

# Design a Wireless Covert Channel Based on Dither Analog Chaotic Code


Pengcheng Cao, Nanjing University of Science and Technology, China

Weiwei Liu, Nanjing University of Science and Technology, China

Guangjie Liu, Nanjing University of Information Science and Technology, China

Jiangtao Zhai, Nanjing University of Information Science and Technology, China

Xiao-Peng Ji, Nanjing University of Information Science and Technology, China

 <https://orcid.org/0000-0001-6094-4626>

Yuewei Dai, Nanjing University of Information Science and Technology, China

Huiwen Bai, Nanjing University of Science and Technology, China

## ABSTRACT

To conceal the very existence of communication, the noise-based wireless covert channel modulates secret messages into artificial noise, which is added to the normal wireless signal. Although the state-of-the-art work based on constellation modulation has made the composite and legitimate signal undistinguishable, there exists an imperfection on reliability due to the dense distribution of covert constellation points. In this study, the authors design a wireless covert channel based on dither analog chaotic code to improve the reliability without damaging the undetectability. The dither analog chaotic code (DACC) plays the role as the error correcting code. In the modulation, the analog variables converted from secret messages are encode into joint codewords by chaotic mapping and dither derivation of DACC. The joint codewords are mapped to artificial noise later. Simulation results show that the proposed scheme can achieve better reliability than the state-of-the-art scheme while maintaining the similar performance on undetectability.

## KEYWORDS

Dither Analog Chaotic Code, Dither Derivation, Reliability, Undetectability, Wireless Covert Channel

## INTRODUCTION

Covert channel is a specific branch of data hiding which aims to deliver secret messages to the potential receivers without causing the attentions of the third parties(Zander, Armitage, & Branch, 2007). The secret messages in covert channels are always embedded in multimedia files(Cheddad, Condell, Curran, & Kevitt, 2010; Vojt, #283, Holub, & Fridrich, 2013), network packets(Gianvecchio, Wang, Wijesekera, & Jajodia, 2008; Mileva & Panajotov, 2014; Shah, Molina, & Blaze, 2006), or communication behaviors. The network covert channel is most popular type, in which network

DOI: 10.4018/IJDCF.2021030108

This article, published as an Open Access article on February 15, 2021 in the gold Open Access journal, The International Journal of Digital Crime and Forensics (IJDCF) (converted to gold Open Access January 1, 2021), is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

packets are used as the carrier. Secret messages are transmitted by padding some bits into the packet headers (Mileva & Panajotov, 2014) or manipulating the packet timing information (Gianvecchio et al., 2008; Shah et al., 2006). However, as the most widely-studied branch of covert channels, pattern matching (Zhai, Liu, & Dai, 2013) and some statistic-based detection tools (Fahimeh Rezaei, Hempel, & Sharif, 2017) have been applied to threaten the network covert channels.

With the development of wireless communication, wireless covert channels have begun to draw researchers' attentions, in which the secret messages are embedded by modifying wireless communication protocol fields or wireless signals. Due to the localized transmission of wireless communication, wireless covert channels are difficult to access. The warden must set observation points in each possible hotspot, capture and analyze massive wireless signals. The detection of wireless covert channels is more difficult than the packet level analysis of network covert channels.

Earlier wireless covert channels were established by padding or modifying the redundant fields of wireless communication protocols. In several wireless covert channels, the secret messages were embedded in the padding of frames, headers of the MAC, RLC, and PDCP (Grabska & Szczypiorski, 2014; Szczypiorski & Mazurczyk, 2010), the phase of STF, the frequency of CFO and Cyclic Prefix in Wi-Fi system (Classen, Schulz, & Hollick, 2015). The subcarriers reserved in OFDM-based system can also be used to transmit secret messages (Hijaz & Frost, 2010). However, these wireless covert channels are weak to the detection methods based on matching the fields of wireless communication protocols (Fatemeh Rezaei, Hempel, Peng, Qian, & Sharif, 2013).

Due to channel interference in practical wireless environment, the distortion of the wireless signal is inherent. Later, the noise-based wireless covert channels were established by converting the secret messages into the artificial noise for transmission. There are two benches of the researches on these wireless covert channels. One is the research on the theoretical covert capacity of the wireless covert channels. Assume that the warden have full knowledge of normal channel noise and the artificial noise can be transmitted directly, the theoretical covert capacity is got while meeting the undetectability that the warden can not distinguish the normal channel noise and artificial noise by hypothesis testing and relative entropy. The limits on undetectability of those wireless covert channels was studied in (Bloch, 2015), which was extended to the network with friendly nodes producing artificial noise (Soltani, Goeckel, Towsley, Bash, & Guha, 2018) and wireless relay networks (Hu et al., 2018).

The other bench is the research on the algorithm of these wireless covert channels. The research assumes that the warden have partial knowledge of normal channel noise and the artificial noise is always added to the normal wireless signal for transmission, then the wireless covert channels are proposed and benchmarked on undetectability and reliability. The undetectability of noise-based wireless covert channels was guaranteed by bringing random noise into the generation of artificial noise. In the work (Dutta, Saha, Grunwald, & Sicker, 2012), the artificial noise was generated by dirty constellation, which composes of the signal modulated from secret messages and random noise. Later, multiplex technique is also employed to add random noise into the signal to generate artificial noise (Kitano, Iwai, & Sasaoka, 2011). In our prior work (Cao et al., 2018), the artificial noise modulated from secret messages by constellation shaping modulation can maintain the same distribution as that of normal channel noise. Although the state-of-the-art schemes have achieved good performance on undetectability, the artificial noise is vulnerable to channel interferences owing to its dense distribution.

In this study, a wireless covert channel based on dither analog chaotic code is proposed to improve the reliability while maintaining the performance on undetectability. The dither analog chaotic code (DACC) encodes the analog variables converted from secret messages into the joint codewords by chaotic mapping and dither derivation. Chaotic mapping encodes the analog variables into chaotic codewords, and dither derivation generates the dither codewords from chaotic codewords to protect their signs. Simulation results show that the reliability of the proposed scheme is significantly improved while maintaining similar undetectability when compared with the state-of-the-art schemes.

The following are the key contributions of this paper:

1. We introduce the analog chaotic code to the noise-based wireless covert channels for the sake of improving their reliability.
2. According to the distribution of normal channel noise, the dither derivation in dither analog chaotic code is proposed to get a better performance.

The rest of the paper is organized as follows. In the next section, some backgrounds including general framework of noise-based wireless covert channels and performance metrics are introduced. In Section 3, some related works on wireless covert channels are summarized. In Section 4, we describe the proposed wireless covert channel based on dither analog chaotic code. Section 5 gives the simulation results on undetectability and reliability. Finally, Section 6 concludes the whole paper.

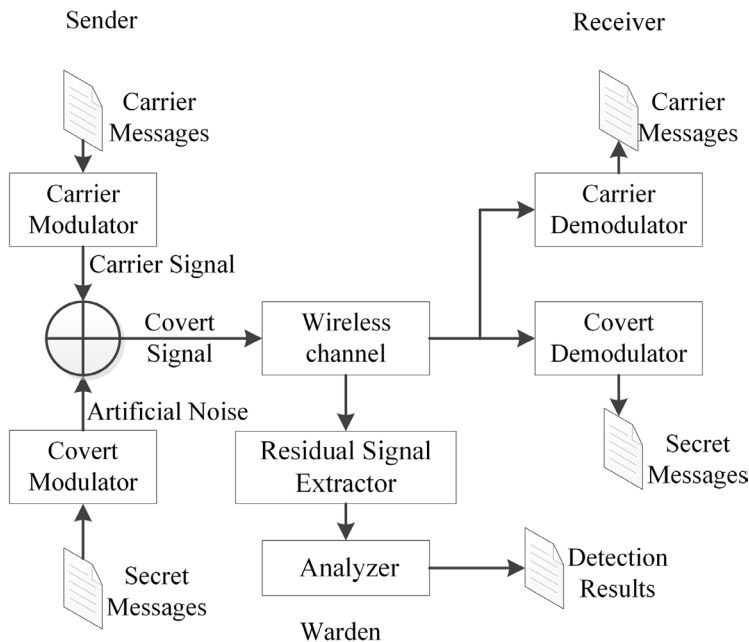
## BACKGROUNDS

### General Framework of Noise-Based Wireless Covert Channels

Due to inherent channel interference in wireless communication, the noise-based wireless covert channels are established by modulating the secret message into artificial noise and adding it to the carrier signal. The general framework of noise-based wireless covert channel is illustrated in Figure 1. Since OFDM has been the dominant modulation technique in wireless communication, we concentrate on the wireless covert channels in OFDM-based system in this study, some signal processing steps irrelevant to the implementation of covert channels, e.g. IFFT, FFT, adding and removing Cyclic Prefix, are omitted.

