An Intermittent Cooperative Jamming Strategy for Securing Energy-Constrained Networks

Qinghe Gao, *Student Member, IEEE*, Yan Huo, *Member, IEEE*, Tao Jing, *Member, IEEE*, Liran Ma, *Member, IEEE*, Yingkun Wen, *Student Member, IEEE*, and Xiaoshuang Xing, *Member, IEEE*

***Abstract*— Friendly jamming is an unconventional approach to secure wireless communications. Specifically, a friendly jammer transmits jamming signals to an eavesdropper while a legitimate transmitter is sending data. The jamming signals only interfere with the eavesdropper, and thus, prevent data from being disclosed to unintended parties. Mainstream jamming schemes adopt a continuous jamming strategy (CJS), where the jammer is required to constantly transmit jamming signals in the entire duration of the legitimate transmission. In certain scenarios, however, the CJS may lead to excessive jamming, and cause a waste of energy and the degradation of jamming efficiency. To address the drawbacks of the CJS, we propose the concept of an intermittent jamming strategy (IJS), where a jammer alternates between jamming and non-jamming modes during the legitimate transmission. In this paper, we study the feasibility of the IJS for physical layer security. We first introduce a new metric to jointly measure security requirements and energy costs. Next, we formulate and solve an optimization problem with respect to the jamming duration proportion and the jamming power. Finally, we verify the feasibility of the IJS through extensive simulation experiments under different modulation methods.**

***Index Terms*— Cooperative jamming scheme, intermittent jamming strategy, physical layer security, bit error rate, energy efficiency.**

I. Introduction

WIRELESS communication networks are the backbone of many services such as sensing and monitoring [1], [2], smart home [3], [4], and emergency response [5], [6]. In these services, sensitive data is prone to eavesdropping by unintended receivers due to the broadcast nature of wireless channels [7], [8]. To prevent an eavesdropper from decoding the sensitive information, researchers have proposed cooperative jamming based physical layer security solutions [9]–[11]. In a cooperative jamming scheme, one or more users are employed as friendly jammers to transmit interference signals.

Cooperative jamming schemes typically exploit the channel characteristic difference between a legitimate receiver and an eavesdropper. Specifically, jamming signals are formed based on the difference to degrade eavesdropping channels while ensuring the quality-of-service (QoS) of legitimate channels [12], [13]. Mainstream jamming schemes typically adopt a strategy that requires a jammer to continuously transmit jamming signals when a legitimate user is sending data. We call this a continuous jamming strategy (CJS). The rationale behind a CJS is that the entirety of the legitimate signal needs to be protected from eavesdropping. However, this rationale may be fundamentally flawed based on the following observations. In an analog communication system, received signals cannot be successfully decoded if a certain percent of the signals is damaged (e.g., 30% or more in 1G mobile systems). Additionally, if the bit-error-rate (BER) of a digital signal rises to a certain level, its bearing messages cannot be extracted [14]. Lastly, each part of the received signals may not be of the same importance in the decoding process [15]. Forward error correction (FEC) bits, for example, are more critical to correct decoding. Thus, continuously jamming the unnecessary parts of the entire signal leads to a waste of energy and the degradation of jamming efficiency.

The above observations motivate us to investigate the feasibility of an intermittent jamming strategy (IJS) that is able to ensure security with less jamming time. To the best of our knowledge, there is little research on the feasibility of an IJS for physical layer security in the literature [16]. An IJS is considered to be feasible under either of the following two conditions: i) it can achieve an identical level of security compared with a CJS with less energy consumption; or, ii) it can obtain a higher level of security than a CJS with the same energy consumption. Our feasibility study needs to address two major challenges. Firstly, we need to develop a new metric to measure the performance of an IJS. Secondly, we need to find the appropriate jamming duration for each transmission. Coping with these challenges is essential for the design of an IJS with the goal of balancing the trade-off between security requirements and energy efficiency.

Manuscript received December 18, 2018; revised April 29, 2019 and June 27, 2019; accepted August 16, 2019. Date of publication August 26, 2019; date of current version November 19, 2019. The authors would like to thank the National Natural Science Foundation of China (Grant No. 61871023, 61931001, 61572070, and 61602062), the Natural Science Foundation of Jiangsu Province (BK20160410) and the National Science Foundation of the US under grant OAC-1829553 and CNS-1912755. The associate editor coordinating the review of this article and approving it for publication was X. Wang. *(Corresponding author: Qinghe Gao.)*

Q. Gao, Y. Huo, T. Jing, and Y. Wen are with the School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China (e-mail: qhgao_wnip@bjtu.edu.cn; yhuo@bjtu.edu.cn; tjing@bjtu.edu.cn; 16111024@bjtu.edu.cn).

L. Ma is with the Department of Computer Science, Texas Christian University, Fort Worth, TX 76129 USA (e-mail: l.ma@tcu.edu).

X. Xing is with the School of Computer Science and Engineering, Changshu Institute of Technology, Suzhou 215500, China (e-mail: xiaoshuangxing87@gmail.com).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2019.2937303

Without the loss of generality, we employ a typical four-user system model to analyze the feasibility of an IJS. This model consists of a legitimate transmitter, a legitimate receiver, an eavesdropper, and a friendly jammer. The jammer can switch between a jamming mode and a non-jamming mode. Specifically, the jammer transmits jamming signals in the jamming mode and stops in the non-jamming mode. In this paper, for simplicity, we assume that the jammer sleeps during the non-jamming mode for energy conservation. A longer sleeping duration can save more energy, while may degrade the protection of the legitimate signals. Thus, the jamming duration proportion (JDP) is critical to strike a balance between security and energy saving.

To obtain the optimal JDP, we first define a new metric to jointly measure security requirements and energy costs. This metric is termed as BER-gap-energy-efficiency (BGEE) and is calculated as the ratio between the achievable BER gap and the total consumed energy per second. The BER gap is the difference between the BER of Eve and the BER of Bob. Next, we formulate an optimization problem with respect to JDP and the jamming power. This problem is with the objective of maximizing the BGEE under the BER constraint of the legitimate receiver and total energy constraint. We solve this problem by transforming it into two subproblems: i) the JDP optimization subproblem under a fixed jamming energy; and, ii) the jamming power optimization subproblem with the given optimal JDP. By solving the first subproblem, we analyze the feasibility of the IJS according to the optimal JDP values. By solving the second subproblem, we further optimize jammer's transmit power. According to the solutions, we discuss the applicability of the IJS and the CJS. Finally, we verify the feasibility of an IJS through an extensive simulation experiments under different modulation methods. Simulation results demonstrate that the BER of eavesdropper under the IJS is higher than that under the CJS when less jamming energy is available.

The main contributions of our work are summarized as follows.

- We are the first to show that an IJS is feasible with less jamming energy. With the same jamming energy, an IJS can cause a higher BER of the eavesdropper than a CJS, especially when the available jamming energy is lower than a specific threshold.
- We employ the average BER as the performance metric in our proposed strategy. Compared with the security capacity used in the CJS, this metric can reflect the jamming effect on eavesdropper's receptions more intuitively, which is beneficial for adaptively adjusting jamming strategies.
- We conduct extensive experiments on the BER performance under multiple typical modulation methods, including BPSK, MSK, GMSK, QPSK, 16 QAM, and 64 QAM. Simulation results verify that our proposed IJS is preferable to the CJS under low energy constraints.

The rest of the paper is organized as follows. We give the review of related works in Section II. Then our system model and the optimization problem are described in Section III, followed by problem solutions and discussions in Section IV. Numerical results and analyses are given in Section V. Last, we conclude the paper in section VI.

II. Related Work

Cooperative jamming schemes have been widely used in wireless networks to protect legitimate signals [17]–[19]. Researchers usually maximized secrecy capacity (SC) to enhance the transmission security by optimizing the jamming power and beamforming vectors [20]–[22]. These works usually assumed that the channel state information (CSI) of the eavesdropper was perfectly known, because the secrecy capacity is defined as the difference between the channel capacity of a legitimate channel and that of an eavesdropping channel [23]. However, it is difficult to know perfect CSI of the passive eavesdropper in practice. Thus, researchers studied the cases where only statistic CSI of eavesdroppers were known. Under these cases, secrecy outage probability (SOP) was employed to analyze the transmission security [24]–[27]. The SOP is referred to as the probability that the expected secrecy capacity is lower than a predetermined threshold. Under the constraints of SC or SOP, researchers also considered the problems of boosting the energy efficiency [28]–[30]. Dehghan *et al.* explored the energy efficiency of cooperative beamforming methods in a wireless ad hoc relaying network [28]. Under the premise of ensuring a minimum SC for the primary user in a cognitive radio network (CRN), Gabry *et al.* proposed a resource allocation algorithm to maximize the energy efficiency of the secondary user that is selected as a friendly jammer [29]. Under a similar CRN model as the one in [29], Wen *et al.* jointly considered the energy efficiency and the security requirement. They improved the secrecy energy efficiency (SEE) that was defined as the ratio between the SC and total energy costs [30].

