Selective Modulation and Cooperative Jamming for Secure Communication in Untrusted Relay Systems

Li Huang(✉), Xiaoxu Wu, and Hang Long

Beijing University of Posts and Telecommunications, Beijing, China
huangliqiaoyi@163.com

Abstract. In this paper, an innovative secure communication scheme for untrusted relay systems is proposed. The source and jamming signals are jointly designed based on the selective modulation. The source signal adopts selective modulation, composed of one selection bit and one or more signal bits. The selection bit is employed to carry confidential information, while the signal bits are generated randomly and are modulated the random signal. The selection bit determines the transmit slot/frequency of signal bits, namely, the random signal. The design of the cooperative jamming signal includes two parts, adjusting the signal transmit power and rotating the signal phase. The simulation results demonstrate that our proposed scheme can make the bit error ratio of the selection bit at the untrusted relay to be 0.5. That is, there is no confidential information leakage at the relay node. Besides, the proposed scheme is superior to the Gaussian jamming signal in terms of the secrecy capacity.

Keywords: Physical layer security · Cooperative systems · Selective modulation

1 Introduction

In wireless communication systems, propagation paths are severely affected by the environment. As a result, the signal fading is more obvious and the performance of direct link is relatively terrible. With the collaboration of relays, the communication performance can be improved and the communication range can be expanded. Meanwhile, the transmissions in wireless networks have broadcast nature, which makes transmitted information more vulnerable to be eavesdropped.

In cooperative relay systems, the relay nodes are commonly assumed to be trusted. During the transmission, the relay is responsible for amplifying and forwarding the signal [1,2] or serving as a cooperative jamming node to interference

Supported by National Nature Science Foundation of China (NSFC) Project 61931005.

H. Gao et al. (Eds.): ChinaCom 2021, LNICST 433, pp. 351–365, 2022.
https://doi.org/10.1007/978-3-030-99200-2_27

the eavesdropper [3–5]. Nevertheless, the relay may be a potential eavesdropper, intercepting confidential information. Thus, studying the security of untrusted relay systems is extremely significant.

Ref. [6–13] have researched untrusted relay systems, where the source and the destination nodes exchange information through untrusted relays. In 2007, Oohama took the lead in studying relay channel coding to prevent wiretapping [6]. The destination node is employed to send cooperative jamming signals, proving that the positive secrecy rate is achievable in [7]. A novel beamforming design is proposed in [8], directing the cooperative jamming signal to an untrusted relay. The authors of [9] propose a joint design for the precoding of useful and jamming signals to maximize the secrecy capacity. Besides the precoding at source and destination nodes, the precoding at relay is also designed to maximize the secrecy rate in [10].

The existing works mostly adopt the secrecy capacity or the secrecy rate or the secrecy outage probability to estimate the security of untrusted relay systems [6–10]. In addition, Ref. [11–13] adopt the bit error rate (BER) and the symbol error rate (SER) as evaluation criteria. In [11], the BER at the untrusted relay can approximate 0.5 by employing a greedy algorithm. The authors of [12] consider designing the amplitude and phase of the jamming signal. The simulation results demonstrate that the SER at the trusted relay will approach 15/16 while the signal-to-noise ratio (SNR) is greater than 25 dB. Ref. [13] proposes a constellation rotation aided scheme to prevent eavesdropping. However, there are some deficiencies in these schemes. The greedy algorithm complexity is high [11], the required SNR is comparatively high [12] and a certain amount of confidential information may be intercepted at untrusted relay [13].

In this paper, selective modulation is proposed to improve the security combined with cooperative jamming. Selective modulation refers to extending the source signal by one dimension. The source signal is composed of one selection bit and signal bits, where the selection bit carries confidential information and determine the transmit time/frequency of signal bits; signal bits are used to bear the random signal and do not carry useful information. The cooperative jamming signal is designed according to channel state information (CSI). The main contributions of this paper can be summarized as follows:

(1) Different from existing signal designs in untrusted relay systems, the source signal adopts selective modulation by extending the signal dimension to transmit confidential information.
(2) The selective modulated source signal and cooperative jamming are jointly designed to realize zero confidential information leakage at the untrusted relay. The algorithm complexity is decreased compared with [11]; the required SNR is reduced compared with [12] and in contrast to [13], confidential information leakage at untrusted relay is completely suppressed.

The remainder of this paper is organized as follows. In Sect. 2, the untrusted relay system model with destination-aided cooperative jamming is presented. Section 3 presents the proposed selective modulation and cooperative jamming.

The security scheme design without leakage is proposed in Sect. 4. Section 5 provides simulation results and conclusions are drawn in Sect. 6.

Notation: $\mathcal{E}(\cdot)$ denotes mathematical expectation. P(A) is the probability that the event A occurs. min(·) is the minimum function.

2 System Model

As described in Fig. 1, there is a two-hop untrusted relay system based on cooperative jamming. The system consists of a source node S, a destination node D and an untrusted relay node R. S and D solely communicate under the collaboration of R. R amplifies and forwards the received information without altering it. Besides, R acts as a potential eavesdropper, intercepting confidential information. Define the S-R, R-S, R-D and D-R channels as h_{SR}, h_{RS}, h_{RD} and h_{DR}, respectively.

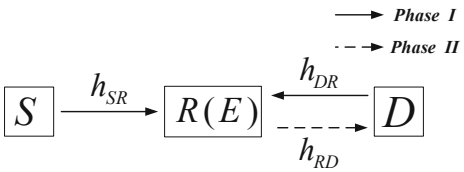

Fig. 1. Untrusted relay system with destination-aided cooperative jamming.