At the sender, the carrier and secret messages are modulated into carrier signal and artificial noise respectively. The covert signal generated by adding the artificial noise to carrier signal is transmitted from the sender to the receiver. At the receiver, the carrier messages and secret messages can both be demodulated from the covert signal by carrier and covert demodulators respectively.

Figure 1. General framework of noise-based wireless covert channels



Due to the broadcast nature of wireless signal, some radio interception devices deployed by the potential wardens can also capture the covert signal. To find out the existence of secret messages, the warden may extract the residual signal by removing the carrier signal from the captured covert signal, then analyze the characteristics of the residual signal to obtain the detection results. In this study, we assume that the warden has partial administrative authority over the distribution of channel noise in legitimate transmission by capturing massive normal channel noise.

## Performance Metrics

Undetectability and reliability are the two main goals in the design of the wireless covert channels. In (Dutta et al., 2012), error vector magnitude (EVM), peak to average power ratio (PAPR) and temporal variation of average signal power are used to measure the undetectability of wireless covert channels. In our prior work (Cao et al., 2018), the KS test and regularity test for residual signal are also employed to measure the undetectability, which are developed from the detection methods for covert timing channels. To the best of our knowledge, there still exist no generally accepted performance metrics for wireless covert channels, especially on undetectability. We give the measure methods on undetectability and reliability for noise-based wireless covert channels as follows:

### *Undetectability*

Kullback-Leibler (KL) test (Archibald & Ghosal, 2014; Cachin, 2004) and Kolmogorov-Smirnov (KS) test (Cabuk, Brodley, & Shields, 2004) are employed to evaluate the undetectability of noise-based wireless covert channels, which are based on the distribution differences between target samples and reference samples. The KL divergences and KS distances are obtained using the distribution of I/Q components, magnitudes, and phases of the residual signal and reference channel noise. It is very hard to get the stable reference channel noise when the channel state may varies rapidly. After extracting the residual signal, the warden needs to seek the approximate reference of channel noise or construct it using distribution estimation methods. Moreover, the warden may deploy more than one radio interception device in specific area. Some of the radio interception devices may be deployed closer to the sender when compared with the receiver, which always means more moderate channel interference. Consequently, the undetectability of noise-based wireless covert channels should be benchmarked under noisy channel with a range of signal-to-noise ratios (SNR). A wireless covert channel can be viewed undetectable when the detection tools are ineffective under noisy channel with higher SNR.

### *Reliability*

The reliability of noise-based wireless covert channels is measured in terms of the bit error rate (BER) of secret message bits for a given covert transmission rate  $R$  under the common additive white Gaussian noise (AWGN) channel and common multipath fading channel. The covert transmission rate  $R$  is defined as the average number of secret message bits transmitted per subcarrier in OFDM-based wireless communication system.

## RELATED WORK

Wireless covert channels embed secret messages in normal wireless communication to conceal their existence. The earlier researchers introduce the method of network covert channels into the design of wireless covert channels. The secret messages are transmitted by modifying padding of frames, headers of the MAC, RLC and PDCP in the LTE systems (Grabska & Szczypiorski, 2014; Szczypiorski & Mazurczyk, 2010). The subcarriers of specific frequency reserved in OFDM-based system are used to transmit the secret messages with little effect on normal communication (Hijaz & Frost, 2010). Several types of wireless covert channels established on Wi-Fi communication protocol were introduced, which transmit secret messages by modifying the phase of short training field, the

frequency of the Carrier Frequency Offset and Cyclic Prefix(Classen et al., 2015). Wireless covert channels based on the coordinated operations in the control channel and data channel of MIMO system were proposed(Wang et al., 2017). These wireless covert channels are very weak to field-matching methods.

Due to channel interferences in practical wireless communication, the distortion of the wireless signal is inherent. The noise-based wireless covert channels were established by modulating the secret messages into the artificial noise for transmission. There are two benches of the researches on the noise-based wireless covert channels. The research on the theoretical covert capacity of the wireless covert channels assumes that the warden have full knowledge of normal channel noise, and the theoretical covert capacity is got while meeting the undetectability that the warden can not distinguish the normal channel noise and artificial noise by hypothesis testing and relative entropy. The limits on undetectability of those wireless covert channels was studied in (Bloch, 2015). Then, the theoretical capacity of the wireless covert channel was improved when there are some friendly nodes producing artificial noise which are close to warden in the network(Soltani et al., 2018). The theoretical capacity of the wireless covert channel wireless relay networks is also studied (Hu et al., 2018).

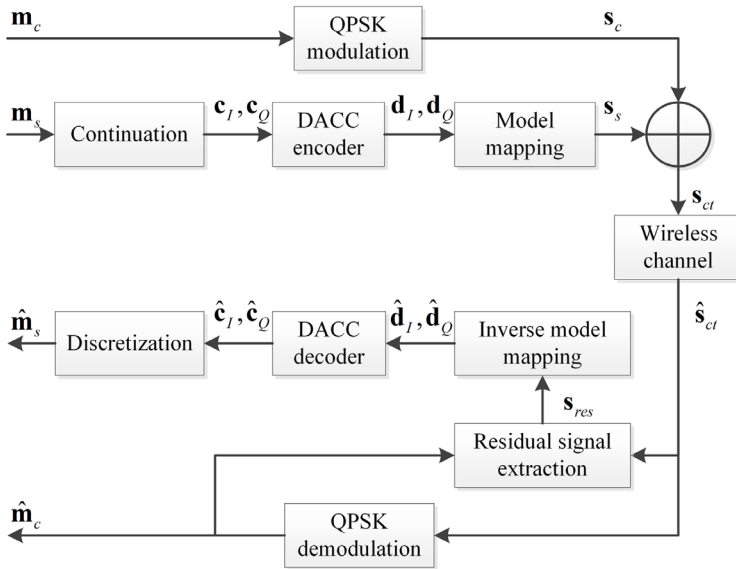
The research on the algorithm of the wireless covert channels is conducted at the same time. The research assumes that the warden have partial knowledge of normal channel noise and the artificial noise is always added to the carrier signal for transmission, and benchmark the wireless covert channels on undetectability and reliability. The wireless covert channel based on multiplex technique (WCC-MT) was proposed, in which random noise was added to eliminate the regularity of the artificial noise(Kitano et al., 2011). The power of the artificial noise and the random noise must be lower than that of the carrier signal. The spread spectrum technique is also applied to the secret messages so that the required power of artificial noise can be reduced to guarantee the reliability of the overt communication. This wireless covert channel was extended to the MIMO system (Hokai, Sasaoka, & Iwai, 2014). To conceal existence of artificial noise better, a wireless covert channel based on dirty constellation (WCC-DC) was proposed (Dutta et al., 2012). The secret messages are modulated as the additional points around the normal constellation points. The artificial noise at covert subcarriers was mixed with random noise at non-covert subcarriers, which can conceal the regularity resulting from artificial noise. Moreover, the mapping sequence is required to separate the artificial noise and random noise. WCC-MT and WCC-DC need extra power or bandwidth for adding random noise to achieve undetectability, and the regularity of residual signal may result in vulnerability to some statistical tests when the channel condition between warden and the sender is good (Szczypiorski, Janicki, & Wendzel, 2015). A wireless covert channel based on constellation shaping modulation is proposed to improve the undetectability (Cao et al., 2018). Using the characteristics of normal channel noise, the secret messages are converted into the artificial noise by constellation shaping modulation, which makes the artificial noise distribute like normal channel noise. Although the state-of-the-art through noise-based wireless covert channel schemes have good performance on undetectability, the reliability of the wireless covert channel has a degradation owing to the dense distribution of covert constellation points.

