Hindawi
Security and Communication Networks
Volume 2018, Article ID 1214681, 15 pages
https://doi.org/10.1155/2018/1214681

Research Article

A Wireless Covert Channel Based on Constellation Shaping Modulation

Pengcheng Cao,[1] Weiwei Liu,[1] Guangjie Liu,[1] Xiaopeng Ji,[1] Jiangtao Zhai,[2] and Yuewei Dai[2]

[1] *The School of Automation, Nanjing University of Science and Technology, Nanjing 210094, China*
[2] *The School of Electrical and Computer Engineering, Jiangsu University of Science and Technology, Zhenjiang 212003, China*

Correspondence should be addressed to Guangjie Liu; gjieliu@njust.edu.cn

Received 29 September 2017; Accepted 4 December 2017; Published 8 January 2018

Academic Editor: Rémi Cogranne

Wireless covert channel is an emerging covert communication technique which conceals the very existence of secret information in wireless signal including GSM, CDMA, and LTE. The secret message bits are always modulated into artificial noise superposed with cover signal, which is then demodulated with the shared codebook at the receiver. In this paper, we first extend the traditional KS test and regularity test in covert timing channel detection into wireless covert channel, which can be used to reveal the very existence of secret data in wireless covert channel from the aspect of multiorder statistics. In order to improve the undetectability, a wireless covert channel for OFDM-based communication system based on constellation shaping modulation is proposed, which generates additional constellation points around the standard points in normal constellations. The carrier signal is then modulated with the dirty constellation and the secret message bits are represented by the selection mode of the additional constellation points; shaping modulation is employed to keep the distribution of constellation errors unchanged. Experimental results show that the proposed wireless covert channel scheme can resist various statistical detections. The communication reliability under typical interference is also proved.

1. Introduction

Covert channel is a specific application of data hiding with the requirement that the hidden secret data is undetectable. It is always classified by the employed carrier; the most popular type of covert channels is network covert channels, which is based on network traffic; information is embedded by manipulating the packet timing information [1–4] or pudding some bits into the packet headers [5]. As the youngest branch of covert channels, wireless covert channel conceals the very existence of secret information by modulating it into the delivered wireless signal [6] or modifying some redundant fields of wireless communication protocols [7]. Wireless covert channels have received increasing attentions because the ubiquitous nature of wireless devices and their localized transmission make it difficult to detect their presence.

Several kinds of wireless covert channels have been proposed [6–16]. In [7, 13], the secret data is embedded in the redundant fields of wireless communication protocols such as padding of frames, headers of the MAC, RLC, and PDCP. In [8], the subcarriers in OFDM-based system which are reserved for channel spacing or synchronization of sender and receiver and to mitigate poor channel response are used to transmit the secret data. The covert transmission in the unused subcarriers has little effect on the normal information transmission. In [12], several wireless covert channels are introduced with the secret data embedded in the phase of short training field, the frequency of long training field, and cyclic prefix in WiFi system. In [14, 15], the secret data are transmitted by covert relay on top of the cover data in wireless relay networks. In [16], the wireless covert channels are presented based on the coordinated operations in the control channel and data channel of MIMO system. These kinds of wireless covert channels are effective but applicable to the specific wireless communication system.

In OFDM-based wireless communication, the deviations of the received signal from the ideal signal which can be called constellation errors are found to widely exist due to channel

impairments and hardware impairments. So the secret data can be modulated into signal similar to constellation errors to resist the detection. In [9], the artificial noise signal generated by secret data is added to the cover signal directly. In this scheme, the spread spectrum technique is applied in the artificial noise signal so that the artificial noise signal has little influence on the transmission of cover signal. The informed receiver can extract the secret data by removing the cover signal. This covert channel is generalized to the MIMO system later [11]. However, those covert channels are easily interfered by wireless channel noise.

Recently, a wireless covert channel based on dirty constellation is proposed which modulates the secret information bits into constellation errors around the normal constellation points [6]. The additional constellation points are added into the original constellation which will be used for modulating instead of the original points. The secret information bits are represented by the selection of these additional constellation points; for example, four additional constellation points can be used to represent two secret message bits. The generation mode of these additional constellation points can be controlled by a shared secret key. However, when the detector is near the sender, the regularity of dirty constellation may result in the poor resistance to some statistical detection [17].

In this paper, the wireless covert channel with constellation shaping modulation is proposed. The model of constellation error is used for the design of dirty constellation. For each subcarrier of OFDM, the distribution of the in-phase and quadrature (I/Q) vectors of the constellation error is calculated with the constellation at the normal receiver; the secret information is modulated into artificial noise that distributes as the real channel noise. Compared with the existing dirty constellation scheme, the undetectability and reliability can both be improved. In addition, the mapping sequence is unnecessary to be synchronized in the proposed scheme.

This paper is organized as follows. In the next section, some background and related works including wireless covert channel with dirty constellation are introduced. In Section 3, some typical detection schemes in the field of covert timing channels are developed into wireless covert channels. In Section 4, we describe the proposed wireless covert channel scheme based on constellation shaping modulation. Section 5 gives the experimental results on undetectability and reliability. Finally, Section 6 concludes the whole paper.

2. Wireless Covert Channel with Dirty Constellation

In the wireless covert channels with dirty constellation (WCC-DC), the secret message bits can be transmitted as the constellation error of the normal cover signal in order to reduce the suspicion by all uninformed observers. The wireless covert channel relies on that the cover message bits are transmitted at a low rate (BPSK or QPSK) with supplemental redundancy that can be utilized as an additional QPSK signal by an informed receiver.

With the example of QPSK, the process at the sender in the wireless covert channel with dirty constellation is demonstrated in Figure 1. First, the mapping sequence bits

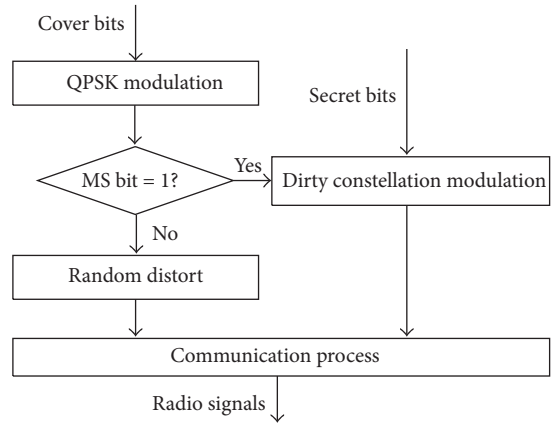

Figure 1: Process at the sender in WCC-DC.

are checked after the cover message bits are modulated by QPSK constellation. The mapping sequence bits are used to select the appropriate mapping for covert and noncovert subcarriers. For example, the mapping sequence bit can be set to "1" if corresponding cover signal of the subcarrier is chosen to embed the secret message bits by dirty constellation, and the mapping sequence bit is set to "0" if corresponding cover signal of the subcarrier is just random distorted to mimic the influence of various interferences. The embedding rate of the wireless covert channels depends on the proportion of the mapping sequence length for the number of "1." The mapping sequence bits must be shared between the sender and informed receiver. Then the covert signal and noncovert signal are blended for transmission. With some communication processes such as IFFT, adding cyclic prefix and so on, the covert signal is transmitted as radio signal. At the informed receiver, the covert signal is picked out by the mapping sequence bits and the secret message bits are extracted by the corresponding demodulation of dirty constellation. Even when an adversary has access to the I/Q vectors of the covert signal, they will interpret the point cloud as a noisy version of a valid QPSK constellation and would not suspect the presence of a covert channel.

The dirty constellation based on QPSK is shown in Figure 2(a). In this paper, normal constellation point denotes the ideal constellation point of cover message bits, covert constellation point denotes the corresponding constellation point of the secret message bits around normal constellation points, and the cover signal denotes the corresponding signal of the ideal constellation point of cover message bits. The covert signal denotes the signal of secret constellation point which contains both cover and secret message bits. I vector and Q vector denote the components in I-plane and Q-plane of the constellation.

To generate the covert signal, the covert constellation points are located around the ideal QPSK constellation points of the cover signal. To modulate a covert subcarrier carrying the cover and covert bits together, the cover constellation point is first chosen, specifying the quadrant, followed by remapping that point to one of the four covert QPSK points around the chosen cover QPSK point. Then the dirty

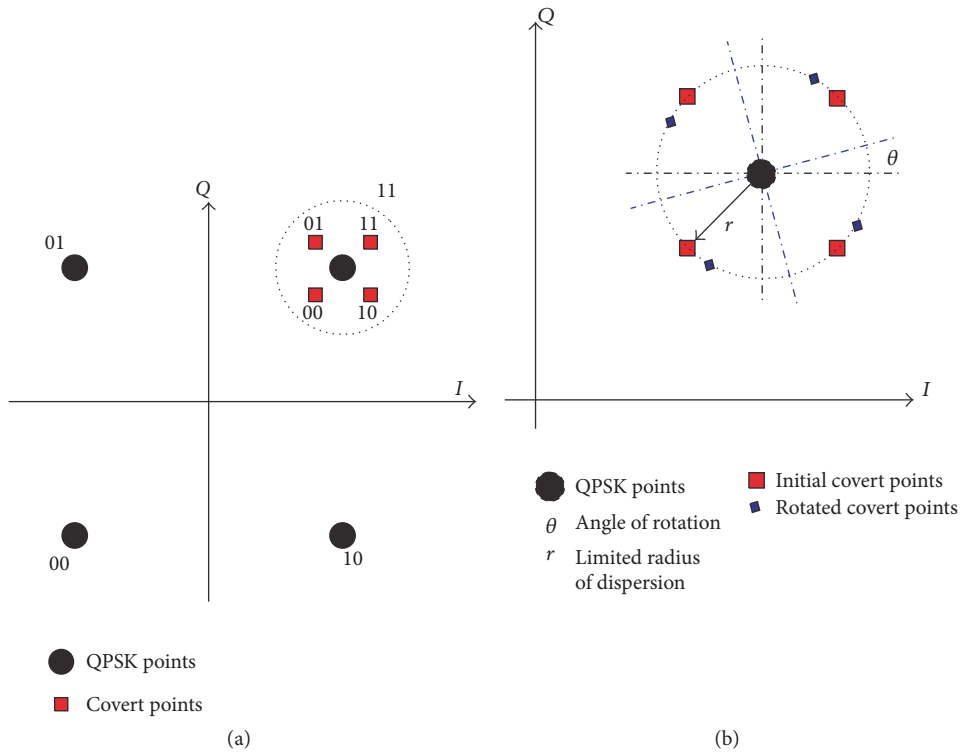

Figure 2: Dirty constellation: (a) covert QPSK constellation and (b) covert constellation.