With double guarantee on the security and the energy efficiency, cooperative jamming schemes were growingly applied into energy constrained networks [1], [31]. However, existing jamming strategies assumed that the jammer continuously transmitted jamming signals simultaneously with the legitimate transmission. This CJS usually accompanies with high energy consumptions [3], [8]. For better supporting CJS in energy constrained networks, researchers utilized an energy harvesting method to broaden the source of energy supply for low energy jammers [32]–[34]. The authors proposed a cooperative zero-forcing jamming scheme in wireless sensor networks [1]. They employed the simultaneous wireless information and power transportation (SWIPT) method to provide energy for jammers. Mobini *et al.* proposed an energy harvesting based cooperative scheme where the source node charged the trusted relay node and the jammer node to enhance the security of communication [33]. Similarly, a wireless powered cooperative jamming scheme based on a harvest-then-jam protocol was employed to protect the legitimate communication in an orthogonal frequency division multiplexing (OFDM) system. The harvest-then-jam protocol was proceeded in two slots. In the first slot, the source sent dedicated energy signals to power the jammer. In the second slot, the jammer used the harvested energy to jam the eavesdropper so as to protect the communication from the source to the destination [34].

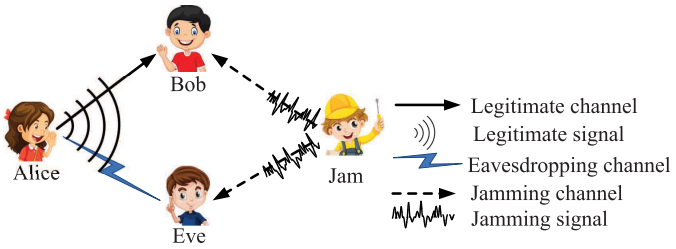


Fig. 1. Four-user wiretap channel model.

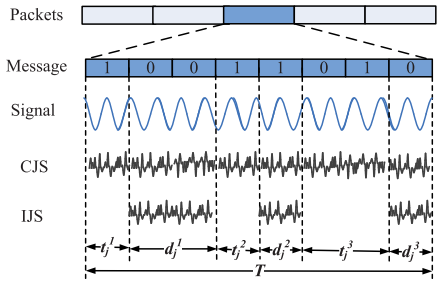


Fig. 2. Transmit signals

However, it is now difficult to apply the energy harvesting based schemes in reality. On one hand, the energy harvesting phase and the jamming phase cannot be proceeded in the same time because most jammers only support the half-duplex mode. Reserving time for harvesting energy decreases the jamming time, which degrades the jamming efficiency of the CJS. On the other hand, the amount of the energy harvested from the RF signals is usually at a level less than 10mW [35]. With such a low amount of power, battery-enabled devices are far from capable of supporting the CJS. Thus, it is necessary to investigate the feasibility of an IJS that can save energy with less jamming time while ensuring secure communication.

The intermittent jammers [36] have been employed to attack/block communications with the advantage of saving energy. Existing works mainly focused on designing jamming schemes to strengthen attacks [37] and devising countermeasures against the intermittent jamming [38]. Motivated by the energy-saving advantage of the intermittent jammer, we employ it to protect legitimate users' communication instead of attacking users' communication. Allouche *et al.* proposed a temporal jamming scheme where jammers produced noise for a certain portion of the legitimate transmission time. By applying a certain distribution function to model the jamming time length, they obtained the jammers' activities from a probability perspective via using a polynomial solution [39]. Motivated by the temporal jamming in this paper, we proposed the IJS. Different from the polynomial solutions given by Allouche, we would derive the best JDP according to the channel conditions and give the application scenarios of the CJS and the IJS.

III. Model and Problem Formulation

A. System Model

We consider a general four-user wiretap channel model as shown in Fig. 1. A legitimate transmitter (Alice) sends secret messages to a legitimate receiver (Bob). A passive eavesdropper (Eve) intends to interpret the legitimate messages. A friendly jammer (James) is assigned to transmit jamming signals to interfere with Eve. By appropriately designing the transmit time length and the transmit power of the jammer, we need to make Eve decode its received signals in a large BER or even cannot decode its reception, meanwhile guarantee approximately error-free messages received by Bob.

To achieve the above secure transmission, traditionally, the jammer is required to simultaneously and continuously transmit jamming signals with the transmission of Alice. We call this case as the CJS, shown in Fig. 2, where jamming signals continue for the whole duration of Alice's signal transmission. Different from the CJS, we propose the IJS, where the jammer just intermittently transmits jamming signals during Alice's transmission. The jamming process is composed of multiple jamming durations and multiple jamming intervals. As shown in Fig. 2, the jamming duration, denoted by d_j, refers to the time length of the jammer's transmission. The jamming interval, represented by t_j, is the time length between two jamming transmissions. Since there is no jamming signals are transmitted in jamming intervals, we can call them as non-jamming durations. We define a new parameter called as JDP, denoted by α, as the ratio between the summation of jammer's jamming durations to Alice's transmission duration (e.g., JDP equals $(d_j^1 + d_j^2 + d_j^3)/T$ in Fig. 2).

During the jamming duration, the BER is determined by the composite effects of the jamming signals combined with the thermal background noise and it can be expressed as p_e^j. The BER during the non-jamming duration is due to the thermal background noise, e.g., additive white Gaussian noise (AWGN) and it can be denoted as p_e^n. Since the IJS includes jamming and non-jamming durations, the overall BER in the IJS is the time-averaged value between these two kinds of BERs, which can be expressed as [15], [39]

$$p_e = \alpha p_e^j + (1-\alpha) p_e^n, \tag{1}$$

where $0 < \alpha < 1$ holds for the IJS. The case of $\alpha = 1$ corresponds to the CJS and, thus, the overall BER in the CJS equals the BER during the jamming duration.

Note that we mainly discuss the transmission BER instead of the information BER for twofold reasons. On the one hand, the transmission BER is defined as the number of detected bits that are incorrect before error correction divided by the total number of transferred bits [40]. Since it depends on the channel conditions and the power of signals, it can directly reflect the impact of jamming signals, which is exactly what we tend to study. On the other hand, the information BER is calculated after error correction and mainly affected by the strength of error correction. For the legitimate receiver Bob, the error correction can make the information BER much lower than the transmission BER and even cancel all errors caused by jamming signals. But the error correction is disabled at Eve if its transmission BER is beyond a threshold. Therefore, we just need to maximize the transmission BER of Eve under the condition that the transmission BER of Eve is higher than

a threshold while that of Bob is lower than another threshold. These two constraints are also consistent with the requirements of the reliable and secure communication.

B. Problem Formulation

In this paper, we focus on verifying the feasibility of the IJS. The IJS is said to be feasible if its jamming efficiency is higher than the CJS. To measure the jamming efficiency, we propose a new parameter named as ***BER-gap-energy-efficiency (BGEE)*** under the guarantee of the reliable and the secure communication. This parameter is computed as the ratio between the BER gap and the totally consumed energy per second, where the BER gap is the difference between Eve's BER (i.e., p_{e_E}), and Bob's BER (i.e., p_{e_B}). Specifically, the expression of BGEE is given by

$$BGEE = \frac{p_{e_E} - p_{e_B}}{RE_b + P_J}, \quad \text{for } p_{e_B} < \eta_B \quad \text{and} \quad p_{e_E} > \eta_E, \tag{2}$$

where R is the transmission rate of Alice, E_b is the energy per bit, and P_J is the energy the jammer consumes to transmit jamming signals per second. Note that P_J is exactly the actual jamming power in CJSs, while the actual jamming power in the IJS is P_J/α. η_B and η_E are the BER thresholds for Bob and Eve, respectively.

