. To ensure P2P secure communication, we adopt the artificial noise technique to interfere the potential eavesdroppers, and propose the jamming insertion for narrowband waveform (JI4Narrow) scheme in Section III and the jamming insertion for broadband waveform (JI4Broad) scheme in Section IV for both kinds of P2P wireless communication systems, respectively. For better understanding, we show the research idea diagram of this paper in Figure 2.

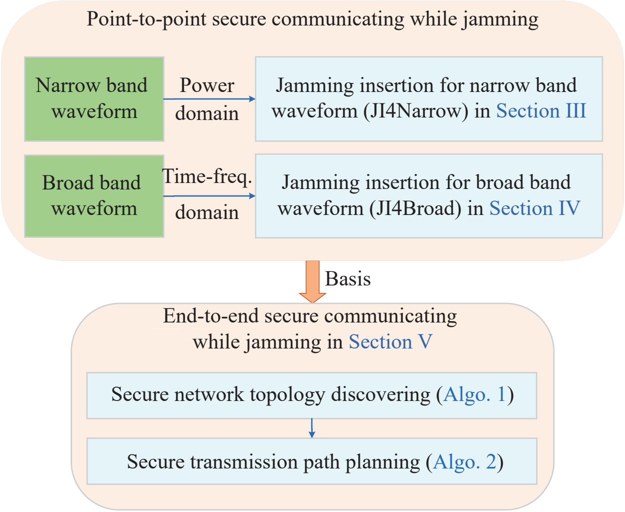

Point-to-point secure communicating while jamming
Narrow band waveform
Power domain
Jamming insertion for narrow band waveform (JI4Narrow) in Section III
Broad band waveform
Time-freq. domain
Jamming insertion for broad band waveform (JI4Broad) in Section IV
Basis
End-to-end secure communicating while jamming in Section V
Secure network topology discovering (Algo. 1)
Secure transmission path planning (Algo. 2)

Figure 2 Research idea diagram of this paper.

Based on $P1$, we further find a secure transmission path from s to d, known as the E2E multi-hop secure transmission problem $P2$. We formulate this problem as follows:

$$\begin{aligned} P2: & \underset{\{n_i,n_j,n_i^c,n_j^c\}}{\text{find}} \; r_s^c = \{(s,s^c)\ldots,(n_i,n_i^c),\ldots, \\ & \qquad\qquad (n_j,n_j^c),\ldots,d\} \\ \text{s.t. } & C1: \forall n_i,n_j,n_i^c,n_j^c \in \mathcal{U}, \\ & C2: c_{n_i,n_{i+1}} = 1 \end{aligned} \tag{3}$$

where n_i^c is the cooperative interferer of the i-th legal transmitter n_i. This n_i^c should satisfy the following requirements:

$$\begin{aligned} & n_i^c = \text{find}\,\{l\} \\ \text{s.t. } & C1: l \notin r_s, \\ & C2: l, n_i \in N_e(k), \\ & C3: l = \arg \min_{\{l\in\mathcal{U}\}} \{e_{k,l}\} \end{aligned} \tag{4}$$

where $N_e(k)$ denotes the set of k-th eavesdropper's neighbors, and is expressed as $N_e(k)=\{j, c_{k,j}=1 \cap k \in \mathcal{E}\}$. Besides, $e_{k,l}$ refers to the weight on the edge from the k-th eavesdropper to the l-th legal user, which is proportional to $d_{k,l}$. That is, in formula (4), we find the l with minimal distance to the k-th eavesdropper. In $P2$, constraint $C1$ ensures that all the intermediate nodes including the transmitter and cooperative interferer all belongs to legal users. Constraint $C2$ require that node n_i is within the communication coverage of n_{i+1}. To handle $P2$, we propose a two-stage E2E communication while jamming method in multi-hop wireless communication, which consists of secure network topology discovering stage and secure transmission path planning stage in Section V as shown in Figure 2.

III. JI4Narrow Scheme for P2P Narrow-Band Communication Systems

In this section, we propose a jamming insertion for narrow band waveform (JI4Narrow) scheme inspired by the idea of PDM belonging to one of non-orthogonal multiple access (NOMA) technology [27].

In the PDM scheme, multiple signals with different level of transmit power can be superimposed over the air to exploit the differentiated channel gain between the transmitter and multiple receivers. At the receiver side, each signal of interest can decode sequentially via the successive interference cancellation (SIC) principle. As shown in Figure 3, the jamming insertion based on PDM consists one legal transmitter, legal receiver, cooperative interferer and eavesdropper. In this scenario, the legal transmitter sends traffic information to the legal receiver. Meanwhile, the eavesdropper tries to eavesdrop to obtain the traffic information. The cooperative interferer transmits the jamming signal aligned with the legal transmitter to interfere with the eavesdropper. Here, the legal transmitter and receiver, cooperative interferer and eavesdropper occupies the same channel. Thus, we can transform $P1$ into $P1^n$ as below:

$$\begin{aligned} P1^n: & \max_{\{p_i,p_i^c,w_i,w_i^c\in\mathcal{U}\}} R_{n_i,n_i^r}^s \\ \text{s.t. } & C1: p_i \le P_{\max}, \\ & C2: p_i^c \le P_{\max}^c, \\ & C3: R_{n_i,n_i^e}^e \le R_{\max}^e,\ \forall n_i^e \in \mathcal{E} \cap c_{n_i,n_i^e} = 1 \end{aligned} \tag{5}$$

Here, we have $w_i = w_i^c = W$ for narrow band waveform. Thus, we exploit the PDM technology and try to decide the transmit power and modulation constellations of the legal transmitter and cooperative interferer, respectively.

In particular, we treat the AN signal sent by the cooperative interferer as the base layer greater transmit power signal while taking the traffic information transmitted by the legal transmitter as the upper layer smaller transmit power signal. To illustrate this method clearly, as shown in Figure 3, two modulated quadrature phase shift keying (QPSK) signal superpose over the air

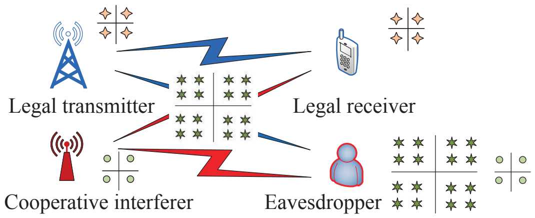


Figure 3 Illustration of JI4Narrow scheme.

to form the modulated 16 quadrature amplitude modulation (16QAM) signal.