constellation is further improved to reduce the probability of detection by adversaries. The covert points are put closer to the ideal QPSK point and remapped symmetrically around the QPSK points with a mutual separation of $2/\sqrt{42}$, which is a distance equal to that of a 64 QAM constellation. The I/Q vectors of the covert constellation points are randomized with a Gaussian distribution but limit their dispersion to a radius of $\sqrt{2/42}$. The limitation of dispersion ensures that the covert constellation points are hidden in the cloud of a dispersed (noisy) QPSK point cloud. To have the covert symbols blend with the cloud of the random distorted QPSK points, the covert constellation points are rotated round the corresponding ideal QPSK point for every subcarrier that is mapped to a covert constellation as shown in Figure 2(b). The rotation is performed using a monotonically increasing angle θ; the sender and receiver both start with $\theta = 0^\circ$ at the start of the packet and increment θ for each covert subcarrier.

Even if the dirty constellation is improved, there is always a finite probability that the covert constellations are visible with all subcarriers transmitting covert signal. So only a part of subcarriers are chosen to transmit the covert signal. In order to avoid sudden changes in the modulation characteristics, the cover signal transmitted by noncovert subcarriers should always be distorted to mimic the influence of practical channels.

3. Countermeasures for Wireless Covert Channel Detection

As a covert communication technique aiming to deliver secret data via public wireless channel, the wireless covert channels should be secure against various detections. In other words, the covert transmissions in wireless channels have to be indistinguishable from normal transmissions. However, to the best of our knowledge, there still exist no specialized works concerning the detection of wireless covert channels. In the field of signal analysis, the frequency spectrum is always used to measure the difference between two signals. In [6], error vector magnitude (EVM) of constellations, peak to average power ratio (PAPR), and temporal variation of average signal power are used to measure the signal distortion in wireless covert communication. In fact, statistic-based detection should also be developed like covert timing channels [18–20]. In this paper, we propose Kolmogorov-Smirnov (KS) test [18] and regularity test [19] in wireless covert channel, which can be used to measure the difference between cover and covert signal from the aspect of frequency and regularity characteristic. The KS test is a shape test and the regularity test is a high order statistic-based test.

3.1. Kolmogorov-Smirnov Test in Wireless Covert Channel. In an OFDM system, we select the I/Q vectors and magnitudes in constellation of all the subcarriers as the detection objects, which can be captured by vector-signal analyzers or software defined radios. Denote $\mathbf{s}_a$ and $\mathbf{s}_b$ as the normal wireless signal and target wireless signal, respectively. The I/Q vectors and magnitudes corresponding to $\mathbf{s}_a$ are denoted by $\mathbf{a}^I = (a_1^I, \ldots, a_n^I)$, $\mathbf{a}^Q = (a_1^Q, \ldots, a_n^Q)$, and $\mathbf{a}^M = (a_1^M, \ldots, a_n^M)$, respectively. And the I/Q vectors and magnitudes corresponding to $\mathbf{s}_b$ are denoted by $\mathbf{b}^I = (b_1^I, \ldots, b_n^I)$, $\mathbf{b}^Q = (b_1^Q, \ldots, b_n^Q)$, and $\mathbf{b}^M = (b_1^M, \ldots, b_n^M)$, respectively.

The KS test statistic measures the maximum distance between distribution of $\mathbf{a}^{\delta}$ and $\mathbf{b}^{\delta}$ with $\delta \in \{I, Q, M\}$ to determine whether or not the distribution of $\mathbf{b}^{\delta}$ differs from that of $\mathbf{a}^{\delta}$. The histogram of the elements of $\mathbf{a}^{\delta}$ and $\mathbf{b}^{\delta}$ is made into K bins which are denoted by $B_1^{\delta}, \ldots, B_K^{\delta}$. The number of the elements of $\mathbf{a}^{\delta}$ and $\mathbf{b}^{\delta}$ in B_i^{δ} is denoted by $H_a^{\delta}(i)$ and $H_b^{\delta}(i)$ with $i \in \{1, 2, \ldots, K\}$, respectively. The cumulative distribution functions of $\mathbf{a}^{\delta}$ and $\mathbf{b}^{\delta}$ in B_i^{δ} are defined by

$$F_a^{\delta}(i) = \frac{\sum_{\alpha=1}^{i} H_a^{\delta}(\alpha)}{n}, \qquad F_b^{\delta}(i) = \frac{\sum_{\alpha=1}^{i} H_b^{\delta}(\alpha)}{n}. \tag{1}$$

The Kolmogorov-Smirnov distance between $\mathbf{a}^{\delta}$ and $\mathbf{b}^{\delta}$ is defined as

$$\text{KSTEST} = \max \frac{\left|\sum_{\alpha=1}^{i} H_b^{\delta}(\alpha) - \sum_{\alpha=1}^{i} H_b^{\delta}(\alpha)\right|}{n}, \quad \forall i \in \{1, 2, \ldots K\}. \tag{2}$$

3.2. Regularity Test in Wireless Covert Channel. For the regularity test in wireless covert channel, $\mathbf{a}^{\delta}$ and $\mathbf{b}^{\delta}$ with $\delta \in \{I, Q, M\}$ are divided into n/w sets $(\mathbf{a}^{\delta}_{\text{sub-1}}, \ldots, \mathbf{a}^{\delta}_{\text{sub-}n/w})$ and $(\mathbf{b}^{\delta}_{\text{sub-1}}, \ldots, \mathbf{b}^{\delta}_{\text{sub-}n/w})$, respectively. Each set contains w elements, respectively, which are denoted by $(\mathbf{a}^{\delta}_{\text{sub-1}}, \ldots, \mathbf{a}^{\delta}_{\text{sub-}n/w})$ and $(\mathbf{b}^{\delta}_{\text{sub-1}}, \ldots, \mathbf{b}^{\delta}_{\text{sub-}n/w})$ where $\mathbf{a}^{\delta}_{\text{sub-}i} = (a^{\delta}_{(i-1)\cdot w+1}, \ldots, a^{\delta}_{i\cdot w})$ and $\mathbf{b}^{\delta}_{\text{sub-}i} = (b^{\delta}_{(i-1)\cdot w+1}, \ldots, b^{\delta}_{i\cdot w})$. Then, for each set in $\mathbf{a}^{\delta}$, the standard deviation of the set $\mathbf{a}^{\delta}_{\text{sub-}i}$ is computed as

$$\sigma_i^{\delta} = \text{STDEV}\left(a^{\delta}_{(i-1)\cdot w+k},\ \forall k \in \{1, 2, \ldots w\}\right). \tag{3}$$

The regularity of $\mathbf{a}^{\delta}$ is the standard deviation of the pairwise differences between each σ_i^{δ} and σ_j^{δ} for all sets with $i < j$.

$$\text{regularity}_a^{\delta} = \text{STDEV}\left(\frac{\left|\sigma_i^{\delta} - \sigma_j^{\delta}\right|}{\sigma_i^{\delta}},\ i < j,\ \forall i, j\right). \tag{4}$$

The regularity of $\mathbf{b}^{\delta}$ which is denoted by $\text{regularity}_b^{\delta}$ can be obtained with (4). The regularity test in wireless covert channel determines whether or not the regularity of $\mathbf{a}^{\delta}$ and $\mathbf{b}^{\delta}$ is different. If the $|\text{regularity}_b^{\delta} - \text{regularity}_a^{\delta}| > \Delta$, the target signal $\mathbf{s}_b$ is determined to be the covert one.

3.3. Adversary Model. The KS test and regularity test in wireless covert channels require the samples for reference which can be captured from the normal constellation errors of the received signal. In practice, the transmitted signal in OFDM-based wireless communication is easily interfered by channel fading and noise. It is very hard to model the characteristics of the constellation errors of the received signal as it varies greatly with the power of the noise changing. Thus the referred normal constellation errors of the received signal on different channel conditions are required for the practical detection of the wireless covert channels. In this paper, we assume that the detector has the knowledge of the wireless covert channel schemes and has access to normal constellation errors of the received signal on different channel conditions. When the detector captures the signal, he can get the appropriate referenced signal for detection.

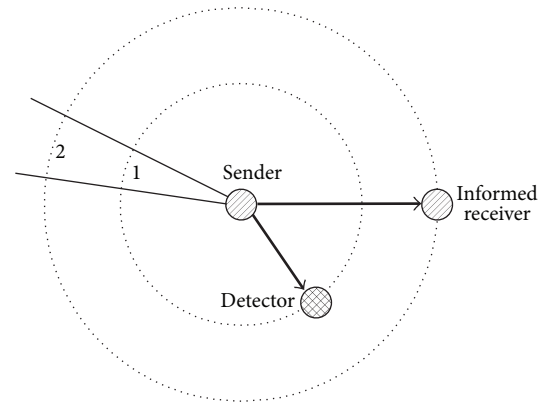

Figure 3: Adversary model on the condition that the detector is closer to the sender.