Assuming that a typical two-phase protocol is adopted. In the first phase, S sends the signal x_S to R with the transmit power P_S, while D cooperates in sending jamming signals with the transmit power P_J. Thus, the received signal at untrusted relay R is obtained as

$$y_R = \sqrt{P_S} h_{SR} x_S + \sqrt{P_J} h_{DR} J_D + n_R, \tag{1}$$

where x_S is the signal transmitted by S, J_D is the jamming signal sent by D, and $n_R \sim \mathcal{CN}(0, \sigma_R^2)$ is the noise at R.

In the second phase, R amplifies and forwards the received signal

$$x_R = \beta y_R, \tag{2}$$

where β is the power constraint coefficient at R, and the power of R is constrained by $\mathcal{E}(x_R^H x_R) = P_R$.

The signal received at D is

$$y_D = h_{RD} x_R + n_D, \tag{3}$$

where $n_D \sim \mathcal{CN}(0, \sigma_D^2)$ is the additive noise at D.

After receiving the signal, D can cancel the jamming signal using self-interference cancellation. Thus, the performance of the legitimate node is almost unaffected by jamming signals.

3 Selective Modulation and Cooperative Jamming

In this section, we propose the selective modulation for the source signal and analyze the security of untrusted relay systems based on selective modulation and cooperative jamming.

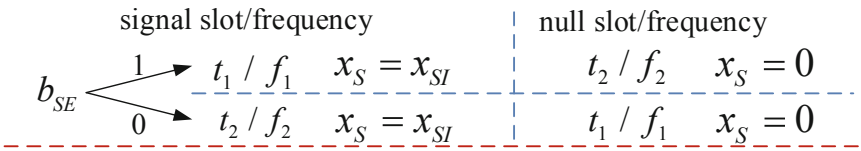

Fig. 2. Selective modulation.

The selective modulation refers to the fact that the source signal is extended by one dimension and the extended dimension can be time, frequency. The source signal bits are divided into two parts, one selection bit b_{SE} and one or more signal bits b_{SI}. As for signal bits b_{SI}, they are generated randomly without protected information. Assuming signal bits b_{SI} are modulated into the random signal x_{SI}. The selection bit b_{SE} is used to select the transmitted time/frequency of signal bits b_{SI}, namely, the random signal x_{SI}.

It is worth noting that only the selection bit b_{SE} bears confidential information in our proposed scheme. The signal bits b_{SI} are merely applied to carry the random signal x_{SI}, preventing the untrusted relay from eavesdropping on the selection bit b_{SE}.

As depicted in Fig. 2, S generates one selection bit b_{SE} to determine the transmitted slot/frequency of the random signal x_{SI}. S only selects one slot/frequency to send the random signal in every two slots/frequencies, and a null signal is transmitted at the other slot/frequency, that is, to send nothing. Assuming that if $b_S = 1$, the modulated signals x_S sent by S are x_{SI} and 0 at two slots t_1 and t_2 or at two frequencies f_1 and f_2, respectively. If $b_S = 0$, x_S are 0 and x_{SI} at t_1 and t_2 or f_1 and f_2.

According to whether S sends the random signal or not, the transmitted slots/frequencies are divided into signal slot/frequency and null slot/frequency. That is, if $b_S = 1$, t_1/f_1 is signal slot/frequency and t_2/f_2 is null slot/frequency; if $b_S = 0$, t_2/f_2 is signal slot/frequency and t_1/f_1 is null slot/frequency.

Figure 3 describes the system model with selective modulation and jamming signal, including signal slot/frequency in Fig. 3(a) and null slot/frequency in Fig. 3(b). The source signal adopts selective modulation, while the jamming signal is sent by the destination node D at each slot/frequency.

As shown in Fig. 3(a), at signal slot/frequency, $x_S = x_{SI}$. With (1), in the first phase, the received signal at R is

$$y_{RS} = \sqrt{P_S} h_{SR} x_{SI} + \sqrt{P_J} h_{DR} J_{DS} + n_{RS}, \tag{4}$$

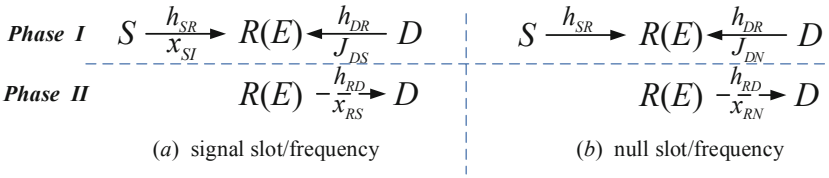

Fig. 3. System with selective modulation and cooperative jamming.

where x_{SI} is the signal transmitted by S with $\mathcal{E}(x_{SI}^H x_{SI}) = 1$, J_{DS} is the jamming signal sent by D with $\mathcal{E}(J_{DS}^H J_{DS}) = 1$, and $n_{RS} \sim \mathcal{CN}(0, \sigma_R^2)$ is the noise at R.

With (2), at signal slot/frequency, R amplifies and forwards the received signal

$$x_{RS} = \beta y_{RS}. \tag{5}$$

Similarly, at null slot/frequency, $x_S = 0$, as shown in Fig. 3(b). The received signal at R is

$$y_{RN} = \sqrt{P_J} h_{DR} J_{DN} + n_{RN}, \tag{6}$$

where J_{DN} is the jamming signal with $\mathcal{E}(J_{DN}^H J_{DN}) = 1$, and $n_{RN} \sim \mathcal{CN}(0, \sigma_R^2)$.

