Exploiting Correlation Characteristics to Detect Covert digital communication

Shuhua Huang[1*], Weiwei Liu[1], Guangjie Liu[2], Yuewei Dai[2] and Wen Tian[1]
[1] Nanjing University of Science and Technology
Nanjing, 210094, China
[e-mail: shhuang1003@163.com, lwwnjust@njust.edu.cn, csusttianwen@163.com]
[2]Nanjing University of Information Science and Technology
Nanjing, 210044, China
[e-mail: gjieliu@gmail.com, dywjust@163.com]
*Corresponding author: Shuhua Huang

Received March 30, 2020; revised June 26, 2020; revised July 21, 2020; accepted August 3, 2020; published August 31, 2020

Abstract

As a widely used way to exfiltrate information, wireless covert channel (WCC) brings a serious threat to communication security, which enables the wireless communication process to bypass the authorized access control mechanism to disclose information. Unlike the covert channel on the network layer, wireless covert channels on the physical layer (WCC-P) is a new covert communication mode to implement and improve covert wireless communication. Existing WCC-P scheme modulates the secret message bits into the Gaussian noise, which is also called covert digital communication system based on the joint normal distribution (CJND). Finding the existence of this type of covert channel remains a challenging work due to its high undetectability. In this paper, we exploit the square autocorrelation coefficient (SAC) characteristic of the CJND signal to distinguish the covert communication from legitimate communication. We study the sharp increase of the SAC value when the offset is equal to the symbol length, which is caused by embedding secret information. Then, the SAC value of the measured sample is compared with the threshold value to determine whether the measured sample is CJND sample. When the signal-to-noise ratio reaches 20db, the detection accuracy can reach more than 90%.

Keywords: covert channel detection, wireless communications, Gaussian distribution correlation coefficient, autocorrelation

This work was supported by The National Natural Science Foundation of China(Grant No. 61472188, 61602247, 61702235, U1636117), Natural Science Foundation of Jiangsu Province(Grant No. BK20150472, 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), Fundamental Research Funds for the Central Universities (30920140121006, 30915012208).

http://doi.org/10.3837/tiis.2020.08.023 **ISSN : 1976-7277**

1. Introduction

Network covert channels (NCC) are a policy for leaking information in violation of security policies. The use of NCC to hide malicious activities is increasing, which poses a serious threat to Internet users.[1]. Most early covert channels are based on wired local area networks. The most common covert channel type is network covert channel based on network traffic. They can modify the application layer and embed secret information in the image[2], or the secret information is encoded by using the packet timing [3-6] and the reserved bits on the protocol layer [7].

As one of the rapidly developing industries, wireless communication technology has attracted researchers' attention. The wireless covert channel (WCC) has a good advantage in information hiding due to the complexity and randomness of the wireless communication channel. Due to the randomness and redundancy of wireless network protocols, wireless covert channels on protocol layer are easy to be generated. Several covert channels based on the wireless protocol layer have been proposed in [8, 9] by embedding secret information in the padding and header of the MAC, RLC, and PDCP. The implementation difficulty of this kind of covert channel is relatively low, but the firewall can easily find most types of modifications [10]. In contrast, the wireless covert channel on the physical layer (WCC-P) contains a lot of noise and random signal changes, which makes the covert channel challenging to be detected by the detector.

In [11], the possibility of establishing the covert channel in the WIFI system is analyzed, focusing on the use of physical layer characteristics. The OFDM Cyclic Prefix, additional subcarriers, Carrier Frequency Offset, and Short Training Field are used to design four types of covert channel schemes, and the feasibility is studied in practice. In [12], a WCC-P scheme is proposed based on constellation shape modulation, which moves the original standard constellation points to achieve the embedding of secret information. In [13], a covert communication system is proposed using correlation coefficients of two continuous Gaussian sequences(CJND). In this covert communication system, the receiver estimates the correlation coefficients of two consecutive signals and parses the binary message bits. The scheme has a certain anti-detection capability because Gaussian white noise is almost always unavoidable in wireless communication.

In the security realm, as we all know, the detection of covert channels [14] is a challenging task. For the detection of wireless covert channels, it is mainly divided into two categories, namely the protocol layer and the physical layer. The covert channel on the protocol layer primarily uses redundant bits and padding bits to implement embedding of secret information. Effective detection methods for these covert channels are achieved by extracting, comparing and judging the information of the protocol redundancy bits and padding bits. For the detection of covert channels on the physical layer, there are three kinds of detection tests: shape detection, regularity detection, and entropy detection. The shape of traffic mainly includes some first-order features, such as the mean, variance and the probability density distribution. Kolmogorov-Smirnov test [15] is an effective method to detect covert channels based on probability density distribution. The regularity of traffic [16, 17] mainly includes high-order statistics. Finally, the entropy test is used to describe the similarity between the two distributions. Steven Gianvecchio and Haining Wang [18] proposed a new approach to detect covert timing channels based on the entropy.