In [6], it is assumed that the informed receiver and the detector are located at the same place. However, the wireless channel conditions of the informed receiver and the detector are always different in real world. The detector may set more than one signal analyzer in some area. Due to the broadcast nature of the radio signal' transmission, one of the detector's signal analyzers may receive the radio signal with less interference and higher transmission SNR than the informed receiver which is illustrated in Figure 3. The undetectability of a wireless covert channel should be benchmarked under noisy channel with a range of noise SNRs. If the wireless covert channel can achieve well performance on detection under noisy channel with higher SNR, it can be proved undetectable and vice versa.

4. Wireless Covert Channel with Constellation Shaping Modulation

In this section, we propose a wireless covert channel with constellation shaping modulation (WCC-CSM). Its general framework for OFDM-based wireless communication system is demonstrated in Figure 4. In this paper, we assume that the common QPSK is the modulation scheme for each subcarrier of the OFDM-based wireless communication. All subcarrier can be used to establish wireless covert channel in the proposed scheme. The secret message bits are modulated into artificial noise signal by constellation shaping modulation. In every subcarrier, the artificial noise signal is added to the cover signal to generate the covert signal. The detailed description of the framework is given as follows.

In the framework, the cover data bits $\mathbf{m}_c$ are first modulated into the cover signal $\mathbf{s}_c$ by QPSK. With the distribution of the referred normal constellation errors $\mathbf{s}_{\text{normal}}$, the secret message bits $\mathbf{m}_s$ are modulated into the artificial noise $\mathbf{s}_s$

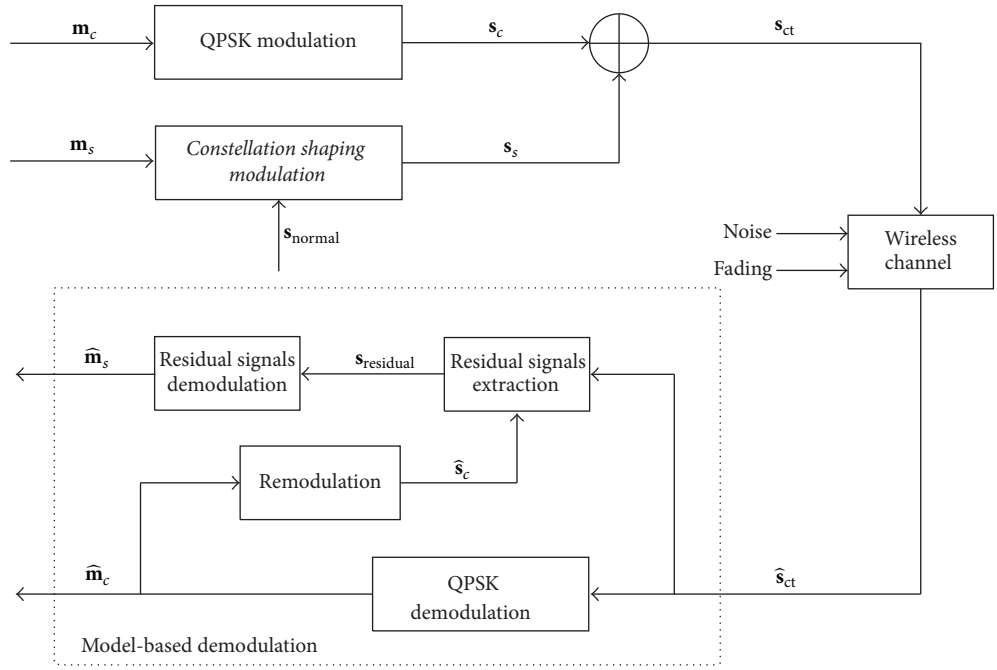

Figure 4: The framework of proposed wireless covert channel.

with constellation shaping modulation. The covert signal $\mathbf{s}_{ct}$ is generated by adding artificial noise signal $\mathbf{s}_s$ to the cover signal $\mathbf{s}_c$. The covert signal $\mathbf{s}_{ct}$ is translated into radio signal by a series of wireless communication processes, for example, IFFT and adding cyclic prefix, which are omitted in the framework. The receiver captures the covert signal $\widehat{\mathbf{s}}_{ct}$, which is the noisy version of the covert signal $\mathbf{s}_{ct}$ under the channel of various interferences. Then the received cover message bits $\widehat{\mathbf{m}}_c$ are demodulated by QPSK, and the residual signal $\mathbf{s}_{residual}$ are extracted by removing the reconstructed cover signal $\widehat{\mathbf{s}}_c$ from $\widehat{\mathbf{s}}_{ct}$. At last, the secret message bits $\widehat{\mathbf{m}}_s$ can be demodulated from $\mathbf{s}_{residual}$.

As shown in Figure 4, the proposed framework consists of constellation shaping modulation, the model-based demodulation. These are described in detail in the following subsections.

4.1. Constellation Shaping Modulation. The constellation shaping modulation is employed to generate the artificial noise signal $\mathbf{s}_s$ with secret message bits $\mathbf{m}_s$ embedded. The normal constellation errors $\mathbf{s}_{normal}$ are first divided into a certain amount of bins to capture the information about the distribution. Since the I vectors and Q vectors in constellation are orthogonal, the parameters of the distribution of $\mathbf{s}_{normal}$ can be obtained in different planes, respectively. Then, with the parameters of the distribution in each plane, the secret message bits $\mathbf{m}_s$ can be modulated into the I/Q vectors of artificial noise signal $\mathbf{s}_s$. The distribution of the I/Q vectors of $\mathbf{s}_s$ is kept the same as that of normal constellation errors $\mathbf{s}_{normal}$.

The secret message bits are denoted by $\mathbf{m}_s = (m_{s1}, \ldots, m_{sn})$. The I/Q vectors of artificial noise signal $\mathbf{s}_s$ are denoted by $\mathbf{x}_s^I + j \cdot \mathbf{x}_s^Q$. Here $\mathbf{x}_s^I, \mathbf{x}_s^Q$ are the I/Q vectors of the artificial noise signal at the sender satisfying $\mathbf{x}_s^I = (x_{s1}^I, \ldots, x_{sn}^I)$, $\mathbf{x}_s^Q = (x_{s1}^Q, \ldots, x_{sn}^Q)$. The constellation shaping modulation function is defined as

$$F_{\mathrm{CMS}}(\mathbf{m}_s) = \mathbf{x}_s^I + j \cdot \mathbf{x}_s^Q. \tag{5}$$

The I/Q vectors of the normal constellation errors captured from the actual communication are input to constellation shaping modulation for binning, which are denoted by $\mathbf{x}_{\mathrm{normal}}^I + j \cdot \mathbf{x}_{\mathrm{normal}}^Q$ when $\mathbf{x}_{\mathrm{normal}}^I = (x_{\mathrm{normal},1}^I, \ldots, x_{\mathrm{normal},N}^I)$, $\mathbf{x}_{\mathrm{normal}}^Q = (x_{\mathrm{normal},1}^Q, \ldots, x_{\mathrm{normal},N}^Q)$. Take I plane, for example, the histograms of $\mathbf{x}_{\mathrm{normal}}^I$ are divided by bins $[B_{L,1}, B_{U,1}]$, $\ldots, [B_{L,L}, B_{U,L}]$, where $B_{L,i}$ and $B_{U,i}$ are the low bound and up bound of the ith bins and the bounds satisfying $B_{L,i} = B_{U,i-1}$. The number of $\mathbf{x}_{\mathrm{normal}}^I$ in $[B_{L,i}, B_{U,i}]$ is denoted by $H_{\mathrm{normal}}^I(i)$. In this paper, the bins are divided with equiprobable area; it can be written as

$$H_{\mathrm{normal}}^I(i) = \frac{N}{L}, \quad \forall i \in \{1, \ldots, L\}. \tag{6}$$

The example of histogram of $\mathbf{x}_{\mathrm{normal}}^I$ with equal bins under Gaussian noise is illustrated in Figure 5. While the bins have different widths, the total area of each bin is equal.

It is assumed that there are two secret message bits embedded in one artificial noise signal in a subcarrier, so the element in $\mathbf{m}_s$ can be further written as $m_{si} = (m_{si,1}, m_{si,2}) \in \{00, 01, 11, 10\}$, $i = 1, \ldots, n$. The bit $m_{si,1}$ can be embedded in corresponding I vector x_{si}^I, and the bit $m_{si,2}$ can be embedded in corresponding Q vector x_{si}^Q. the center line α in I plane is obtained as the boundary $B_{U,L/2}$ or $B_{L,L/2+1}$.

$$\alpha = B_{L,L/2+1} = B_{U,L/2}. \tag{7}$$

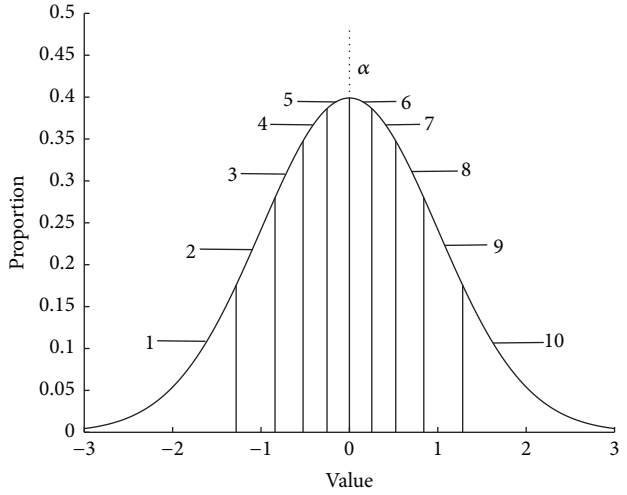

Figure 5: The equiprobable bins in I plane with $L = 10$.