Here note that the over-air superposed modulated 16QAM signal, known as is different from the traditional modulated 16QAM signal. The 16QAM signal is composed of two independent orthogonal 4 amplitude shift keying (4ASK) signal, where only one way signal can carry effective data information, since the signal constellation points' distance and their corresponding transmit power relationship are fixed. In contrast, in the PDM signal, the transmit power relationship between signal constellation points depends on the specific transmit power layer of each channel signal, which is changeable. Besides, each channel signal in the PDM are superimposed in a non-orthogonal approach, which can carry multiple data information and be varied dynamically based on the specific demand.

As shown in Figure 3, taking each channel QPSK modulated signal as an example, the low-power signal constellation is composed of 4 independent constellation points, where the transmit power from each constellation point to the origin is denoted as p_2. Meanwhile, the high-power signal constellation is also consisted of 4 independent constellation points, where the transmit power from each constellation point to the origin is denoted as p_1. Here, we have $p_1 > p_2 \geq 0$. In the PDM mechanism, the above low-power and high-power signals are superimposed over the air, where the superimposed constellation diagram is displayed on the right side of Figure 3. The superimposed transmitted signal can be shown as

$$x = x_1\sqrt{p_1} + x_2\sqrt{p_2} \tag{6}$$

where x_1 and x_2 refer to the transmit signal of the cooperative interferer and the legal transmitter respectively.

Then, the received signal at the legal receiver can be expressed as

$$y_1 = h_{1,c}x_1\sqrt{p_1} + h_{1,t}x_2\sqrt{p_2} + n_1 \tag{7}$$

where $h_{1,c}$ and $h_{1,t}$ denote the channel gain from the cooperative interferer to the legal receiver and that from the legal transmitter to the legal receiver, respectively. Besides, n_1 refers to the white Gaussian noise at the legal receiver. Similarly, the received signal at the eavesdropper can be expressed as

$$y_2 = h_{2,c}x_1\sqrt{p_1} + h_{2,t}x_2\sqrt{p_2} + n_2 \tag{8}$$

where $h_{2,c}$ and $h_{2,t}$ denote the channel gain from the cooperative interferer to the eavesdropper and that from the legal transmitter to the eavesdropper, respectively. Besides, n_2 refers to the white Gaussian noise at the eavesdropper. Here, the 4 grey circles are the positions of the original high-power signal constellation points, and orange low-power signals are superimposed on the each high-power signals to form a new 16 green star constellation diagram. The actual received signal at the receiver side is the 16 green star constellation points. As for the specific transmit power allocation for p_1 and p_2, our previous works have investigated this problem from a green communication perspective in [28], the MIMO case in [29], and under the bit error rate (BER) constraint in [30], respectively. Besides, the outage probability and ergodic sum rate of cognitive radio non-orthogonal multiple access assisted intelligent transportation system network was studied under imperfect SIC and channel estimation errors in [31].

Once the receiving the superimposed signal, the legal receiver can demodulate the underlayer high-power interference signal, and then demodulate the lower-power signal to obtain the traffic information according to the SIC principle. To be specific, the legal receiver first sorts the received signal in a descending order, decode the received signal with the strongest received power while treating other received signal as noise. Then, the receiver subtract this signal from the whole received signal, and decode the signal with second strongest receiver power while treating the remaining received signal as noise, and so on, until decode all the received signal. In this scenario of interest, we decode the x_1 first, and subtract this received signal from the received signal y_1, which is shown as below:

$$y_1^1 = y_1 - \hat{h}_{1,c}\hat{x}_1\sqrt{p_1} \tag{9}$$

where $\hat{h}_{1,c}$ is the estimation of $h_{1,c}$. Then, we decode x_2 from (9) as $\hat{x_2}$.

Here, note that the SIC algorithm can be applied to various wireless communication systems, such as single antenna system, multi-antenna system, OFDM system, NOMA system, and so on. The illustrative analysis of the detailed SIC algorithm in single antenna and multi-antenna OFDM systems are discussed in [32]. As for the practical implementation of SIC algorithm, the authors in [33] presented a pioneering NOMA testbed based on universal software radio peripheral (USRP) B210 for Wi-Fi networks with the SIC ability. Meanwhile, in this paper, we have also implemented the SIC algorithm in the WARP platform.

As for the eavesdropper, it usually adopts the blind signal detection technique to demodulate the received superimposed signal y_2 in (8), which may identify this signal either as the superimposed 16 QAM signal or only the underlayer high-power QPSK interference signal, since the eavesdropper is unaware of the cooperative transmission between the legal transmitter and its corresponding cooperative interferer and also unknown of the channel gains $h_{2,t}$ and $h_{2,c}$ in (8). In both cases, the eavesdropper cannot demodulate the traffic information. In this sense, we can see that the proposed JI4Narrow scheme can ensure the secure transmission of traffic information even in the presence of the eavesdropper with the aid of cooperative interferer. Furthermore, in the JI4N arrow scheme, the legal user's traffic information is transmitted via the non-orthogonal way, which exhibits a higher spectrum efficiency compared with the traditional orthogonal transmission in spite of the complex receiver at the legal receiver side.

IV. JI4Broad Scheme for P2P Broadband Communication Systems

In this section, we first discuss some key design in the broadband system such as OFDM, and then propose the JI4Broad scheme for broadband waveform.

1. Key design in broadband OFDM system

We consider that the legal users adopt the OFDM technique for broadband communication. The principle of OFDM is to divide the data transmission channel into multiple mutually orthogonal sub-channel, transform the high-speed data stream into multiple parallel low-speed data stream, and modulate these low-speed data stream on the carrier of each orthogonal sub-channel for transmission, which can be efficiently implemented via the fast Fourier transform (FFT) technique. At the receiver side, these mutually orthogonal received signals are separated via the inverse fast Fourier transform (IFFT) technique.

To decode the OFDM signal correctly, the frequency/time synchronization and channel estimation is essential. To this end, some known signal are inserted into the OFDM symbols termed as the OFDM preamble. To enable the cooperation between legal transmitter and cooperative interferer, we design the OFDM preambles for the legal transmitter and cooperative interferer respectively, which is shown as below.

As shown in Figure 4, the OFDM preambles of the legal transmitter and cooperative interferer consist of the short training symbols (STS), long training symbols (LTS) and zero symbols. Here, the STS contains 30 repeated short training symbols with the period of 16, thus, the length of each STS is 480. The LTS for the legal transmitter such as LTS_T1, LTS_T2, and those for the cooperative interferer, namely, LTS_J1, LTS_J2 include 2.5 repeated long training sequence with the period of 64, which last for 160. The length of zero training sequence is equal to that of the LTS. Besides, the preamble length of traffic information and interference signal is 1120.

