Hindawi
Security and Communication Networks
Volume 2021, Article ID 6919530, 15 pages
https://doi.org/10.1155/2021/6919530

Research Article

The Optimal Carrier-Secret Ratio for Wireless Covert Channels Based on Constellation Shaping Modulation

Sen Qiao,[1] **Guangjie Liu**,[1] **Xiaopeng Ji**,[1] **and Weiwei Liu**[2]

[1]*School of Electrical and Information Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China*
[2]*School of Automation, Nanjing University of Science and Technology, Nanjing 210094, China*

Correspondence should be addressed to Guangjie Liu; gjieliu@gmail.com

Received 26 April 2021; Revised 13 July 2021; Accepted 2 November 2021; Published 3 December 2021

Academic Editor: Vijayakumar Pandi

Copyright © 2021 Sen Qiao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless covert communication is an emerging communication technique that prevents eavesdropping. This paper considers the bit error ratio (BER) problem of covert communication based on constellation shaping modulation (CSM). The impact of carrier-secret ratio (CSR) on BER is studied and the approximate solution of optimal CSR is obtained. Then, we extended the conclusion to typical communication scenarios with one and more relays where the undetectability and reliability were analyzed and inspected. It is proved that there also exists the optimal CSR in scenarios with relays. Additionally, it is found that the undetectability under the constraints of constant total power depends on the eavesdropper's position, and we found an undetectability deterioration area (UDA) in the scenario of relays. Simulation results show the existence of optimal CSR and its impact on transmission performance.

1. Introduction

Due to the openness of wireless channels, wireless communication systems are extremely vulnerable to attacks, counterfeiting, and eavesdropping. With the advent of the Internet of Things (IoT) era, a large number of smart devices are connected and controlled to meet various requirements. Hence, it is very important to safeguard the information against security breaches and to ensure the privacy of communication.

To ensure the security of personal information, some efficient anonymous authentication schemes have been proposed to adapt to different scenarios [1–3]. Multiple technologies are integrated to promote the realization of the Internet of Things (IoT), including wireless sensor networks (WSNs), radio frequency identification (RFID), machine to machine (M2M), and low-power personal area networks (PANs) [4]. To ensure the high efficiency of information channels from the clients to the cloud server, Ahmad proposed a new variant of the optimistic concurrency control protocol to avoid using the upstream communication channel all the time [5]. The most important precondition of secure and reliable group communication is an efficient group key distribution. Azees and Vijayakumar proposed a computationally efficient group key distribution scheme for secure group communication based on bilinear pairing [6]. As the number of devices connected to supporting platforms continues to increase, some proper means for access control are demanding, such as authentication and authorization method [7, 8], image watermarking [9], and cloud computing [10].

However, the challenges of information security and privacy are not limited to the above. Count on the rapid growth of telecommunication field new challenges arises [11]. Eavesdroppers can intercept the wireless communication signals and try to get the communication contents, which poses a great threat to the security and privacy of the communication. In order to ameliorate the undetectability of private information, information hiding technology gradually becomes necessary. As a branch of modern information hiding technology in the field of wireless communication, wireless covert channels hide the transmission

process of information that needs to be kept secret in the process of normal wireless communication. Even if an eavesdropper intercepts the communication signal, it cannot be distinguished from normal wireless communication.

Based on the ubiquitous channel noise phenomenon, modulation-type wireless covert communication modulates the secret information into an artificial noise signal, which is superimposed on the normal communication signal. It is the most widely used physical-layer wireless covert communication at present. The basic theory and performance limit of the covert communication in AWGN channels are discussed in Reference [12]. It is indicated that at most $O(\sqrt{n})$ bits can be transmitted to the receiver reliably without being detected by the detector.

1.1. Motivations. In modulation-type wireless covert communication, the bit error ratio (BER) of covert information is usually much greater than that of the carrier signal. The problems of BER are always solved by means of coding or increasing the power of covert signals. Yet, the difficulty of decryption and the transmission rate of the covert messages will deteriorate with encoding. By means of increasing the transmission power, undetectability will deteriorate [13]. In Reference [14], relays are proposed to increase the power of covert signal received. But it has not been simulated with specific modulation methods, and no one has considered whether the optimal power ratio of covert signal exists. We plan to research the undetectability and reliability of wireless covert communication in the scenario of relays based on a specific modulation method. And consider whether there exists an optimal carrier-secret ratio (CSR), which can ameliorate the reliability of covert communication under the premise of meeting the requirements of undetectability.

1.2. Contributions. The contributions of our work are as follows:

(1) We investigated the relationship between BER, CSR, and SNR in wireless covert channels with constellation shaping modulation. We obtained the approximate solution of optimal CSR and extended it to several scenarios with relays. With the approximate solution of optimal CSR, the process of searching for an actual optimal CSR can be accelerated when some optimization algorithms are adopted such as gradient descent and conjugate gradient.

(2) We found an undetectability deterioration area (UDA) in the scenario of one relay and two relays, and the undetectability deteriorates when an eavesdropper is in it. The UDA can be used to avoid the deterioration of undetectability with an improper set of relays. Otherwise, eavesdroppers can detect in the UDA to improve detection efficiency.

The remainder of this paper is organized as follows: in the next section, some background including wireless covert channel with dirty constellation and wireless covert channel with constellation shaping modulation is introduced; in Section 3, we introduced the basis of our scheme including the classic system model and binary hypothesis testing; in Section 4, the relationship between BER, CSR, and SNR in wireless covert channels with constellation shaping modulation is investigated. The approximate solution of optimal CSR is obtained and extended to several scenarios of relays, in which undetectability deterioration areas (UDAs) were found and analyzed; Section 5 gives the experimental results on undetectability and reliability; and finally, Section 6 concludes the whole paper.

2. Related Works

2.1. Background. Wireless covert communication mainly involves three factors of inspection: undetectability, reliability, and communication rate. At present, there is no special detection work to measure undetectability for noisy wireless covert communication. References [13, 15, 16] take KL divergence between residual and ambient noise as parameters to inspect undetectability. Reference [17] inspects the undetectability with KS distance between residual and ambient noise.

Reliability refers to the ability of wireless covert communication to resist channel interference. Channel interference may come from the natural fading of the channel, or from the jammer. To resist channel interference, multihop relaying is a frequently used method [18]. Reference [19] evaluated and optimized the covert communications by designing the parameters of the multihop network, including the coding rates, transmit power, and required number of hops.

The researchers further analyzed the covert communication capacity of multiple scenarios with multiple unfavorable factors to the eavesdropper, including three aspects of the transmitter [20, 21], receiver [22–24], and additional nodes [25–28]. The methods of covert communication include artificial additional signal noise, artificial coding domain error, insertion of additional signal band, etc. The research results in this field have also been further extended to other communication scenarios such as relay communication [14, 29], multiantenna [30, 31], and broadcast communication [32–34].

2.2. Wireless Covert Channel with Dirty Constellation. In the wireless covert channel with dirty constellation (WCC-DC), the secret message bits can be transmitted as the constellation error of the normal signal in order to reduce the suspicion by all uninformed detectors.

The framework of a wireless covert channel with dirty constellation is shown in Figure 1(a). The wireless covert channel is implemented on the wireless communication physical layer with OFDM structure. The transmitter divides all OFDM subcarriers into secret subcarriers and normal subcarriers. On the secret subcarrier, the carrier information is modulated in QPSK to obtain the carrier signal, and then the covert signal modulated by QPSK is superposed on the carrier signal. The covert constellation points are rotated at a

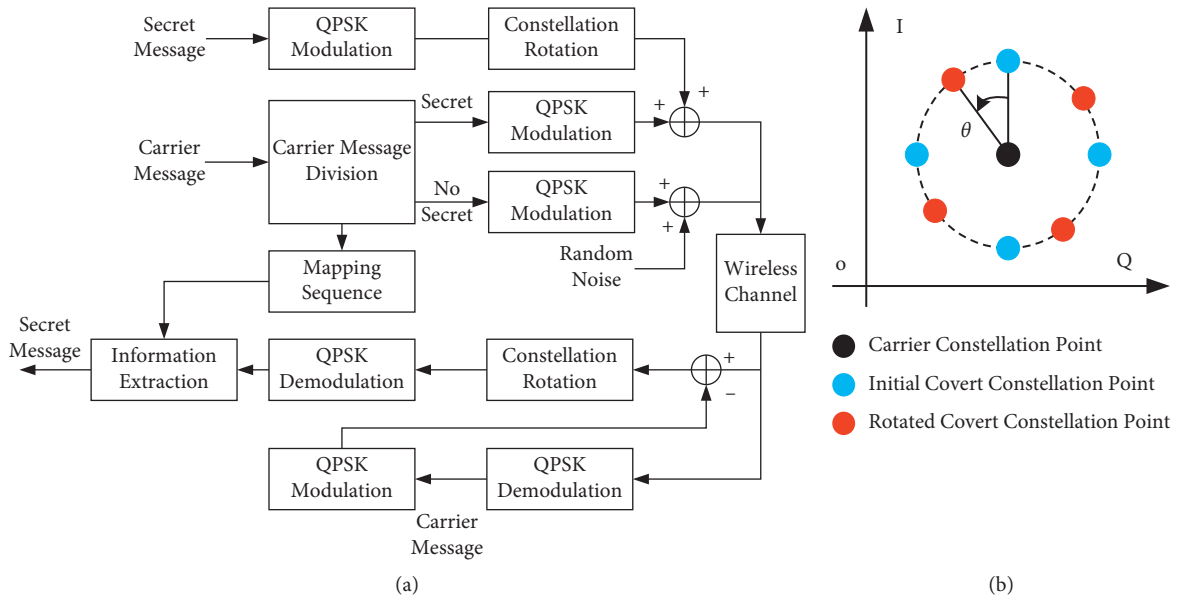

Figure 1: The schematic diagram of WCC-DC: (a) the framework of WCC-DC and (b) rotation of covert constellation.

certain angle around normal constellation points, as shown in Figure 1(b). On the normal subcarrier, carrier information is modulated in QPSK to obtain the carrier signal, and then the random noise is superimposed. The purpose of the rotation of signal-loaded signals and the superimposition of random noise is to remove the regularity of secret signals in the constellation. The subcarrier partition results of the wireless covert channel should be shared between the transmitter and the receiver.