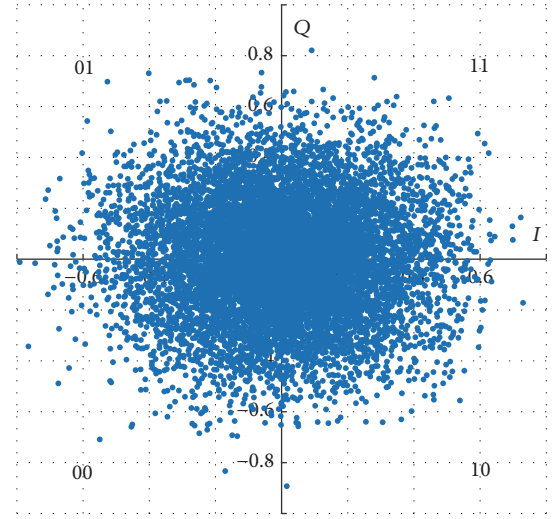

Figure 6: Extracted modulation error in constellation.

The corresponding center value of each bin are obtained as $\mathbf{c} = (c_1, c_2, \ldots, c_L)$ satisfying

$$c_i = \frac{1}{2}\left(B_{L,i} + B_{U,i}\right), \quad \forall i \in \{1, 2, \ldots, L\}. \tag{8}$$

The bit $m_{si,1}$ can be modulated into the corresponding I vector x_{si}^I according to the below equation.

$$x_{si}^I = \begin{cases} c_i, & m_{si,1} = 0,\ R \cdot \dfrac{N}{2} \in \left[\dfrac{N}{L} \cdot (i-1), \dfrac{N}{L} \cdot i\right], \\ c_j, & m_{si,1} = 1,\ (R+1) \cdot \dfrac{N}{2} \in \left[\dfrac{N}{L} \cdot (j-1), \dfrac{N}{L} \cdot j\right]. \end{cases} \tag{9}$$

Here, R is a random number with uniform distribution on $[0, 1]$. Equation (9) keeps that the distribution of the regenerated I vectors is the same as that of the normal constellation errors in the histogram with L bins meanings. The center lines α of histogram of $\mathbf{x}_{\text{normal}}^I$ should be shared with the informed receiver. The modulation in Q plane works in the same way. As shown in Figure 6, the I/Q vectors of artificial noise signal are the complex modulation vectors with the similar distribution to that of normal constellation errors in plain sight.

4.2. Model-Based Demodulation. The model-based demodulation is used to extract the residual signal and demodulate the secret message bits. The I/Q vectors of received covert signal $\widehat{\mathbf{s}}_{\text{ct}}$ are denoted by $\widehat{\mathbf{x}}_{\text{ct}}^I + j \cdot \widehat{\mathbf{x}}_{\text{ct}}^Q$; the received cover message bits denoted by $\widehat{\mathbf{m}}_c$ can be demodulated by QPSK with

$$F_{\text{de-QPSK}}\left(\widehat{\mathbf{x}}_{\text{ct}}^I + j \cdot \widehat{\mathbf{x}}_{\text{ct}}^Q\right) = \widehat{\mathbf{m}}_c. \tag{10}$$

Then the cover message bits $\widehat{\mathbf{m}}_c$ are remodulated by QPSK to acquire the ideal I/Q vectors of received cover signal $\widehat{\mathbf{s}}_c$ in each subcarrier.

$$F_{\text{QPSK}}\left(\widehat{\mathbf{m}}_c\right) = \widehat{\mathbf{x}}_c^I + j \cdot \widehat{\mathbf{x}}_c^Q. \tag{11}$$

Here $\widehat{\mathbf{x}}_c^I, \widehat{\mathbf{x}}_c^Q \in \{-1/\sqrt{2}, 1/\sqrt{2}, \}^n$ are the ideal normalized I/Q vectors of the received cover signal by QPSK modulation.

The informed receiver can extract the I/Q vectors of residual signal $\mathbf{s}_{\text{residual}}$ with

$$\mathbf{x}_{\text{residual}}^I + j \cdot \widehat{\mathbf{x}}_{\text{residual}}^Q = \left(\widehat{\mathbf{x}}_{\text{ct}}^I - \widehat{\mathbf{x}}_c^I\right) + j \cdot \left(\widehat{\mathbf{x}}_{\text{ct}}^Q - \widehat{\mathbf{x}}_c^Q\right). \tag{12}$$

Then the secret message bits can be extracted from the I/Q vectors $\mathbf{x}_{\text{residual}}^I + j \cdot \widehat{\mathbf{x}}_{\text{residual}}^Q$ of residual signal by the corresponding demodulation algorithm.

$$F_{\text{de-shaping}}\left(\mathbf{x}_{\text{residual}}^I + j \cdot \widehat{\mathbf{x}}_{\text{residual}}^Q\right) = \widehat{\mathbf{m}}_s. \tag{13}$$

Taking I plane, for example, with the I vector $x_{\text{residual},i}^I$ of residual signal and the corresponding center line value α shared between the sender and the receiver, the secret message bits can be demodulated with (14). The demodulation in Q plane works in the same way.

$$\widehat{m}_{si,1} = \begin{cases} 0, & x_{\text{residual},i}^I < \alpha, \\ 1, & x_{\text{residual},i}^I \geq \alpha. \end{cases} \tag{14}$$

Since the I/Q vectors of residual signal have the similar distribution to that of normal constellation errors in our proposed scheme directly, the undetectability of the proposed wireless covert channel is better than that of the wireless covert channels with dirty constellation which can be considered as the state-of-the-art existing method. At the same time, the constellation errors in each subcarrier can be used to transmit the secret data; the mapping sequence in the wireless covert channel with dirty constellation [6] is not necessary. No extra bandwidth is required for transmitting the shared mapping sequence.

5. Experimental Results

5.1. Experimental Setup. In this section, we benchmark the proposed scheme by examining the undetectability and

reliability. The cover message bits and the secret message bits are both provided by a pseudo-random bits generator. The wireless communication is set on an 802.11a/g PHY layer. The wireless covert channel is performed on all 100000 symbols. There are 48 subcarriers in a symbol in transmissions. TGn channel models are selected for the wireless channel models in simulation experiment [21]. The TGn channel models B and D chosen for the simulation experiment on 802.11a/g PHY layer are universal. The sender and informed receiver are kept stationary. So the Doppler shift of the wireless communication is negligible. The normal constellation errors with the size $N = 2000$ can be selected from the residual signal with the specific relative power captured from the actual communication. So the rest of the residual signal is used to be referenced normal constellation errors for detection. In the IEEE 802.11a/g standard [22], the modulation error at the sender for a QPSK modulation is mandated to be no more than 10 dB or 13 dB from an ideal modulation with different code rates. The relative powers of chosen normal constellation error are set to −10 dB and −13 dB. The wireless covert channel with dirty constellation (WCC-DC) is chosen for comparison in some simulation experiments. This covert channel with only 10% subcarriers carrying the secret message bits has been proved safe enough in [6]. The undetectability of the proposed wireless covert channels is measured by KS test and regularity test. In KS test, the KS distance is computed with 1920 constellation errors in subcarriers which are the constellation errors in 20 symbols. In regularity test, we compute the regularity measures for 1920 constellation errors under set size $w = 48$. The detection measures of the I vectors, Q vectors, and magnitudes of constellation errors are presented in the range of transmission SNR $= 10, \ldots, 40$. The reliability of the proposed wireless covert channels is measured by BER.

5.2. Undetectability. The relationship of undetectability and the number of the bins L in the proposed scheme is considered. The wireless channel models in experiments are all set to be TGn channel model B. The relative power of normal constellation errors is set to be $P_e = -10$ dB. The KS distances and regularity measures of I vectors, Q vectors, and magnitudes of constellation errors in the proposed wireless covert channels are presented in Figures 7 and 8 with $L = 50, 100, 200$. The detection measures of the wireless covert channels with dirty constellation (WCC-DC) are also presented for comparison. Each detection measure is obtained as an average over repeated experiments. In Figures 7(a) and 7(b), with the transmission SNR increasing, the KS distances between I vectors and Q vectors of constellation errors in the proposed wireless covert channels with different bin numbers remain almost unchanged, and the KS distances between I vectors and Q vectors in WCC-DC slightly increase. In Figure 7(c), with the transmission SNR increasing, the KS distances between magnitudes of constellation errors in all the proposed wireless covert channels are kept steady, but the KS distances between magnitudes in WCC-DC obviously increase. increase. In Figures 8(a) and 8(b), the regularity measures of I vectors and Q vectors of constellation errors in WCC-DC and proposed methods are only a little different from those of referenced normal constellation errors. In Figure 8(c), the regularity measures of magnitudes of constellation errors in all the proposed wireless covert channels are only a little different from those of referenced normal constellation errors, but the regularity measures of magnitudes in WCC-DC are a little higher than those of referenced normal constellation errors.

It is shown that the undetectability is not concerned with the bin numbers in proposed wireless covert channels. The undetectability of the proposed wireless covert channel is better than that of existing methods, especially with high transmission SNR.