Here, note that the STS for traffic information and that for jamming signal are the same. The first LTS for the traffic information and zero sequence are cross-staggered with the first LTS and zero sequence for jamming signal, which can facilitate the demodulation of the superimposed signal including the traffic information and jamming signal over the air. Meanwhile, the LTS_T2 and LTS_J2 are used to estimate the channel. In this paper, we adopt the least square method to estimate the channel gain from the legal transmitter to the legal receiver and from the cooperative interferer to the legal receiver.

Furthermore, the comb pilot is used as the OFDM pilot. The pilot design of traffic information and jamming signal follows the orthogonality of the code word. The pilot for traffic information is set as $\{1\ \ 1\ \ -1\ \ -1\}$ while that for jamming signal is chosen as $\{1\ \ 0\ \ 0\ \ -1\}$. Here, note that the specific number mentioned here is just for illustration. In fact, any reasonable setting can be applied to the proposed scheme.

2. JI4Broad scheme for broadband waveform

We utilize these key design of OFDM system mentioned above, and propose a jamming insertion for broadband waveform (JI4Broad) method to enable efficient communication for legal users while jamming the eavesdroppers. In this case, we can transform $P1$ into $P1^b$ shown as below:

$$
\begin{aligned}
P1^b: & \max_{\{w_i, w_i^c \in \mathcal{U}\}} R^s_{n_i,n_i^r} \\
\text{s.t. } & C1: w_i + w_i^c = W, \\
& C2: R^e_{n_i,n_i^e} \le R^e_{\max},\ \forall n_i^e \in \mathcal{E} \cap c_{n_i,n_i^e} = 1
\end{aligned} \tag{10}
$$

Here, the legal transmitter and cooperative interferer can transmit their respective signal on different channels or RBs. Thus, p_i and p_i^c can be set as their respective allowed maximal transmit power. We mainly focus how to allocate proper number of RBs for the legal transmitter and cooperative interferer, respectively.

Figure 5 shows the process of the JI4Broad scheme.

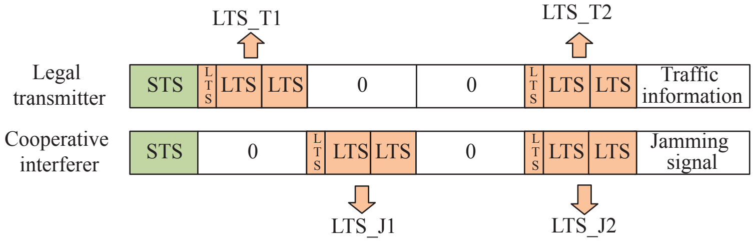


Figure 4 OFDM preamble design.

The legal transmitter sends traffic information via wireless communication to legal receiver, while there are some eavesdroppers aiming to eavesdropping this traffic information. Besides, cooperative interferer will send AN as the jamming signal collaboratively with the legal transmitter. The superposition of interfering signal and traffic signal will be transmitted over the air. Then, we describe the detailed procedure of the JI4Broad scheme, which consists of transmission and receiving stages.

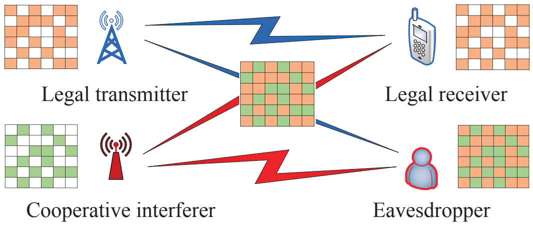


Figure 5 Illustration of JI4Broad scheme.

Transmission stage The legal transmitter will choose a given number of resource blocks (RBs) randomly from the OFDM time-frequency resource map to send the traffic information according to a prefixed random pattern map or the pseudo random sequence which is also known at the legal receiver in advance. Meanwhile, the cooperative jammer selects the remaining complementary RBs in the same OFDM time-frequency resource map to transmit the AN signal known as jamming information. Here, the traffic information randomly locate on the OFDM time-frequency resource map, where the specific information of the traffic corresponds to the chosen OFDM subcarrier and symbols. In this way, the traffic data and interference information will be transmitted together. The superposed signal will fulfill the whole OFDM time-frequency resource map. In other words, during this transmission stage, the traffic information sent by the legal transmitter and the jamming information are complementary on the same OFDM time-frequency resource map. The superposition of traffic and jamming information over the air will fulfill the whole OFDM time-frequency resource map over the time.

Receiving stage The legal receiver would choose the corresponding RBs from the OFDM time-frequency resource map based on the prefixed random pattern map or the pseudo random sequence chosen by the legal transmitter to recover the original traffic information. On contrary, the eavesdroppers receive the superposition signal of traffic and jamming information which occupies the whole broadband, since eavesdroppers are unaware of the random pattern map or the pseudo random sequence chosen by the legal transmitter. To the eavesdroppers, the received superimposed signal always fulfills the whole broadband and keeps unchanged with the time. Thus, there is no risk for eavesdroppers to decode the original traffic information sending from the legal transmitter.

Here, note that the JI4Broad scheme can be viewed as an extension of traditional frequency hopping technology. In the traditional frequency hopping technique, the transmitter usually sends information just on the chosen subchannel based on the frequency hopping map, which can be easily detected, tracked and even predicted by potential eavesdroppers. However, the JI4Broad scheme is quite different, since the received signal at eavesdroppers is the superposition of traffic information and the jamming signal which occupies the whole broadband and keeps unchanged with the time. Thus, the proposed JI4Broad scheme is more secure.

V. Communicating While Jamming Scheme in E2E Multi-Hop Wireless Communication Networks

According to the P2P communicating while jamming schemes mentioned in Section III and IV, we further investigate the communication while jamming schemes for E2E multi-hop wireless communication network. To this end, we propose a two-stage end-to-end communication while jamming method to handle $P2$, which consists of secure network topology discovering stage and secure transmission path planning stage.

1. Secure network topology discovering

The target of secure network topology discovering scheme is to eliminate the communication links with eavesdropper threats. The basic idea of secure network topology discovering scheme is to delete the link only containing one candidate relay node within the communication range of the eavesdropping node in the ad hoc network, because if the relay node is planned as a transmission node, the traffic information will be eavesdropped and decoded when it is transmitted to this relay node due to the lacking of additional node acting as the cooperative interferer. Therefore, deleting the insecure transmission links and obtaining the secure communication topology are the basis for the path planning in the communication while jamming scheme in end-to-end wireless communication networks.

Then, we propose the secure network topology discovering method in Algorithm 1.