With (2), at null slot/frequency, R amplifies and forwards the received signal

$$x_{RN} = \beta y_{RN}. \tag{7}$$

According to (2), β can be expressed as

$$\begin{aligned} \beta &= \sqrt{\frac{2P_R}{E\left(y_{RS}^H y_{RS}\right) + E\left(y_{RN}^H y_{RN}\right)}} \\ &= \sqrt{\frac{2P_R}{E\left(h_{SR}^H h_{SR}\right) P_S + 2E\left(h_{DR}^H h_{DR}\right) P_J + 2\sigma_R^2}}. \end{aligned} \tag{8}$$

Assuming that the channel fading is relatively slow and CSI remains identical during two slots/frequencies. According to (4), at signal slot/frequency, the equivalent received signal at R is

$$y'_{RS} = \frac{y_{RS}}{\sqrt{P_S} h_{SR}} = x_{SI} + \frac{\sqrt{P_J} h_{DR}}{\sqrt{P_S} h_{SR}} J_{DS} + \frac{n_{RS}}{\sqrt{P_S} h_{SR}}. \tag{9}$$

With (6), at null slot/frequency, the equivalent received signal at R is

$$y_{RN}{}' = \frac{y_{RN}}{\sqrt{P_S} h_{SR}} = \frac{\sqrt{P_J} h_{DR}}{\sqrt{P_S} h_{SR}} J_{DN} + \frac{n_{RN}}{\sqrt{P_S} h_{SR}}. \tag{10}$$

Define the ratio of the amplitude of the cooperative jamming signal to that of the source signal at the untrusted relay as

$$a = \left| \frac{\sqrt{P_J} h_{DR}}{\sqrt{P_S} h_{SR}} \right|, \tag{11}$$

and the phase difference between the D-R and S-R channels is

$$\theta = \text{angle}\left(\frac{h_{DR}}{h_{SR}}\right). \tag{12}$$

Based on (9), (10), (11) and (12), y'_{RS} and y'_{RN} can be rewritten as

$$y'_{RS} = x_{SI} + a\mathrm{e}^{j\theta} J_{DS} + n'_{RS}, \tag{13}$$

$$y_{RN}{}' = a\mathrm{e}^{j\theta} J_{DN} + n'_{RN}, \tag{14}$$

where n'_{RS}, n'_{RN} are the equivalent noise at R, $n_{RS}, n_{RN} \sim \mathcal{CN}\left(0, \sigma^2\right)$, $\sigma^2 = \sigma_R^2 / \left(P_S |h_{SR}|^2\right)$.

In general, the receiver judges the slot/frequency with higher power as the slot/frequency where the signal is sent. This signal demodulation method is simple. The proposed selective modulation aims to decrease the complexity of communication systems. Thus, the untrusted relay and the destination node adopt this signal demodulation method in this paper.

If the power magnitude of the received signal at R is uncertain at signal and null slots/frequencies, so that the untrusted relay cannot distinguish signal slot/frequency. Therefore, the probability of R guessing the signal slot/frequency correctly is 0.5, that is, BER of the selection bit at R is 0.5.

According to (13) and (14), the power of equivalent signals at the untrusted relay R are $\left|x_{SI} + a\mathrm{e}^{j\theta} J_{DS} + n_{RS}{}'\right|^2$ and $\left|a\mathrm{e}^{j\theta} J_{DN} + n_{RN}{}'\right|^2$ at signal and null slots/frequencies, respectively.

Compared with null slot/frequency, if the probability of the equivalent signal at R with higher and lower power at signal slot/frequency is equal, the error probability of R distinguishing signal slot/frequency will be 0.5. That is, the BER of the selection bit at R is 0.5. Under this condition, zero secret information leakage can be achieved at untrusted relay R.

On this basis, the joint design of the source signal and the jamming signal is proposed in next sections. It aims to make the power of signals received by R at signal and null slots/frequencies satisfy

$$\begin{aligned} &\mathrm{P}\left(\left|x_{SI} + a\mathrm{e}^{j\theta} J_{DS} + n_{RS}{}'\right|^2 > \left|a\mathrm{e}^{j\theta} J_{DN} + n_{RN}{}'\right|^2\right) \\ &= \mathrm{P}\left(\left|x_{SI} + a\mathrm{e}^{j\theta} J_{DS} + n_{RS}{}'\right|^2 < \left|a\mathrm{e}^{j\theta} J_{DN} + n_{RN}{}'\right|^2\right). \end{aligned} \tag{15}$$

4 Security Scheme Design

The previous section presents the system security analysis with selective modulation and cooperative jamming. To achieve absolute secure communication, the BER of the selection bit at R is required to be 0.5. The magnitude of received signals power at R must be uncertain between signal and null slots/frequencies. The signal power at signal slot/frequency is related to the random signal, the

jamming signal and noise, while the signal power at null slot/frequency is solely related to jamming signal and noise.

In this section, the random signal x_{SI} and the jamming signal J_D are designed jointly on the basis of the system security analysis. Furthermore, the security scheme design without leakage is proposed.

4.1 Signal Design Based on MPSK

As for selective modulation, we find that MPSK is optimal to improve the security compared with amplitude shift keying (ASK) and quadrature amplitude modulation (QAM). Assuming that the random and jamming signals are MPSK modulated. The random signal x_{SI} is M_1PSK modulated,

$$x_{SI} = \mathrm{e}^{j\theta_S},$$

where $M_1 = 2^{n_1}$, $n_1 = 1, 2, 3, 4...$, θ_S is the phase of x_{SI}, $\theta_S = (2l_1 - 1)\,\pi/M_1$, $l_1 \in \{1, 2, 3...M_1\}$.