Then, we concentrate on the relationship of undetectability and the wireless channel models. The bin number in the proposed wireless covert channels is set to be $L = 100$. The normal constellation errors are applied with the relative power $P_e = -10$ dB. The detection measures of I vectors, Q vectors, and magnitudes of constellation errors in the proposed wireless covert channels in TGn channel models B and D are presented in Figures 9 and 10. The detection measures of the wireless covert channels with dirty constellation (WCC-DC) are also presented for comparison. Each detection measure is obtained as an average over repeated experiments. In Figures 9(a)–9(c), the KS distances of I vectors, Q vectors, and magnitudes of constellation errors in proposed wireless covert channel and WCC-DC are almost equal in different channel models. With the transmission SNR increasing, the KS distances between I vectors, Q vectors, and magnitudes of constellation errors in the proposed wireless covert channels are kept steady in different channel models, and the KS distances between I vectors, Q vectors, and magnitudes in WCC-DC also increase in different channel models. In Figures 10(a)–10(c), the regularity measures of I vectors, Q vectors, and magnitudes of constellation errors in the proposed wireless covert channels and referenced normal constellation errors are almost equal, the regularity measures of I vectors and Q vectors of constellation errors in WCC-DC are only little different from those of referenced normal constellation errors, and the regularity measures of magnitudes in WCC-DC are a little higher than those of referenced normal constellation errors in different channel models.

It is shown that the undetectability of the proposed wireless covert channel is not related to wireless channel models. And the undetectability of the proposed wireless covert channel is better than that of existing methods in different channel models.

At last, relationship of the undetectability and the relative power of normal constellation errors is discussed. The bin number in the proposed wireless covert channels is set to be $L = 100$. The detection measures of I vectors, Q vectors, and magnitudes of constellation errors in the proposed wireless covert channels are presented in Figures 11 and 12 with the relative power of normal constellation errors $P_e = -10$ dB and $P_e = -13$ dB in TGn channel models B and D. Each detection measure is obtained as an average over repeated experiments. With the transmission SNR increasing, the KS distances between I vectors, Q vectors, and magnitudes of constellation errors in the proposed wireless covert channels are almost steady with different relative power of normal

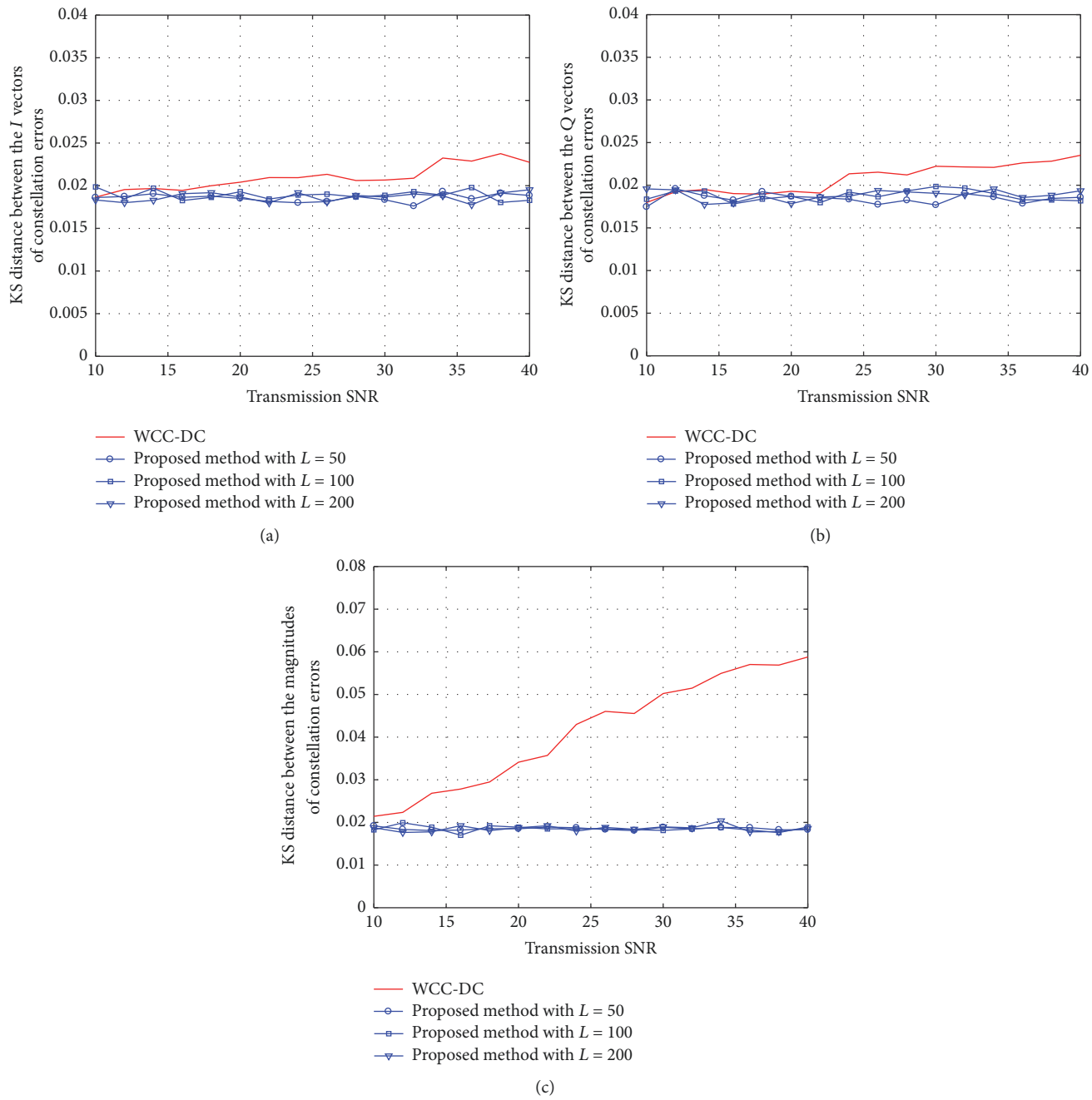

Figure 7: KS distances between (a) I vectors, (b) Q vectors, and (c) magnitudes of constellation errors with different bin numbers.

constellation errors and channel models, and the regularity measures of I vectors, Q vectors, and magnitudes in the proposed wireless covert channels are little different from those of referenced normal constellation errors.

It is shown that the undetectability in the proposed wireless covert channels is kept almost unchanged with different relative power of normal constellation errors.

5.3. Reliability. The relationship of reliability and the number of the bins L in the proposed scheme is considered. The wireless channel model in experiments is set to be TGn channel model B. The relative power of normal constellation errors is set to be $P_e = -10$ dB. The BERs of the proposed wireless covert channels are presented in Figure 15 with $L = 50, 100, 200$. The BER of WCC-DC is also presented for comparison. Each bit error rate is obtained as an average over repeated experiments. In Figure 13, the bit error rates of the proposed wireless covert channels are almost equal with different bin numbers. The bit error rates of WCC-DC are lower than those of all the proposed wireless covert channels. The degradation of reliability is considered as the cost for the improvement in undetectability. Given that the covert transmission rate of the proposed wireless covert channels is ten times as large as that in WCC-DC, the experimental

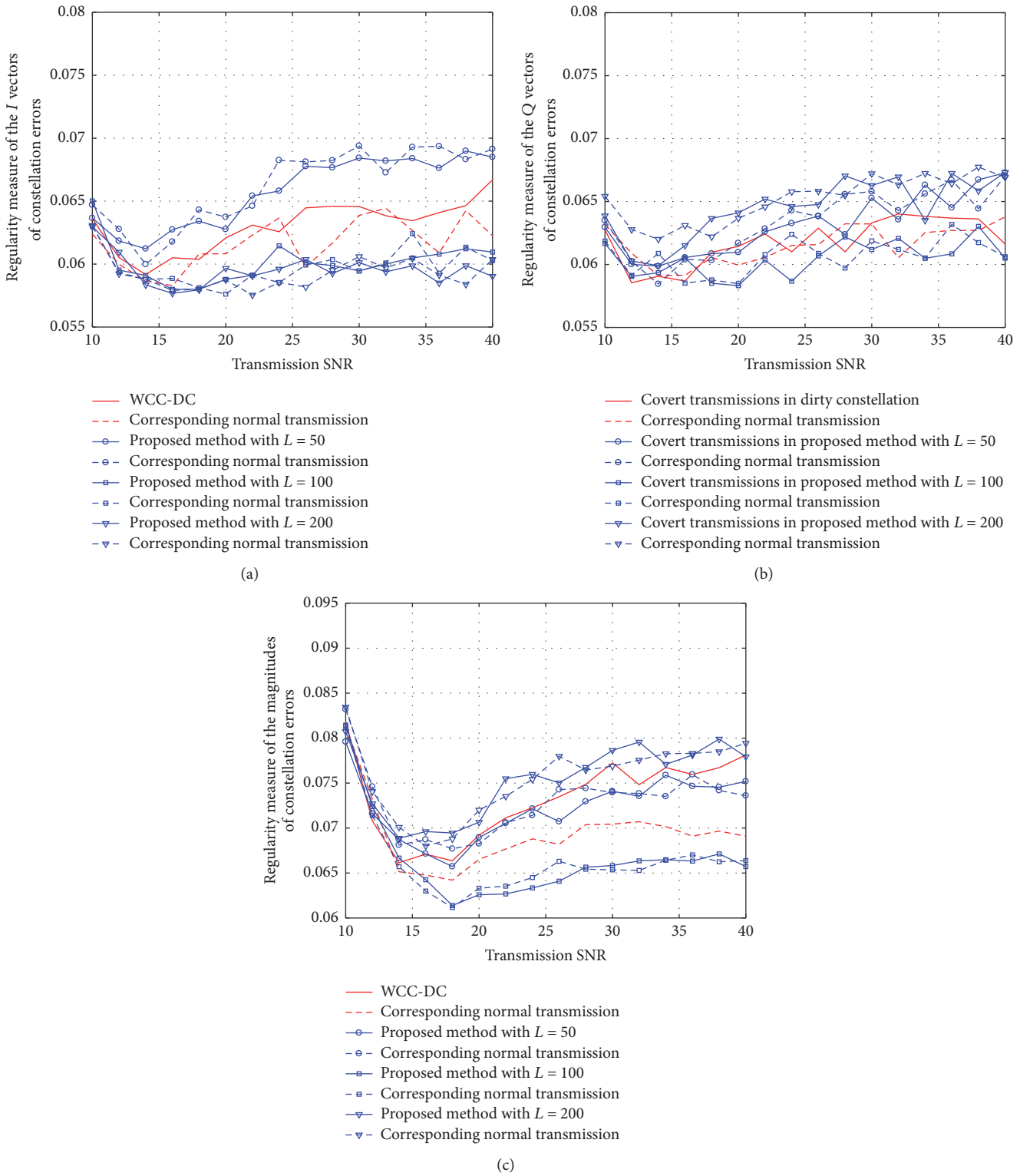

FIGURE 8: Regularity measures of (a) I vectors, (b) Q vectors, and (c) magnitudes of constellation errors with different bin numbers.

results of reliability with the same covert transmission rate are presented later.