In this paper, we propose a scheme to detect the CJND covert channel based on the SAC characteristic of the time-domain communication signal. Autocorrelation is used to find the repeating patterns or identifying fundamental frequencies that disappear in the harmonic frequencies of signals. For the received CJND communication sequence, when the offset is equal to the symbol length, the SAC value will peak. By comparing the relationship between the peak value and the threshold value, it is judged whether the received communication signal is a CJND signal. More specifically, we investigate the detection rate of the CJND signal under different channel scenarios and the influence on the detection result when synchronization error occurs. The simulation results show that the correlation detection scheme is effective in detecting the CJND covert channel.

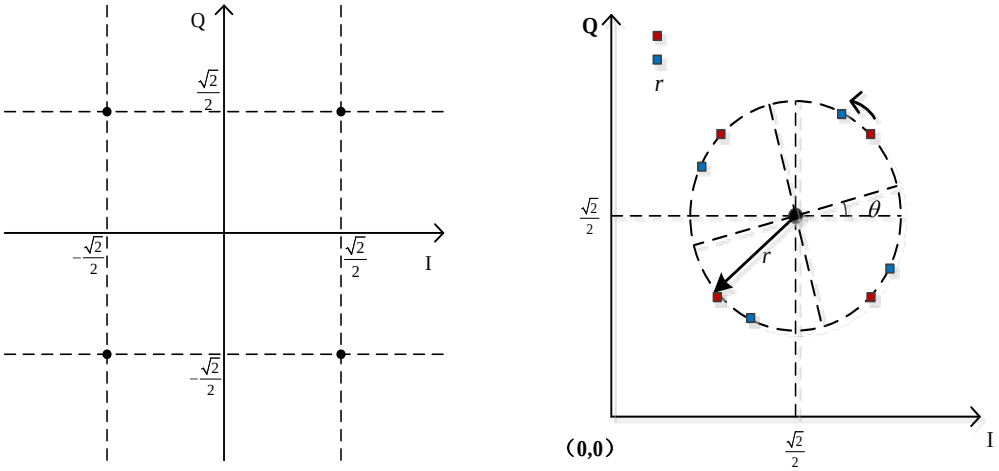
This paper is organized as follows: we introduce the background and related work of covert channels on the physical layer in Section 2. The correlations characteristic for the legitimate and CJND communication signal is described in Section 3. Section 4 describes the scheme to detect the CJND covert channel. Section 5 validates the effectiveness of the detection method in this paper through simulation. Finally, Section 6 concludes the paper and discusses directions for our future work.

2. Related Work

With the development of wireless communication technologies, more and more wireless covert channels on the physical layer are proposed. There are two types of WCC-P schemes: time-domain and frequency-domain. In terms of WCC-P, the time-domain covert channel refers to covert channels that modify the time-domain sequence to transmit information. In contrast, the frequency domain refers to covert communication that changes the position of the constellation points. In general, frequency domain covert channels have higher capacity, but time-domain covert channels are more difficult to detect. Compared with time-domain covert channels, frequency-domain covert channels are more difficult to implement.

2.1 Covert communication through dirty constellations

Aveek Dutta et al. [19] proposed a WCC-P communication scheme based on the existing OFDM modulation scheme. This covert channel achieves good throughput and has a low probability of detection.



(a) QPSK modulation (b) Dirty Constellations modulation

Fig. 1. Constellations distribution

The information is concealed within “dirty” constellations that mimic the noise caused by hardware defects and channel conditions. The mapping sequence bits are used to select the appropriate mapping for covert and non-covert subcarriers. More specifically, for the covert subcarriers, **Fig. 1(b)** corresponds to the upper right quadrant of the constellations of the QPSK constellation shown in **Fig. 1(a)**.

The constellation points are transferred from the original position to the red dot according to the secret information. The dispersion of covert constellation points is limited to a radius of $\sqrt{1/21}$. The constellation points are modulated to the blue dot by rotating the axis. The rotation is performed with a monotonically increasing rotation angle θ; the transmitter and receiver both start with $\theta = 0^{\circ}$.

To make the modulation points of the secret information closer to hardware imperfections and channel conditions. For the cover subcarriers, the random noise (Meet Gaussian distribution in the in-phase and quadrature (I/Q) vectors) is added to the original constellation points.