The jamming signal J_D is M_2PSK modulated,

$$J_D = \mathrm{e}^{j\theta_D},$$

where $M_2 = 2^{n_2}$, $n_2 = 1, 2, 3, 4...$, θ_D is the phase of J_D, $\theta_D = (2l_2 - 1)\,\pi/M_2$, $l_2 \in \{1, 2, 3...M_2\}$.

For brevity of exposition, we define

$$M_0 = \max\left(M_1, M_2\right). \tag{16}$$

The complex Gaussian noise may be complicated to analyze. Without loss of generality, theoretical analysis ignores the noise received at R but simulation results consider the effect of noise. Thus, the signals power received by R are simplified as $\left|x_{SI} + a\mathrm{e}^{j\theta}J_{DS}\right|^2$ at signal slot/frequency and $\left|a\mathrm{e}^{j\theta}J_{DN}\right|^2$ or a^2 at null slot/frequency. Based on (15), if the complex Gaussian noise is not considered, the condition for zero confidential information leakage at R is

$$\mathrm{P}\left(\left|x_{SI} + a\mathrm{e}^{j\theta}J_{DS}\right|^2 > a^2\right) = \mathrm{P}\left(\left|x_S + a\mathrm{e}^{j\theta}J_{DS}\right|^2 < a^2\right), \tag{17}$$

where J_{DS} is the cooperative jamming signal sent by D and have the same distribution as J_D. Thus, we have $J_{DS} = J_D$. Without the noise being considered, at signal slot/frequency, the signal power received by R can be expressed as

$$\begin{aligned}\left|x_{SI} + a\mathrm{e}^{j\theta}J_{DS}\right|^2 &= \left(x_{SI} + a\mathrm{e}^{j\theta}J_D\right)\left(x_{SI} + a\mathrm{e}^{j\theta}J_D\right)^{\mathrm{H}} \\ &= x_{SI}x_{SI}^H + \left(a\mathrm{e}^{j\theta}J_D\right)\left(a\mathrm{e}^{j\theta}J_D\right)^{\mathrm{H}} + x_{SI}\left(a\mathrm{e}^{j\theta}J_D\right)^{\mathrm{H}} + a\mathrm{e}^{j\theta}J_Dx_{SI}^H \\ &= 1 + a^2 + a\mathrm{e}^{j\theta_S-\theta-\theta_D} + a\mathrm{e}^{j\theta+\theta_D-\theta_S} \\ &= 1 + a^2 + 2a\cos\left(\theta_S - \theta_D - \theta\right).\end{aligned} \tag{18}$$

Since the random signal x_{SI} is M_1PSK, the period of θ_S is $2\pi/M_1$. Similarily, the period of θ_D is $2\pi/M_2$ as for jamming signal J_D. Thus, x_{SI} and J_D can be expressed as followed:

$$x_{SI} = \mathrm{e}^{j(\theta_S + 2\pi/M_1)}, \tag{19}$$

$$J_D = \mathrm{e}^{j(\theta_D - 2\pi/M_2)}. \tag{20}$$

Substituting (19) or (20) for (18), the signal power at signal slot/frequency can be rewritten as

$$\begin{aligned} \left|x_{SI} + a\mathrm{e}^{j\theta} J_{DS}\right|^2 &= 1 + a^2 + 2a\cos\left(\theta_S - \theta_D - \theta + 2\pi/M_1\right) \\ &= 1 + a^2 + 2a\cos\left(\theta_S - \theta_D - \theta + 2\pi/M_2\right). \end{aligned} \tag{21}$$

Comparing (18) with (21), it can be shown that the signal power at signal slot/frequency is a periodic function of the channel phase difference θ. If $M_1 \neq M_2$, the minimum positive period of θ is

$$\min\left(\frac{2\pi}{M_1}, \frac{2\pi}{M_2}, \left|\frac{2\pi}{M_1} - \frac{2\pi}{M_2}\right|\right) = \frac{2\pi}{M_0}; \tag{22}$$

if $M_1 = M_2 = M_0$, the minimum positive period is

$$\min\left(\frac{2\pi}{M_1}, \frac{2\pi}{M_2}\right) = \frac{2\pi}{M_0}. \tag{23}$$

According to the characteristics of MPSK modulation, if the signal phase is reversed, it is still MPSK. Thus, x_{SI} and J_D can be expressed as $x_{SI} = \mathrm{e}^{-j\theta_S}$, $J_D = e^{-j\theta_D}$. Integrating them into (18), we can obtain the expression

$$\begin{aligned} \left|x_{SI} + a\mathrm{e}^{j\theta} J_{DS}\right|^2 &= 1 + a^2 + 2a\cos\left(-\theta_S + \theta_D - \theta\right) \\ &= 1 + a^2 + 2a\cos\left(\theta_S - \theta_D + \theta\right). \end{aligned} \tag{24}$$

Compared with (18), the signal power at signal slot/frequency is also an even function of θ.

In summary, the signal power received by R at signal slot/frequency is function of θ and is also an even function of θ. It can be concluded that the period of θ is $2\pi/M_0$ and the symmetry axis is π/M_0. Thus, the effective range of θ is $[0, \pi/M_0]$.