Then, we concentrate on the relationship of the reliability and the wireless channel models. The bin number in the proposed wireless covert channels is set to be $L = 100$. The relative power of normal constellation errors is set to be $P_e = -10$ dB. The BERs of the proposed wireless covert channels is presented in Figure 14 in TGn channel models B and D. The BER of WCC-DC is also presented for comparison. Each bit error rate is obtained as an average over repeated

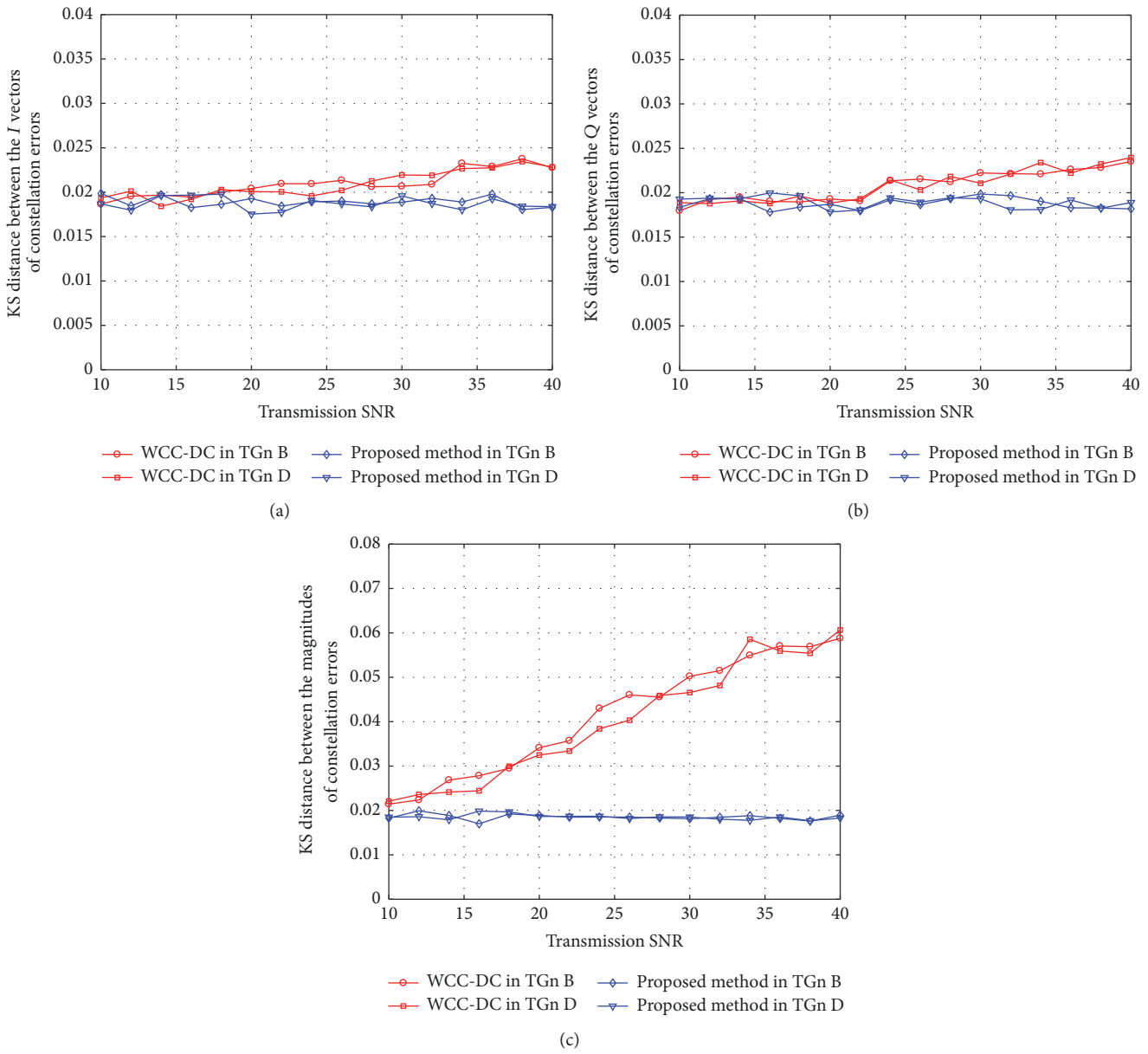

FIGURE 9: KS distances between (a) I vectors, (b) Q vectors, and (c) magnitudes of constellation errors in different channel models.

experiments. The bit error rates of two kinds of the wireless covert channels in TGn model B are all lower than those in TGn model D. The bit error rates of WCC-DC are lower than those of the proposed wireless covert channels in each channel model. So the reliability of the proposed wireless covert channel is better in the channel with less fading.

The relationship of the reliability and the relative power of normal constellation errors is discussed. The bin number in the proposed wireless covert channels is set to be $L = 100$. The BERs of the proposed wireless covert channels are presented in Figure 16 with the relative power of normal constellation errors $P_e = -10$ dB and $P_e = -13$ dB in TGn channel models B and D. Each bit error rate is obtained as an average over repeated experiments. In Figure 15, the bit error rates of the proposed wireless covert channels in TGn model B are lower than that in TGn model D with the equal relative power of normal constellation errors. The bit error rates of the proposed wireless covert channels with bigger relative power of normal constellation errors are lower than those with less relative power of normal constellation errors in each channel model. The reliability of the proposed wireless covert channels gets better with relative power of normal constellation errors increasing.

At last, the experiment of reliability of the two kinds of wireless covert channels with the same covert transmission rate is performed in Figure 16. The bin number in the proposed wireless covert channels is set to be $L = 100$. The wireless channel model in experiment is set to be TGn channel model B. The relative power of normal constellation errors is set to be $P_e = -10$ dB. The direct sequence spread

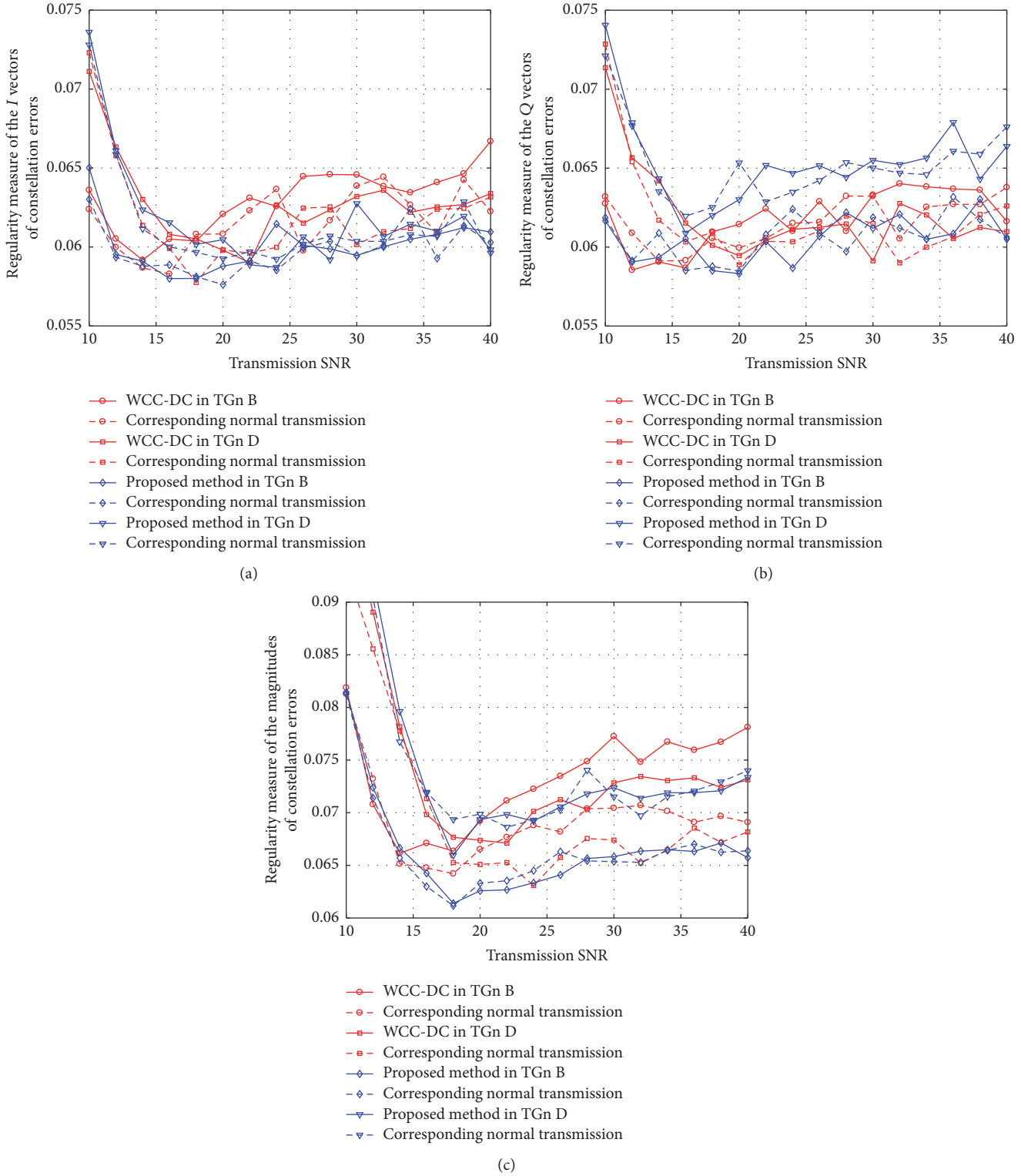

Figure 10: Regularity measures of (a) I vectors, (b) Q vectors, and (c) magnitudes of constellation errors in different channel models.

spectrum codes are applied in the secret message bits in the proposed wireless covert channels with $m = 10$. The BER of WCC-DC is presented for comparison. Each bit error rate is obtained as an average over repeated experiments. The bit error rates of the proposed wireless covert channels with the direct sequence spread spectrum codes are lower than those of WCC-DC.