Algorithm 1 Secure network topology discovering method

```
Input: the ad hoc network topology matrix $\boldsymbol{C}$ and the eavesdroppers' network topology matrix $\boldsymbol{E}$.
Output: the secure network topology matrix $\boldsymbol{C}_s=(c_{i,j})_{M\times M}$.
1: each node in the ad hoc networks sends Hello packet to its neighbors periodically, and obtain the network topology matrix $\boldsymbol{C}=(c_{i,j})_{M\times M}$;
2: the cluster node incorporates the eavesdroppers' network topology matrix $E$ into the above $C$ as the joint network topology $\boldsymbol{C_E}=[\boldsymbol{C}\ \ \boldsymbol{E}^{\mathrm{T}}]=[(c_{i,j})_{M\times M}\ \ (e_{j,i})_{M\times K}]$, and broadcast the network topology packet to all the other nodes;
3: each node can obtain the communication nodes topology matrix $E_N=(q_i)_{l\times K}$ within each eavesdropper's communicating range based on $\boldsymbol{C_E}$;
4: for each eavesdropping node $w_i$, delete the nodes with-
```

```
   out the cooperative interferer and their corresponding links, if the node $w_i$'s $q_i = 1$, then find the communication node $n_j$ with $e_{j,i} \le d_{j,e}$, set the weight between this node $n_i$ and its neighbors as $\infty$ in $\boldsymbol{C}$;
5: repeat Step 4 until all the eavesdropping nodes are searched, then set the secure network topology matrix $\boldsymbol{C}_s = \boldsymbol{C}$.
```

Here, the q_i in the matrix $\boldsymbol{E}_N = (q_i)_{l \times n}$ represents the number of communication nodes within the eavesdropping range of the eavesdropper w_i. The communicating node without the cooperative interferer means we cannot find a second communication node as the cooperative interferer within a given eavesdropper's communication range. Besides, the cluster node in Step 2 may be chosen via existing cluster-heads selection schemes where $\boldsymbol{C}_{\boldsymbol{E}}$ are broadcast to all the remaining nodes via multi-hop transmission or acted by the base station (BS) or UAV with a larger communication range where all the other nodes are in its coverage and get the information of $\boldsymbol{C}_{\boldsymbol{E}}$ via broadcasting.

2. Secure transmission path planning

In order to ensure secure traffic transmission in presence of eavesdroppers in an E2E multi-hop wireless communication network, we propose the secure transmission path planning method in Algorithm 2. The idea of this method is described as follows: firstly find a transmission path from the source s to the destination d based on the secure network topology mentioned above via the shortest path routing algorithm such as the well known Dijkstra algorithm; then, choose the corresponding cooperative interferers for those relay nodes potentially threat by the eavesdroppers where one legal transmitter sends traffic information together with its respectively cooperative interferer; finally, obtain a secure transmission path including the relay nodes and their respective cooperative interferers.

Algorithm 2 Secure transmission path planning method

```
Input: the secure network topology matrix $\boldsymbol{C}_s$, the source node $s$, the destination node $d$.
Output: the secure transmission path $r_s$.
1: transform $\boldsymbol{C}_s$ into weighted directed graph $G_s$;
2: utilize the Dijstra algorithm on $G_s$ to find the shortest hop transmission path $r_s = \{s, \ldots, n_i, n_j, n_k, \ldots, d\}$ from the source node $n_s$ to the destination node $n_d$;
3: use the joint network topology $\boldsymbol{C}_{\boldsymbol{E}} = \left[\boldsymbol{C} \ \ \boldsymbol{E}^T\right]$ to obtain the communication nodes within the eavesdropping range of each eavesdropper, establish the set $E_t = \{w_1(e_{1i}, e_{1l}, \ldots), \ldots, w_i(e_{ip}, e_{ik}, \ldots), \ldots, w_n(e_{nj}, e_{nq}, \ldots)\}$ according to the weight between the eavesdropper and communication node in the ascending order;
4: for each transmission node $n_i$ in $r_s$, choose the node which is not in $r_s$ and has the minimum distance weight to the eavesdropper which the current node $n_i$ belongs to as the cooperative interferer $n_i^c$ for the node $n_i$, update $r_s = \{s, \ldots, (n_i, n_i^c), n_j, n_k, \ldots, d\}$;
5: repeat Step 4 until all the nodes in path $r_s$ are searched, then obtain the secure transmission path as $r_s = \left\{(s, s^c), \ldots, (n_i, n_i^c), \left(n_j, n_j^c\right), (n_k, n_k^c), \ldots, d\right\}$.
```

Here, $w_i(e_{ip}, e_{ik}, \ldots)$ in Step 3 represents the distance weight vectors of all the communication nodes within the eavesdropping range of the current eavesdropper w_i, where e_{ip} refers to the distance weight between the communication node n_k and the eavesdropper w_i. Besides, (n_i, n_i^c) denote the secure node pair, where n_i is the legal transmitter while n_i^c referring to the cooperative interferer. Once the traffic information is relayed to node n_i, the node n_i will activate the cooperative interferer n_i^c to transmit the artificial noise to ensure secure transmission in presence of the eavesdroppers.

According to the secure transmission path planning method, we can find a secure transmission path r_s from the source to the destination. Then, the nodes in ad hoc network transmit the traffic information based on the routing information in r_s. For each hop transmission, the secure transmission pair such as (n_i, n_i^c) will adopt the jamming insertion methods such as JI4Narrow and JI4Broad schemes proposed in the previous section. For the other regular nodes without the eavesdropping threat, these relay nodes just transmit the traffic information to the next-hop communication node.

In a word, we can use the proposed secure network topology discovering method in Algorithm 1 and the secure transmission path planning method in Algorithm 2 to achieve the E2E secure transmission in the multi-hop ad hoc network even in presence of multiple eavesdroppers. In other words, we can achieve the communication while jamming in the distributed multi-hop wireless communication network.

VI. Performance Evaluation

In this section, we do experiments and perform simulations to evaluate the performance of the proposed communicating while jamming scheme. Especially, we first present the related parameters settings, then demonstrate the performance assessment of the P2P communication and E2E multi-hop communication scenarios, respectively.

1. Parameters setting

The performance of the proposed communicating while jamming scheme is demonstrated via the simulations and experiments on the specific software and hardware platforms. To be specific, the experiment consists of WARP platform and Matlab R2018b. WARP is a software defined radio based on field programmable gate array (FPGA) which can implement multiple wireless communication protocols [34]. Besides, the spectrum analyzer, oscilloscope, power divider, etc. can be used to observe and analyze the transmitting and receiving signal waveform during the experiment.

The WARP experimenting platform consists of two WARPs, namely WARP1 and WARP2. Here, WARP1 is used to transmit signals while WARP2 is acted as the receiver. We use WARP1 and WARP2 to simulate two pairs of transmitters and receivers, since each WARP has two independent transmission channels and two RF antennas which are denoted as RF_A and RF_B respectively. To be specific, we use the RF_A and RF_B of WARP1 to act as the legal transmitter and its cooperative interferer, respectively. Similarly, the RF_A and RF_B of WARP2 is adopted to act as the legal receiver and the eavesdropper, respectively.