To analyze the feasibility of the IJS, we formulate a following BGEE maximization problem. Under a certain amount of total consumed energy, a higher BGEE means a larger BER gap between Eve and Bob. Meanwhile, the friendly jamming is based on the premise that jamming signals cause few or no errors to Bob, which makes $p^j_{e_E} - p^j_{e_B} \approx p^j_{e_E}$.[1] Thus, we can employ BER-energy-efficiency (BEE) as a substitute metric to measure the jamming efficiency. The BEE is defined as the ratio between the BER of Eve and the total consumed energy. The BGEE maximization problem can be simplified as the following BEE maximization problem,

$$\max_{P_J,\alpha} \ \frac{p_{e_E}}{(RE_b + P_J)} \tag{3a}$$

$$\text{s.t.} \ \ 0 < \alpha \leq 1, \tag{3b}$$

$$P_J \leq P_J^{tol}, \tag{3c}$$

$$p_{e_E} \geq \eta_E, \tag{3d}$$

$$p_{e_B} \leq \eta_B, \tag{3e}$$

where Constraint (3b) is the JDP limitation and (3c) gives the power limitation for the jammer with P_J^{tol} as the maximum tolerant jamming power due to energy constraints. (3d) and (3e) show the BER requirements at Eve and Bob, respectively.

Since the BER is determined by modulation methods of Alice, we investigate the case of the basic binary phase shift keying (BPSK) modulation as an example. Extensions to higher-order modulation methods are straightforward.

[1]On one hand, the BER of Bob should be maintained as low as possible for the reliable communication between Alice and Bob, which is a general premise for the secure communication in physical layer security. On the other hand, the jamming signals are used to degrade the eavesdropping channel as the same time not to influence the legitimate channel, which is another general premise of the cooperative jamming based physical layer security.

IV. Optimization of Intermittent Jamming

In this section we first give the BER definition under the BPSK modulation method. Then we solve the BEE maximization problem by a two-tier approximation method. Last, we analyze and discuss the applicability of the IJS and the CJS.

A. Computation of BER

The received BER under the BPSK modulation depends on the signal energy per bit and the spectral density of interference [41]. Thus, the BER received at Bob and Eve during jamming durations under the BPSK modulation method is computed as

$$p^{j,bpsk}_{e_u} = Q\left(\sqrt{\frac{2|h_{Au}|^2 E_b}{N_0 + |h_{Ju}|^2 N_j/\alpha}}\right), \quad \text{for } u \in \{B, E\}, \tag{4}$$

where h_{Au} and h_{Ju} are the channel conditions from Alice and James to u with $u \in \{B, E\}$ for Bob and Eve,[2] respectively. N_0 is the spectral density of the Gaussian white noise, N_j is the time-averaged spectral density of the jamming signals and is expressed as $N_j = P_J/B_w$. B_w is the transmission bandwidth and $Q(\cdot)$ is the Q-function, which is defined as $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} \exp(\frac{-x^2}{2})dx$. During the non-jamming duration, bit errors are caused by the AWGN. The BER is calculated as

$$p^{n,bpsk}_{e_u} = Q\left(\sqrt{\frac{2|h_{Au}|^2 E_b}{N_0}}\right), \quad \text{for } u \in \{B, E\}. \tag{5}$$

Substituting (4) and (5) into (1), the average BER under the BPSK modulation method is computed as

$$p^{bpsk}_{e_u} = \alpha p^{j,bpsk}_{e_u} + (1-\alpha) p^{n,bpsk}_{e_u}, \quad \text{for } u \in \{B, E\}. \tag{6}$$

Thus, we can obtain the BPSK-based BEE maximization problem by substituting (6) into the the objective function of (3a). Due to the BEE is just convex with respect to α and not convex about P_J, we solve this problem in a two-tier method, which is shown in the **Algorithm 1**. In the outer function, we employ the golden search method to find the optimal jamming power. Under a certain jamming power, α only impacts the numerator of the objective function. Hence, we solve the convex JDP optimization subproblem in the inner function ComputeBEE(N_j).

B. JDP optimization subproblem

The JDP optimization problem is to maximize the BER of Eve under a certain jamming power,

$$\max_{\alpha} \ \ p^{bpsk}_{e_E}, \quad \text{s.t.} \ \ 0 < \alpha \leq 1.$$

[2]In works about the physical layer security, the knowledge of the eavesdropping channel state information is important for designing schemes to guarantee strong security for the intended legitimate receiver. Therefore, the channel conditions about the eavesdropper is generally assumed to be perfectly known [42], [43]. This is possible when a legitimate user whose services are different from that of the intended legitimate receiver is considered as an eavesdropper [44], [45]. Certainly, if a user stays passive for eavesdropping for a long time, the known CSI may be incomplete [46], [47]. We will consider this complex case in our future works.

Algorithm 1: BEE Optimization

Input: The parameters η_E, η_B, $\frac{E_b}{N_0}$,and $N_J^{tol,th}$;
Output: The optimal jamming power P_j^*, the optimal JDP α^*, the maximum BEE at Eve BEE_E^*;

Initialize $\rho = \frac{\sqrt{5}-1}{2}$, $N_j^{min} = 0, N_j^{max} = N_j^{tol,th}$;
Set $N_j^l = N_j^{max} - \rho(N_j^{max} - N_j^{min})$;
Set $N_j^r = N_j^{min} + \rho(N_j^{max} - N_J^{min})$;
repeat
  Compute $Left$ = `ComputeBEE` (N_j^l);
  Compute $Right$ = `ComputeBEE` (N_j^r);
  if $Left \leq Right$ **then**
    $N_j^{min} = N_j^l$;
    $N_j^l = N_j^r$;
    $N_j^r = N_j^{min} + \rho(N_j^{max} - N_j^{min})$;
  else
    $N_j^{max} = N_j^r$;
    $N_j^r = N_j^l$;
    $N_j^l = N_j^{max} - \rho(N_j^{max} - N_j^{min})$;
  end
until $|N_j^r - N_j^l| < \delta$, *δ is the tolerance*;
return $N_j^* = \frac{N_j^{min}+N_j^{max}}{2}$;
Compute the optimal jamming power $P_j^* = N_j^* B_w$;
Calculate the optimal JDP α^*;
Obtain the maximum BEE at Eve BEE_E^*.

Function ComputeBEE(N_j)

Input: Parameters $|h_{JE}|^2$, $|h_{AE}|^2$, E_b, N_0, N_j.
Output: The BEE at Eve $BEE_E(N_j)$.

Obtain $\alpha^*(N_j)$ by solving the JDP optimization problem according to **Theorem 1** and **Theorem 2** ;
Compute $BEE_E(N_j)$ by substituting $\alpha^*(N_j)$ into (3a) ;
return $BEE_E(N_j)$.

Since the BER caused by the AWGN, $p_{e_E}^{n,bpsk}$, is not influenced by jamming signals, it is constant for different values of α. We solve this problem according to two cases: i) the extreme case where the AWGN-based BER can be neglected, that is, $p_{e_E}^{n,bpsk} = 0$; and, ii) the practical case where bit errors are caused by both jamming signals and AWGN, that is, $p_{e_E}^{n,bpsk} > 0$.

1) The Case Without AWGN-Based Errors at Eve: This is the worst case where Eve can decode its received signals without any errors during non-jamming durations. In this case, it is necessary to interfere with Eve by using jamming signals for securing the communication between Alice and Bob. The overall bit error probability is computed as

$$p_{e_E}^{bpsk} \approx \alpha Q\left(\sqrt{\frac{2|h_{AE}|^2 E_b}{|h_{JE}|^2 N_j}\alpha}\right). \tag{7}$$

The approximation is due to $2|h_{AE}|^2 E_b/N_0 \gg 40dB$ indicated by the assumption that $p_{e_E}^{n,bpsk} = 0$.

Theorem 1: Under a certain value of N_j, there is one and only one optimal value of JDP that can be denoted as α^* and computed as

$$\alpha^* = \begin{cases} \dfrac{0.709}{|h_{AE}|^2 E_b/(|h_{JE}|^2 N_j)} & \dfrac{|h_{AE}|^2 E_b}{|h_{JE}|^2 N_j} > 0.709, \\ 1 & \dfrac{|h_{AE}|^2 E_b}{|h_{JE}|^2 N_j} < 0.709, \end{cases} \tag{8}$$

Note that the case where $\alpha^* = 1$ corresponds to the CJS.

Proof: Detailed proof is given in APPENDIX A, where we prove the uniqueness and compute the value of the optimal JDP solution through the deduction of the first-order function and second-order derivative functions of the $p_{e_E}^{bpsk}$ with respect to (w.r.t.) α.

2) The Case With Both AWGN-Based and Jamming-Based Errors at Eve : This is a practical case where error bits occur during both the jamming and non-jamming durations. The BER of Eve is given by (6).