## WIRELESS COVERT CHANNEL BASED ON DITHER ANALOG CHAOTIC CODE

In this section, a wireless covert channel based on dither analog chaotic code (WCC-DACC) is proposed to improve the reliability of covert communication. The dither analog chaotic code (DACC) in the modulation is employed to correct the errors resulting from the channel interference. The general framework of the scheme is demonstrated in Figure 2.

Suppose that the carrier signal  $s_c$  is modulated from the carrier message bits  $m_c$  by QPSK. By the covert modulation based on DACC encoder, the artificial noise  $s_s$  is modulated from secret message bits  $m_s$ . The covert signal  $s_{ct}$  is generated by adding artificial noise  $s_s$  to the carrier signal

Figure 2. Framework of wireless covert channel based on dither analog chaotic code



$s_c$ . At the receiver, the captured covert signal  $\hat{s}_{ct}$  is the noisy version of  $s_{ct}$  under channel interference. The carrier message bits  $\hat{m}_c$  are QPSK demodulated from  $\hat{s}_{ct}$ . By covert demodulation based on DACC decoder, the secret message bits  $\hat{m}_s$  are demodulated from the residual signal  $s_{res}$ , which is extracted from the covert signal  $\hat{s}_{ct}$ .

The description of covert modulation based on DACC encoder and the corresponding demodulation are detailed in the following subsections.

### Covert Modulation Based on DACC Encoder

The covert modulation based on DACC encoder is employed to generate the artificial noise from the secret message bits. The secret message bits are first converted into analog variables. Then, the analog variables are encoded by DACC encoder including chaotic mapping and dither derivation. Chaotic mapping encodes analog variables into chaotic codewords. According to the distribution of reference normal channel noise, the dither derivation generated the dither codewords from the chaotic codewords to protect their signs. Then the artificial noise is generated from the joint codewords composed of chaotic and dither codewords by model mapping.

The secret message bits are denoted by  $\mathbf{m}_s = (m_s[1], \dots, m_s[N_m])$ . The secret message bits in I and Q axes can be denoted by  $\mathbf{m}_{sI} = (m_{sI}[1], \dots, m_{sI}[N_m])$  and  $\mathbf{m}_{sQ} = (m_{sQ}[1], \dots, m_{sQ}[N_m])$  respectively in which the elements satisfy  $m_s[i] = (m_{sI}[i], m_{sQ}[i]), i = 1, \dots, N_m$ . We assume that there are  $2n$  secret message bits embedded in a subcarrier, so the element in the secret message bits n I and Q axes can be denoted as  $m_{sI}[i], m_{sQ}[i] \in \{0, 1\}^n$ . Here  $n$  is the length of the secret message unit in I or Q axis. The artificial noise  $\mathbf{s}_s$  are denoted by  $\mathbf{x}_s + j \cdot \mathbf{y}_s$ . Here  $\mathbf{x}_s, \mathbf{y}_s$  are the components of the artificial noise in I and Q axes of the constellation at the sender satisfying  $\mathbf{x}_s = (x_s[1], \dots, x_s[N_s]), \mathbf{y}_s = (y_s[1], \dots, y_s[N_s])$ .

Take I axis for example, the secret message bits  $\mathbf{m}_{s_I}$  are first converted into the analog variables with uniform distribution  $U(0,1)$  in continuation. The continuation function is denoted as (1):

$$\mathbf{c}_I = \left\lfloor \frac{\mathbf{m}_{s_I}}{|S|} + \mathbf{r}_I \right\rfloor \bmod 1 \quad (1)$$

Here  $S$  is the set of all the possible units of the secret message bits in I axis the number of which satisfies  $|S| = 2^n$ . And  $\mathbf{r}_I$  are the sequence of random numbers with uniform distribution on  $(0,1)$ . The continuation makes the analog variables  $\mathbf{c}_I$  distribute uniformly on  $(0,1)$ .

Then the analog variables  $\mathbf{c}_I$  with uniform distribution  $U(0,1)$  are encoded into the joint codewords  $\mathbf{d}_I$  by DACC encoder. In the DACC encoder, the chaotic mapping takes the element of analog variables  $c_I[i]$  as source symbol, encodes it to chaotic codewords which are denoted as  $d_{cI}[i] = (d_{cI,i}[1], d_{cI,i}[2], \dots, d_{cI,i}[k]), k \geq 2$ . Here  $k$  is the code length of chaotic code, the code rate is written as  $\alpha = 1/k$ . In these codewords, the first code word is initial state which is equal to the source symbol  $d_{cI,i}[1] = c_I[i]$ , and  $d_{cI,i}[j], 2 \leq j \leq k$  is chaotic state generated iteratively by non-linear chaotic mapping. The classic tent mapping is employed as chaotic mapping in this study which is shown in Figure 3. The chaotic mapping function  $F_{cm}(\cdot)$  is given as (2):

$$d_{cI,i}[j] = F_{cm}(d_{cI,i}[j-1]) = 1 - 2 \left| d_{cI,i}[j-1] - \frac{1}{2} \right| \quad (2)$$

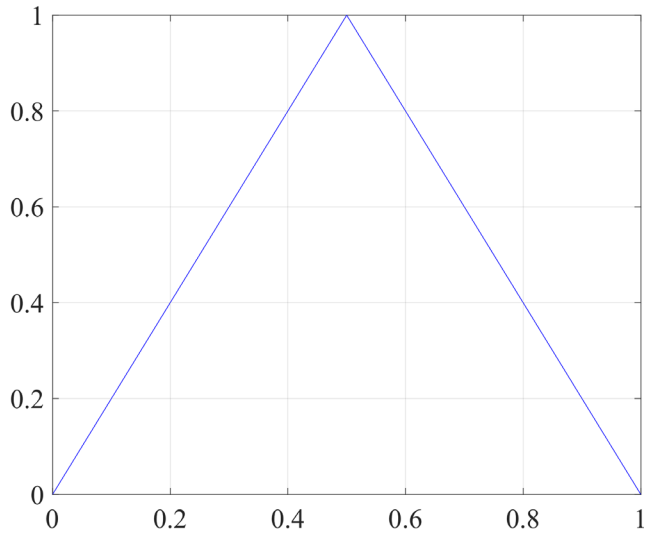
The sign of a codeword which determines what region this codeword belongs to is represented as  $g_{cI,i}[j] = \text{sgn}(d_{cI,i}[j] - 1/2)$ . So the chaotic mapping function can be furtherly written as (3):

$$d_{cI,i}[j] = 1 - 2g_{cI,i}[j-1] \left( d_{cI,i}[j-1] - \frac{1}{2} \right) \quad (3)$$

Due to the mapping in Figure 3 and the distribution of analog variables, it is straightforward to verify that the Eq. (3) leads the chaotic codewords to uniformly distribute on  $(0,1)$ .