However, the wireless covert channel with dirty constellation has a high BER when the power of covert signal is low. When we increase the power of covert signal, the undetectability of covert communication deteriorates. Therefore, Cao et al. [35] proposed a covert communication method based on constellation shaping modulation (WCC-CSM).

2.3. Wireless Covert Channel with Constellation Shaping Modulation. The general framework for the wireless communication system with constellation shaping modulation is demonstrated in Figure 2. We suppose that each subcarrier m_c of the OFDM wireless communication is modulated by QPSK. In the proposed scheme, we can use all subcarriers to establish the wireless covert communication. With constellation shaping modulation, the secret information m_s is modulated into an artificial noise signal S_s. Then, the artificial noise signal S_s is superimposed on the carrier signal S_c to generate the secret subcarrier S_{ct}.

To generate the secret artificial noise signal S_s, the cumulative distribution function (CDF) F_{CDF} of noise is estimated with the reference channel noise data S_0.

The secret information is denoted by $m_s = (m_{s,1}, m_{s,2}, \ldots m_{s,N})$, and the artificial noise signals S_s are divided into I/Q vectors, which are denoted by $x_s^I + j \cdot x_s^Q$. Here, x_s^I is the I vector of artificial noise signals denoted by $x_s^I = [x_{s,1}^I, x_{s,2}^I, x_{s,3}^I, \ldots x_{s,N}^I]$, and x_s^Q is the Q vector denoted by $x_s^Q = [x_{s,1}^Q, x_{s,2}^Q, x_{s,3}^Q, \ldots x_{s,N}^Q]$. The constellation shaping modulation function is defined as

$$F_{\mathrm{SMF}}(m_s) = S_s = x_s^I + j \cdot x_s^Q. \tag{1}$$

For shaping modulation, the transmitter firstly transforms the secret information m_s into continuous variables d_i, and then d_i are mapping to artificial noise signal S_s with CDF of the reference channel noise S_{normal}.

The transform function of d_i is defined as follows:

$$d_i = \frac{m_{s,i} + r}{2}. \tag{2}$$

We denote r as a random number distributed in the interval (0, 1). And the mapping function which transforms m_s into S_s is defined as

$$S_s = F_{\mathrm{CDF}}^{-1}(d_i). \tag{3}$$

The mapping function F_{CDF}^{-1} is the inverse function of cumulative distribution function of S_{normal}. Then, the artificial noise signal S_s is superimposed on carrier signal S_c to generate secret subcarrier S_{ct}.

The received secret subcarrier is denoted by $\widehat{S}_{ct}$. The I/Q vectors of secret subcarrier $\widehat{S}_{ct}$ are denoted by $\hat{x}_{ct}^I + j \cdot \hat{x}_{ct}^Q$, the subcarrier $\hat{m}_c$ can be demodulated with QPSK:

$$\hat{m}_c = F_{de\text{-}\mathrm{QPSK}}\left(\hat{x}_{ct}^I + j \cdot \hat{x}_{ct}^Q\right), \tag{4}$$

and the subcarrier $\hat{m}_c$ will be modulated by QPSK again to acquire the ideal the subcarrier $\widehat{S}_c$:

$$\widehat{S}_c = F_{\mathrm{QPSK}}(\hat{m}_c) = \hat{x}_c^I + j \cdot \hat{x}_c^Q. \tag{5}$$

We denote $\hat{x}_c^I + j \cdot \hat{x}_c^Q$ as the I/Q vectors of $\widehat{S}_c$. The receiver can obtain the ideal subcarrier $\hat{x}_c^I + j \cdot \hat{x}_c^Q$, and then the residual signal (i.e., artificial noise $\widehat{S}_s$) can be extracted with

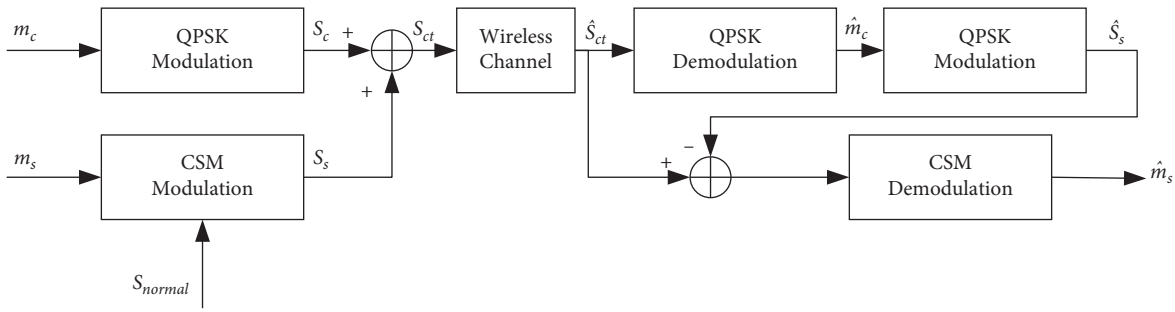

Figure 2: The framework of WCC-CSM wireless covert channel.

$$\widehat{S}_s = \widehat{S}_{ct} - \widehat{S}_c = \left(\hat{x}_{ct}^I - \hat{x}_c^I\right) + j \cdot \left(\hat{x}_{ct}^Q - \hat{x}_c^Q\right). \tag{6}$$

We denote the I/Q vectors of artificial noise $\widehat{S}_s$ as $\hat{x}_s^I + j \cdot \hat{x}_s^Q$. The artificial noise $\widehat{S}_s$ can be transformed into $\widehat{d}_i$ by the cumulative distribution function F_{CDF} with

$$\widehat{d}_i = F_{\text{CDF}}\left(\widehat{S}_s\right). \tag{7}$$

The receiver can demodulate the secret information $\hat{m}_s$ by the covert demodulation constellation (CDC), which is illustrated in Figure 3.

The four black points are the ideal constellation points; the red regions are the distribution areas of secret subcarrier with artificial noise. The function of covert demodulation constellation is denoted by $F_{\text{CDC}}(\cdot)$:

$$\hat{m}_s = F_{\text{CDC}}\left(d_i\right). \tag{8}$$

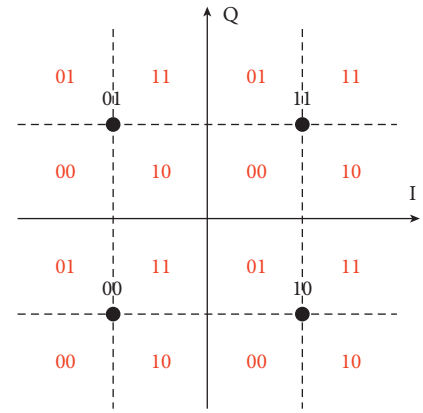

Figure 3: Covert demodulation constellation of WCC-CSM.

3. Basis of Our Scheme

3.1. System Model. Similar to the famous Alice–Bob model [36], the standard wireless covert channel system model includes the transmitter (i.e., Alice), the receiver (i.e., Bob), and the detector (i.e., Willie).

Willie observes the channel to detect whether Alice transmits or not. Willie's probability of detection error consists of two components: the probability of missed detection and the probability of false alarm.

The literature as seen in the aforementioned works only mentioned the impact of finite samples (i.e., finite $m[i]$) on the detection performance at Willie. It is numerically shown that with noise uncertainty at Willie, there may exist an optimal number of samples that maximize the communication rate subject to $\xi \geq 1 - \varepsilon$, where ξ is the sum of P_F (i.e., false alarm rate) and P_M(i.e., miss detection rate) at Willie and ε is an arbitrarily small number. We define $0 < \varepsilon \leq 1$ as the maximum acceptable detection rate of Willie.

3.2. Binary Hypothesis Testing at Willie. According to the system model shown in Figure 4, the performance elements of the wireless covert channel mainly include two aspects: undetectability and reliability.