Theorem 2: Under the case with both AWGN-based and jamming-based errors at Eve, the optimal JDP is calculated as

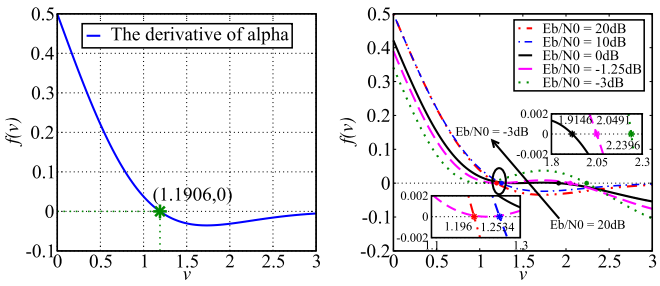
$$\alpha^* = \begin{cases} \dfrac{|h_{JE}|^2 N_j}{2|h_{AE}|^2 E_b/v^{*2} - N_0}, & v^* < \sqrt{\dfrac{2|h_{AE}|^2 E_b}{|h_{JE}|^2 N_j + N_0}}, \\ 1, & v^* > \sqrt{\dfrac{2|h_{AE}|^2 E_b}{|h_{JE}|^2 N_j + N_0}}, \end{cases} \tag{9}$$

where v^* is the value of $v = \sqrt{\frac{2|h_{AE}|^2 E_b}{|h_{JE}|^2 N_j/\alpha + N_0}}$ that can make the first-order derivative function of $p_{e_E}^{bpsk}$ w.r.t. α equal to 0, i.e., $f(v^*) = 0$.

Proof: See details in APPENDIX B.

Proposition 1: The BER of Eve under the IJS is higher than that under the CJS if the available jamming energy is lower than a threshold and otherwise the latter is higher than the former.

Proof: Fig.3(b) illustrates the derivation functions w.r.t. α under several cases of E_b/N_0, including $E_b > N_0$, $E_b = N_0$, and $E_b < N_0$. Together with the proof in APPENDIX B, we can see that the BER of Eve is a convex function of α for all cases. Furthermore, the lower the E_b/N_0 is, the larger the v^*. This indicates that a larger N_j meets the result of $\alpha^* = 1$ more easily according to (9). Thus, there exists a boundary value N_j^{th} that makes $\alpha^* < 1$ when $N_j < N_j^{th}$ and $\alpha^* = 1$ when $N_j \geq N_j^{th}$. We can take this boundary value as the jamming energy threshold $N_j^{\alpha,th}$. When the available jamming energy is minor than $N_j^{\alpha,th}$, the IJS can be applied to achieve higher BER at Eve than the CJS.



(a) The case where $p_{e_E}^{n,bpsk} = 0$, and $v = \sqrt{\frac{2|h_{AE}|^2 E_b}{|h_{JE}|^2 N_j/\alpha}}$. (b) Other cases where $p_{e_E}^{n,bpsk} > 0$, and $v = \sqrt{\frac{2|h_{AE}|^2 E_b}{|h_{JE}|^2 N_j/\alpha + N_0}}$.

Fig. 3. The first-order derivative of $p_{e_E}^{bpsk}$ w.r.t. α.

C. Discussion on the Applicability of the IJS and the CJS

Given an amount of jamming energy, the actual jamming power in CJS and IJS are different due to the differences of actual jamming durations. As a result, the BERs of Eve under the IJS and the CJS are also distinct. Based on these differences, the applicability of the IJS and the CJS are discussed as follows.

The discussions are based on the relationship between the four jamming energy thresholds $N_j^{tol,th}$, $N_j^{\alpha,th}$, $N_j^{E,th}$ and $N_j^{B,th}$. Note that the BER thresholds of η_E and η_B are assumed to satisfy conditions of $N_j^{E,th} < N_j^{B,th}$ and $N_j^{tol,th} < N_j^{E,th}$. The former condition guarantees the BER of Bob is lower than that of Eve. The latter one ensures the jamming energy is enough to interfere with the eavesdropper.

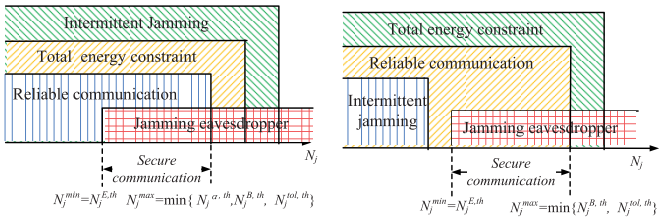
Specifically, these four thresholds for the case without AWGN-based errors at Eve are computed as

$$\begin{aligned}
N_J^{E,th} &= \frac{\eta_E E_b |h_{AE}|^2}{0.083|h_{JE}|^2},\\
N_J^{tol,th} &= P_J^{tol}/B_w,\\
N_J^{\alpha,th} &= \frac{E_b|h_{AE}|^2}{0.709|h_{JE}|^2},\\
N_J^{B,th} &= \frac{E_b|h_{AE}|^2}{0.709|h_{JE}|^2}\frac{\eta_B - Q\left(\sqrt{\gamma}\right)}{Q\left(\sqrt{\frac{1}{\frac{1}{\gamma}+\frac{1}{0.709}\frac{|h_{AE}|^2|h_{JB}|^2}{|h_{JE}|^2|h_{AB}|^2}}}\right)},\\
\gamma &= \frac{2|h_{AB}|^2 E_b}{N_0}.
\end{aligned}$$

Moreover, the four thresholds for the case with both AWGN-based and jamming-based errors at Eve are computed as follows,

$$\begin{aligned}
a &= \frac{|h_{JE}|^2}{2|h_{AE}|^2 E_b/v^{*2} - N_0},\\
N_j^{\alpha,th} &= \frac{1}{a},\\
N_j^{tol,th} &= P_J^{tol}/B_w,\\
N_j^{u,th} &= \frac{\eta_u - p_{e_u}^{n,bpsk}}{p_{e_u}^{j,bpsk} - p_{e_u}^{n,bpsk}}, u \in \{E,B\},\\
p_{e_u}^{n,bpsk} &= Q\left(\sqrt{\frac{2|h_{Au}|^2 E_b}{N_0}}\right), u \in \{E,B\},\\
p_{e_B}^{j,bpsk} &= Q\left(\sqrt{\frac{1}{\frac{|h_{JB}|^2}{|h_{JE}|^2}\left(\frac{|h_{AE}|^2}{|h_{AB}|^2 v^{*2}} - \frac{1}{\gamma}\right) + \frac{1}{\gamma}}}\right),\\
p_{e_E}^{j,bpsk} &= Q(v^*),\\
\gamma &= \frac{2|h_{AB}|^2 E_b}{N_0}.
\end{aligned}$$

We can see that these thresholds are determined by the channel conditions, the transmit power of Alice ($P_A = E_b R$) and the AWGN power ($2B_w N_0$). According to different communication environments, we give cases in Fig. 4 where the variable range of N_j is denoted by $N_j \in [N_j^{min}, N_j^{max}]$. As shown in Fig. 4(a), N_j is in the domain $[N_j^{min}, N_j^{max}]$ with $N_j^{min} = N_j^{E,th}$ and $N_j^{max} = \min\{N_j^{tol,th}, N_j^{\alpha,th}, N_j^{B,th}\}$.



(a) $N_j^{E,th} < N_j^{\alpha,th}$. (b) $N_j^{E,th} > N_j^{\alpha,th}$.

Fig. 4. The range of N_j for reliable and secure communication.

Under these cases, we can employ the IJS to achieve the reliable and secure communication. There are also some cases where $N_j^{E,th} > N_j^{\alpha,th}$ shown in Fig. 4(b), which belongs to the CJS.

For the sake of completeness, we list the eight conditions and the feasible domains of $[N_j^{min}, N_j^{max}]$ for the IJS and the CJS to achieve reliable and secure communication in the Table I. The top four cases can only utilize the IJS. To be specific, the conditions in Case 1, Case 2, and Case 3 satisfy the limitation of $N_j^{tol,th} < N_j^{\alpha,th}$ required by the **Proposition 1**. Therefore, the IJS under these three cases can cause higher BER of Eve than the CJS. Although the condition of Case 4 does not satisfy the limitation of **Proposition 1**, the N_j^{max} of its feasible domain is minor than $N_j^{\alpha,th}$. Thus, the IJS can cause more errors at Eve than the CJS under its feasible domain.

As for Case 5 and Case 6, both the IJS and the CJS can meet the requirements of reliable and secure communication. Since each strategy has its own strengths, to select the IJS or the CJS under these two cases lies in application scenarios. For example, under the scenario where the energy is sufficient and sustainable, the CJS should be employed to achieve a high BER at Eve. Under the scenario of SWIPT like [32]–[34], the non-jamming durations of IJS can be utilized to harvest energy so as to supply power during the jamming durations.