It can be learned that all the signs of the chaotic codewords  $g_{cI,i}[1], g_{cI,i}[2], \dots, g_{cI,i}[k]$  represent the quantization interval of source symbol  $d_{cI,i}[1]$ . The more the number of signs, the smaller the quantization interval. So the signs of the codewords  $g_{cI,i}[1], g_{cI,i}[2], \dots, g_{cI,i}[k]$  at the decoder can offer an estimation of  $d_{cI,i}[1]$  with the precision up to  $1/2^k$ . We can also see that the smaller the index  $j$  of  $g_{cI,i}[j]$  is, the more important it is for the estimation of  $d_{cI,i}[1]$  at the decoder. As a result, the signs are important in decoding of the codewords, and  $g_{cI,i}[1]$  is the most important sign. The dither derivation in DACC encoder generates the dither codewords from the chaotic codewords to protect the signs. The corresponding dither codewords are represented as  $d_{dI}[i] = (d_{dI,i}[1], \dots, d_{dI,i}[k])$ . For a chaotic codeword  $d_{cI,i}[j]$ , the dither derivation function is denoted as (4):

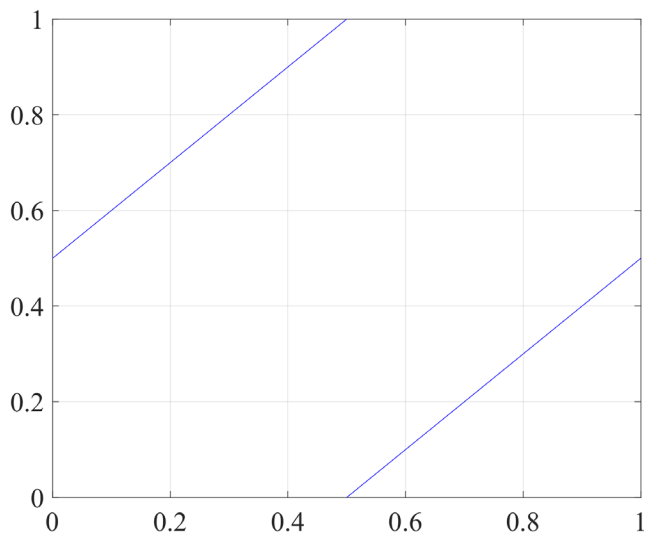
Figure 3. Tent chaotic mapping



$$d_{dl,i}[j] = \left( d_{cl,i}[j] + \frac{1}{2} \right) \bmod 1 \quad (4)$$

The mapping of dither derivation is shown in Figure 4. The sign of the dither codeword is contrary to that of the chaotic codeword  $g_{dl,i}[j] = -g_{cl,i}[j]$ . The absolute differential value of the dither and chaotic codeword is  $|d_{dl,i}[j] - d_{cl,i}[j]| = 1/2$ . According to the centered dense distribution of the normal channel noise in I and Q axes, the components far away from center value have better interference resistance than those near center value. The dither derivation ensure that there is a

Figure 4. Dither derivation mapping





codeword far away from center value between  $d_{ct,i}[j]$  and  $d_{dt,i}[j]$  which means the sign of the codeword is robust to the interferences. The joint codewords with the length  $2kN_m$  which consists of chaotic and dither codewords is denoted as  $d_I[i] = (d_{ct}[i], d_{dt}[i])$ . Due to the mapping in Figure 4 and the distribution of chaotic codewords, it is straightforward to verify that the Eq. (4) leads the dither codewords to distribute uniformly on (0,1). So the joint codewords also distribute uniformly on (0,1).

Then the components of the artificial noise in I axis are generated from the joint codewords  $\mathbf{d}_I$  by model mapping. The model mapping function is shown in (5):

$$\mathbf{x}_s = F^{-1}(\mathbf{d}_I) \quad (5)$$

where  $F^{-1}(\cdot)$  is the converse cumulative distribution function (CDF) of normal channel noise in I axis which keeps the distribution of the generated I components the same as that of the normal channel noise. And the length of the artificial noise in I axis is  $N_s = 2kN_m$ . The covert modulation in Q axis works in the same way. the covert transmission rate can be got by (6):

$$R = \frac{2N_m n}{N_s} = \frac{n}{k} \quad (6)$$

### Covert Demodulation Based on DACC Decoder

After the receiver gets the covert signal, the covert demodulation based on DACC decoder is employed to extract the secret message bits from the residual signal which is extracted from the covert signal. As shown in the framework, the residual signals extraction, converse model mapping, DACC decoder and discretization in covert demodulation are detailed.

The residual signal is first extracted from the received covert signal. The received covert signal  $\hat{S}_{ct}$  are denoted by  $\hat{x}_{ct} + j \cdot \hat{y}_{ct}$ . The cover message bits demodulated by QPSK is denoted by  $\hat{m}_c$  which are re-modulated by QPSK to acquire the ideal carrier signal denoted by  $\hat{S}_c = \hat{x}_c + j \cdot \hat{y}_c$ . The residual signal  $S_{res}$  is extracted by (7):

$$S_{res} = \hat{S}_{ct} - \hat{S}_c = (\hat{x}_{ct} - \hat{x}_c) + j \cdot (\hat{y}_{ct} - \hat{y}_c) \quad (7)$$

Take I axis for example, the I components of residual signal are converted into joint codewords by converse model mapping. The converse model mapping function is given as (8):

$$\hat{d}_I = F_{res}(\hat{x}_{ct} - \hat{x}_c) \quad (8)$$

Here  $F_{res}(\cdot)$  is the CDF of residual signal.

Then the DACC decoder takes the joint codewords  $\hat{d}_I$  as input, decodes them to the analog variables  $\hat{c}_I$ . The chaotic and dither codewords  $\hat{d}_{ct}, \hat{d}_{dt}$  can be separated from joint codewords

$\hat{d}_I$ . The fused chaotic codewords are generated by codewords fusion. For a chaotic codeword  $d_{cl,i}[j]$  and the corresponding dither codeword  $d_{dl,i}[j]$ , the codewords fusion function is shown as (9):

$$d_{fl,i}[j] = \begin{cases} \hat{d}_{cl,i}[j], & \left| \hat{d}_{cl,i}[j] - \frac{1}{2} \right| \geq \left| \hat{d}_{dl,i}[j] - \frac{1}{2} \right| \\ \left( \hat{d}_{dl,i}[j] + \frac{1}{2} \right) \bmod 1, & \text{otherwise} \end{cases} \quad (9)$$

The sign of the fused codewords is denoted as  $g_{fl,i}[j] = \text{sgn}(d_{fl,i}[j] - 1/2)$ . The codewords fusion selects the codewords with little interference between  $d_{cl,i}[j]$  and  $d_{dl,i}[j]$ .

After fused codewords are got, the analog variables are achieved by ML decoding. For an analog variable  $c_I[i]$ , the corresponding fused chaotic codewords are  $d_{fl,i}[1], d_{fl,i}[2], \dots, d_{fl,i}[k]$  in which the signs are  $g_{fl,i}[1], g_{fl,i}[2], \dots, g_{fl,i}[k]$ . The inverse chaotic map function  $F_{cm}^{-1}(\cdot)$  is represented as (10):

$$d_{cl,i}[j-1] = F_{cm}^{-1}(d_{cl,i}[j]) = \frac{1 - d_{cl,i}[j]}{2} \cdot g_{cl,i}[j-1] + \frac{1}{2} \quad (10)$$

Assumed that the signs of  $d_{cl,i}[j]$  and  $d_{fl,i}[j]$  are the same, the differences between them satisfy (11):

$$\left| d_{fl,i}[j-1] - F_{cm}^{-1}(d_{cl,i}[j]) \right| = \frac{\left| F_{cm}(d_{fl,i}[j-1]) - d_{cl,i}[j] \right|}{2} \quad (11)$$