In communication, Alice totally transmits n symbols to Bob. We denote the finite block as $m[i](i \in [1, n])$, which consists of normal information $m_c[i]$ and secret information $m_s[i]$, while Willie is passively collecting $m[i]$ observations on Alice's transmission in order to detect the presence of her secret information (i.e., whether Alice is transmitting secret information). We denote the AWGN at Bob and Willie as $r[i] \sim CN(0, \sigma_w^2)$. The received signal at Willie for each signal symbol is given by

$$y_w[i] = m[i] + r[i]. \tag{9}$$

The main purpose of Willie is to confirm whether Alice transmits or not. We define two hypotheses, H_0 and H_1, to distinguish these two cases:

$$\begin{cases} H_0 \colon m[i] = m_c[i], \\ H_1 \colon m[i] = m_c[i] + m_s[i]. \end{cases} \tag{10}$$

H_0 denotes the null hypothesis, where Alice is not transmitting secret information. H_1 denotes the alternative hypothesis, where Alice is transmitting secret information. In the covert communication, the ultimate goal of Willie is to minimize the total error rate (i.e.ξ). We denote T and F as binary decisions that infer whether Alice is transmitting or not. The false alarm rate and miss detection rate are given by

$$\begin{cases} P_F = P_r\left(T|H_0\right), \\ P_M = P_r\left(F|H_1\right). \end{cases} \tag{11}$$

Suppose Willie performs the optimal detect. Following Pinsker's inequality [37, 38]

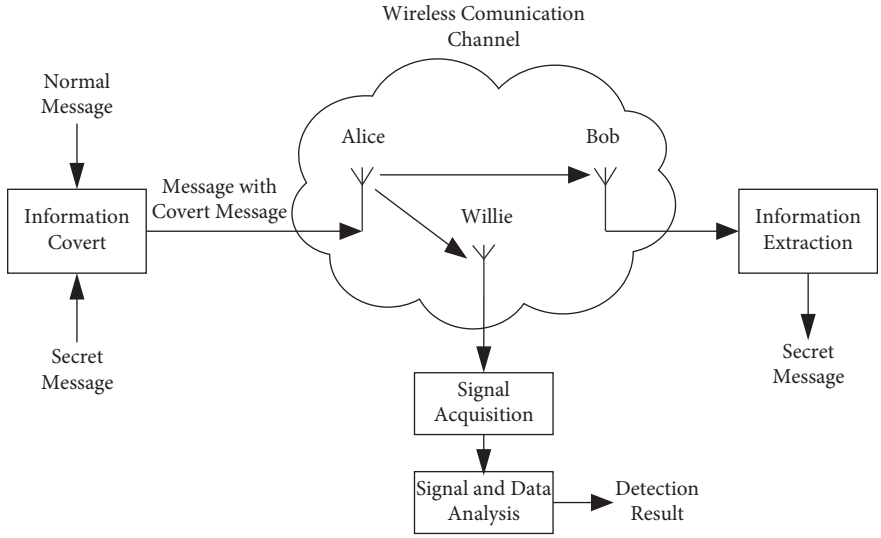

Figure 4: The framework of wireless covert communication.

$$P_F + P_M \geq 1 - \sqrt{\frac{1}{2} D(P_0 \| P_1)}, \tag{12}$$

where relative entropy $D(P_0 \| P_1)$ (also called KL divergence) is defined as follows:

$$D(P_0 \| P_1) = \int_n p_0(x) \ln \frac{p_0(x)}{p_1(x)} \mathrm{d}x, \tag{13}$$

where n is the value range of x. We denote $p_1(x)$ as the distribution of a sequence $m[i]$, which detected by Willie, and $p_0(x)$ denotes the distribution of a sequence $m_c[i]$, which detected when Alice is not transmitting.

The KL divergence is always used to calculate the correlation between distributions. Except KL divergence, we can also use KS distance (also called Kolmogorov–Smirnov statistic) to calculate the distance between distributions. The KS distance is defined as follows:

$$D_{KS} = \max \left| F_1(x) - F_0(x) \right|. \tag{14}$$

$m_1[i]$ and $m_0[i]$ are both divided into K bins. The number of the elements in $m_1[i]$ and $m_0[i]$ are denoted by $h_1(j)$ and $h_0(j)$, $j \in (1, 2 \ldots K)$. The cumulative distribution functions of $m_1[i]$ and $m_0[i]$ are defined as follows:

$$\begin{aligned} F_1(x) &= \frac{\sum_{j=1}^{x} h_1(j)}{n}, \\ F_0(x) &= \frac{\sum_{j=1}^{x} h_0(j)}{n}. \end{aligned} \tag{15}$$

Willie always set threshold Γ of KL divergence and KS distance to judge whether there is communication.

$$\begin{cases} \Pr(T | D(P_0 \| P_1) > \Gamma \| D_{KS} > \Gamma), \\ \Pr(F | D(P_0 \| P_1) < \Gamma \| D_{KS} < \Gamma). \end{cases} \tag{16}$$

To measure the reliability of the communication, we denote BER as follows:

$$P_e = \frac{n_{\text{error}}}{n}, \tag{17}$$

where n_{error} is the number of error symbols.

4. Optimal Carrier-Secret Ratio for WCC-CSM

4.1. Classic Scenario. After the secret subcarrier $\widehat{S}_{ct}$ transmitting through the wireless channel, the receiver can get the output of the slow-fading channel as $\widehat{S} = [\widehat{S}_{ct}(1), \widehat{S}_{ct}(2), \ldots \widehat{S}(N)]$ with

$$\widehat{S}_{ct}[i] = \sqrt{P_t} \cdot \frac{\sqrt{\lambda_0}}{\left(\sqrt{d_{tr}}\right)^{\alpha}} \cdot h_A \cdot S_{ct}[i] + n_A[i], \tag{18}$$

where P_t denotes the transmission energy of transmitter; λ_0 denotes the wavelength of the signal; h_A denotes the complex baseband equivalent channel coefficient of the main channel between the transmitter (i.e., Alice) and receiver (i.e., Bob); and n_A denotes zero-mean circularly symmetric complex Gaussian noise. And we also have two real variables d_{tr} and $\alpha \in R$ that denote the distance and path-loss exponent of the channel between Alice and Bob, respectively. The path-loss exponent α takes a value between 2 and 4. In free space, microwave transmission has path-loss exponent$\alpha = 2$.

The detector (i.e., Willie) can receive the output as $\widehat{y}_{\text{willie}} = [\widehat{y}_{\text{willie}}(1), \widehat{y}(2), \ldots \widehat{y}_{\text{willie}}(N)]$ with

$$\widehat{y}_{\text{willie}}[i] = \sqrt{P_t} \cdot \frac{\sqrt{\lambda_0}}{\left(\sqrt{\mathrm{d}_{\text{Willie}}}\right)^{2}} \cdot h_W \cdot S_{ct}[i] + n_W[i]. \tag{19}$$

h_W denotes the complex baseband equivalent channel coefficient of the main channel between the transmitter (i.e., Alice) and detector(i.e., Willie); d_{Willie} denotes the distance exponent between Alice and Willie. The noise n_W also follows a zero-mean circularly symmetric complex Gaussian distribution.

Theorem 1. *The undetectability of wireless covert communication deteriorates with the increase of CSR.*

Proof. As is mentioned above, the probability of detection error must satisfy a lower boundary of

$$P_F + P_M \geq 1 - \sqrt{\frac{1}{2} D(P_0 \| P_1)}. \tag{20}$$

Considering equations (13) and (20) jointly, we can obtain the lowest boundary is at the lowest "KL divergence," We denote $p_1(x)$ as the distribution of residual signal $\widehat{S}_s$, which detected by Willie, and $p_0(x)$ denotes the distribution of the reference channel noise S_0. The artificial noise S_s is the mapping of $S_0 \sim N(0, \sigma_\omega^2)$; thus, we can obtain the residual signal $\widehat{S}_s \sim N(0, \sigma_\omega^2) \sim (0, P + \sigma_\omega^2)$. P denotes the energy of the signal, which received by Bob or Willie. The "KL divergence" of S_0 and $\widehat{S}_s$ can be expressed as

$$\begin{aligned} D(S_0 \| \widehat{S}_s) &= \int_n p_0(x) \ln \frac{p_0(x)}{p_1(x)} \mathrm{d}x, \\ &= \int_n \frac{1}{\sqrt{2\pi}\sigma_\omega} e^{-x^2/\sigma_\omega^2} \cdot \ln\left(\frac{\sigma_s}{\sigma_\omega} \cdot e^{x^2/\sigma_\omega^2 - x^2/\sigma s} \right) \mathrm{d}x \\ &= \int_n \frac{1}{\sqrt{2\pi}\sigma_\omega} e^{-x^2/\sigma_\omega^2} \cdot \left(\ln\left(\frac{\sqrt{P + \sigma_\omega^2}}{\sigma_\omega} \right) + \frac{x^2 \cdot P}{(P + \sigma_\omega^2) \cdot \sigma_\omega^2} \right) \mathrm{d}x \\ &= \frac{1}{2} \left(\ln \frac{P + \sigma_\omega^2}{\sigma_\omega^2} - \frac{P}{P + \sigma_\omega^2} \right) \end{aligned} \tag{21}$$

As is illustrated in equation (21), the "KL divergence" increases with the increase of P. Even the zero-mean circularly symmetric complex Gaussian noise with the same variance has different distributions. In order to calculate the "KL divergence", we divide both S_0 and $\widehat{S}_s$ into K bins, the probability in j bins are denoted by $P_{S0}(j)$ and $P_{\mathrm{Sres}}(j)$, $j \in (1, 2 \ldots K)$. The expression (21) can be expressed as

$$D(S_0 \| \widehat{S}_s) = \int_n P_{S0}(x) \ln \frac{P_{S0}(x)}{P_{\mathrm{Sres}}(x)} \mathrm{d}x. \tag{22}$$

With the increase of K, $P_{S0}(j)$ and $P_{\mathrm{Sres}}(j)$ will approach $p_0(x)$ and $p_1(x)$. However, if the K is too great, the P_F will be great. If the K is too small, the P_M will be great. We need to choose a suitable value of K. In this paper, we set $K = 100$.