The IJS can be applied into all the above six cases due to the condition of $N_j^{E,th} < N_j^{\alpha,th}$. However, this condition does not hold for Case 7 and Case 8, where $N_j^{E,th}$ is higher than $N_j^{\alpha,th}$. Thus, CJS is necessary to combat Eve under these two cases.

V. Numerical Results and Analyses

In this section, we conduct simulation experiments to verify the feasibility and jamming efficiency of the IJS, then compare the performance of the IJS and the CJS to verify their applicability given in IV-C.

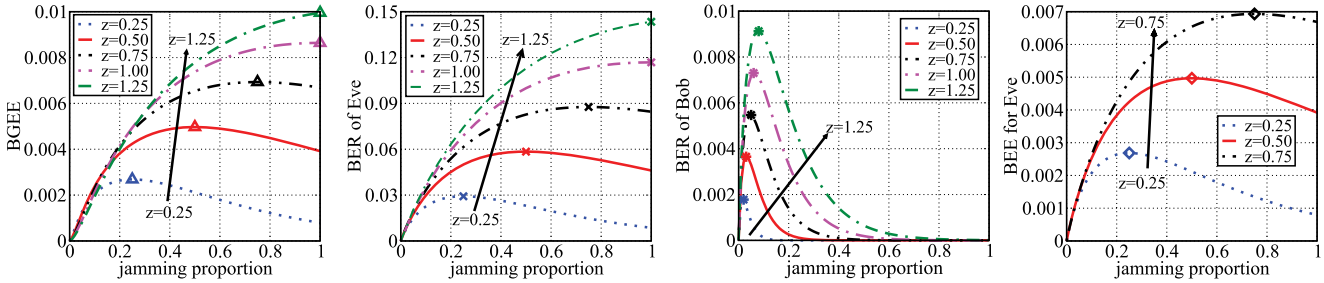
A. Performance Analyses Under the Case Without AWGN-Based Errors at Bob and Eve

We analyze the influence of α and N_j on the jamming power $P_J = N_j B_w$ on the jamming efficiency. According to (10), $\alpha^* < 1$ is given by the condition where $\frac{|h_{AE}|^2 E_b}{|h_{JE}|^2 N_j} > 0.709$. Thus, we set a parameter z as follows to reflect the value of

TABLE I

APPLICABILITY DISCUSSION IN TERMS WITH FEASIBLE DOMAIN OF N_j

Case Number	Conditions	IJS		CJS	
		N_j^{min}	N_j^{max}	N_j^{min}	N_j^{max}
1	$N_j^{E,th} < N_j^{tol,th} < N_j^{B,th} < N_j^{\alpha,th}$	$N_j^{E,th}$	$N_j^{tol,th}$	N/A	N/A
2	$N_j^{E,th} < N_j^{tol,th} < N_j^{\alpha,th} < N_j^{B,th}$	$N_j^{E,th}$	$N_j^{tol,th}$	N/A	N/A
3	$N_j^{E,th} < N_j^{B,th} < N_j^{tol,th} < N_j^{\alpha,th}$	$N_j^{E,th}$	$N_j^{B,th}$	N/A	N/A
4	$N_j^{E,th} < N_j^{B,th} < N_j^{\alpha,th} < N_j^{tol,th}$	$N_j^{E,th}$	$N_j^{B,th}$	N/A	N/A
5	$N_j^{E,th} < N_j^{\alpha,th} < N_j^{B,th} < N_j^{tol,th}$	$N_j^{E,th}$	$N_j^{\alpha,th}$	$N_j^{\alpha,th}$	$N_j^{B,th}$
6	$N_j^{E,th} < N_j^{\alpha,th} < N_j^{tol,th} < N_j^{B,th}$	$N_j^{E,th}$	$N_j^{\alpha,th}$	$N_j^{\alpha,th}$	$N_j^{tol,th}$
7	$N_j^{\alpha,th} < N_j^{E,th} < N_j^{tol,th} < N_j^{B,th}$	N/A	N/A	$N_j^{E,th}$	$N_j^{tol,th}$
8	$N_j^{\alpha,th} < N_j^{E,th} < N_j^{B,th} < N_j^{tol,th}$	N/A	N/A	$N_j^{E,th}$	$N_j^{B,th}$



(a) BGEE vs. α (b) BER of Eve vs. α (c) BER of Bob vs. α (d) BEE of Eve vs. α

Fig. 5. The influences of JDP and the jamming energy on the jamming efficiency.

jamming energy,

$$z = \frac{N_j}{|h_{AE}|^2 E_b/(0.709|h_{JE}|^2)}. \tag{10}$$

The jamming energy is proportional to the value of z.

1) Performance of Jamming Efficiency: As shown in Fig. 5(a), we measure the BGEE in (2) w.r.t. α under different values of z. Under cases of $z < 1$, BGEEs first increase and then decrease with the increasing of α. The maximum BGEEs are obtained at JDPs that are lower than 1, which refers to the IJS. Under cases of $z \geq 1$, BGEEs are proportional to α. The maximum BGEEs are achieved when $\alpha = 1$, which corresponds to the CJS. These results testify Proposition 1 and the applicability of the IJS and CJS given by IV-C. When the jamming energy is lower than the threshold calculated by $z = 1$, the IJS can obtain a higher jamming efficiency than the CJS. When it is greater than this threshold, the CJS outperforms the IJS. Furthermore, for a certain α, the larger the value of z, the higher the BGEE. Thus, a higher jamming energy is more benefit for jamming the eavesdropper on the basis of guaranteeing the reliable communication.

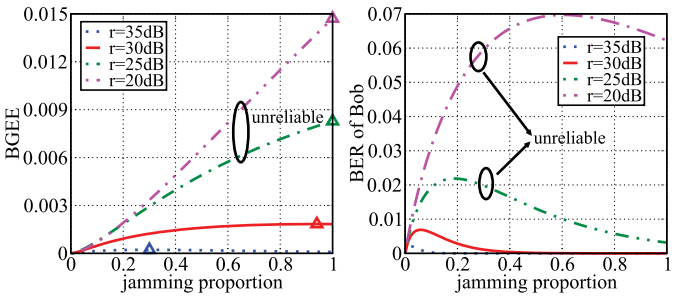
2) The Jamming Effect on Eve and Bob: The BER of Eve and that of Bob are shown in Fig. 5(b) and Fig. 5(c), respectively. Similar to Fig. 5(a), for a certain value of z less than 1, the BER of Eve first rises and then drops with the increase of α, as shown in Fig. 5(b). This verifies the Theorem 1 where the BER of Eve is a convex function w.r.t. α for each fixed N_j. When $z \geq 1$, the BER of Eve keeps increasing with the upticks of α. Under these cases, the maximum BERs of Eve are obtained when $\alpha = 1$, which indicate the CJS. Besides, for a specific value of α, the BER of Eve increases with the increasing of z. This is an intuitive result where more jamming energy is benefit for interfering the eavesdropper no matter how long the jamming process lasts.

TABLE II

OPTIMAL JAMMING PROPORTION FOR DIFFERENT METRICS

value \ z / items	0.25	0.50	0.75	1.00	1.25
$\alpha^*(\max \mathrm{p}_{\mathrm{e_B}}^{\mathrm{bpsk}})$	0.02	0.03	0.05	0.06	0.08
$\alpha^*(\max \mathrm{p}_{\mathrm{e_E}}^{\mathrm{bpsk}})$	0.25	0.50	0.75	1.00	1.00
$p_{e_B}^{bpsk}(10^{-6})$	0.238	0.476	0.714	0.925	1.190
$p_{e_E}^{bpsk}(10^{-1})$	0.292	0.584	0.876	1.169	1.432

As shown in Fig. 5(c), the BER of Bob is also a convex function of α. Compared with the BER of Eve shown by Fig. 5(b), the BER of Bob is much lower than that of Eve under the same value of z and α. To be specific, the JDPs that maximize $p_{e_B}^{bpsk}$ and $p_{e_E}^{bpsk}$ are denoted as $\alpha^*(\max p_{e_B}^{bpsk})$ and $\alpha^*(\max p_{e_E}^{bpsk})$, respectively. They are listed in the first two rows of Table II. In the last two rows of Table II, we give



(a) BGEE vs. α (b) BER of Bob vs. α

Fig. 6. The jamming efficiency with respect to α and E_b/N_0.

values of $p_{e_B}^{bpsk}$ and $p_{e_E}^{bpsk}$ with respect to $\alpha^*(\max p_{e_E}^{bpsk})$. We can see that $p_{e_B}^{bpsk}$ and $p_{e_E}^{bpsk}$ do not reach their maximum values at the same time. The $p_{e_B}^{bpsk}$ under $\alpha^*(\max p_{e_E}^{bpsk})$ is at the level of 10^{-6}, which satisfies the requirement of the reliable communication [41]. The $p_{e_E}^{bpsk}$ is much higher than $p_{e_B}^{bpsk}$ under $\alpha^*(\max p_{e_E}^{bpsk})$, which guarantees Eve cannot obtain correct legitimate messages. Thus, we can employ the value of $\alpha^*(\max p_{e_E}^{bpsk})$ as the optimal JDP to meet the demand of the reliable and secure communication.