The ML decoding algorithm is to minimize the sum of Euclid distance between  $d_{cl,i}[j]$  and  $d_{fl,i}[j]$ , which is denoted as  $\varepsilon_{I,i}[i]$ . By Eq.(11), the sum of Euclid distance can be written as (12):

$$\begin{aligned} \varepsilon_{I,i}[i] &= \sum_{j=1}^k (d_{fl,i}[j] - d_{cl,i}[j])^2 \\ &= \sum_{j=1}^k (d_{fl,i}[j] - F_{cm}^{j-k}(d_{cl,i}[k]))^2 \\ &= \sum_{j=1}^k 2^{2(j-k)} (F_{cm}^{k-j}(d_{fl,i}[j]) - d_{cl,i}[k])^2 \end{aligned} \quad (12)$$

where  $F_{cm}^{-j}(\cdot)$  and  $F_{cm}^j(\cdot)$  is j-fold compositions of  $F_{cm}^{-1}(\cdot)$  and  $F_{cm}(\cdot)$ . Then, differentiate Eq. (12) with respect to  $d_{cl,i}[k]$ , and let the derivative equals to 0, the decoder gets a rough estimation of  $d_{cl,i}[k]$  which is denoted by (13):

$$\hat{d}_{cI,i} [k] = \frac{\sum_{j=1}^k 2^{2(j-k)} F_{cm}^{k-j} (d_{fl,i} [j])}{\sum_{j=1}^k 2^{2(j-k)}} \quad (13)$$

As the signs are got, the analog variable is obtained as (14):

$$\hat{c}_I [i] = \hat{d}_{cI,i} [1] = F_{cm}^{1-k} (\hat{d}_{cI,i} [k]) \quad (14)$$

Then the secret messages are converted from analog variables by discretization. The discretization function is shown as (15):

$$\hat{m}_{st} [i] = \left\lfloor 2^n \cdot \left[ (\hat{c}_I [i] - r_I [i]) \bmod 1 \right] + 0.5 \right\rfloor \quad (15)$$

Here  $r_I [i]$  is a random number shared between the sender and receiver. The covert demodulation in Q axis works in the same way.

## SIMULATION RESULTS

In this section, wireless covert channel based on dither analog chaotic code (WCC-DACC) is benchmarked on undetectability and reliability. We compare the proposed scheme with three noise-based wireless covert channels. Wireless covert channels based on dirty constellation (WCC-DC) (Dutta et al., 2012) and wireless covert channels based on multiplex technique (WCC-MT) (Kitano et al., 2011) are earlier proposed noise-based schemes. Wireless covert channel based on constellation shaping modulation (WCC-CSM)(Cao et al., 2018) is the state-of-the-art noise-based scheme.

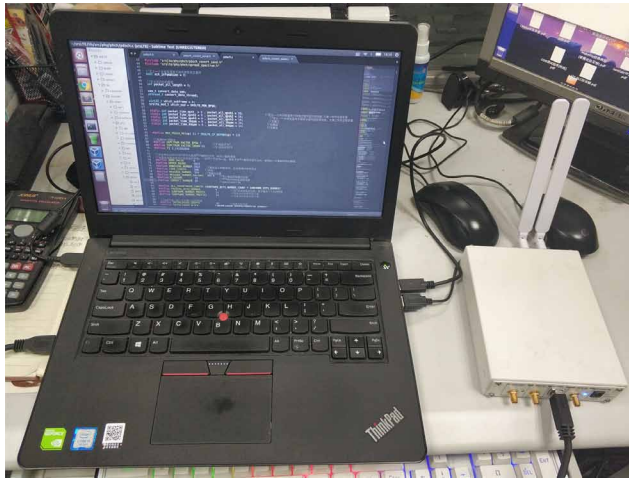
### Simulation Setup

The wireless communication system in simulation is set in a OFDM-based physical layer. The parameters of wireless communication are listed in Table 1. We use software defined radio (SDR) platform to capture massive data of normal channel noise with different SNRs. The SDR platform consists of USRP B210 and srsLTE which are shown in Figure 5. The captured normal channel noise is employed in the simulation. The ITU-R indoor office A channel (“Guidelines for evaluation of radio transmission technologies for IMT-2000,” 1997) is chosen as classic multipath fading channel for the simulation experiment. Assume that the sender, receiver and warden are kept stationary during communication, the Doppler shift is negligible. The carrier and secret message bits are both provide by a pseudo-random bits generator.

Table 1. Parameters of OFDM-based wireless communication

Modulation	QPSK
Number of modulated subcarriers	300(512 FFT)
Cyclic Prefix	128 samples/symbol
Sampling Time	1/(15000*512) second
Wireless Channel Model	ITU-R indoor office A

Figure 5. SDR platform consists of the USRP B210 and srsLTE



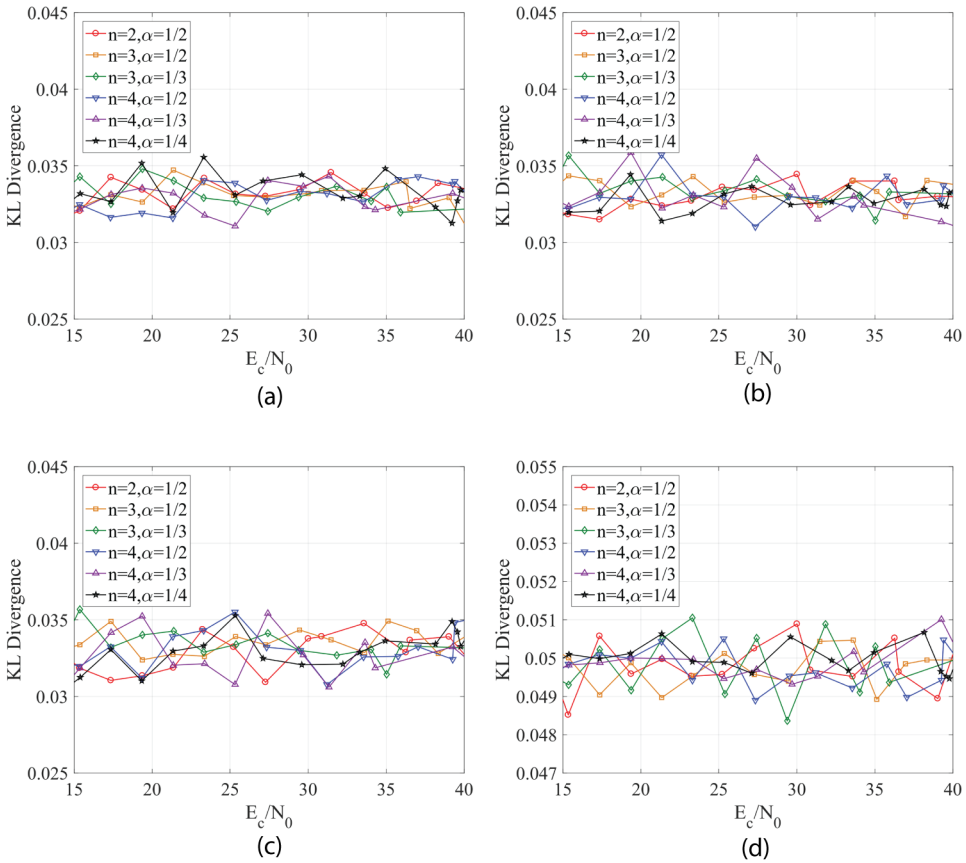
In order to make a fair comparison, the carrier signal to artificial noise ratio is set to be 13dB in WCC-DACC and WCC-CSM. In WCC-DC, there are 10% subcarriers carrying the secret message bits which are modulated into QPSK points with a mutual separation of a 64QAM constellation. At other non-covert subcarriers, the carrier signal to random noise ratio is set to be 13dB. In WCC-MT, artificial noise is generated by QPSK. The powers of artificial noise and random noise are set to be equal, and the carrier signal to the sum of artificial noise and random noise is set to be 13dB.