4.2 Security Analysis Based on MPSK

According to (18), as the values of the amplitude ratio a and the channel phase difference θ are certain, the signal power at signal slot/frequency depends on the difference $\theta_S - \theta_D$. Since $\theta_S, \theta_D \in [0, 2\pi]$, $\theta_S - \theta_D \in [-2\pi, 2\pi]$.

For brevity of analysis, we restrict the difference $\theta_S - \theta_D$ to the range of $0 \sim 2\pi$. If $\theta_S - \theta_D \notin [0, 2\pi]$, it can be mapped into the corresponding interval since the period of phase is 2π.

<1> $M1 = M2 = M_0$

Assuming that both the random signal x_{SI} and the jamming signal J_D are M_0PSK. The phase difference of x_{SI} and J_D can be expressed as

$$\theta_S - \theta_D = 2l_3\pi/M_0, \tag{25}$$

where, $l_3 = (l_1 - l_2 + M_0) \bmod M_0$.

Thus, $l_3 = 0, 1, 2, 3...M_0 - 1$ and l_3 is a uniform distribution.

1) $M_0 = 2$

Assuming that x_{SI} and J_D are BPSK, so the effective range of θ is $[0, \pi/2]$, $l_3 = 0, 1$. If $l_3 = 0$, $\theta_S - \theta_D - \theta = -\theta$; if $l_3 = 1$, $\theta_S - \theta_D - \theta = \pi - \theta$.

If $l_3 = 0$, we have $\cos(\theta_S - \theta_D - \theta) \geq 0$, $1 + a^2 + 2a\cos(\theta_S - \theta_D - \theta) > a^2$. That is, the signal power at signal slot/frequency is greater than null slot/frequency as $l_3 = 0$ and the probability is 0.5. In order to realize zero confidential information leakage at R, $1 + a^2 + 2a\cos(\theta_S - \theta_D - \theta) < a^2$ is required if $l_3 = 1$ according to (17). That is, $1 + a^2 - 2a\cos\theta < a^2$ is required to satisfy. Thus, we can obtain $\cos\theta > 1/2a$, namely, $\theta < \arccos(1/2a)$. Besides, $\cos\theta \leq 1$, so $a > 1/2$ is required.

To summarize, if x_{SI} and J_D are BPSK, the BER of the selection bit b_{SE} at R is 0.5 under the condition that $a > 1/2$ and $0 \leq \theta < \arccos(1/2a)$.

2) $M_0 > 2$

Both x_{SI} and J_D are M_0PSK, the effective range of θ is $[0, \pi/M_0]$ and $l_3 = 0, 1, 2, 3...M_0 - 1$.

If $l_3 \in [0, M_0/4]$, $-\pi/2 < \theta_S - \theta_D - \theta \leq \pi/2$; if $l_3 \in [3M_0/4 + 1, M_0 - 1]$, $3\pi/2 \leq \theta_S - \theta_D - \theta < 2\pi$. Thus, if $l_3 \in [0, M_0/4] \cup [3M_0/4 + 1, M_0 - 1]$, we have $1 + a^2 + 2a\cos(\theta_S - \theta_D - \theta) > a^2$.

Since the length of $[0, M_0/4] \cup [3M_0/4 + 1, M_0 - 1]$ is half the length $[0, M_0 - 1]$, we can obtain that $\mathrm{P}\left(\left|x_{SI} + a\mathrm{e}^{j\theta}J_{DS}\right|^2 > a^2\right) = 0.5$.

Similarly, if $l_3 \in [M_0/4 + 1, 3M_0/4]$, we have $\pi/2 + 2\pi/M_0 - \theta \leq \theta_S - \theta_D - \theta \leq 3\pi/2 - \theta$. Meanwhile, $1 + a^2 + 2a\cos(\theta_S - \theta_D - \theta) < a^2$ is required. If $\theta \in [0, \pi/M_0]$, the maximum value of $1 + a^2 + 2a\cos(\theta_S - \theta_D - \theta)$ will be $1 + a^2 + 2a\cos(3\pi/2 - \theta)$. Thus, $1 + a^2 + 2a\cos(3\pi/2 - \theta) < a^2$, namely, $1 - 2a\cos(\pi/2 - \theta) < 0$ is required. On the basis of this, we can obtain the condition for zero confidential information leakage at R is that $a > 1/2\cos(\pi/2 - \theta)$ and $\theta > \pi/2 - \arccos(1/2a)$.

To summarize, if x_{SI} and J_D are M_0PSK, the BER of the selection bit b_{SE} at R is 0.5 under the condition that $a > 1/2\cos(\pi/2 - \pi/M_0)$ and $\pi/2 - \arccos(1/2a) < \theta \leq \pi/M_0$,

<2> $M_1 \neq M_2, M_0 = \max(M_1, M_2)$

Suppose $M_1 > M_2$, we can have $M_1 = M_0$ and $M_2 = M_0/k$, where $k = 2, 4, 8, ..M_0/2$. The phase of x_{SI} and J_D can be expressed as $\theta_S = (2l_4 - 1)\pi/M_0$ and $\theta_D = (2l_5 - 1)\pi/M_2 = (2l_5 - 1)k\pi/M_0$, where $l_4 \in \{1, 2, 3...M_0\}$, $l_5 \in \{1, 2, 3...M_0/k\}$.

The phase difference of x_{SI} and J_D can be expressed as

$$\theta_S - \theta_D = (2l_6 + 1)\,\pi/M_0, \tag{26}$$

where $l_6 = [l_4 - 1 - (2l_5 - 1)\,k/2 + M_0] \bmod M_0$. Thus, $l_6 = 0, 1, 2, 3...M_0 - 1$ and l_6 is a uniform distribution.