P_{Willie} denotes the signal energy detected by Willie. P_{ideal} denotes the ideal signal energy. The "KL divergence" can be expressed as

$$\begin{aligned} D(S_0 \| \widehat{S}_s) &= \frac{1}{2} \left(\ln \frac{P + \sigma_\omega^2}{\sigma_\omega^2} - \frac{P}{P + \sigma_\omega^2} \right) \\ &= \frac{1}{2} \left(\ln \frac{P_{\mathrm{Willie}} - P_{\mathrm{ideal}}}{\sigma_\omega^2} - \frac{P_{\mathrm{Willie}} - P_{\mathrm{ideal}} - \sigma_\omega^2}{P_{\mathrm{Willie}} - P_{\mathrm{ideal}}} \right). \end{aligned} \tag{23}$$

ΔP denotes $P_{\mathrm{Willie}} - P_{\mathrm{ideal}}$. Taking the partial derivative with respect toΔP, equation (23) can be expressed as

$$\frac{\partial D(S_0 \| \widehat{S}_s)}{\partial \Delta P} = \frac{1}{2} \left(\frac{\Delta P - \sigma_\omega^2}{\Delta P^2} \right). \tag{24}$$

ΔP can be expressed as

$$\Delta P \approx \left(1 - \frac{1}{CSR} \right) \cdot P_{\mathrm{Willie}} + \sigma_\omega^2. \tag{25}$$

Analysis: Considering expression equations (24) and (25) jointly, we can get $\partial D(S_0 \| \widehat{S}_s) / \partial \Delta P > 0$. The KL divergence increases with the increase of ΔP. With the P_{Willie} unchanged, ΔP increases with the increase of CSR. Hence, the KL divergence increases with the increase of CSR.

The KL divergence increases with the increase of P_{Willie}. When the KL divergence is greater than Γ, Willie judges there is covert communication. When the KL divergence equals to Γ, the corresponding SNR_0 can be expressed as

$$\mathrm{SNR}_0 = P_0 \cdot \frac{\lambda_0 \cdot h_0^2}{d_0^2}. \tag{26}$$

If $\mathrm{SNR} < \mathrm{SNR}_0$, the covert communication will not be detected. When the transmission power is constant, the threshold detection distance d_0 can be illustrated in Figure 5. The purple dotted circle is the equipower line in which the covert communication will not be detected with "KL divergence."

The probability of undetected P_{ud} can be expressed as

$$P_{u\,d} = \Pr\left\{ P_t \cdot \frac{\lambda_0 \cdot h_W^2}{d_W^2} < \mathrm{SNR}_0 \right\}. \tag{27}$$

□

Theorem 2. *There exists an optimal ratio between the carrier signal and secret signal no matter what the value of SNR is. The BER minimizes at the optimal ratio.*

Proof. The reliability of the system is inspected by the BER. The BER of QPSK is

$$P_{\mathrm{eQPSK}} = \frac{1}{2} \mathrm{erfc}(\sqrt{r}). \tag{28}$$

$\mathrm{erfc}(\cdot)$ denotes the Gauss error function, r denotes the signal-noise ratio. The BER of covert communication is denoted as P_{ecov}, which can be expressed as

$$\begin{aligned} P_{\mathrm{ecov}} &= 1 - \left[1 - P_{e,mc} \right] \cdot \left[1 - P_{e,sc} \right] \\ &= 1 - \left[1 - \mathrm{erfc}\left(\sqrt{\frac{\mathrm{SNR} \cdot \mathrm{CSR}}{\mathrm{SNR} + \mathrm{CSR} + 1}} \right) \right] \left[1 - \mathrm{erfc}\left(\sqrt{\frac{\mathrm{SNR}}{\mathrm{CSR} + 1}} \right) \right]. \end{aligned} \tag{29}$$

SNR denotes the signal-noise ratio of $\widehat{S}_{ct}$ to S_0, CSR denotes the carrier-secret ratio of S_c to S_s. Considering the range of SNR and CSR, the expression (29) can be approximated as

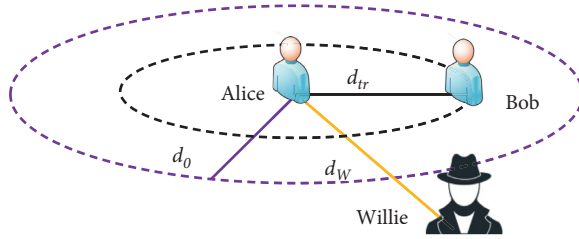

Figure 5: Location diagram of Alice, Bob, and Willie.

$$P_{\text{ecov}} = 1 - \left[1 - P_{e,mc}\right] \cdot \left[1 - P_{e,sc}\right] \approx 1 - \text{erf}\left(\sqrt{0.75 \times \text{CSR}}\right) \cdot \text{erf}\left(\sqrt{\frac{\text{SNR}}{\text{CSR}}}\right). \tag{30}$$

Taking the partial derivative with respect to CSR, the equation (30) can be expressed as

$$\frac{\partial P_{\text{ecov}}}{\partial C\ SR} = -\left[\left(\frac{1}{\sqrt{\pi}} \cdot e^{-0.75CSR} \cdot \frac{\sqrt{0.75}}{\sqrt{CSR}} \cdot \text{erf}\left(\sqrt{\frac{\text{SNR}}{0.75\text{CSR}}}\right)\right) - \left(\text{erf}\left(\sqrt{\text{CSR}}\right) \cdot \frac{1}{\sqrt{\pi}} \cdot e^{-\text{SNR/CSR}} \cdot \sqrt{SNR} \cdot CSR^{-3/2}\right)\right]. \tag{31}$$

Analysis: Let the $\partial P_{\text{ecov}}/\partial\text{CSR}$ equals zeros. We can obtain

$$\begin{aligned}\frac{1}{\sqrt{\pi}} \cdot e^{-0.75\text{CSR}} \cdot \frac{\sqrt{0.75}}{\sqrt{\text{CSR}}} \cdot \text{erf}\left(\sqrt{\frac{\text{SNR}}{0.75\text{CSR}}}\right) &= \text{erf}\left(\sqrt{\text{CSR}}\right) \cdot \frac{1}{\sqrt{\pi}} \cdot e^{-\text{SNR/CSR}} \cdot \sqrt{\text{SNR}} \cdot \text{CSR}^{-3/2} \text{erf}\left(\sqrt{\frac{\text{SNR}}{0.75\text{CSR}}}\right) \cdot e^{-0.75\text{CSR}} \\ &\cdot \sqrt{0.75\text{CSR}} = \text{erf}\left(\sqrt{\text{CSR}}\right) \cdot e^{-\text{SNR/CSR}} \cdot \sqrt{\frac{\text{SNR}}{\text{CSR}}}.\end{aligned} \tag{32}$$

The equality can be established when $\text{CSR} = \sqrt{4/3\text{SNR}}$, which is the optimal CSR. We can obtain the lowest BER at the optimal CSR. The expression (29) can be expressed as Figure 6.

As can be seen from Figure 6, P_{ecov} minimizes at the optimal CSR. And the approximate solution we obtained is consistent with the theoretical P_{ecov} in Figure 6. With the approximate solution of optimal CSR, the process of searching for an actual optimal CSR can be accelerated when some optimization algorithms are adopted such as gradient descent and conjugate gradient.

As wireless communication is affected by channel fading, it is often necessary to set one or more relays to extend the communication distance. Therefore, the relay communication scenarios are described in details in the following subsections. □

4.2. One-Relay Scenario. Covert information is always transmitted with low power; we can set relays to extend the transmission distance. Each relay employs the amplify-and-forward (AF) protocol and has two phases. Alice transmits signal in one phase; the relay amplifies the signal and forwards to Bob in another phase. We can set the positions of Alice, Bob, Willie, and relay as illustrated in Figure 7(a). d_{tr} denotes the distance between Alice and Bob; d_{trr} denotes the distance between Alice and relay; and d_{rb} denotes the distance between relay and Bob. If we keep the total transmission energy constant, the transmission energy of Alice and relay are both $0.5P_t$, and we can obtain the output of the covert channel:

$$\begin{cases} \widehat{y}_{\text{relay}}[i] = \sqrt{\frac{P_t}{2}} \cdot \frac{\sqrt{\lambda_0}}{d_{\text{trr}}} \cdot h_A \cdot S_{ct}[i] + n_A[i], \\ \widehat{y}_{\text{Bob}}[i] = \sqrt{\frac{P_t}{2}} \cdot \frac{\sqrt{\lambda_0}}{d_{rb}} \cdot h_B \cdot \widehat{y}_{\text{relay}}[i] + n_B[i]. \end{cases} \tag{33}$$

As is illustrated in Figure 7(a),

$$d_{rb} + d_{\text{trr}} = d_{tr}. \tag{34}$$

We can obtain the signal which is received by Bob:

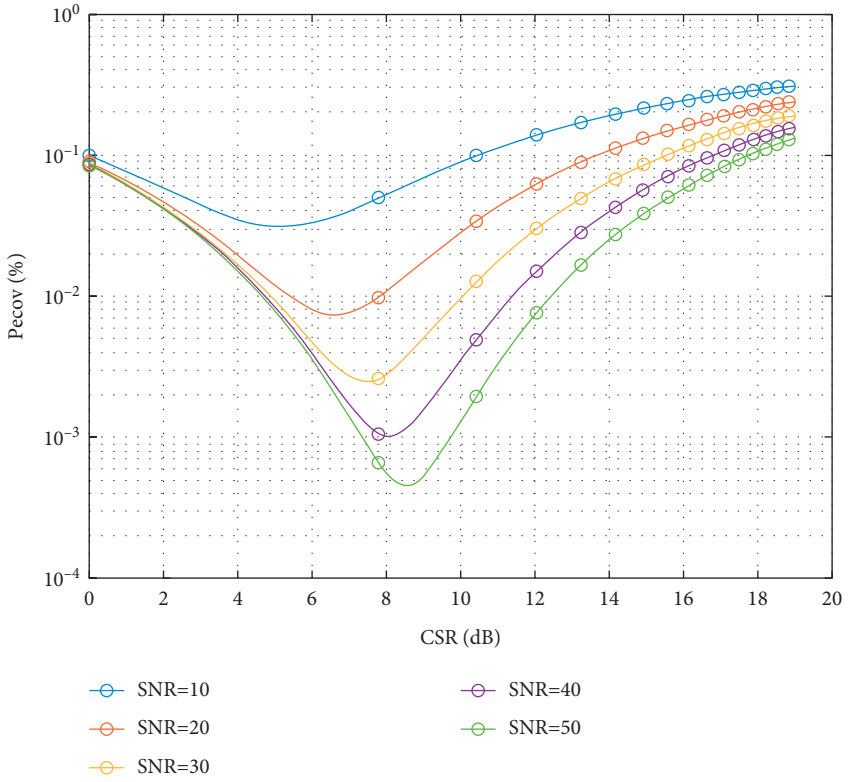

Figure 6: BER curve in AWGN channel.