The undetectability of all the wireless covert channels is measured by the KL divergences and KS distances of the I components, Q components, magnitudes and phases of residual signal with the same transmission rate. The approximate reference of channel noise is sought from the massive data of normal channel noise. The KL divergences and the KS distances are computed with 2000 components in an axis, and they are all presented with different carrier signal to channel noise ratios  $E_c/N_0 = 15, \dots, 40\text{dB}$ . The reliability of the wireless covert channels is measured by BERs of secret message bits with the same transmission rate. The direct sequence spread spectrum codes based on M-sequence are applied in the secret message bits to keep the covert transmission rate equal in all schemes. All wireless covert channels are performed on more than 100000 symbols. Each detection measure or BER is obtained as an average over repeated experiments.

### Undetectability

The KL divergences and KS distances of I components, Q components, magnitudes and phases of residual signals are calculated to measure the undetectability of the proposed scheme. The covert transmission rate is set to  $R = 0.2$  with the application of direct sequence spread spectrum codes in WCC-MT, WCC-CSM and WCC-DACC. The KL divergences and the KS distances of I components, Q components, magnitudes and phases of residual signal in WCC-DACC with different secret message units and the chaotic code rates  $n = 2, \alpha = 1/2; n = 3, \alpha = 1/2, 1/3; n = 4, \alpha = 1/2, 1/3, 1/4$  are presented in Figure 6 and 7. In Figure 6 and 7, there are little differences between the detection measures of all components of residual signal in WCC-DACC with different secret message units and chaotic code rates. As  $E_c/N_0$  increases, the KL divergences and KS distances with different secret message units and chaotic code rates remain almost stationary. It shows that the detection

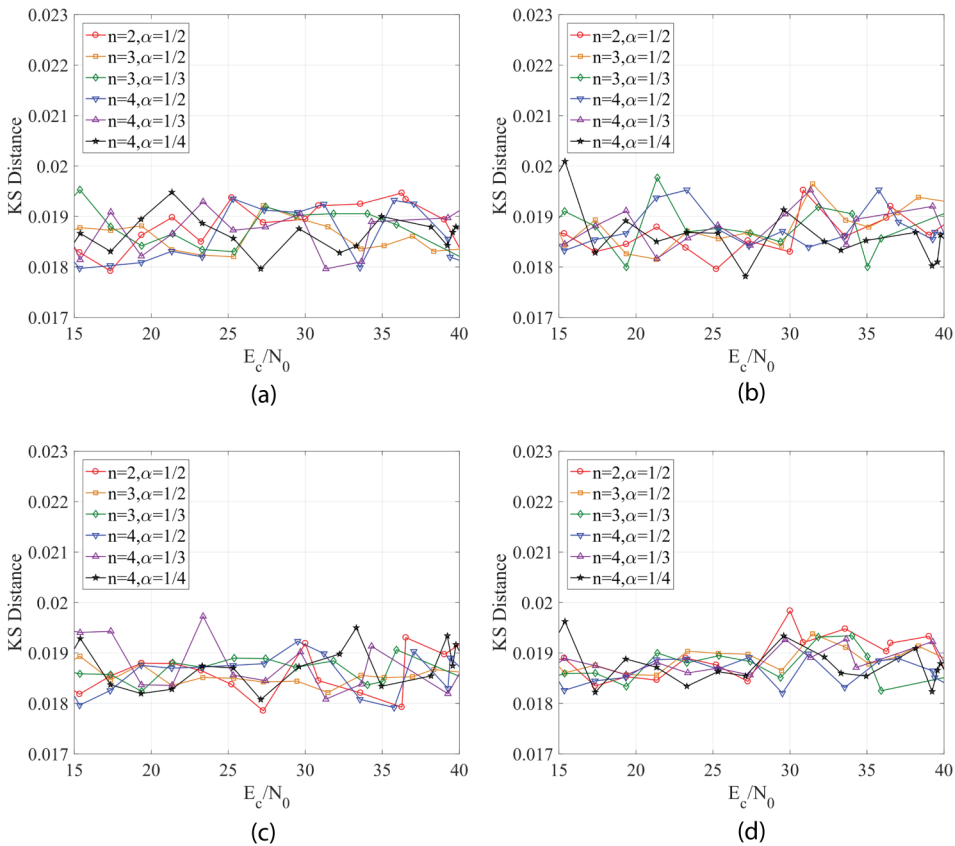
Figure 6. KL divergences of (a) I components, (b) Q components, (c) magnitudes and (d) phases in WCC-DACC with different secret message units and chaotic code rates



measures of the proposed schemes with different secret message units and chaotic code rates remain unchanged.

Then, we compare the undetectability of proposed scheme with that of three wireless covert channels. In WCC-DACC, the length of the secret message unit and the chaotic code rate are set to be  $n = 2, \alpha = 1/2$ . The KL divergences and KS distances of I components, Q components, magnitudes and phases of residual signal in proposed schemes are presented in Figure 8 and 9. The KL divergences and KS distances of WCC-DC, WCC-MT and WCC-CSM are presented for comparison. In Figure 8(a), 8(b), 9(a) and 9(b), with  $E_c/N_0$  increasing, the KL divergences and KS distances of I and Q components in WCC-DC and WCC-MT are increasing slightly while those in WCC-CSM and WCC-DACC are steady. In Figure 8(c) and 9(c), the KL divergences and KS distances of magnitudes in WCC-CSM and WCC-DACC keep steady, however those in WCC-DC and WCC-MT increase obviously. In Figure 8(d) and 9(d), the KL divergences and KS distances of phases of residual signal in all schemes are almost unchanged with  $E_c/N_0$  increasing. It shows that proposed scheme has no degradations on undetectability compared with WCC-CSM. The undetectability of WCC-DACC is better than that of WCC-DC and WCC-MT with the same covert transmission rate, especially at the higher carrier signal to channel noise ratio.

Figure 7. KS distances of (a) I components, (b) Q components, (c) magnitudes and (d) phases in WCC-DACC with different secret message units and chaotic code rates