It is proved that the proposed wireless covert channels are more reliable than WCC-DC with the same covert transmission rate.

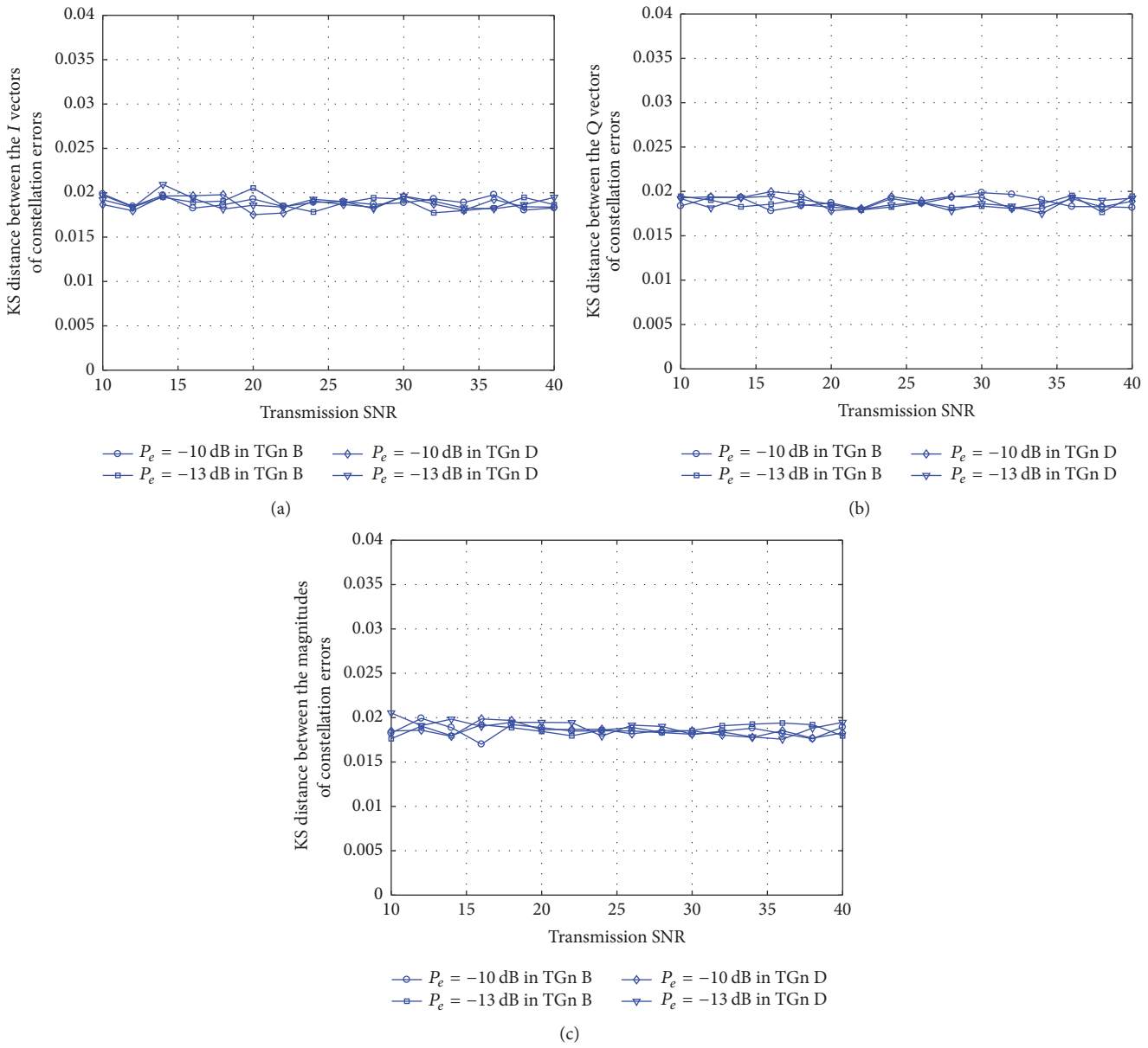

Figure 11: KS distances between (a) I vectors, (b) Q vectors, and (c) magnitudes of constellation errors with different relative powers.

6. Conclusions

Undetectability and reliability are the main aims of wireless covert channel. In this paper, we extend the detection of covert timing channel to the wireless covert channel. To improve undetectability, the wireless covert channel is proposed based on constellation shaping modulation; the constellation errors with the secret message bits embedded are distributed as normal constellation errors. The security against the detection and the reliability of the proposed wireless covert channel are improved with the same covert transmission rate.

Even if the proposed scheme can achieve high undetectability, the reliability of the proposed wireless channel needs to be strengthened. In the same framework, the bins near center line in I/Q plane are kept unused for guard band to improve the reliability and keep the undetectability of our future work.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grants nos. 61472188, 61602247,

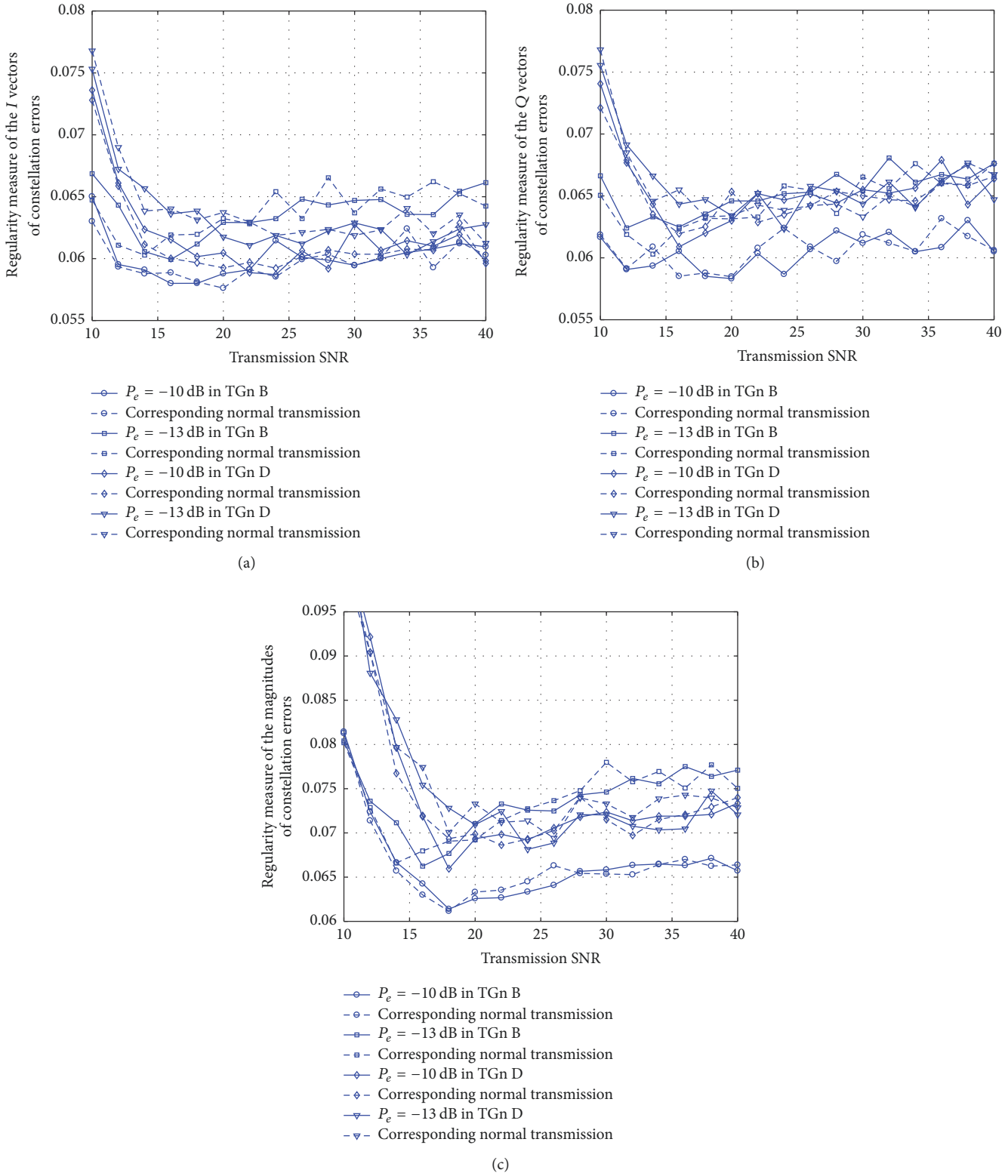

Figure 12: Regularity measures of (a) I vectors, (b) Q vectors, and (c) magnitudes of constellation errors with different relative powers.