2.2 Wireless Covert Channel with Constellation Shaping Modulation

Cao [12] proposed a WCC-P scheme with constellation shaping modulation(WCC-CSM). As shown in **Fig. 2**. Through constellation shaping modulation, the secret information bits are modulated into artificial noise signals. In each subcarrier, an artificial noise signal is added to the cover constellation to generate the covert constellation signal.

The secret message bits are denoted by $m_s = \{m_{s1}, m_{s2}, ..., m_{sn}\}$. Where, $m_{si} = (m_{si,1}, m_{si,2}) \in \{00,01,10,11\}$. The I/Q vectors of artificial noise signal s_s are indicated by $x_s^I + j \cdot x_s^Q$. Here, x_s^I and x_s^Q satisfy the distribution of channel noise ($x_{normal}^I + j \cdot x_{normal}^Q$) in the I/Q vectors. Take the I vector, the histograms of x_{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 lower bound and upper bound of the i-th bins.

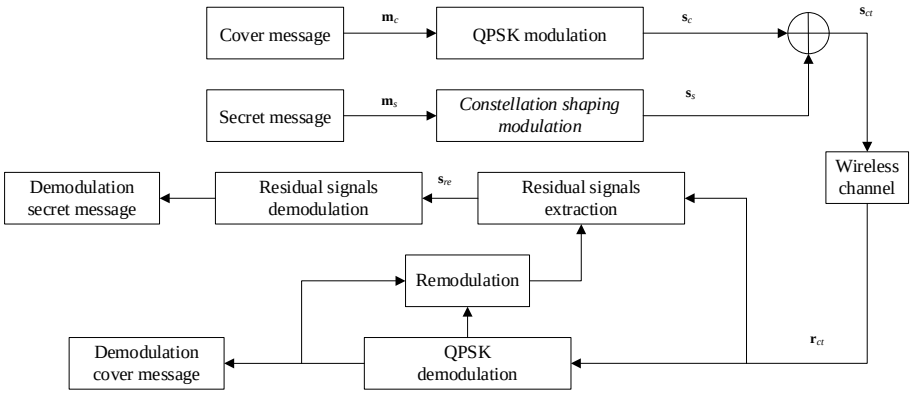


Fig. 2. The flow chart of WCC-CSM scheme

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

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

where R is a random number with uniform distribution on [0, 1], L is the number of bins, N is the length of channel noise, and $c_i=\frac{1}{2}(B_{L,i}+B_{U,i})$. The center line α of histogram of x_{normal}^{I} should be shared with the informed receiver to demodulate the secret information according to the below equation. The modulation and demodulation in the Q plane work in the same way.

$$\hat{m}_{si,1}=\begin{cases} 0, & x_{re}^{I}<\alpha \\ 1, & x_{re}^{I}\geq\alpha \end{cases} \tag{2}$$

2.3 Covert digital communication systems based on the joint normal distribution

Xu Z J [13] proposed a WCC-P communication system which uses the correlation coefficient of two consecutive Gaussian sequences to embed secret information. In this system, if the binary message bit is logic 'i', an independent and identical distributed Gaussian sequence is added to the communication signal. The correlation coefficient between the Gaussian sequence and the previous Gaussian sequence is $\rho=\rho_i$ ($i\in\{0,1\}$). As shown in **Fig. 3**, the secret binary bits are 010….

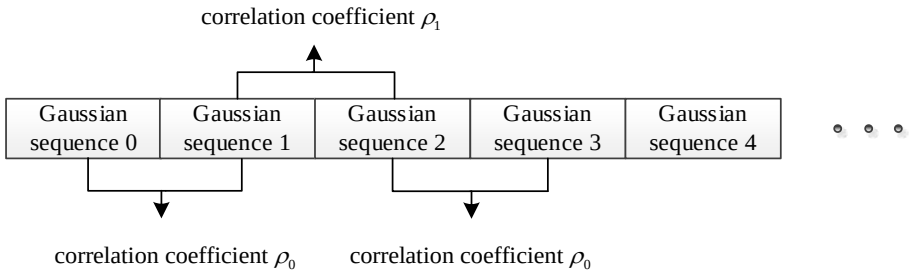


Fig. 3. Signal symbols of the CJND

More specifically, the first group transmitted Gaussian sequence (Gaussian sequence 0) satisfies the standard Gaussian distribution. The Gaussian noise generator generates Gaussian sequences (η_j) with the identical distribution length as Gaussian sequence 0 for each binary bit. If the message bit is logic 'i', then the Gaussian sequence, $n_j=\rho_i n_{j-1}+\sqrt{1-\rho_i^2}\eta_j$, is transmitted ($i\in\{0,1\}$, $j\in N^+$). Finally, the receiver estimates the correlation coefficient of the two consecutive received signal and determines the transmitted binary bit.