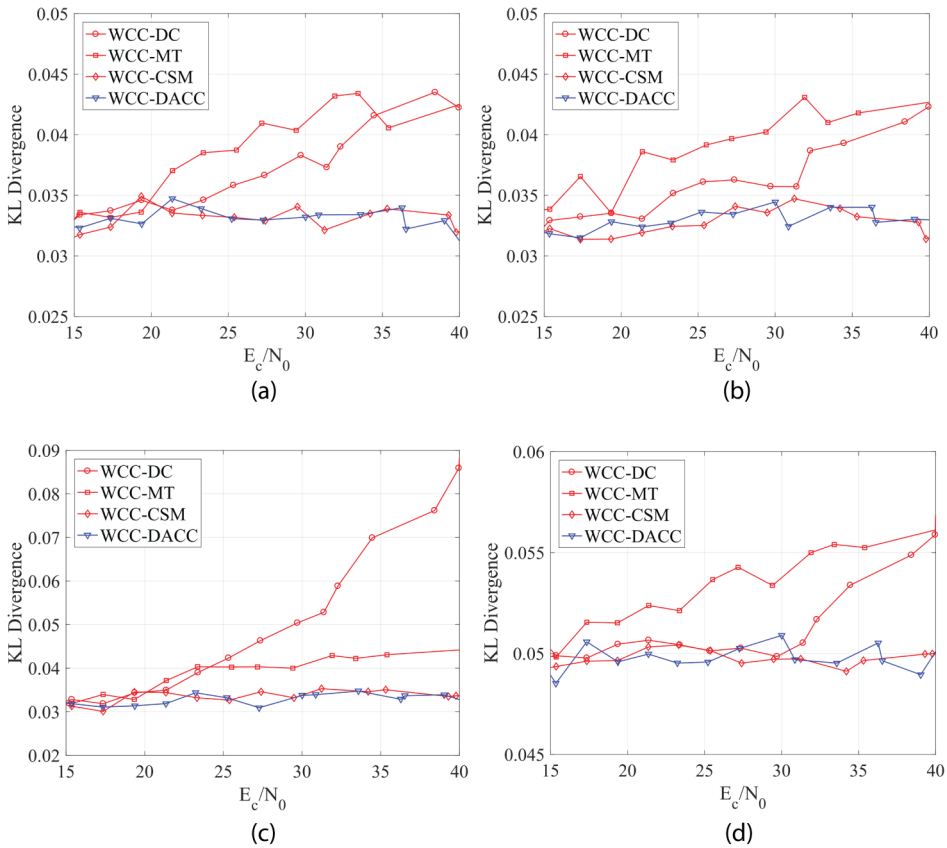


## Reliability

We calculate the BERs of the secret message bits in WCC-DACC. First, in order to verify the effectiveness of dither derivation (DD), the BERs of the secret message bits in WCC-DACC and the scheme without DD are presented in Figure 10. The length of the secret message unit is set to be  $n = 2, 3$ . The chaotic code rate in the proposed schemes is set to  $\alpha = 1/2$  while the code rate in the schemes without DD is set to be  $\alpha = 1/4$ . In Figure 10, with the same the secret message unit, the BERs of the secret message bits in WCC-DACC are less than those without DD. The simulation results show that the application of dither derivation protects the signs of the codewords effectively and improves the reliability of proposed scheme furtherly.

Then, the BERs of the secret message bits in WCC-DACC with different the secret message units and chaotic code rates  $n = 2, \alpha = 1/2; n = 2, \alpha = 1/2, 1/3; n = 2, \alpha = 1/2, 1/3, 1/4$  are presented in Figure 11. In Figure 11, with the same chaotic code rate, the BERs of the secret message bits are increasing obviously with length of the secret message unit increasing. However, with the same the secret message unit and increasing chaotic code rates, the BERs are decreasing. The schemes with the same covert transmission rate have the similar BERs.

Figure 8. KL divergences of (a) I components, (b) Q components, (c) magnitudes and (d) phases in WCC-DACC and existing methods



At last, we compare the BERs of WCC-DACC with that of three wireless covert channels, which are performed in Figure 12. The length of the secret message unit and the chaotic code rate are set to be  $n = 2, \alpha = 1/2$ . The BERs of WCC-DC, WCC-MT and WCC-CSM are presented for comparison. The direct sequence spread spectrum codes based on M-sequence are applied in all schemes to keep the equal covert transmission rate  $R = 0.2$ . In Figure 12, the BERs of WCC-DACC are lower than those of WCC-DC, WCC-MT and WCC-CSM. In summary, it is proved that the proposed wireless covert channels are more reliable than WCC-DC, WCC-MT and WCC-CSM with equal covert transmission rate.

## CONCLUSION

In this paper, we propose a wireless covert channel based on dither analog chaotic code to enhance reliability. The dither analog chaotic code is employed to encode the analog variables converted from secret messages into the joint codewords, which consist of chaotic and dither codewords. The chaotic mapping in DACC encodes chaotic codewords from analog variables. According to the distribution of normal channel noise, dither derivation generates dither codewords from chaotic codewords to protect their signs. Compared with state-of-the-art wireless covert channels, the reliability of the proposed schemes is improved while the undetectability is maintained unchanged.

Figure 9. KS distances of (a) I components, (b) Q components, (c) magnitudes and (d) phases in WCC-DACC and existing methods

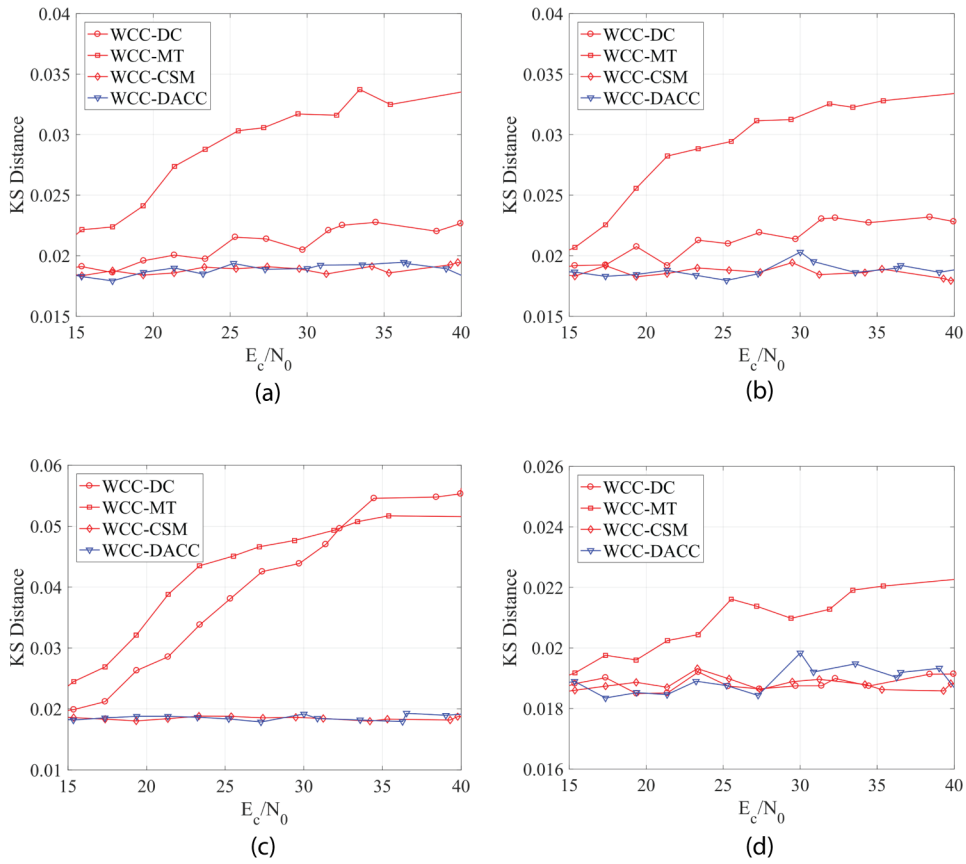


Figure 10. BERs of WCC-DACC with and without dither derivation

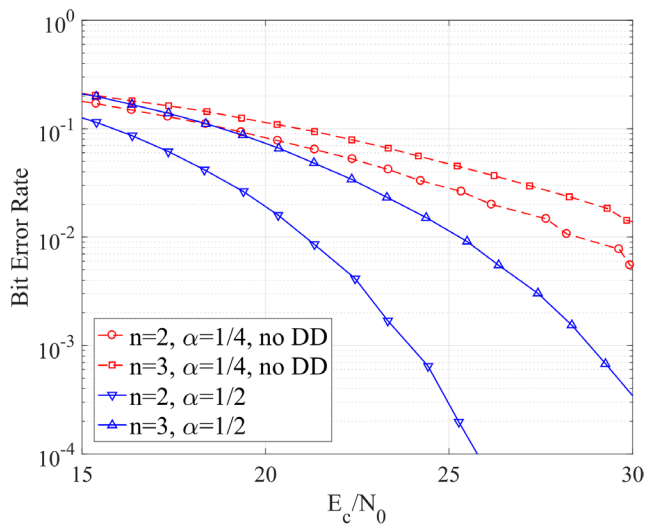




Figure 11. BERs of WCC-DACC with different the secret message units and chaotic code rates