In our experiment, the upper computer is used as the WARP control terminal. Besides, the WARP platforms are connected to the switch through twisted pair. Then, the Matlab simulation program is running on the upper computer, where the operation data is sent to the WARP platform through the switch for transmission. To be more specific, the default IP address of WARP1 is chosen as 10.0.0.1, while that of WARP2 is set as 10.0.0.2. The IP of the upper computer is set as 10.0.0.250 which is within the same network with WARPs for connectivity. The baseband gain of the transmitting node is 0 dB; while the RF gain is chosen as 15 dB. Besides, the baseband gain of the receiving node is 15 dB, and the RF gain is 24 dB.

2. P2P communication while jamming performance evaluation

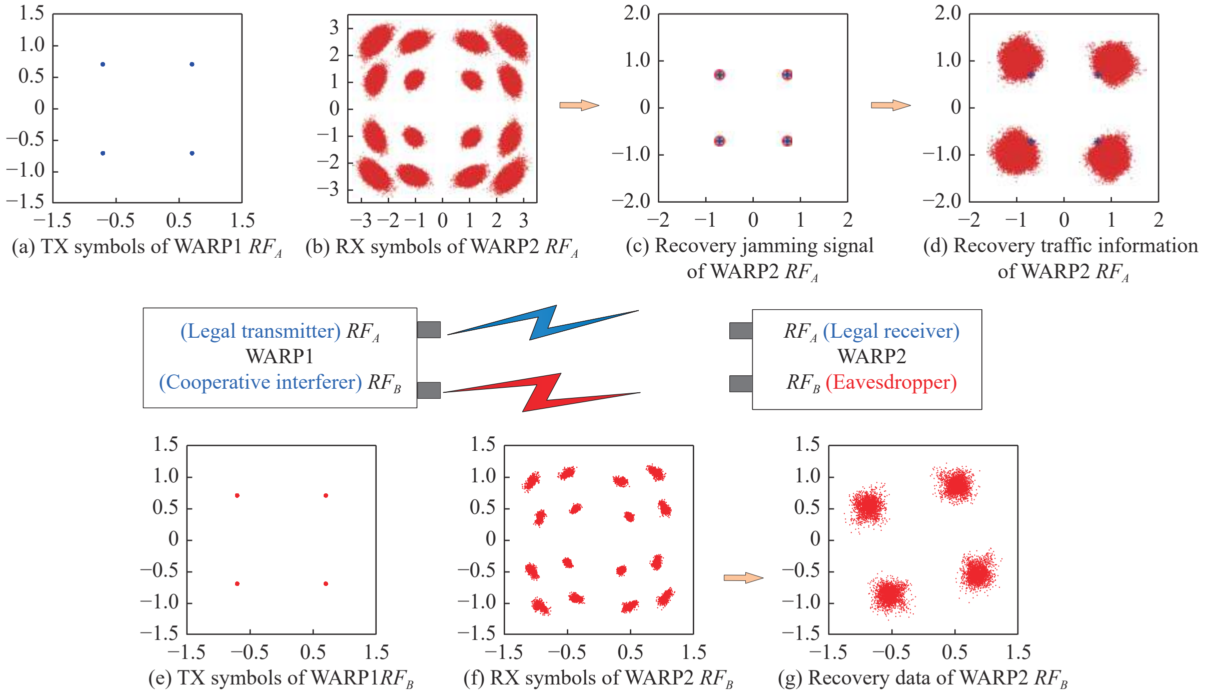
In this part, we demonstrate the performance of the proposed JI4Narrow and JI4Broad schemes for P2P communication scenario respectively.

1) Performance of the proposed JI4Narrow scheme

In the JI4Narrow experiment, the legal transmitter, namely, RF_A of WARP1, sends the low transmit power traffic signal, while the cooperative interferer acted by RF_B of WARP1 sends the corresponding high power jamming interference signal known as AN, where both signal are modulated by QPSK. Figure 6 shows the transmitted signal of the legal transmitter and cooperative interferer, and the receiving constellation points of legal receiver and eavesdropper.

In general, Figure 6 illustrate the related results in the whole experiment process for the JI4Narrow scheme. Specifically, Figure 6(a) shows the sending traffic information symbols by the legal transmitter (implemented by RF_A of WARP1) and Figure 6(e) demonstrates the sending artificial noise symbols of the cooperative interferer (implemented by RF_B of WARP1). Then, Figure 6(b) displays the received symbols at the legal receiver (implemented by RF_A of WARP2). Here, the legal receiver received the superimposed signal including traffic information and artificial noise. Similarly, Figure 6(f) shows the received symbols at the eavesdropper (implemented by RF_B of WARP2), which is also the superimposed signal. Figure 6(c) illustrates the recovery artificial noise known as jamming signal at the legal receiver, since the legal receiver exploits the SIC algorithm and decodes the jamming signal with bigger transmitted power first. Figure 6(d) shows the recovery traffic information intended for the legal receiver, where the legal receiver subtracts the jamming signal from the received superimposed signal, and then decode the traffic information.

However, the eavesdropper is unknown of the specific modulation and transmit power information of superimposed signal, and can only decode the received signal by the blind signal detection. Thus, as shown in Figure 6(g) the eavesdropper acted by RF_B of WARP2 purely de-



(a) TX symbols of WARP1 RF_A (b) RX symbols of WARP2 RF_A (c) Recovery jamming signal of WARP2 RF_A (d) Recovery traffic information of WARP2 RF_A

(e) TX symbols of WARP1RF_B (f) RX symbols of WARP2 RF_B (g) Recovery data of WARP2 RF_B

Figure 6 Data successful transmission rate performance in J4Narrow scheme.

codes the receiving superimposed signal as QSPK, since he is unaware of the structure and specific transmitter power allocation of the superimposed signal. In other words, the eavesdropper can use the blind signal detection method to decode the superimposed signal, which may identify the received signal either as the superimposed signal or as the underlay high power interference signal. Neither can the eavesdropper restore the legal transmitter's traffic signal correctly.

Therefore, we can conclude that in the proposed JI4N arrow scheme, the eavesdropper cannot recover the traffic information accurately, which can ensure the secure communication for legal users in this scenario. That is, the JI4Narrow scheme can achieve communicating while jamming even in presence of potential eavesdroppers.