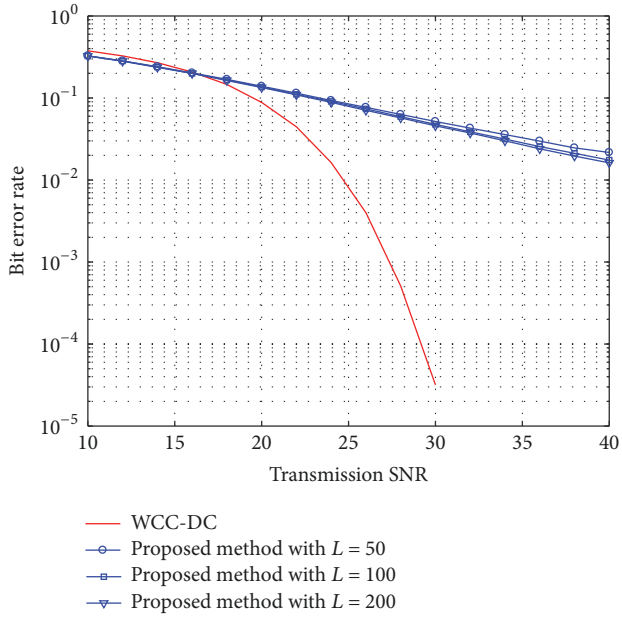

Figure 13: BERs of the proposed wireless covert channels with different bin numbers.

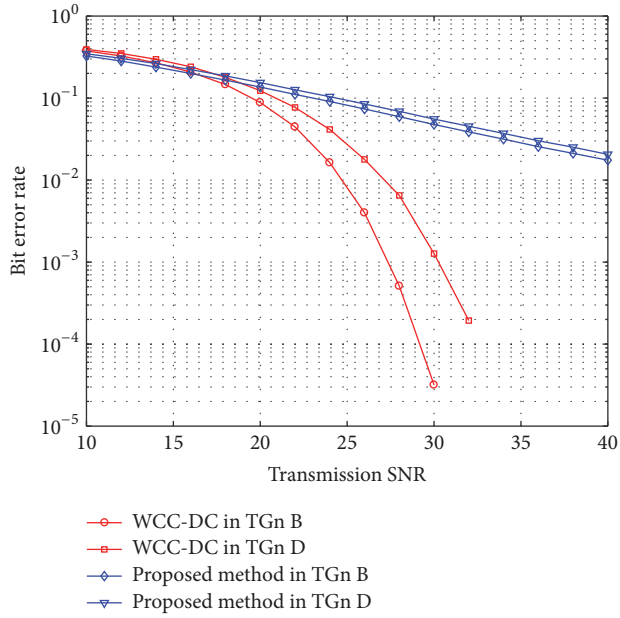

Figure 14: BERs of the proposed wireless covert channels in different channel models.

61702235, and U1636117), Natural Science Foundation of Jiangsu Province (Grants nos. BK20150472 and BK20160840), National Key Technology Research and Development Program of the Ministry of Science and Technology of China (Grant no. 2014BAH41B01), CCF-VENUSTECH Foundation (Grant no. 2016011), and Fundamental Research Funds for the Central Universities (30920140121006 and 30915012208).

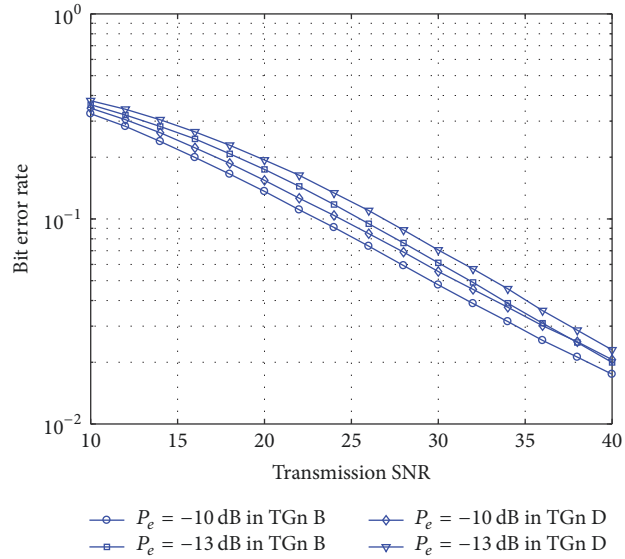

Figure 15: BERs of the proposed wireless covert channels with different relative powers.

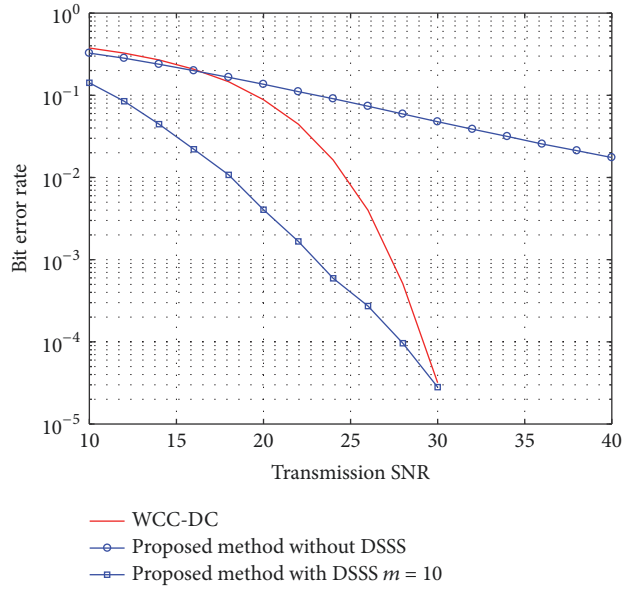

Figure 16: BERs of the proposed wireless covert channel with same covert transmission rate.

References

[1] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, "Model-Based Covert Timing Channels: Automated Modeling and Evasion," in *International Symposium on Recent Advances in Intrusion Detection*, pp. 211–230, 2008.

[2] K. Kothari and M. Wright, "Mimic: An active covert channel that evades regularity-based detection," *Computer Networks the International Journal of Computer & Telecommunications Networking*, vol. 57, pp. 647–657, 2010.

[3] R. J. Walls, K. Kothari, and M. Wright, "Liquid: A detection-resistant covert timing channel based on IPD shaping," *Computer Networks*, vol. 55, no. 6, pp. 1217–1228, 2011.

[4] G. Liu, J. Zhai, and Y. Dai, "Network covert timing channel with distribution matching," *Telecommunication Systems*, vol. 49, no. 2, pp. 199–205, 2012.

[5] A. Mileva and B. Panajotov, "Covert channels in TCP/IP protocol stack - extended version," *Central European Journal of Computer Science*, vol. 4, no. 2, pp. 45–66, 2014.

[6] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, "Secret agent radio: Covert communication through dirty constellations," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 7692, pp. 160–175, 2013.

[7] I. Grabska and K. Szczypiorski, "Steganography in long term evolution systems," in *Proceedings of the 2014 IEEE Computer Society's Security and Privacy Workshops, SPW 2014*, pp. 92–99, May 2014.

[8] Z. Hijaz and V. S. Frost, "Exploiting OFDM systems for covert communication," in *Proceedings of the 2010 IEEE Military Communications Conference, MILCOM 2010*, pp. 2149–2155, November 2010.

[9] T. Kitano, H. Iwai, and H. Sasaoka, "A wireless Steganography technique by embedding DS-SS signal in digital mobile communication systems," *Science Engineering Review of Doshisha University*, vol. 52, pp. 127–134, 2011.

[10] T. Yucek and H. Arslan, *Covert OFDM transmission using cyclic prefix*, 2012.

[11] K. Hokai, H. Sasaoka, and H. Iwai, "Wireless steganography using MIMO system," in *Proceedings of the 5th IEEE International Conference on Communications and Electronics, IEEE ICCE 2014*, pp. 560–565, August 2014.

[12] J. Classen, M. Schulz, and M. Hollick, "Practical covert channels for WiFi systems," in *Proceedings of the 3rd IEEE International Conference on Communications and Network Security, CNS 2015*, pp. 209–217, September 2015.

[13] K. Szczypiorski and W. Mazurczyk, "Hiding data in OFDM symbols of IEEE 802.11 networks," in *Proceedings of the 2010 2nd International Conference on Multimedia Information Networking and Security, MINES 2010*, pp. 835–840, November 2010.

[14] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," *Information Theory*, 2017.

[15] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communication in wireless relay networks," *Information Theory*, 2017.

[16] X. Wang, Y. Liu, X. Lu, S. Lv, Z. Shi, and L. Sun, "CovertMIMO: A covert uplink transmission scheme for MIMO systems," in *Proceedings of the ICC 2017 - 2017 IEEE International Conference on Communications*, pp. 1–6, Paris, France, May 2017.

[17] K. Szczypiorski, A. Janicki, and S. Wendzel, ""The good, the bad and the ugly": Evaluation of Wi-Fi steganography," *Journal of Communications*, vol. 10, no. 10, pp. 747–752, 2015.

[18] P. Peng, P. Ning, and D. S. Reeves, "On the secrecy of timing-based active watermarking trace-back techniques," in *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, pp. 334–348, May 2006.

[19] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert timing channels: Design and detection," in *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004*, pp. 178–187, October 2004.

[20] S. Gianvecchio and H. Wang, "An Entropy-Based Approach to Detecting Covert Timing Channels," *IEEE Transactions on Dependable & Secure Computing*, vol. 8, pp. 307–316, 2011.

[21] E. Perahia and R. Stacey, *Next generation wireless LANs*, Cambridge University Press, 2008.

[22] IEEE, "Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) Specifications," in *The 5-Ghz Band*, pp. C1–C1184, IEEE, 2003.