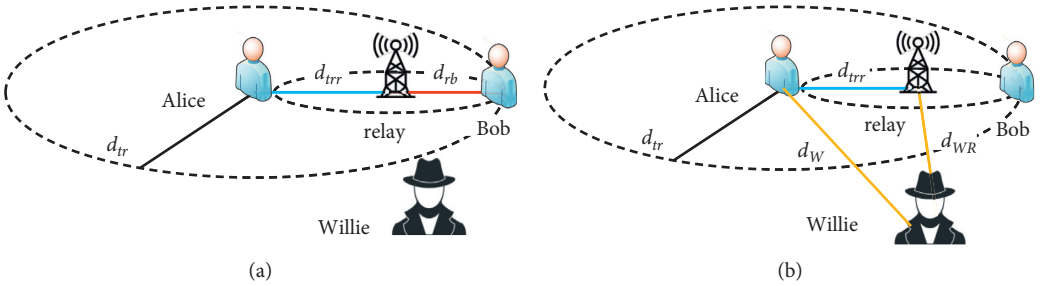

Figure 7: Diagram of relay location: (a) relay at random position and (b) relay in middle.

$$\hat{y}_{\text{Bob}}[i] = \sqrt{\frac{P_t}{2}} \cdot \frac{\sqrt{\lambda_0}}{d_{rb}} \cdot h_B \cdot \left(\sqrt{\frac{P_t}{2}} \cdot \frac{\sqrt{\lambda_0}}{d_{\text{trr}}} \cdot h_A \cdot S_{ct}[i] + n_A[i] \right) + n_B[i],$$
$$= \frac{P_t}{2} \cdot \frac{\lambda_0}{d_{rb} \cdot d_{\text{trr}}} \cdot h_B \cdot h_A \cdot S_{ct}[i] + n_C[i] \tag{35}$$

In free space, the signal which is received by Bob is only about the energy and distance. So the optimization position of the relay is in the middle of Alice and Bob (i.e., $d_{rb} = d_{trr}$), as can be seen in Figure 7(b).

The distance between Willie, Alice, and relay are denoted by d_W and d_{WR}. The probability of undetectability P_{ud} can be expressed as

$$P_{ud} = \Pr\left\{ \frac{P_t}{2} \cdot \frac{\lambda_0 \cdot h_A^2}{d_W^2} < \text{SNR}_0 \right\} \cdot \Pr\left\{ \frac{P_t}{2} \cdot \frac{\lambda_0 \cdot h_B^2}{d_{WR}^2} < \text{SNR}_0 \right\}. \tag{36}$$

Construct a coordinate system with Alice as the origin of the coordinate axis. We can obtain the coordinates of Alice $(0, 0)$, Bob $(2d_{trr}, 0)$, relay $(d_{trr}, 0)$, and Willie $(X_{\text{Willie}}, Y_{\text{Willie}})$.

In the AWGN channel, the power of signal received by Willie is just related to distance and transmit power. We can get "equipower lines" in the scenario of no relay and one relay.

Then, the power detected by Willie can be expressed as

$$2\left[\left(X_{\text{Willie}} - d_{trr}\right)^2 + Y_{\text{Willie}}^2\right] = \left(X_{\text{Willie}}\right)^2 + \left(Y_{\text{Willie}}\right)^2. \tag{37}$$

Equation (37) can be expressed as

$$\left(X_{\text{Willie}} - 2d_{\text{trr}}\right)^2 + Y_{\text{Willie}}^2 = \left(\sqrt{2}\, d_{\text{trr}}\right)^2. \tag{38}$$

We denoted the circle expressed in equation (38) as the undetectability deterioration area (UDA). The undetectability deteriorates with setting relay when Willie is in the UDA. And the eavesdropper can detect in the UDA to improve detection efficiency.

It is illustrated in Figure 8, the green dotted line is UDA. If Willie is in the UDA, the P_{ud} will decrease in the scenario of one relay and the consequent deterioration of undetectability. Correspondingly, the undetectability will ameliorate if Willie is outside the green dotted circle. When William is on the green dotted line, the P_{ud} will be constant.

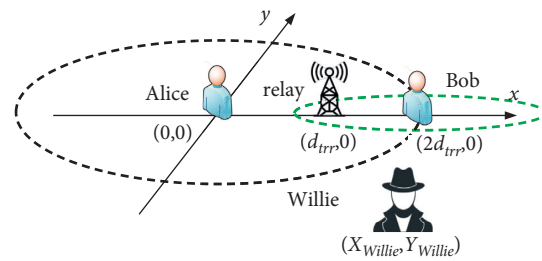

Figure 8: Power comparison of classic scenario and one relay scenario.

The BER of covert communication $P_{\text{ecov.r1}}$ can be expressed as

$$\begin{aligned} P_{\text{ecov.}r1} = 1 - \left[1 - P_{e,mc1}\right] \cdot \left[1 - P_{e,sc1}\right]\left[1 - P_{e,mc2}\right] \cdot \left[1 - P_{e,sc2}\right] + o(\Delta) \approx 1 \\ - \left\{\left[1 - \text{erfc}\left(\sqrt{\frac{2\text{SNR} \cdot \text{CSR}}{2\text{SNR} + \text{CSR} + 1}}\right)\right]\left[1 - \text{erfc}\left(\sqrt{\frac{2\text{SNR}}{\text{CSR} + 1}}\right)\right]\right\}^2. \end{aligned} \tag{39}$$

Referring expression (32), we can obtain the local minimum of $P_{\text{ecov.r1}}$ at CSR = $\sqrt{4/3\text{SNR}}$, which is the optimal CSR.

4.3. Two-Relay Scenario. Based on the above, we discuss the two-relay scenario. If we keep the total transmission energy constant, the transmission energy of Alice, relay1, and relay2 are all $P_t/3$. We can obtain the output of the covert signal:

$$\begin{cases} \widehat{y}_{\text{relay1}}[i] = \sqrt{\dfrac{P_t}{3}} \cdot \dfrac{\sqrt{\lambda_0}}{d_{\text{trr}}} \cdot h_A \cdot S_{ct}[i] + n_A[i], \\ \widehat{y}_{\text{relay2}}[i] = \sqrt{\dfrac{P_t}{3}} \cdot \dfrac{\sqrt{\lambda_0}}{d_{\text{trr}}} \cdot h_B \cdot \widehat{y}_{\text{relay1}}[i] + n_B[i], \\ \widehat{y}_{\text{Bob}}[i] = \sqrt{\dfrac{P_t}{3}} \cdot \dfrac{\sqrt{\lambda_0}}{d_{\text{trr}}} \cdot h_C \cdot \widehat{y}_{\text{relay2}}[i] + n_C[i]. \end{cases} \tag{40}$$

As can be seen in Figure 9, the distances between Willie and Alice, relay1, and relay2 are denoted by d_{WR}, d_{WR1}, and d_{WR2}, respectively.

The probability of undetected P_{ud} can be expressed as

$$P_{u\,d} = \Pr\left\{\frac{P_t}{3} \cdot \frac{\lambda_0 \cdot h_A^2}{d_W^2} < SNR_0\right\} \cdot \Pr\left\{\frac{P_t}{3} \cdot \frac{\lambda_0 \cdot h_B^2}{d_{WR1}^2} < SNR_0\right\} \cdot \Pr\left\{\frac{P_t}{3} \cdot \frac{\lambda_0 \cdot h_C^2}{d_{WR2}^2} < SNR_0\right\}. \tag{41}$$

Further extension, the probability of undetectability for n hops can be expressed as

$$P_{u\,d} = \prod_n \Pr\left\{\frac{P_t}{n} \cdot \frac{\lambda_0 \cdot h_n^2}{d_{Wn}^2} < SNR_0\right\}. \tag{42}$$

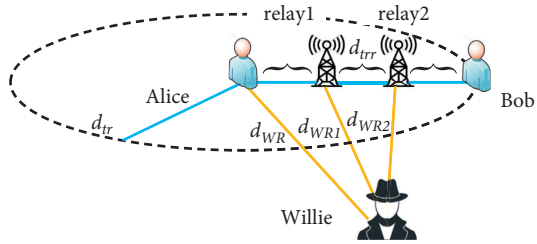

Figure 9: Diagram of two relays location.

The UDA of relay1 can be expressed as

$$3\left[\left(X_{\text{Willie}} - d_{\text{trr}}\right)^2 + Y_{\text{Willie}}^2\right] = X_{\text{Willie}}^2 + Y_{\text{Willie}}^2. \tag{43}$$

Equation (43) can be converted to

$$\left(X_{\text{Willie}} - \frac{3}{2}d_{\text{trr}}\right)^2 + Y^2 = \left(\frac{\sqrt{3}}{2}d_{\text{trr}}\right)^2. \tag{44}$$

The UDA of relay2 can be expressed as

$$3\left[\left(X_{\text{Willie}} - 2d_{\text{trr}}\right)^2 + Y_{\text{Willie}}^2\right] = X_{\text{Willie}}^2 + Y_{\text{Willie}}^2. \tag{45}$$

Equation (45) can be converted to

$$\left(X_{\text{Willie}} - 3d_{\text{trr}}\right)^2 + Y^2 = \left(\sqrt{3}\,d_{\text{trr}}\right)^2. \tag{46}$$

As can be seen in Figure 10, the circles expressed in equations (44) and (46) are UDAs. If Willie is in the blue or green dotted circle, the undetectability will deteriorate.