Figure 7 shows the data successful transmission rate of the legal user and eavesdropper with the increasing transmit power ratio. Here, the transmit power ratio is defined as p_1/p_2. The legal user can decode the up-layer low transmit power traffic signal whenever the modulation scheme is BPSK or QPSK provided that the appropriate transmit power ratio is chosen. As for the eavesdropper, the data accuracy rate under BPSK is about 50% while that under QPSK is only 25%, which is the performance under the blind signal detection scheme. In this sense, we claim that the eavesdropper cannot decode the traffic signal for legal receiver correctly whenever which kind of modulation scheme is used.

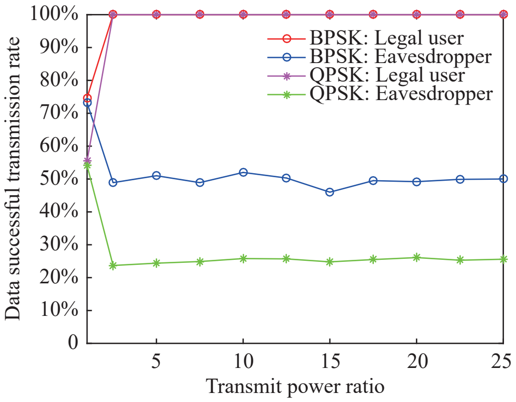


Figure 7 Sending and receiving diagram in J4Narrow scheme.

In Figure 8, the RF_A and RF_B of WARP1 are acted as the legal transmitter and cooperative interferer. To better illustrate the performance, we use an image as the traffic information for legal user, and the random noise as the interference. Accordingly, the RF_A and RF_B of WARP2 are treated as the legal receiver and eavesdropper. The center frequency of OFDM signal is set as 2.432 GHz.

At the transmitter side, the 75 pixels × 56 pixels image is transformed as a serial of decimal data within the range $\{0, 1, 2, \ldots, 15\}$. The number of decimal data after conversion is 25200. Then, we convert these decimal data in parrel and insert them in the even number of the sub-carriers in the OFDM symbol.

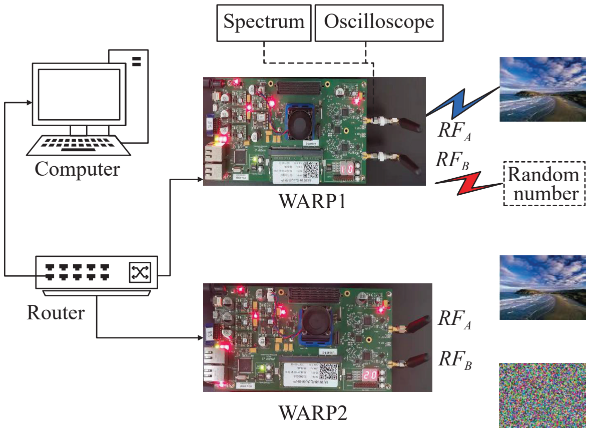


Figure 8 J4Broad transmission experiment diagram.

Here, the OFDM symbol consists of 64 sub-carriers, in which the 8th, 22nd, 44th, and 58th subcarriers are used for piloting signal while the 1st and 28th–38th sub-carriers are for zero padding. Then, the even numbering sub-carriers in the remaining 48 sub-carriers, that is, 22 sub-carriers, used to carry the image data. To ensure the positive integer of the number of OFDM symbols, the image data needs to be filled with zeros. After zero padding, the number of decimal image data is 25212. The number of OFDM symbols is 1146. The number of odd indexing sub-carriers is 26. We randomly generate 29796 random integer number within $\{0, 1, 2, \ldots, 15\}$, and insert these random integer into the odd number of sub-carriers in the OFDM symbols which are transmitted through the RF_B of WARP1. In other words, the image data is transmitted via RF_A while the random integers are sent via RF_B. Both data are adopted the 16QAM modulation. These two signal are superimposed over the air fulfilling the entire OFDM bandwidth.

At the receiving side, the WARP firstly synchronize the symbol timing, correct the carrier frequency offset, and estimate the channel gain. Then, the legal user extracts the bit information on the even indexing subcarriers from the entire OFDM time-frequency resource according to the random spectrum selected by the sending RF_A signal, and restore the decimal image data from the corresponding subcarrier, as shown in Figure 8.

Since the receiving RF_A knows the insertion position of the image data, the original sending image can be recovered. The random spectrum selected by the transmitter RF_A of WARP1 is unknown to the eavesdropper RF_B of WARP2. Because of the random inserting interference, the RF_B of WARP2 receives mixed information which is full of the entire OFDM resources. As a result, the RF_B of WARP2 cannot distinguish the image information from the random number, so it cannot demodulate the image. The garbled picture shown in Figure 8 appears. It can be seen from the constellation diagram of received signals that the signal quality received by legal users and eavesdroppers are both very good, which does not affect the received signal-to-noise ratio of legal users.

In Figure 9, we can see that the receiver BER in barrage jamming scheme for both legal user and eavesdropper are above 90%, while that in the proposed JI4Broad scheme for legal users is below 10% while that for the eavesdropper are above 90%, which shows the advantages of the proposed JI4Broad scheme.

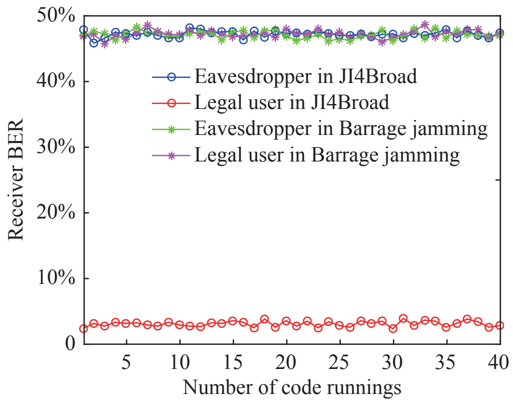


Figure 9 Illustration of JI4Broad scheme.

In a word, the JI4Broad scheme shows the promising performance compared with the barrage jamming scheme in the presence of eavesdropping.

3. E2E communication while jamming performance evaluation

To assess the performance of the secure transmission path planning method, we adopt Visual Studio to simulate the path planning process. In case 1, the number of eavesdroppers is set as 5. The number of communication nodes varies from 10 to 100. The network topology among these communication nodes are randomly generated while setting these nodes' connectivity as 4 to simulate the random user distribution in practical. The position relationship between eavesdropping nodes and the communication node are also produced randomly. The simulation result is shown in Figure 10. In case 2, the number of communication nodes is fixed as 100. We change the number of eavesdroppers from 5 to 13. The corresponding result is illustrated in Figure 11.