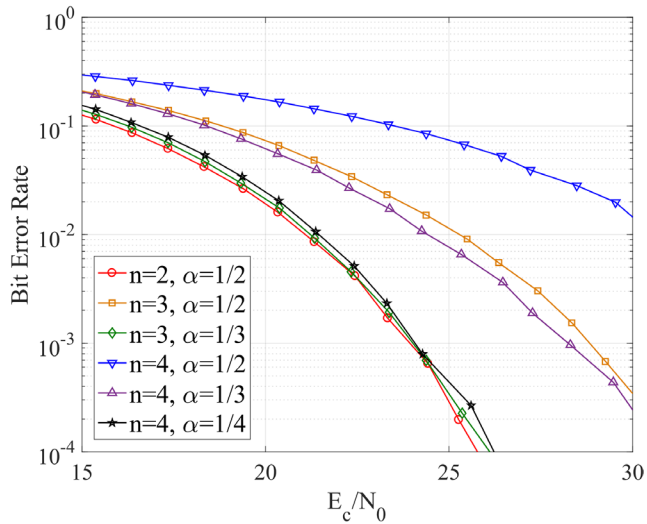
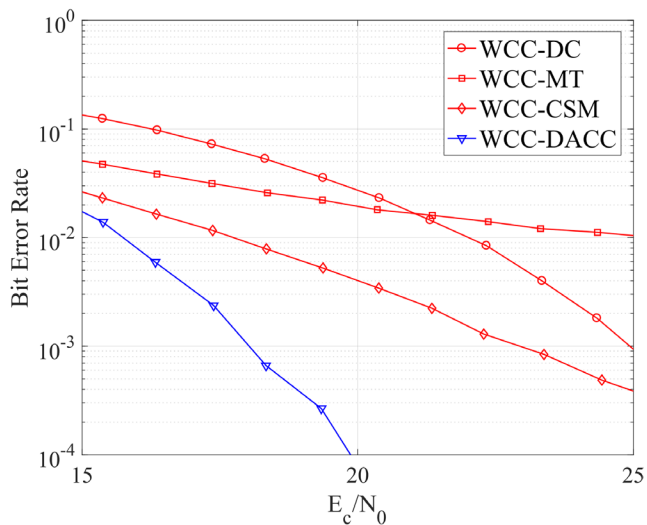


Figure 12. BERs of WCC-DACC and existing methods with equal transmission rate



Even if the proposed schemes can achieve high undetectability and reliability, some characteristics of wireless communication can be used to improve the performance of the covert channels. In the more generalized framework, we can modify both the control channel and data channel to improve the reliability and keep the undetectability is our future work.

## ACKNOWLEDGMENT

This work was supported by The National Natural Science Foundation of China (Grant No. 61602247, 61702235, U1836104, U1636117), Natural Science Foundation of Jiangsu Province(Grant No. BK20160840) and Fundamental Research Funds for the Central Universities (30918012204).

## REFERENCES

- Archibald, R., & Ghosal, D. (2014). A comparative analysis of detection metrics for covert timing channels. *Computers & Security, 45*(8), 284–292. doi:10.1016/j.cose.2014.03.007
- Bloch, M. R. (2015). Covert Communication over Noisy Channels: A Resolvability Perspective. *IEEE Transactions on Information Theory, 62*(5), 2334–2354. doi:10.1109/TIT.2016.2530089
- Cabuk, S., Brodley, C. E., & Shields, C. (2004). *IP Covert Timing Channels: design and detection*. Paper presented at the ACM Conference on Computer and Communications Security, CCS 2004, Washington, DC. doi:10.1145/1030083.1030108
- Cachin, C. (2004). An information-theoretic model for steganography. *Information and Computation, 192*(1), 41–56. doi:10.1016/j.ic.2004.02.003
- Cao, P., Liu, W., Liu, G., Ji, X., Zhai, J., & Dai, Y. (2018). A Wireless Covert Channel Based on Constellation Shaping Modulation. *Security and Communication Networks, 2018*, 1–15. doi:10.1155/2018/1214681
- Cheddad, A., Condell, J., Curran, K., & Kevitt, P. M. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing, 90*(3), 727–752. doi:10.1016/j.sigpro.2009.08.010
- Classen, J., Schulz, M., & Hollick, M. (2015). *Practical covert channels for WiFi systems*. Paper presented at the Communications and Network Security. doi:10.1109/CNS.2015.7346830
- Dutta, A., Saha, D., Grunwald, D., & Sicker, D. (2012). *Secret Agent Radio: Covert Communication through Dirty Constellations*. Paper presented at the International Conference on Information Hiding.
- Gianvecchio, S., Wang, H., Wijesekera, D., & Jajodia, S. (2008). *Model-Based Covert Timing Channels: Automated Modeling and Evasion*. Paper presented at the International Symposium on Recent Advances in Intrusion Detection. doi:10.1007/978-3-540-87403-4\_12
- Grabska, I., & Szczypiorski, K. (2014). *Steganography in Long Term Evolution Systems*. Paper presented at the Security and Privacy Workshops. doi:10.1109/SPW.2014.23
- Guidelines for evaluation of radio transmission technologies for IMT-2000. (1997). *Recommendation ITU-R M.1225*.
- Hijaz, Z., & Frost, V. S. (2010). *Exploiting ofdm for covert communication*. Paper presented at the Military Communications Conference, 2010 - MILCOM 2010.
- Hokai, K., Sasaoka, H., & Iwai, H. (2014). *Wireless steganography using MIMO system*. Paper presented at the IEEE Fifth International Conference on Communications and Electronics.
- Hu, J., Yan, S., Zhou, X., Shu, F., Li, J., & Wang, J. (2018). Covert communication achieved by a greedy relay in wireless networks. *IEEE Transactions on Wireless Communications, 17*(7), 4766–4779. doi:10.1109/TWC.2018.2831217
- Kitano, T., Iwai, H., & Sasaoka, H. (2011). A wireless Steganography technique by embedding DS-SS signal in digital mobile communication systems. *Science & Engineering Review of Doshisha University, 52*, 127–134.
- Mileva, A., & Panajotov, B. (2014). Covert channels in TCP/IP protocol stack - extended version. *Central European Journal of Computer Science, 4*(2), 45–66.
- Rezaei, F., Hempel, M., Peng, D., Qian, Y., & Sharif, H. (2013). *Analysis and evaluation of covert channels over LTE advanced*. Paper presented at the Wireless Communications and Networking Conference (WCNC). doi:10.1109/WCNC.2013.6554855
- Rezaei, F., Hempel, M., & Sharif, H. (2017). Towards a Reliable Detection of Covert Timing Channels over Real-Time Network Traffic. *IEEE Transactions on Dependable and Secure Computing, 14*(3), 249–264. doi:10.1109/TDSC.2017.2656078
- Shah, G., Molina, A., & Blaze, M. (2006). *Keyboards and covert channels*. Paper presented at the Conference on Usenix Security Symposium.

- Soltani, R., Goeckel, D., Towsley, D., Bash, B. A., & Guha, S. (2018). Covert wireless communication with artificial noise generation. *IEEE Transactions on Wireless Communications*, 17(11), 7252–7267. doi:10.1109/TWC.2018.2865946
- Szczypiorski, K., Janicki, A., & Wendzel, S. (2015). “The Good, The Bad And The Ugly”: Evaluation of Wi-Fi Steganography. *Computer Science*.
- Szczypiorski, K., & Mazurczyk, W. (2010). *Hiding Data in OFDM Symbols of IEEE 802.11 Networks*. Paper presented at the Multimedia Information Networking and Security, International Conference on.
- Vojt, Holub, C., & Fridrich, J. (2013). *Digital image steganography using universal distortion*. Paper presented at the ACM Workshop on Information Hiding and Multimedia Security.
- Wang, X., Liu, Y., Lu, X., Lv, S., Shi, Z., & Sun, L. (2017). *CovertMIMO: A covert uplink transmission scheme for MIMO systems*. Paper presented at the ICC 2017 - 2017 IEEE International Conference on Communications. doi:10.1109/ICC.2017.7996863
- Zander, S., Armitage, G., & Branch, P. (2007). *A Survey of Covert Channels and Countermeasures in Computer Network Protocols*. IEEE Press. doi:10.1109/COMST.2007.4317620
- Zhai, J., Liu, G., & Dai, Y. (2013). Detection of TCP covert channel based on Markov model. *Telecommunication Systems*, 54(3), 333–343. doi:10.1007/s11235-013-9737-7