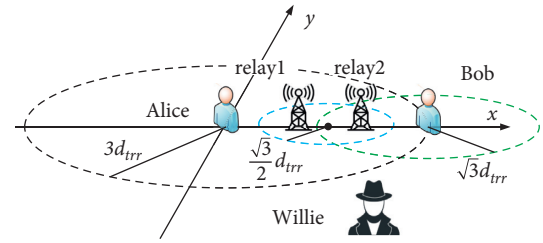

Figure 10: Power comparison of the classic scenario and two-relay scenario.

Correspondingly, the undetectability will ameliorate if Willie is outside the blue and green dotted circles.

The BER of covert communication $P_{\text{ecov.r2}}$ can be expressed as

$$\begin{aligned} P_{\text{ecov.r2}} = {} & 1 - \left[1 - P_{e,mc1}\right] \cdot \left[1 - P_{e,sc1}\right]\left[1 - P_{e,mc2}\right] \cdot \left[1 - P_{e,sc2}\right]\left[1 - P_{e,mc3}\right] \cdot \left[1 - P_{e,sc3}\right] + o(\Delta) \approx 1 \\ & - \left\{\left[1 - \text{erfc}\left(\sqrt{\frac{3\text{SNR} \cdot \text{CSR}}{3\text{SNR} + \text{CSR} + 1}}\right)\right]\left[1 - \text{erfc}\left(\sqrt{\frac{3\text{SNR}}{\text{CSR} + 1}}\right)\right]\right\}^3. \end{aligned} \tag{47}$$

It has been proved that there exists an optimal CSR, and we can obtain the minimum of $P_{\text{ecov.r2}}$ at CSR = $\sqrt{4/3\text{SNR}}$.

5. Experimental Result

5.1. Experimental Setup. In this section, we inspect the undetectability and reliability to benchmark the proposed scheme. We set the wireless communication on an 802.11a/g PHY layer. The wireless covert channel is performed on all 100000 symbols. In transmissions, there are 48 subcarriers in a symbol. Simulation experiments are carried out in wireless channel models of AWGN channel models [39]. In some simulations, the wireless covert channel with dirty constellation (WCC-DC) is chosen for comparison. The undetectability is inspected by "KL divergence" and "KS distance". The undetectability measures of I vectors, Q vectors, magnitudes, and phases of constellation errors are presented in the range of transmission power SNR = 10, . . ., 40 dB. The reliability is measured by BERs.

5.2. Undetectability. Willie (i.e., detector) observes the channel to judge whether Alice (i.e., transmitter) is transmitting in the covert channel or not. There must be a threshold Γ to compare the value of "KL divergence" and "KS distance". If the Γ is great, the P_F will be too great. If the Γ is small, the P_M will be too great. In this paper, we set the Γ of four measures of "KL divergence" as [0.04, 0.04, 0.055, 0.055], and the Γ of "KS distance" as [0.025, 0.025, 0.025, 0.025].

In this section, we set the number of bins $K = 100$. Four samples were chosen for comparison, and the samples are as follows: WCC-DC with CSR = 5 dB and CSR = 10 dB, WCC-CSM with CSR = 5 dB, and CSR = 10 dB.

As can be seen in Figure 11, the "KL divergence" of WCC-CSM with CSR = 5 dB and CSR = 10 dB meet the threshold Γ [0.04, 0.04, 0.055, 0.055] in the range of SNR = 10, . . ., 40 dB. The resulting KL divergence is lower than the KL divergence achieved with WCC-DC.

In Figure 11(a), WCC-DC with CSR = 10 dB meets the threshold Γ of I vectors in the range of SNR = 10, . . ., 30 dB. The "KL divergence" of WCC-DC with CSR = 10 dB exceeds the

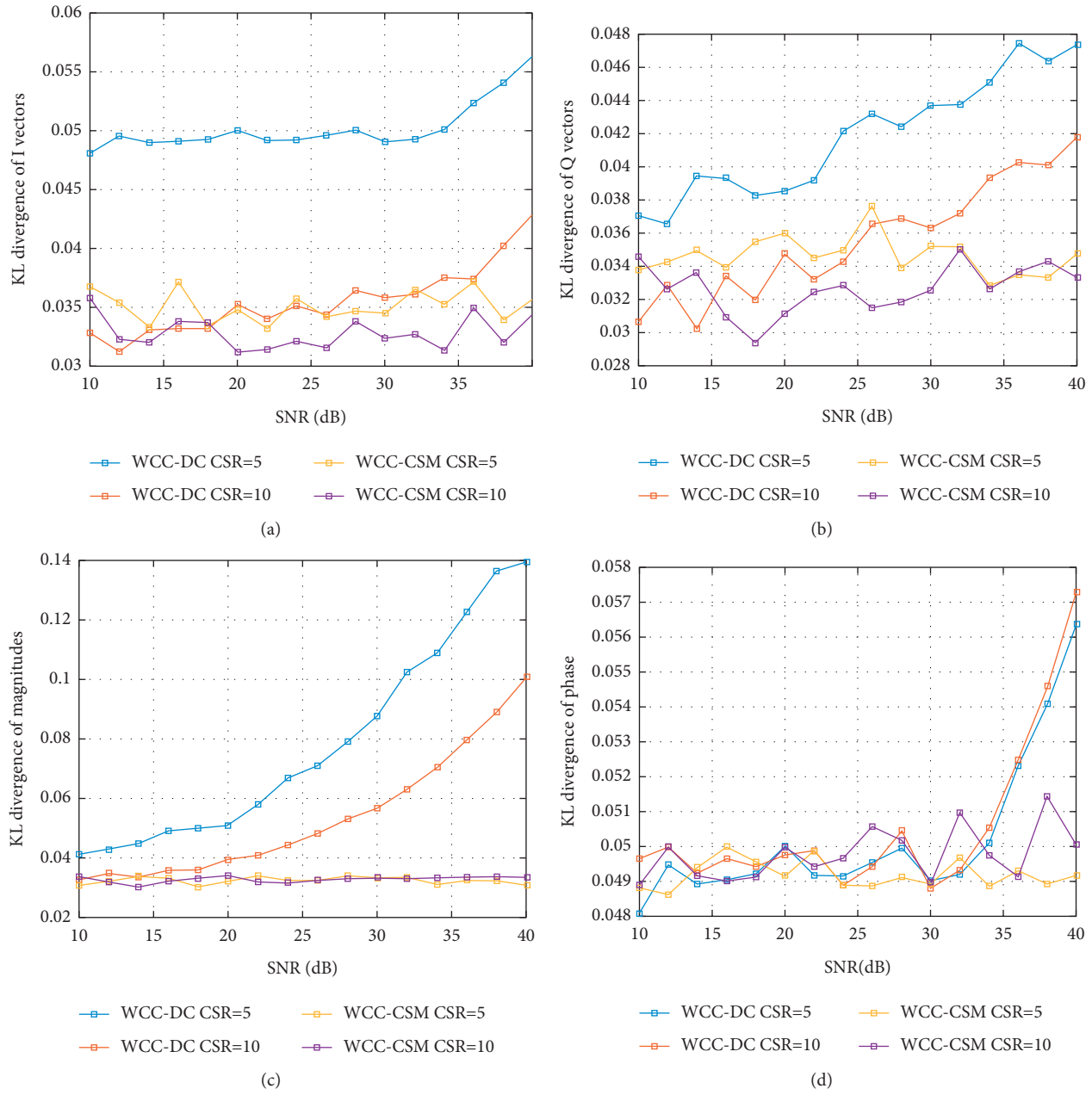

Figure 11: KL divergence of constellation errors with different CSRs: (a) KL divergence of I vectors, (b) KL divergence of Q vectors, (c) KL divergence of magnitudes, and (d) KL divergence of phase.

threshold Γ when SNR = 40 dB, and WCC-DC with CSR = 5 dB exceeds the threshold in the range of SNR = 10,. . .40 dB. In Figure 11(b), the "KL divergence" of WCC-DC with CSR = 5 dB exceeds the threshold Γ at SNR = 23 dB. The "KL divergence" of WCC-DC with CSR = 10 dB exceeds the threshold Γ at SNR = 33 dB. In Figures 11(c) and 11(d), WCC-DC with CSR = 5 dB exceeds the threshold Γ at SNR = 23 dB and SNR = 38 dB, and WCC-DC with CSR = 10 dB exceeds the threshold Γ at SNR = 28 dB and SNR = 37 dB.

As can be seen in Figure 12, WCC-CSM meets the threshold Γand WCC-CSM has a smaller "KS distance" than WCC-DC in the range of SNR = 10, . . ., 40 dB. The "KS distance" of WCC-CSM changes little with different CSRs. And we can regulate the CSR without exceeding the threshold Γ of "KS distance." In Figures 12(a)–12(c), the "KS distance" of WCC-DC with $CSR = 5$ dB exceeds the threshold at $SNR = 10$ dB. In Figure 12(c), the "KS distance" of WCC-DC with CSR = 10 dB exceeds the threshold at SNR = 13 dB.

We can come to a stage conclusion, WCC-CSM meets the threshold of "KL divergence" and "KS distance" in the range of SNR = 10, . . ., 40 dB. Hence, we can regulate the CSR to reduce the BER without exceeding the threshold of "KL divergence" or "KS distance."