Compared with (18), there only exists a phase shift of π/M_0. Thus, the required range of a is identical and the required range of θ has the phase shift of π/M_0. On this basis, we can obtain that the required range of θ is $\pi/2 + \pi/M_0 - \arccos(1/2a) < \theta \leq 2\pi/M_0$. Since the symmetry axis of θ is π/M_0, it can be mapped into the interval $[0, \pi/M_0]$ and the range is $0 \leq \theta < \arccos(1/2a) + \pi/M_0 - \pi/2$.

To summarize, if x_{SI} and J_D are M_1PSK and M_2PSK, respectively, $M1 \neq M2$, the BER of the selection bit b_{SE} at R is 0.5 under the condition that $a > 1/2\cos(\pi/2 - \pi/M_0)$ and $0 \leq \theta < \arccos(1/2a) + \pi/M_0 - \pi/2$.

In conclusion, if $M_1 = M_2 = M_0 > 2$, the BER of the selection bit b_{SE} at R is 0.5 under the condition that $a > 1/2\cos(\pi/2 - \pi/M_0)$ and $\pi/2 - \arccos(1/2a) < \theta \leq \pi/M_0$; if $M_1 = M_2 = 2$ or $M_1 \neq M_2$ and $M_0 = \max(M_1, M_2)$, the BER of the selection bit b_{SE} at R is 0.5 under the condition that $a > 1/2\cos(\pi/2 - \pi/M_0)$ and $0 \leq \theta < \arccos(1/2a) + \pi/M_0 - \pi/2$.

Through the above analysis, the signal power at null slot/frequency depends on the amplitude ratio a, while the signal power at signal slot/frequency is related to the values of a, θ and $\theta_S - \theta_D$. It can be observed from (11) and (12) that the values of a and θ are independent of the signal modulation.

Besides, the scheme with M_1PSK-modulated x_{SI} and M_2PSK-modulated J_D has the same distribution of $\theta_S - \theta_D$ as the scheme with M_2PSK-modulated x_{SI} and M_1PSK-modulated J_D. Thus, the two schemes are equivalent in system security with selective modulation and cooperative jamming. Compared to the scheme with $M_1 = M_2 = M_0$, there only exists the phase shift of π/M_0 in the scheme with $M_1 \neq M_2, M_0 = \max(M_1, M_2)$.

4.3 Security Scheme Design Without Leakage

In this section, we propose the security scheme without leakage. Through the security analysis based on MPSK, it can be concluded that if the amplitude ratio a is greater than the corresponding threshold and the channel phase difference θ is limited in a certain range, zero confidential information leakage at R can be achieved. However, the values of a and θ are arbitrary in practical communication system.

In the presented system model, the jamming signal J_D is sent by D. D can cancel it by self-interference cancellation so that the design of J_D has little effect on the received performance of D. Thus, the jamming signal is designed to realize zero confidential information leakage.

According to (11), the transmit power P_J of the jamming signal can be adjusted to make $a > 1/2\cos(\pi/2 - \pi/M_0)$. Based on (12), θ depends on the channels in practical system and cannot be changed directly. Thus, the phase of the jamming signal is designed as

$$J'_D = \mathrm{e}^{j\theta'_D} = J_D \mathrm{e}^{j\theta_{\Delta D}}, \tag{27}$$

where $\theta_{\Delta D}$ is a variable related to θ.

The phase difference can be rewritten as

$$\theta_S - \theta'_D - \theta = \theta_S - \theta_D - (\theta_{\Delta D} + \theta). \tag{28}$$

If $M_1 = M_2 = M_0 > 2$, $\theta_{\Delta D}$ is designed to make

$$\pi/2 - \arccos(1/2a) - \theta < \theta_{\Delta D} \leq \pi/M - \theta; \tag{29}$$

if $M_1 = M_2 = 2$ or $M_1 \neq M_2$ and $M_0 = \max(M_1, M_2)$, $\theta_{\Delta D}$ is designed to make

$$-\theta \leq \theta_{\Delta D} < \arccos(1/2a) + \pi/M - \pi/2 - \theta. \tag{30}$$

In this paper, a security scheme without leakage is proposed. The source signal adopts selective modulation, including one selection bit and signal bits. The selection bit bears confidential information and the signal bits carry modulated signals x_{SI}. The source node S generates one selection bit b_{SE} to determine the transmitted slot/frequency of MPSK modulated x_{SI}. Meanwhile, the jamming signal J_D is designed according to the related CSI and the modulation order. The proposed scheme can achieve zero confidential information leakage at the untrusted relay.

5 Simulation Results

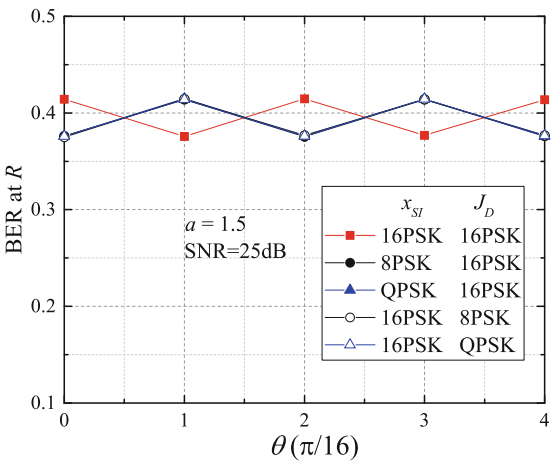

Fig. 4. BER at R (E) versus θ with $a = 1.5$ and SNR = 25 dB.