2.4 Stable non-Gaussian noise parameter modulation

Cek and Savaci [20] proposed a WCC-P system based on stable non-Gaussian (SNG) noise. Due to interference and fading in wireless network communication, the noise in the communication channel

often satisfies the SNG distribution. Taking the α -stable distribution noise ($X \sim S_{\alpha}(\gamma,\beta,\mu)$) [13] as an example, they set the parameter $\beta=\mu=0$ to make the noise X appear symmetrical, and modify the parameter α to embed secret information. When the transmitted hidden bit is 1, they set $\alpha=\alpha_1$ to generate the corresponding symmetric α_1 -stable noise $X_1 \sim S_{\alpha_1}(\gamma,\beta,\mu)$. When the transmitted hidden bit is 0, they set $\alpha=\alpha_2$ to generate the corresponding symmetric α_2 -stable noise $X_2 \sim S_{\alpha_2}(\gamma,\beta,\mu)$. Finally, all the generated α -stable distribution noises are spliced together in order. The receiver performs demodulation of information by estimating the parameter α of the received noise signal.

3. Correlation measures

In this section, firstly, we introduce the correlation and autocorrelation, and then analyze the SAC characteristic of the CJND scheme. Finally, we propose the design of the CJND channel detection scheme based on the SAC characteristic.

3.1 Correlation and autocorrelation

Assuming that there are two one-dimensional data sets X and Y , the correlation coefficient is defined as:

$$Corr(X,Y)=\frac{Cov(X,Y)}{\sqrt{Var(X)}\sqrt{Var(Y)}} \tag{3}$$

where $Cov(X,Y)$ is the covariance between X and Y . $Var(X)$ and $Var(Y)$ are the variance of X and Y respectively.

Autocorrelation is the mutual correlation between sequence and itself at different time points. It's a function of the time difference between the two observations of the similarity. It is utilized to find repeating patterns or identify fundamental frequencies that disappear in the signal's harmonic frequencies. For a sequence X of length n, the autocorrelation coefficient with a lag of h can be expressed as：

$$\gamma=\frac{\sum_{i=1}^{n-h}(x_i-\hat{\mu})(x_{i+h}-\hat{\mu})}{\sum_{j=1}^{n}(x_i-\hat{\mu})^2} \tag{4}$$

where $\hat{\mu}=\frac{1}{n}\sum_{i=1}^{n}x_i$ is the mean of the sequence X .

3.2 Correlation analysis for CJND scheme

For the CJND scheme, the binary bits are embedded by the correlation coefficient ρ_i ($i\in\{0,1\}$, $\rho_0=-\rho_1$) of the two consecutive gaussian distribution sequences. For two independent Gaussian distributions, the correlation coefficient between them is close to zero. The two adjacent Gaussian sequences for the CJND method are respectively $n_j=\rho_i n_{j-1}+\sqrt{1-\rho_i^2}\eta_j$ and $n_{j\text{-}1}$ (η_j, n_j and $n_{j\text{-}1}\sim N(0,1)$), and the correlation

coefficient can be expressed as:

$$\begin{aligned} Corr(n_{j-1}, n_j) &= \frac{Cov(n_{j-1}, (\rho_i n_{j-1} + \sqrt{1-\rho_i^2}\eta_j))}{\sqrt{Var(n_{j-1})}\sqrt{Var(n_j)}} \\ &= Cov(n_{j-1}, \rho_i n_{j-1}) + Cov(n_{j-1}, \sqrt{1-\rho_i^2}\eta_j) \approx \rho_i \end{aligned} \tag{5}$$

For the transmitted Gaussian noise sequence, $s_j = \begin{cases} \eta & 0 < j \le h \\ \rho_i s_{j-h} + \sqrt{1-\rho_i^2}\varepsilon_i & j > h \end{cases}$ (η and $\varepsilon \sim N(0, \delta^2)$). h is the length of the symbol. For the transmitted sequence with the length of n, we set $\hat{s} = s^2$, $x = s_{1\ldots(n-h)}$ and $y = s_{(1+h)\ldots n}$. The SAC value for s with a lag of h can be expressed as:

$$\begin{aligned} \gamma &= \frac{E[(\hat{S}_i - \mu)(\hat{S}_{i+h} - \mu)]}{\sqrt{Var(\hat{S}_i)}\sqrt{Var(\hat{S}_{i+h})}} \\ &= \frac{E[(X^2 - \mu)((\rho_i X + \sqrt{1-\rho_i^2}\varepsilon)^2 - \mu)]}{Var(\hat{S})} \end{aligned} \tag{6}$$