3) The BEE of Eve Under IJS: Since we simplify the BGEE maximization problem as a BEE maximization problem in (3a), we simulate the BEE performance of Eve under the cases of IJS given by Fig. 5(d). We can see that the BEE is a convex function with respect to α, which is consistent with BGEE under the case of IJS. Furthermore, under each certain z, the value of α that maximizes BEE of Eve equals to the value that maximizes the BGEE. Thus, it is reasonable to transform the BGEE optimization problem to a BEE optimization problem.

B. Performance Analyses With Both AWGN-Based and Jamming-Based Errors at Bob and Eve

In this experiment, we set four different received signal-to-noise ratios (SNRs) at Eve, which are denoted as $r = |h_{AE}|^2 E_b/N_0 \in \{35dB, 30dB, 25\ dB, 20dB\}$. N_j is set as the threshold value given by $z = 1$ in the above subsection. Note that we fix $|h_{AE}|$, thus a lower r means a lower E_b/N_0. As shown in Fig. 6(a), when r is $r = 35dB$ or $r = 30dB$, the BGEE is a convex function with respect to α. This is the case of IJS and suggests that the given jamming energy is lower than the threshold calculated by (9). When r decreases into $r = 25dB$ or $r = 20dB$, the BGEE is an increasing function with respect to α and $\alpha^* = 1$. This indicates that the given jamming energy goes beyond the thresholds obtained from (9). Since the jamming energy is fixed in this experiment, the boundary thresholds for $\alpha^* < 1$ decrease with the decreasing of E_b/N_0. This is consistent with the phenomenon where v^* rises with the decreasing of E_b/N_0, which is shown by Fig. 3(b).

As shown in Fig. 6(b), the BER of Bob increases with the decreased SNRs. When the SNR is $r = 25dB$ and $r = 20dB$, the BER of Bob goes beyond the BER constraints (i.e., 10^{-6} [41])with respect to α^* that maximize BGEE. This is because when the SNR decreases to a certain value, the BER is very high even without jamming signals. In these cases, the reliable communication can not be guaranteed.

TABLE III

CALCULATIONS OF SER AT EVE AND THE IJS JAMMING ENERGY THRESHOLDS FOR DIFFERENT MODULATION METHODS

Modulation	SER	$N_{j,m}^{\alpha,th}$
BPSK	$\alpha Q\left(\sqrt{\frac{2\lvert h_{AE}\rvert^2 E_b}{\lvert h_{JE}\rvert^2 N_j/\alpha}}\right)$	N_{th}
MSK	$\alpha Q\left(\sqrt{\frac{1.7\lvert h_{AE}\rvert^2 E_b}{\lvert h_{JE}\rvert^2 N_j/\alpha}}\right)$	$0.68N_{th}$
GMSK	$\alpha Q\left(\sqrt{\frac{1.36\lvert h_{AE}\rvert^2 E_b}{\lvert h_{JE}\rvert^2 N_j/\alpha}}\right)$	$0.85N_{th}$
QPSK	$1-\left[1-\alpha Q\left(\sqrt{\frac{\lvert h_{AE}\rvert^2 E_b}{\lvert h_{JE}\rvert^2 N_j/\alpha}}\right)\right]^2$	$0.5N_{th}$
16QAM	$1-\left[1-\frac{3}{2}\alpha Q\left(\sqrt{\frac{4}{5}\frac{\lvert h_{AE}\rvert^2 E_b}{\lvert h_{JE}\rvert^2 N_j/\alpha}}\right)\right]^2$	$0.4N_{th}$
64QAM	$1-\left[1-\frac{7}{4}\alpha Q\left(\sqrt{\frac{2}{7}\frac{\lvert h_{AE}\rvert^2 E_b}{\lvert h_{JE}\rvert^2 N_j/\alpha}}\right)\right]^2$	$0.14N_{th}$

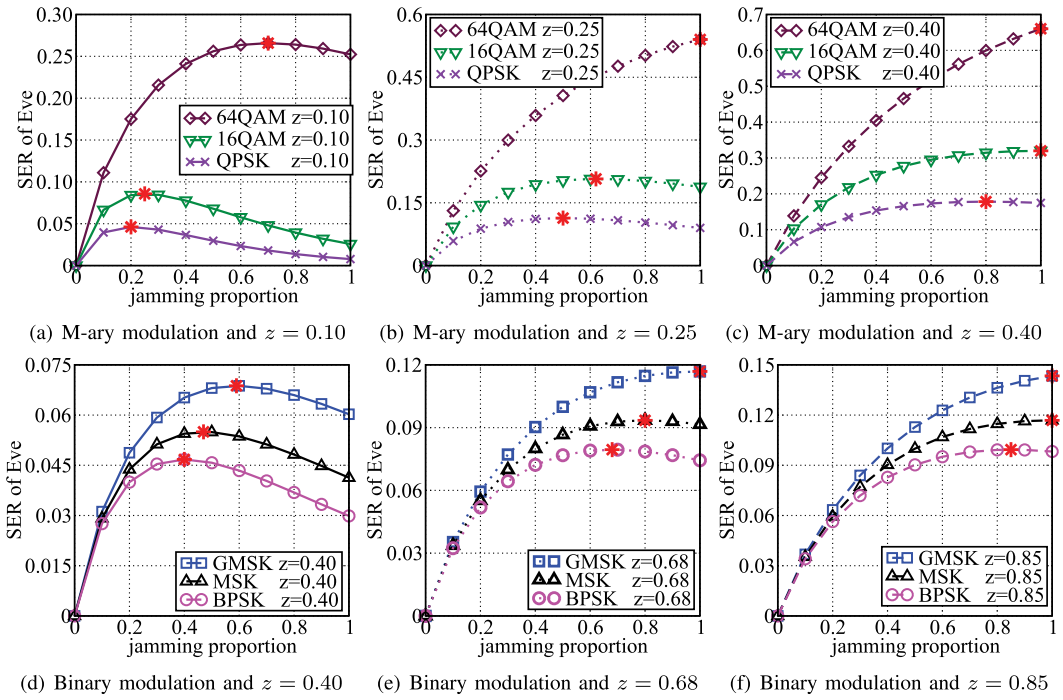
C. Performance Comparison of Different Modulation Methods

In this subsection, we simulate the jamming effect on Eve under different modulation methods, including the binary modulation (BM) methods and multi-ary modulation methods (MM). For BM methods besides the basic BPSK, we also consider the Minimum Frequency Shift Keying (MSK) which is one of the continuous phase frequency shift keying (CPFSK) methods and the Gaussian Filtering Minimum Frequency Shift Keying (GMSK) which has been widely used in 2G mobile communication systems. For MM methods, we consider the typical Quadrature Phase Shift Keying (QPSK) and the Quadrature Amplitude Modulation (QAM).

Since more than one bits are modulated into one symbol in MM methods, the symbol errors should be considered to measure the jamming effects. Thus, in this subsection, we employ the symbol error rate (SER) as our performance metric. Note that the SER of each BM method equals to its BER because one bit represents one symbol. The expressions of SERs for different modulation methods under the case without AWGN errors are shown in Table III.

As we can see from Fig. 7, for each modulation method, the error rate at Eve increases with z, because a higher z means a higher jamming power. For a same value of z, such as $z = 0.40$, the error rate of different modulation methods are in the ascending order as $p_{se_E}^{bpsk} < p_{se_E}^{msk} < p_{se_E}^{gmsk} < p_{se_E}^{qpsk} < p_{se_E}^{16qam} < p_{se_E}^{64qam}$. This is due to that the distances of the transmitted symbols for the latter modulation method are smaller than that for the former modulation method.

Furthermore, for a certain value of z, the optimal values of α^* vary from different modulation methods (w.r.t. α^* for each z, the maximum SERs are marked by red stars). This is because the jamming energy thresholds, denoted as $N_{j,m}^{\alpha,th}$, vary with each other. To be specific, the threshold of the BPSK is calculated as $N_{j,bpsk}^{\alpha,th} = \frac{|h_{AE}|^2 E_b}{0.709|h_{JE}|^2} = N_{th}$, thus,



(a) M-ary modulation and $z = 0.10$ (b) M-ary modulation and $z = 0.25$ (c) M-ary modulation and $z = 0.40$

(d) Binary modulation and $z = 0.40$ (e) Binary modulation and $z = 0.68$ (f) Binary modulation and $z = 0.85$

Fig. 7. The SER of Eve vs. α and N_j under different modulation methods.