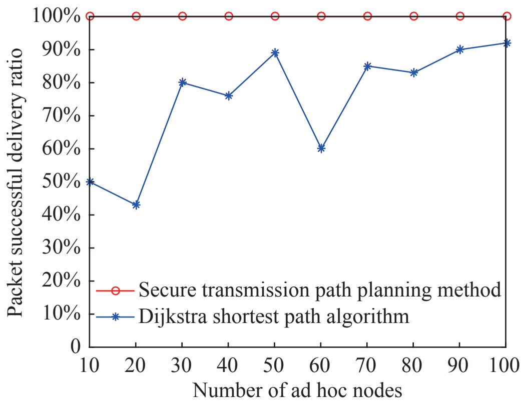


Figure 10 Packet successful delivery ratio versus number of ad hoc nodes.

As shown in Figures 10 and 11, we can see that the packet successful delivery ratio of the proposed secure transmission path planning method is obviously bigger than that of the Dijkstra shortest path algorithm. This is because that the insecure communication links are deleted while the cooperative interferer is chosen to aid the secure transmission for those potentially eavesdropping links.

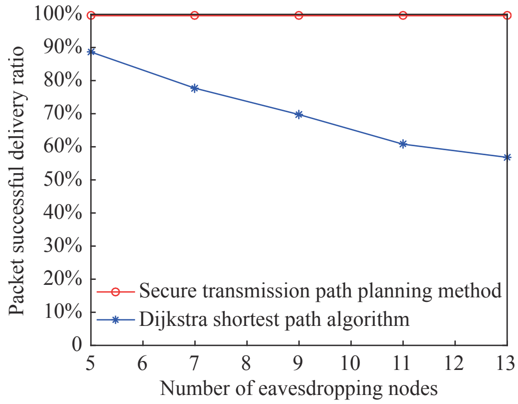


Figure 11 Packet successful delivery ratio versus number of eavesdropping nodes.

In particular, from Figure 10, we can see that the successful packet delivery ratio of Dijkstra shortest path algorithm is fluctuated with the increasing number of communication nodes, since the positions of these communication nodes and eavesdropping nodes are both randomly generated. Meanwhile, the proposed secure transmission path planning method can always ensure the 100% packet successful delivery ratio, which shows the superior of the proposed scheme.

In Figure 11, we can see that the successful packet delivery ratio of Dijkstra shortest path algorithm decreases nearly linearly with the increasing number of eavesdropping nodes, since the eavesdropping risk of each communication node increases in this situation. In contrast, the proposed secure transmission path planning method can always achieve the 100% the successful packet delivery ratio, which shows the advantage of the proposed E2E secure communication method in multi-hop wireless communication network.

VII. Conclusions

In this paper, focusing on the E2E secure communication in multi-hop ad hoc wireless communication network, we firstly propose JI4Narrow and JI4Broad schemes for narrow band and broad band systems respectively to ensure the P2P secure transmission of legal users in presence of eavesdropping. In both schemes, a neighboring node is selected as the cooperative interferer to generate the artificial noise known as jamming to aid the regular communication of the legal transmitter. Then, we design the secure network topology discovering method and the secure transmission path planning method to ensure the communication while jamming for E2E multi-hop wireless communication network. Experiments on the WARP platform and simulations results show the feasibility and advantages of the proposed schemes compared with the barrage jamming scheme in the P2P transmission scenario and the Dijkstra shortest path algorithm in the E2E multi-hop network situation respectively. In the future, the intelligent methods such as deep reinforcement learning will be investigated to further improve the performance of communicating while jamming scheme.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 62071283), Shaanxi Key Industrial Innovation Chain Project in Industrial Domain (Grant No. 2020ZDLGY15-09), and the Key Industry Projects in Shaanxi Province (Grant No. 2019ZDLGY09-03).

References

[1] M. Vaezi, A. Azari, S. R. Khosravirad, *et al.*, "Cellular, wide-area, and non-terrestrial IoT: a survey on 5G advances and the road toward 6G," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1117–1174, 2022.

[2] G. Geraci, A. Garcia-Rodriguez, M. M. Azari, *et al.*, "What will the future of UAV cellular communications be? A flight from 5G to 6G," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1304–1335, 2022.

[3] Z. Q. Wang, Y. Du, K. J. Wei, *et al.*, "Vision, application scenarios, and key technology trends for 6G mobile communications," *Science China Information Sciences*, vol. 65, no. 5, article no. 151301, 2022.

[4] Y. L. Zou, J. Zhu, X. B. Wang, *et al.*, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[5] F. Zhou, G. Sun, X. Bai, *et al.*, "A novel method for adaptive SAR barrage jamming suppression," *IEEE Geoscience and Remote Sensing Letters*, vol. 9, no. 2, pp. 292–296, 2012.

[6] Q. Z. Shi, J. J. Huang, T. Xie, *et al.*, "An active jamming method against ISAR based on periodic binary phase modulation," *IEEE Sensors Journal*, vol. 19, no. 18, pp. 7950–7960, 2019.

[7] S. H. Cheng, X. L. Sun, Y. H. Cai, *et al.*, "A joint azimuth multichannel cancellation (JAMC) antibarrage jamming scheme for spaceborne SAR," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 15 pp. 9913–9926, 2022.

[8] T. Cogalan, D. Camps-Mur, J. Gutiérrez, *et al.*, "5G-CLARITY: 5G-advanced private networks integrating 5GNR, WiFi, and LiFi," *IEEE Communications Magazine*, vol. 60, no. 2, pp. 73–79, 2022.

[9] Z. M. Fadlullah, B. M. Mao, and N. Kato, "Balancing QoS and security in the edge: existing practices, challenges, and 6G opportunities with machine learning," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2419–2448, 2022.

[10] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proceedings of the VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference*, Dallas, TX, USA, pp. 1906–1910, 2005.

[11] C. X. Liu, N. Yang, R. Malaney, *et al.*, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7444–7456, 2016.

[12] H. L. He, X. Z. Luo, J. Weng, *et al.*, "Secure transmission in multiple access wiretap channel: cooperative jamming without sharing CSI," *IEEE Transactions on Information Forensics and Security*, vol. 16 pp. 3401–3411, 2021.

[13] D. Xu and H. B. Zhu, "Proactive eavesdropping via jamming over short packet suspicious communications with finite blocklength," *IEEE Transactions on Communications*, vol. 70, no. 11, pp. 7505–7519, 2022.

[14] J. B. Si, Z. H. Cheng, Z. Li, *et al.*, "Cooperative jamming for secure transmission with both active and passive eavesdroppers," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5764–5777, 2020.

[15] X. Jiang, B. Y. Zheng, L. Wang, *et al.*, "Clustering for topological interference management," *Chinese Journal of Electronics*, vol. 31, no. 5, pp. 844–850, 2022.