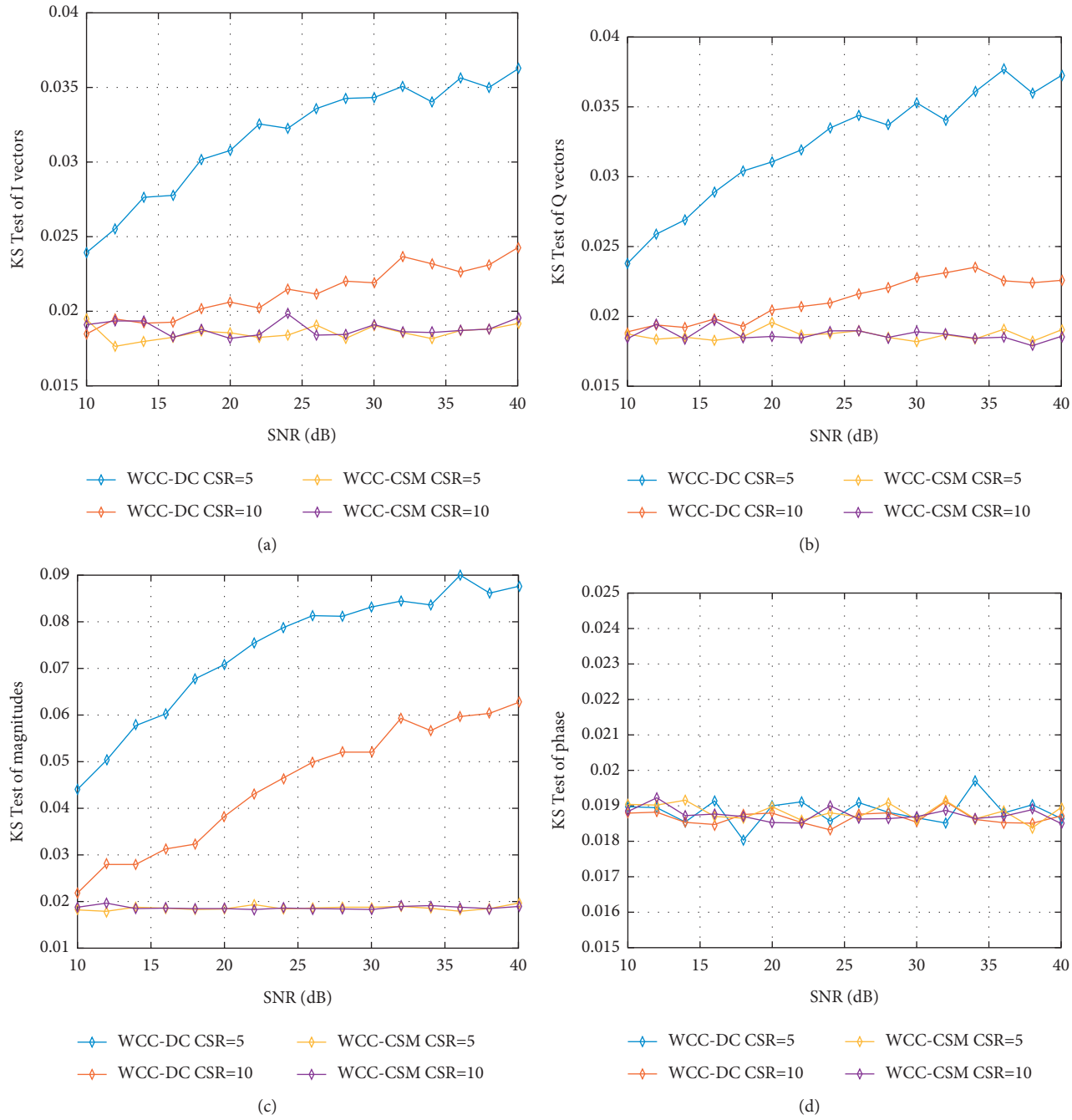

Figure 12: KS distances of constellation errors with different CSRs: (a) KS distances of I vectors, (b) KS distances of Q vectors, (c) KS distances of magnitudes, and (d) KS distances of phase.

5.3. Reliability. The reliability of the system is measured by the BER. As is illustrated in expression (28), the BER decreases with the increase of SNR. In Section 4.1, the optimal *CSR* was proposed. And the approximate solution of optimal CSR is obtained and extended to several scenarios (one relay, two relays). The BER curves of wireless covert channels in several scenarios are shown in Figure 13. The position of Alice, Bob, relay1, and relay 2 was shown in Section 4.

In Figure 13(a), the BER of the classic scenario with different *SNRs* was presented in the range of CSR = 1, 2, . . ., 20 dB. The BER of WCC-CSM with SNR = 15 dB minimizes at CSR = 7 dB, which is 10% lower than the BER at CSR = 15 dB. The approximate solution of optimal CSR is 5 dB. The minimizing BER of WCC-CSM with SNR = 30 dB is 4% at CSR = 8 dB, and the approximate solution of optimal CSR is 7 dB. The minimizing BER of WCC-CSM with SNR = 40 dB is 0.05% at CSR = 9 dB. The theoretical approximation of the optimal CSR·with SNR = 40 dB is 7.5 dB.

It is proved that an optimal CSR exists and the BER minimizes at the optimal CSR. With the increase of SNR, the optimal CSR gradually increases. But the theoretical approximate value of optimal CSR is slightly lower than the

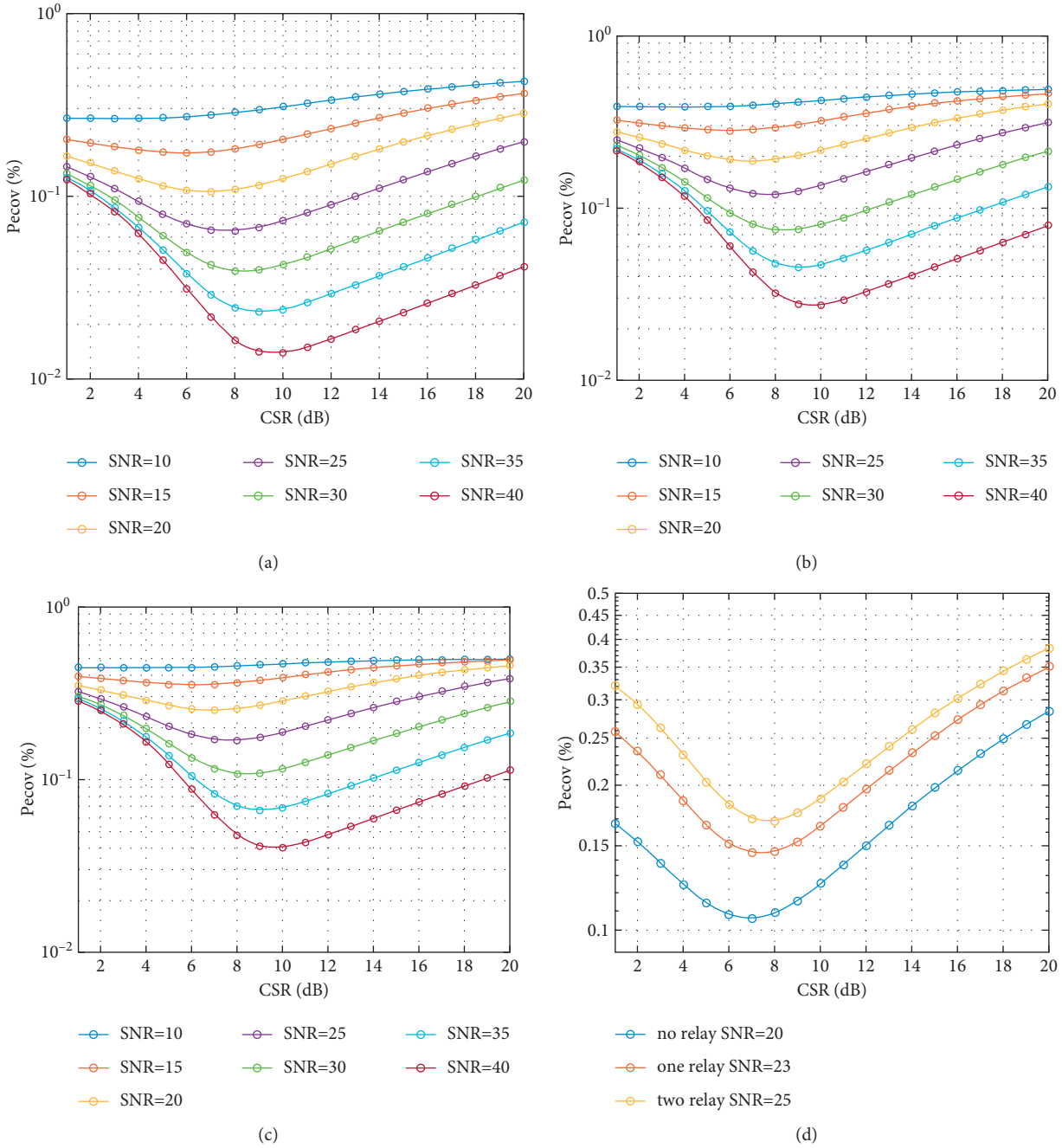

Figure 13: BER of wireless covert channel in typical scenarios. (a) BER of classic scenario with different SNR. (b) BER of one relay with different SNR. (c) BER of two relays with different SNR. (d) Comparison of BER of several scenarios.

simulation results. As can be seen in Figures 13(b) and 13(c), the optimal CSR exists and is slightly higher than the theoretical approximation in scenarios of relays. The BER minimizes at the optimal CSR.