$z = N_j/N_{th}$ according to (10). Similarly, we can compute the thresholds of other modulation methods, shown in the Table III. For each modulation method, if its jamming energy $N_j = zN_{th}$ is lower than the its threshold $N_{j,m}^{\alpha,th}$, the optimal value of α^* is less than 1, which indicates the IJS. While $N_j > N_{j,m}^{\alpha,th}$, α^* equals 1, which refers to the CJS. This result verifies the Proposition 1 is applicable for each one modulation method. That is, the IJS, under any modulation method, is preferable when the available jamming energy is lower than a specific threshold.

VI. Conclusion

In this paper, we first introduced the concept of the IJS, where a jammer alternates between jamming and non-jamming modes. Next, we studied the feasibility of the IJS for physical layer security, which, to the best of our knowledge, has not been addressed in the literature. We developed a new metric to jointly measure security requirements and energy cost. Then, we formulated an optimization problem with respect to JDP and jamming power. Based on the optimal JDP, we discussed the feasibility of the IJS. Finally, we examined the feasibility of the IJS through extensive simulation experiments under different modulation methods. The simulation results demonstrated that the BER of the eavesdropper under the IJS is higher than that of the CJS when less jamming energy is used. As a part of our future work, we will design and implement IJS based jamming schemes for different types of networks.

Appendix A
Proof of Theorem 1

Proof: We start with analyses on how the BER of Eve changes w.r.t. α. The first-order and the second-order derivative of $p_{e_E}^{bpsk}$ given in (7) w.r.t. α is computed as follows,

$$\frac{dp_{e_E}^{bpsk}}{d\alpha} = Q(v) - \frac{v}{2\sqrt{2\pi}}\exp\left(-\frac{v^2}{2}\right), \tag{11}$$

$$\frac{d^2p_{e_E}^{bpsk}}{d\alpha^2} = \frac{A}{4\sqrt{2\pi}}\exp(-\frac{v^2}{2})(v^2-3), = \begin{cases} <0, & v\in(0,\sqrt{3}), \\ =0, & v=\sqrt{3}, \\ >0, & v\in(\sqrt{3},+\infty), \end{cases} \tag{12}$$

where $A = \frac{2|h_{AE}|^2E_b}{|h_{JE}|^2N_j}$ and $v = \sqrt{A\alpha}$. Thus, we have

$$f(v) = \frac{dP_{e,E}^{bpsk}}{d\alpha} = \begin{cases} >0, & v<v^*, \\ =0, & v=v*=1.1906, \\ <0, & v>v^*. \end{cases} \tag{13}$$

which is shown in Fig. 3(a). Furthermore, the results of $f(v)$ w.r.t. the boundary values of α can be calculated as

$$f(v)|_{\alpha\to 0} = Q(0) = 0.5 > 0, \tag{14}$$

$$f(v)|_{\alpha=1} = Q(v) - \frac{v}{2\sqrt{2\pi}}\exp\left(-\frac{v^2}{2}\right)|_{v=\sqrt{A}} \tag{15}$$

$$= \begin{cases} \geq 0, & \sqrt{A}\leq 1.1906, \\ <0, & \sqrt{A}>1.1906. \end{cases} \tag{16}$$

Since $0 < \alpha \leq 1$, we have $v \in (0, \sqrt{A}]$. For the case of $\sqrt{A} \leq 1.1906$, we can see that $v \in (0, \sqrt{A}] \subset (0, \sqrt{3}]$. Under this case, the first order derivative is always positive though continually decreases due to the negative second order derivative. Thus, $p_{e_E}^{bpsk}$ is still gradually increasing with the increases of α and the maximum value is obtained when $\alpha = 1$. For the case of $\sqrt{A} > 1.1906$, $f(v)$ is changing from

positive to negative with only one zero point $f(v^*)=0$ w.r.t. the domain of $\alpha \in (0,1]$ either when $\sqrt{A} < \sqrt{3}$ or when $\sqrt{A} > \sqrt{3}$. Thus, there is only one optimal value which is calculated as α^* by substituting v^* into the expression of v.

APPENDIX B
PROOF OF THEOREM 2

Proof: Similar to the proof of Theorem 1, we calculate the first-order derivative of $p_{e_E}^{bpsk}$ w.r.t. α as follows,

$$\begin{aligned}\frac{dp_{e_E}^{bpsk}}{d\alpha} &= Q(v) - \frac{v}{2\sqrt{2\pi}}\exp\left(-\frac{v^2}{2}\right) \\ &\quad + \frac{N_0}{2|h_{AE}|^2E_b}\frac{v^3}{2\sqrt{2\pi}}\exp\left(-\frac{v^2}{2}\right) \\ &\quad - Q\left(\sqrt{\frac{2|h_{AE}|^2E_b}{N_0}}\right), \\ &= f(v), \end{aligned} \tag{17}$$

where $v=\sqrt{\frac{2B}{C/\alpha+1}}$, $B=\frac{|h_{AE}|^2E_b}{N_0}$, and $C=\frac{N_j|h_{JE}|^2}{N_0}$. The derivation functions with different values of E_b/N_0 and the value of v^* for $f(v^*)=0$ are illustrated in Fig. 3(b).

Then we can compute the second-order derivative function as

$$\frac{d^2p_{e_E}^{bpsk}}{d\alpha^2} = \frac{df(v)}{dv}\frac{dv}{d\alpha}, \tag{18}$$

where $\frac{dv}{d\alpha}>0$ and $\frac{df(v)}{dv}$ is detailed as follows,

$$\begin{aligned}\frac{df(v)}{dv} &= \frac{1}{2\sqrt{2}\pi}\exp\left(-\frac{v^2}{2}\right)\left(-3+v^2+\frac{3}{2B}v^2-\frac{1}{2B}v^4\right), \\ &= \frac{\exp\left(-\frac{v^2}{2}\right)}{4B\sqrt{2}\pi}\left[\left(B-\frac{3}{2}\right)^2-\left(v^2-\frac{3+2B}{2}\right)^2\right], \\ &= \begin{cases} <0, & \begin{cases}\text{for} \quad v^2\in(0,2B), & \text{if} \quad B<\frac{3}{2}, \\ \text{for} \quad v^2\in(0,3), & \text{if} \quad B>\frac{3}{2}, \end{cases} \\ >0, & \text{for} \quad v^2\in(3,2B), \text{if} \quad B>\frac{3}{2}. \end{cases} \end{aligned} \tag{19}$$

Since $\alpha\in(0,1]$, we have $v\in(0,\sqrt{\frac{2B}{C+1}}]\subset(0,\sqrt{2B})$. For the case of $B<\frac{3}{2}$, the second-order derivative is always negative on the definition domain, thus, the first-order derivative is a decreasing function of α and is calculated as

$$f(v)=\begin{cases} >0, & \begin{cases} v\in(0,\sqrt{2B}), & \text{if} \quad v^*>\sqrt{2B}, \\ v\in(0,v^*), & \text{if} \quad v^*<\sqrt{2B}, \end{cases} \\ <0, & v\in(v^*,\sqrt{2B}), \text{if} \quad v^*<\sqrt{2B}. \end{cases} \tag{20}$$

When $v^*>\sqrt{2B}$, the $f(v)$ is always positive, thus $p_{e_E}^{bpsk}$ is an increase function on the definition domain and its the maximum value is obtained when $\alpha=1$. When $v^*<\sqrt{2B}$, $f(v)$ decreases from a positive value to a negative value, thus, the $p_{e_E}^{bpsk}$ first increases and then decreases. The maximum value of $p_{e_E}^{bpsk}$ is just obtained when $f(v)=0$ and the optimal value of α is computed by via v^*.

For the case of $B>\frac{3}{2}$, the second order derivative is first lower then higher than zero, thus, the first order derivative first decreases then increases, where the zero point must be located at the decreasing domain, that is, $v^*<\sqrt{3}$. This is consistent with the results shown in Fig. 3(b) for the three cases of $E_b/N_0=\{0dB,10dB,20dB\}$. Specifically, $f(v)$ decreases from a positive value to the lowest negative value at the point of $v=\sqrt{3}$ then continues to increase with the increasing of v. The right boundary value is negative as follows,

$$f(v)|_{\alpha=1}=f(\sqrt{\frac{2B}{C+1}})<f(\sqrt{2B})=0. \tag{21}$$

Correspondingly, the $p_{e_E}^{bpsk}$ first increases to the highest point corresponding to α^* that is obtained via v^* and then decreases. Therefore, under this case, we have $0<v^*<\sqrt{3}<\sqrt{2B}$ and the optimal value of α is α^*.