The demodulation BER and secrecy capacity are adopted as the evaluating metrics in this section. Figure 4 depicts the BER at R (E) versus θ with $a = 1.5$

and SNR = 25 dB. Assuming that x_{SI} is M_1PSK and J_D is M_2PSK, where $M_0 = \max(M_1, M_2) = 16$. As shown in Fig. 4, the BER at R (E) is a periodic function of the channel phase difference θ. The period of θ is $2\pi/16$ and the symmetry axis is $\pi/16$. The BER at R (E) with 16PSK-modulated x_{SI} and J_D is plotted in the red line. Compared with the other schemes, there only exists the difference of the phase shift $\pi/16$. If the modulation orders of x_{SI} and J_D are different, the BER at R depends on the signal with larger modulation order. If the larger modulation order is identical, these schemes with $M_1 \neq M_2$ are equivalent in system security with selective modulation and cooperative jamming. The simulation results are in accordance with the theoretical analysis.

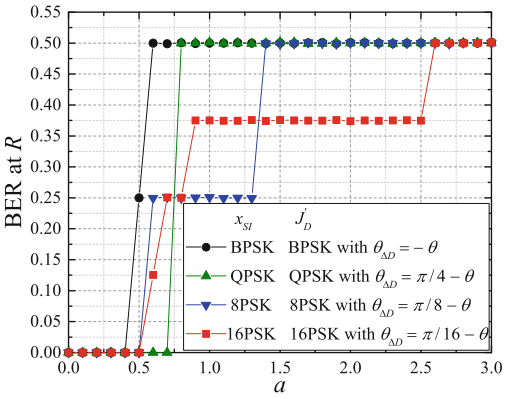

Fig. 5. BER at R (E) versus a without noise.

Figure 5 presents the BER at R (E) versus a without noise under MPSK modulated signals of different order. In our proposed schemes, if the random signal x_{SI} and the jamming signal J_D are BPSK, J_D is designed with the rotation phase of $-\theta$; if x_{SI} and J_D are M_0PSK $(M_0 > 2)$, J_D the designed with the rotation phase of $\pi/M - \theta$. Under these schemes, if $a > 1/2\cos(\pi/2 - \pi/M_0)$, the BER at R is fixed to be 0.5. The lower bound of a increases with M_0. It can be clearly seen that our proposed schemes can make BER at R to be 0.5 without considering complex Gaussian noise. That is, no confidential information leakage can be achieved at the untrusted relay.

Figure 6 and Fig. 7 plots the BERs at R (E) and D versus a at SNR = 20 dB and SNR = 15 dB. The performance of Gaussian jamming signal is also given in the figure as a comparison. In our proposed scheme, x_{SI} is BPSK and J_D is BPSK with the rotation phase of $-\theta$. Compared with Fig. 5, Fig. 6 and Fig. 7 considers the complex Gaussian noise. It can be shown that at SNR = 20 dB, the BER at R (E) is 0.5 if $a \geq 0.7$; at SNR = 15 dB, the BER at R (E) is 0.5 if $a \geq 0.6$. That is, the untrusted relay cannot eavesdrop any useful information. In contrast to Fig. 5, the lower bound of a being 0.5 increases in Fig. 6 and Fig. 7. With the increase of SNR, the lower bound of a will approach 0.5. However,

the BER at R (E) is less than 0.5 with Gaussian jamming signal. Besides, the BER at D are identical and is not affected by the jamming signal. In brief, the proposed scheme performs better than Gaussian jamming signal.

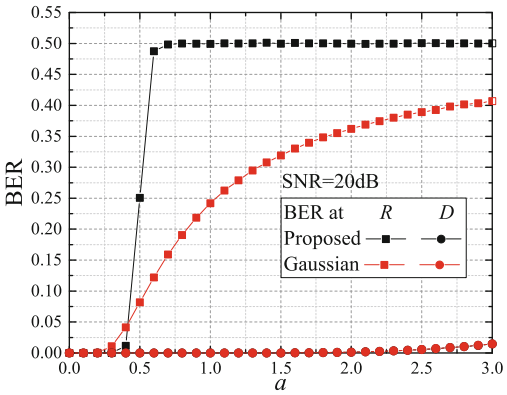

Fig. 6. BERs at R (E) and D versus a with SNR = 20 dB.

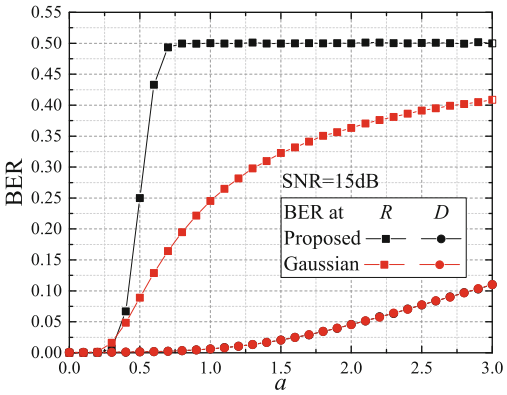

Fig. 7. BERs at R (E) and D versus a with SNR = 15 dB.