[16] A. Gouissem, K. Abualsaud, E. Yaacoub, *et al.*, "Toward secure IoT networks in healthcare applications: a game-theoretic anti-jamming framework," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 19615–19633, 2022.

[17] J. H. Anajemba, C. Iwendi, I. Razzak, *et al.*, "A counter-eavesdropping technique for optimized privacy of wireless industrial IoT communications," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6445–6454, 2022.

[18] B. Okyere, L. Musavian, B. Özbek, *et al.*, "The resilience of massive MIMO PNC to jamming attacks in vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4110–4117, 2021.

[19] Y. Zhou, P. L. Yeoh, C. H. Pan, *et al.*, "Caching and UAV friendly jamming for secure communications with active eavesdropping attacks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 10, pp. 11251–11256, 2022.

[20] Y. Xu, J. Liu, Y. L. Shen, *et al.*, "Incentive jamming-based secure routing in decentralized Internet of Things," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 3000–3013, 2021.

[21] H. Dang-Ngoc, D. N. Nguyen, K. Ho-Van, *et al.*, "Secure swarm UAV-assisted communications with cooperative friendly jamming," *IEEE Internet of Things Journal*, vol. 9, no. 24, pp. 25596–25611, 2022.

[22] D. Li, X. Ma, and W. J. Han, "A point-to-point security communication system: artificial noise jamming insertion," in *Proceedings of the 2021 IEEE 9th International Conference on Information, Communication and Networks (ICICN)*, Xi' an, China, pp. 139–143, 2021.

[23] F. Tong, B. W. Ding, Y. J. Zhang, *et al.*, "A single-anchor mobile localization scheme," *IEEE Transactions on Mobile Computing*, Early Access, 2022.

[24] P. H. Wang, R. Zhou, X. P. Fan, *et al.*, "A distance estimation model for DV-hop localization in WSNs," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 5290–5299, 2023.

[25] Y. Xu, J. Liu, Y. L. Shen, *et al.*, "QoS-aware secure routing design for wireless networks with selfish jammers," *IEEE Transactions on Wireless Communications*, vol. 20, no. 8, pp. 4902–4916, 2021.

[26] J. C. Wang, X. Ma, D. Li, *et al.*, "Reinforcement learning for suppressing eavesdroppers in wireless communication system," in *Proceedings of the 2021 IEEE 9th International Conference on Information, Communication and Networks (ICICN)*, Xi'an, China, pp.159–165, 2021.

[27] L. L. Dai, B. C. Wang, Z. G. Ding, *et al.*, "A survey of non-orthogonal multiple access for 5G," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2294–2323, 2018.

[28] W. J. Han, Y. Zhang, X. J. Wang, *et al.*, "Orthogonal power division multiple access: a green communication perspective," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 12, pp. 3828–3842, 2016.

[29] W. J. Han, X. Ma, X. J. Wang, *et al.*, "Efficient power division multiplexing in MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 21, no. 5, pp. 3438–3451, 2022.

[30] W. J. Han, X. Ma, D. Tang, *et al.*, "Study of SER and BER in NOMA systems," *IEEE Transactions on Vehicular Tech-*

nology, vol. 70, no. 4, pp. 3325–3340, 2021.

[31] X. W. Li, X. S. Gao, Y. T. Liu, *et al.*, "Overlay CR-NOMA assisted intelligent transportation system networks with imperfect SIC and CEEs," *Chinese Journal of Electronics*, vol. 32, no. 6, pp. 1258–1270, 2023.

[32] N. I. Miridakis and D. D. Vergados, "A survey on the successive interference cancellation performance for single-antenna and multiple-antenna OFDM systems," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 312–335, 2013.

[33] E. Khorov, A. Kureev, and I. Levitsky, "NOMA testbed on Wi-Fi," in *Proceedings of the 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Bologna, Italy, pp. 1153–1154, 2018.

[34] K. Amiri, Y. Sun, P. Murphy, *et al.*, "WARP, a unified wireless network testbed for education and research," in *Proceedings of the 2007 IEEE International Conference on Microelectronic Systems Education (MSE'07)*, San Diego, CA, USA, pp. 53–54, 2007.

Xiao MA received the B.S., M.S., and Ph.D. degrees from Xidian University, Xi'an, China, in 2006, 2009, and 2014, respectively. From 2009 to 2010, he was a Software Engineer with ZTE Corporation. Since 2014, he has been with the School of Physics and Information Technology, Shaanxi Normal University, Xi'an, China, where he is currently an Associate Professor. He was a Visiting Scholar with the University of British Columbia, Vancouver, BC Canada. His research interests include wireless communications, mobile ad hoc networks, and concurrent transmission.
(Email: xma@snnu.edu.cn)

Dan LI received the M.S. degree from the Department of Physics and Information Technology, Shaanxi Normal University, Xi'an, China, in 2022. Currently, she is a Software Engineer in the Beijing Aerospace Science and Industry Century Satellite Hi-tech Co., Ltd., Xi'an Branch. Her research interest is wireless network electromagnetic control.
(Email: ldan1201@163.com)

Liang WANG received the B.S. degree in telecommunications engineering and the Ph.D. degree in communication and information systems from Xidian University, Xi'an, China, in 2009 and 2015, respectively. He is currently an Associate Professor with the School of Computer Science, Shaanxi Normal University, Xi'an, China. From 2018 to 2019, he was a Visiting Scholar with the School of Electrical and Computer Engineering, Georgia Institute of Technology, USA. His research interests focus on Internet of things, mobile edge computing, and applications of reinforcement learning and robust design in wireless communications networks.
(Email: wangliang@snnu.edu.cn)

Weijia HAN received the B.S. degree from Northwest University, Xi'an, China, the M.S. degree from Queen's University Belfast, UK, and the Ph.D. degree from Xidian University, Xi'an, China. He is now working as a faculty member in Shaanxi Normal University, Xi'an, China. He had worked as a Visiting Scholar at Texas A&M University, USA. His research interests include sensing and machine learning in cognitive radio networks, resource management and network optimization, and cognitive media access protocol and algorithm design.
(Email: wjhan@snnu.edu.cn)

Nan ZHAO received the B.S., M.S., and Ph.D. degrees from Xidian University, Xi'an, China, in 2003, 2008, and 2012, respectively. Since 2012, he has been with the State Key Laboratory of Integrated Services Networks, Xidian University, where he is currently an Associate Professor. From 2014 to 2015, he was a Visiting Scholar with the Michigan State University, East Lansing, MI, USA. His research interests include physical layer security and physical layer network, green ICT, power division and allocation, social media data mining and information processing.
(Email: zhaonan@xidian.edu.cn)