In summary, for a certain B, if $v^*<\sqrt{2B}$, the optimal value of α is α^* corresponding to v^* and otherwise, the optimal value of α is 1. Furthermore, this threshold is tightened as $v^*<\sqrt{\frac{2B}{C+1}}$ to satisfy the requirement of $\alpha^*\le 1$, as shown in Theorem 2.

REFERENCES

[1] X. Tang, Y. Cai, W. Yang, W. Yang, D. Chen, and J. Hu, "Secure transmission of cooperative zero-forcing jamming for two-user SWIPT sensor networks," *Sensors*, vol. 18, no. 2, p. 331, 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/2/331

[2] S. Cheng, Z. Cai, J. Li, and H. Gao, "Extracting kernel dataset from big sensory data in wireless sensor networks," *IEEE Trans. Knowl. Data Eng.*, vol. 29, no. 4, pp. 813–827, Apr. 2017.

[3] L. Hu *et al.*, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Feb. 2018.

[4] Z. Xu, X. Zhu, and L. Gui, "Security technology of smart home based on Internet of Things," in *Proc. Int. Conf. Elect., Control, Automat. Eng. (ECAE)*, Dec. 2013, pp. 536–540.

[5] D. Jackson and P. Hayes, "Ensuring security of data and information flow in emergency response decision support," in *Proc. ARES*, Aug. 2016, pp. 792–797.

[6] M. Casoni and A. Paganelli, "Security issues in emergency networks," in *Proc. IWCMC*, Jul. 2011, pp. 2145–2150.

[7] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[8] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[9] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[10] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, to be published.

[11] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 148–153, Feb. 2018.

[12] Q. Gao *et al.*, "Optimal stopping theory based jammer selection for securing cooperative cognitive radio networks," in *Proc. GLOBECOM*, Dec. 2016, pp. 1–6.

[13] Z. Li, T. Jing, X. Cheng, Y. Huo, W. Zhou, and D. Chen, "Cooperative jamming for secure communications in MIMO cooperative cognitive radio networks," in *Proc. IEEE ICC*, Jun. 2015, pp. 7609–7614.

[14] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, vol. 2. New York, NY, USA: McGraw-Hill, 1994.

[15] R. Poisel, *Modern Communications Jamming Principles and Techniques*. Norwood, MA, USA: Artech House, 2011.

[16] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[17] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2005, pp. 1501–1506.

[18] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.

[19] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7495–7505, Aug. 2017.

[20] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[21] Q. Gao *et al.*, "Joint design of jammer selection and beamforming for securing MIMO cooperative cognitive radio networks," *IET Commun.*, vol. 11, no. 8, pp. 1264–1274, 2017.

[22] H. Ma, J. Cheng, X. Wang, and P. Ma, "Robust MISO beamforming with cooperative jamming for secure transmission from perspectives of QoS and secrecy rate," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 767–780, Feb. 2018.

[23] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Lab. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, 1984.

[24] H. Long, W. Xiang, and Y. Li, "Precoding and cooperative jamming in multi- antenna two-way relaying wiretap systems without eavesdropper's channel state information," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1309–1318, Jun. 2017.

[25] H. Ma, J. Cheng, and X. Wang, "Cooperative jamming aided robust beamforming for MISO channels with unknown eavesdroppers," in *Proc. GLOBECOM*, Dec. 2017, pp. 1–5.

[26] D. Wang, P. Ren, Q. Du, L. Sun, and Y. Wang, "Security provisioning for MISO vehicular relay networks via cooperative jamming and signal superposition," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10732–10747, Dec. 2017.

[27] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R.-F. Liao, "Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2108–2117, Mar. 2018.

[28] M. Dehghan, D. L. Goeckel, M. Ghaderi, and Z. Ding, "Energy efficiency of cooperative jamming strategies in secure wireless networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3025–3029, Sep. 2012.

[29] F. Gabry, A. Zappone, R. Thobaben, E. A. Jorswieck, and M. Skoglund, "Energy efficiency analysis of cooperative jamming in cognitive radio networks with secrecy constraints," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 437–440, Aug. 2015.

[30] Y. Wen, T. Jing, Y. Huo, Z. Li, and Q. Gao, "Secrecy energy efficiency optimization for cooperative jamming in cognitive radio networks," in *Proc. ICNC*, Mar. 2018, pp. 795–799.

[31] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 3, pp. 1281–1293, Jul. 2016.

[32] H. Chen, C. Zhai, Y. Li, and B. Vucetic, "Cooperative strategies for wireless-powered communications: An overview," *IEEE Wireless Commun.*, vol. 25, no. 4, pp. 112–119, Aug. 2018.

[33] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 621–634, Mar. 2019.

[34] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless powered cooperative jamming for secure OFDM system," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1331–1346, Feb. 2018.

[35] L.-G. Tran, H.-K. Cha, and W.-T. Park, "RF power harvesting: A review on designing methodologies and applications," *Micr. Nano Syst. Lett.*, vol. 5, no. 1, pp. 1–16, Dec. 2017.

[36] K. Pelechrinis, M. Iliofotou, and S. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 245–257, May 2011.

[37] G. Chen and W. Dong, "JamCloak: Reactive jamming attack over cross-technology communication links," in *Proc. ICNP*, Sep. 2018, pp. 34–43.

[38] Y. Liu and P. Ning, "BitTrickle: Defending against broadband and high-power reactive jamming attacks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 909–917.

[39] Y. Allouche *et al.*, "Secure communication through jammers jointly optimized in geography and time," *Pervasive Mobile Comput.*, vol. 41, pp. 83–105, Oct. 2015.

[40] J. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2008.

[41] T. S. Rappaport, *Wireless Communications: Principles Practices*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 1996.

[42] F. Zhu and M. Yao, "Improving physical-layer security for CRNs using SINR-based cooperative beamforming," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1835–1841, Mar. 2016.

[43] S. Wenbo, "Research on physical layer security schemes based on cooperative wireless communication," in *Proc. ICMTMA*, Jun. 2015, pp. 888–891.

[44] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 740–752, Jan. 2016.

[45] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[46] L. Tang, H. Chen, and Q. Li, "Social tie based cooperative jamming for physical layer security," *IEEE Commun. Lett.*, vol. 19, no. 10, pp. 1790–1793, Oct. 2015.

[47] L. Zhang *et al.*, "The performance of the MIMO physical layer security system with imperfect CSI," in *Proc. CNS*, Oct. 2016, pp. 346–347.

Qinghe Gao received the B.E. degree in communication engineering from North China Electric Power University, Baoding, in 2013. She is currently pursuing the Ph.D. degree in communication and information system with Beijing Jiaotong University. She was a Visiting Scholar with the Department of Computer Science, George Washington University, from 2015 to 2017. Her research interests include cognitive radio networks, physical layer security, and energy harvesting.

Yan Huo (M'12) received the B.E. and Ph.D. degrees in communication and information system from Beijing Jiaotong University, Beijing, China, in 2004 and 2009, respectively. He has been a Faculty Member with the School of Electronics and Information Engineering, Beijing Jiaotong University, since 2011, where he is currently a Professor. His current research interests include wireless communication theory, the Internet of Things, security and privacy, cognitive radio, and signal processing.

Tao Jing received the M.S. and Ph.D. degrees from the Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, in 1994 and 1999, respectively. He is currently a Professor with the School of Electronics and Information Engineering, Beijing Jiaotong University, China. His current research interests include capacity analysis, spectrum prediction and resource management in cognitive radio networks, RFID in intelligent transporting systems, and smart phone application.

Liran Ma received the D.Sc. degree in computer science from George Washington University. He is currently an Associate Professor with the Department of Computer Science, Texas Christian University. His current research focuses on wireless, mobile, and embedded systems, including security and privacy, smartphones, smart health, mobile computing, data analytics, the Internet of Things, and cloud computing. It involves building and simulating prototype systems and conducting real experiments and measurements.

Yingkun Wen received the B.S. degree from North China Electric Power University, Baoding, China, in 2015. He is currently pursuing the Ph.D. degree with the School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China. His current research interests include cognitive radio networks, physical layer security, and cooperative communication.

Xiaoshuang Xing received the Ph.D. degree in communication and information systems from Beijing Jiaotong University in 2014. She is currently an Associate Professor with the School of Computer Science and Engineering, Changshu Institute of Technology. Her current research interests include physical layer security, vehicular networks, the IoT networks, and spectrum prediction.