Figure 8 compares the security capacity of the proposed scheme and the Gaussian jamming signal at SNR = 20 dB. In our proposed scheme, x_{SI} is BPSK and J_D is BPSK with the rotation phase of $-\theta$. It can be observed from the figure that the overall security capacity of the proposed scheme is better than that of Gaussian jamming. If $0.6 \leq a \leq 1.6$, the secret capacity with the proposed scheme tends to approach 1. As $a > 1.6$, the security capacity of both schemes tend to decrease. This is because with the increase of a, the BER at D tends to increase as $a > 1.6$. Compared with Fig. 6, as SNR = 20 dB and $a \geq 0.6$, the BER at R is 0.5. That is, even if the security capacity is less than 1 as $a > 1.6$, zero confidential information leakage can still be achieved.

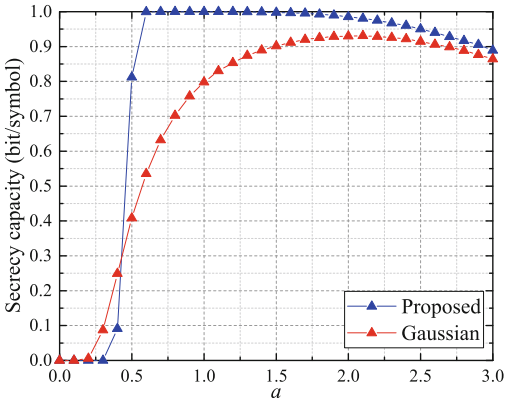

Fig. 8. Security capacity versus a with SNR = 20 dB.

6 Conclusion

In this paper, we proposed an innovative secure communication scheme for untrusted relay systems based on selective modulation and cooperative jamming. The source signal adopted selective modulation and the mapping bits included one selection bit and signal bits. For the proposed selective modulation, multi-bit selective bits are also available. The selection bit determined the transmit slot/frequency of the random signal x_{SI}, bearing confidential information, while the signal bits carried the random signal. The design of the cooperative jamming signal J_D based on MPSK consisted of two parts. The transmit power of J_D was adjusted based on the amplitude ratio a, while the phase of J_D was rotated related to the channel phase θ and the modulation order. The demodulated BER and security capacity were evaluated as security performance metrics. The simulation results demonstrated the proposed scheme can make BER at the untrusted relay to be 0.5, achieving zero confidential information leakage at R. Besides, the proposed scheme performed better than Gaussian jamming signal in the secrecy.

References

1. Long, H., Xiang, W., Li, Y.: Precoding and cooperative jamming in multi-antenna two-way relaying wiretap systems without eavesdroppers channel state information. IEEE Trans. Inf. Forensics Secur. **12**(6), 309–1318 (2017)
2. Xie, W., Liao, J., Yu, C., Zhu, P., Liu, X.: Physical layer security performance analysis of the FD-based NOMA-VC System. IEEE Access **7**, 115568–115573 (2019)
3. Lin, Z., Wang, L., Cai, Y., Yang, W., Yang, W.: Robust secure switching transmission in MISOSE relaying networks with channel uncertainty. In: 2015 International Conference on Wireless Communications Signal Processing, pp. 1–6. IEEE, Nanjing (2015)

4. Sinha, R., Jindal, P.: Performance analysis of cooperative schemes under total transmit power constraint in single hop wireless relaying system. In: 2016 2nd International Conference on Communication Control and Intelligent Systems, pp. 28–31. IEEE, Mathura (2016)
5. Divya, T., Gurrala, K. K., Das, S.: Performance analysis of hybrid decode amplify-forward (HDAF) relaying for improving security in cooperative wireless network. In: 2015 Global Conference on Communication Technologies, pp. 682–687. IEEE, Thuckalay (2015)
6. Oohama, Y.: Capacity theorems for relay channels with confidential messages. In: 2007 IEEE International Symposium on Information Theory, pp. 926–930. IEEE, Nice (2007)
7. He, X., Yener, A.: Two-hop secure communication using an untrusted relay: a case for cooperative jamming. In: IEEE GLOBECOM 2008–2008 IEEE Global Telecommunications Conference, pp. 1–5. IEEE, New Orleans (2008)
8. Mekkawy, T., Yao, R., Tsiftsis, T.A., Xu, F., Lu, Y.: Joint beamforming alignment with suboptimal power allocation for a two-way untrusted relay network. IEEE Trans. Inf. Forensics Secur. **13**(10), 2464–2474 (2018)
9. Zhang, L., Long, H., Huang, L.: Precoding and destination-aided cooperative jamming in MIMO untrusted relay systems. In: 2020 IEEE/CIC International Conference on Communications in China, pp. 605–610. IEEE, Chongqing (2020)
10. Li, Q., Yang, L.: Artificial noise aided secure precoding for MIMO untrusted two-way relay systems with perfect and imperfect channel state information. IEEE Trans. Inf. Forensics Secur. **13**(10), 2628–2638 (2018)
11. Zhang, Q., Gao, Y., Zang, G., Zhang, Y., Sha, N.: Physical layer security for cooperative communication system with untrusted relay based on jamming signals. In: 2015 International Conference on Wireless Communications Signal Processing (WCSP), pp. 1–4. IEEE, Nanjing (2015)
12. Liu, Y., Li, L., Pesavento, M.: Enhancing physical layer security in untrusted relay networks with artificial noise: a symbol error rate based approach. In: 2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM), pp. 261–264. IEEE, La Coruna (2014)
13. Xu, H., Sun, L., Ren, P., Du, Q.: Securing two-way cooperative systems with an untrusted relay: a constellation-rotation aided approach. IEEE Commun. Lett. **19**(12), 2270–2273 (2015)