Comparing the BER under the constraints of constant total power, suppose that the SNR in the classic scenario is 20 dB. The SNR in the scenario of one relay is 23 dB, and the SNR in the scenario of two relays is 25 dB. As can be seen in Figure 13(d), the reliability of classic scenario is optimal and the BER minimizes at the optimal CSR. No error correction coding is used in the paper, and the reliability deteriorates in the scenarios of relays. It is proved that simply setting relays without increasing the total power, the BER of covert communication will deteriorate.

Simulation experiments are carried out in wireless channel models of AWGN channel. As can be seen in Figure 13, we can obtain minimum P_{ecov}, $P_{\text{ecov.r1}}$, and $P_{\text{ecov.r2}}$ at the optimal CSR in the AWGN channel. And the optimal CSR achieved in simulation is slightly higher than the theoretical approximation.

6. Conclusions

Reliability and undetectability are the main aspects of wireless covert communication. We considered the BER problem of covert communication based on WCC-CSM. We studied the impact of carrier-secret ratio (CSR) on the BER and investigated the relationship between SNR, CSR, and BER. We obtained the approximate solution of optimal CSR and extended it to the scenario of relays. With the approximate solution of optimal CSR, the process of searching for an actual optimal CSR can be accelerated. Furthermore, we found that the undetectability under the constraints of constant total power depends on the eavesdropper's position. And we found an undetectability deterioration area (UDA) in the scenario of relays, and undetectability deteriorates with setting relays when an eavesdropper is in the UDA.

The simulation proved that there exists an optimal CSR in the AWGN channel. The transmitter can obtain greater reliability with great undetectability at the optimal CSR. Additionally, the reliability deteriorates with setting relays under the constraints of constant total power. Some error correction coding or other methods must be adopted, avoiding the deterioration of BER.

To improve the detection capability of Willie, it is necessary to find a better way to detect the covert communication except "KL divergence" or "KS distance" in our future work.

Data Availability

The data used to support the findings of this study are included within the supplementary information files.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grants nos. U1836104, 61772281, 61702235, 61801073, 61931004, and 62072250).

Supplementary Materials

These files contain the KL divergence of four vectors, KS distance of four vectors, and BERs of wireless covert communication in typical scenarios. (i) KL divergence of constellation errors with different *CSR*.docx: (a) KL divergence of I vectors, (b) KL divergence of Q vectors, (c) KL divergence of magnitudes, and (d) KL divergence of phase. (ii) KS distances of constellation errors with different *CSR*.docx: (a) KS distances of I vectors, (b) KS distances of Q vectors, (c) KS distances of magnitudes, and (d) KS distances of phase. (iii) BERs of wireless covert communication in typical scenarios.docx: (a) BERs of classic scenario with different SNR, (b) BERs of one relay with different SNR, (c) BERs of two relays with different SNR, and (d) comparison of BERs of several scenarios. (*Supplementary Materials*)

References

[1] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2603–2611, 2019.

[2] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wirelessbody area networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332–342, 2013.

[3] M. Xu, D. Wang, Q. Wang, and Q. Jia, "Understanding security failures of anonymous authentication schemes for cloud environments," *Journal of Systems Architecture*, vol. 118, Article ID 102206, 2021.

[4] B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): architectural aspects, challenges, and protocols," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 21, p. e4946, 2020.

[5] A. Al-Qerem, M. Alauthman, A. Almomani, and B. B. Gupta, "IoT transaction processing through cooperative concurrency control on fog-cloud computing environment," *Soft Computing*, vol. 24, no. 8, pp. 5695–5711, 2020.

[6] M. Azees and P. Vijayakumar, "CEKD: computationally efficient key distribution scheme for vehicular ad-hoc networks," *Australian Journal of Basic and Applied Sciences*, vol. 10, no. 2, pp. 171–175, 2016.

[7] H. Kim, E. Kang, D. Broman, and E. A. Lee, "Resilient authentication and authorization for the Internet of Things (IoT) using edge computing," *ACM Transactions on Internet Technology*, vol. 1, no. 1, pp. 1–27, 2020.

[8] M. A. Christie, A. Bhandar, S. Nakandala et al., "Managing authentication and authorization in distributed science gateway middleware," *Future Generation Computer Systems*, vol. 111, pp. 780–785, 2020.

[9] M. Yamni, A. Daoui, O. El ogri et al., "Fractional Charlier moments for image reconstruction and image watermarking," *Signal Processing*, vol. 171, Article ID 107509, 2020.

[10] P. Sun, "Security and privacy protection in cloud computing: discussions and challenges," *Journal of Network and Computer Applications*, vol. 160, Article ID 102642, 2020.

[11] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "IoT-based big data secure management in the fog over a 6G wireless network," *IEEE Internet of Things Journal*, vol. 8, 2020.

[12] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, 2013.

[13] S. Yan, Y. Cong, S. V. Hanly, and X. Zhou, "Gaussian signalling for covert communications," *IEEE Transactions on Wireless Communications*, vol. 18, no. 7, pp. 3542–3553, 2019.

[14] J. Hu, S. Yan, F. Shu, and J. Wang, "Covert transmission with a self-sustained relay," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4089–4102, 2019.

[15] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8286–8297, 2016.

[16] A. Sheikholeslami, M. Ghaderi, D. Towsley, B. A. Bash, S. Guha, and D. Goeckel, "Multi-hop routing in covert wireless networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 3656–3669, 2018.

[17] S. Lee, R. J. Baxley, J. B. McMahon, and R. S. Frazier, "Achieving positive rate with undetectable communication over MIMO Rayleigh channels," in *Proceedings of the 2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, IEEE, A Coruna, Spain, June 2014.

[18] J. Yao, X. Zhou, Y. Liu, and S. Feng, "Secure transmission in linear multihop relaying networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 2, pp. 822–834, 2017.

[19] Z. Liu, J. Liu, Y. Zeng, J. Ma, and Q. Huang, "On covert communication with interference uncertainty," in *Proceedings of the 2018 IEEE International Conference on Communications (ICC)*, IEEE, Kansas City, MO, USA, May 2018.

[20] J. Hu, K. Shahzad, S. Yan, X. Zhou, F. Shu, and J. Li, "Covert communications with a full-duplex receiver over wireless fading channels," in *Proceedings of the 2018 IEEE International Conference on Communications (ICC)*, IEEE, Kansas City, MO, USA, May 2018.

[21] H.-M. Wang, Y. Zhang, X. Zhang, and Z. Li, "Secrecy and covert communications against UAV surveillance via multihop networks," *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 389–401, 2019.

[22] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, 2018.

[23] F. Shu, T. Xu, J. Hu, and S. Yan, "Delay-constrained covert communications with a full-duplex receiver," *IEEE Wireless Communications Letters*, vol. 8, no. 3, pp. 813–816, 2019.

[24] T. V. Sobers, B. A. Bash, D. Goeckel, S. Guha, and D. Towsley, "Covert communication with the help of an uninformed jammer achieves positive rate," in *Proceedings of the 2015 49th Asilomar Conference on Signals, Systems and Computers*, IEEE, Pacific Grove, CA, USA, November 2015.

[25] R. Soltani, B. Bash, D. Goeckel, S. Guha, and D. Towsley, "Covert single-hop communication in a wireless network with distributed artificial noise generation," in *Proceedings of the 2014 52nd Annual Allerton Conference on communication, control, and computing (Allerton)*, IEEE, Monticello, IL, USA, October 2014.

[26] K. Li, P. A. Kelly, and D. Goeckel, "Optimal power adaptation in covert communication with an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3463–3473, 2020.

[27] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 11, pp. 7252–7267, 2018.

[28] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3737–3749, 2020.

[29] K. Shahzad, "Relaying via cooperative jamming in covert wireless communications," in *Proceedings of the 2018 12th International Conference on Signal Processing and Communication Systems (ICSPCS)*, IEEE, Cairns, Australia, December 2018.

[30] K. S. K. Arumugam, M. R. Bloch, and L. Wang, "Covert communication over a physically degraded relay channel with non-colluding wardens," in *Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT)*, IEEE, Vail, CO, USA, June 2018.

[31] A. Abdelaziz and C. E. Koksal, "Fundamental limits of covert communication over MIMO AWGN channel," in *Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS)*, IEEE, Las Vegas, NV, USA, October 2017.

[32] K. S. K. Arumugam and M. R. Bloch, "Covert communication over broadcast channels," in *Proceedings of the 2017 IEEE Information Theory Workshop (ITW)*, IEEE, Kaohsiung, Taiwan, November 2017.

[33] K. S. Kumar Arumugam and M. R. Bloch, "Embedding covert information in broadcast communications," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2787–2801, 2019.

[34] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, *Secret Agent Radio: Covert Communication through Dirty Constellations*, Springer Berlin Heidelberg, Berlin, Germany, 2013.

[35] P. Cao, W. Liu, G. Liu, X. Ji, J. Zhai, and Y. Dai, "A wireless covert channel based on Constellation shaping modulation," *Security and Communication Networks*, vol. 2018, Article ID 1214681, 15 pages, 2018.

[36] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Advances in Cryptology*Springer, New York, NY, USA, 1984.

[37] E. L. Lehmann and J. P. Romano, *Testing Statistical Hypotheses*, Springer Science & Business Media, New York, NY, USA, 2006.

[38] T. M. Cover, *Elements of Information Theory*, John Wiley & Sons, Hoboken, NJ, USA, 1999.

[39] I. L. M. S. Committee, *Wireless LAN media Access Control (MAC) and Physical Layer (PHY) Specifications*, Standards, London, UK, 2009.