where X and ε are independently identically Gaussian distributed (X, $\varepsilon \sim N(0, \delta^2)$), $\mu = \frac{1}{n}\sum_{i=1}^{n} \hat{s}_i = \delta^2$, $E(X^4) = E(\varepsilon^4) = 3\delta^4$, $E(X^3) = E(\varepsilon^3) = E(X) = E(\varepsilon) = 0$, $E(X^2) = E(\varepsilon^2) = \delta^2$, $Var(\hat{S}) = 2\delta^4$. Then $\gamma = \rho_i^2$.

3.3 SAC Characteristic analysis for CJND received signal

The goal for the detection scheme is to distinguish CJND covert traffic from legitimate traffic. In this paper, the covert channel detection is realized by using the difference of SAC value between covert channel traffic and legitimate traffic in the time domain. In section 3.2, we have analyzed the SAC characteristic of CJND covert traffic. When the offset is equal to the symbol length, the SAC value will appear visible peak. When considering that the channel is ideal, that is, there is no channel fading and noise, then the peak value is ρ_i^2.

3.3.1 SAC value analysis in an AWGN channel

In this case, we consider the AWGN channel, that is, the transmitted signal is only contaminated by white gaussian noise, so the observed signal output from the channel is:

$$r(t) = s(t) + \lambda(t) \sim N(0, \delta_s^2 + \delta_n^2) \tag{7}$$

where $\lambda(t) \sim N(0, \delta_n^2)$ is white Gaussian noise, and $s(t) \sim N(0, \delta_s^2)$ is the transmitted Gaussian sequence. In this paper, h is the length of the symbol, we set $\hat{r} = r^2 \in \hat{R}$, $x = s_{1\ldots(n-h)} \in X$, $y = s_{(1+h)\ldots n} \in Y$, $\lambda_1 = \lambda_{1\ldots(n-h)} \in \Lambda_1$ and $\lambda_2 = \lambda_{(1+h)\ldots n} \in \Lambda_2$. Furthermore, X, Y, Λ_1 and Λ_2 are

independently identically Gaussian distributed (X and $Y \sim N(0,\delta_s^2)$, Λ_1 and $\Lambda_2 \sim N(0,\delta_n^2)$).
$\mu=\frac{1}{n}\sum_{i=1}^{n}\hat{r}_i=\delta_s^2+\delta_n^2$, $Var(\hat{R})=2(\delta_s^2+\delta_n^2)^2$, $E(X^4)=E(Y^4)=3\delta_s^4$, $E(\Lambda_1^4)=E(\Lambda_2^4)=3\delta_n^4$,
$E(X^3)=E(Y^3)=E(X)=E(Y)=0$, $E(\Lambda_1^3)=E(\Lambda_2^3)=E(\Lambda_1)=E(\Lambda_2)=0$,
$E(X^2)=E(Y^2)=\delta_s^2$, $E(\Lambda_1^2)=E(\Lambda_2^2)=\delta_n^2$.

The SAC value for r with a lag of h can be expressed as:

$$\begin{aligned}\gamma&=\frac{E[(\hat{R}_i-\mu)(\hat{R}_{i+h}-\mu)]}{\sqrt{Var(\hat{R}_i)}\sqrt{Var(\hat{R}_{i+h})}}=\frac{E[(X^2-\mu)(Y^2-\mu)]}{Var(\hat{R})}\\&=\frac{\rho_i^2\delta_s^4}{(\delta_s^2+\delta_n^2)^2}=\frac{\rho_i^2}{(1+\frac{\delta_n^2}{\delta_s^2})^2}=\frac{\rho_i^2}{(1+10^{-\frac{\varsigma_1}{10}})^2}\end{aligned} \tag{8}$$

where the signal to noise ratio (SNR) is defined as $\varsigma_1=10\lg(\frac{\delta_s^2}{\delta_n^2})$.

3.3.2 SAC value analysis in a time-invariant multipath channel

In this section, a frequency-flat static channel is considered, the channel gain remains constant. The transmitted signal is also contaminated by the white gaussian noise, then the observed signal from the output of the channel is:

$$r(t)=k\otimes s(t)+\lambda(t) \tag{9}$$

where $k(m)\in R^+(m\in\{1,...,q\})$ is the channel gain, $s(t)\sim N(0,\delta_s^2)$ is the transmitted time-domain signal and $\lambda(t)\sim N(0,\delta_n^2)$ is the white gaussian noise. The SAC value for r with a lag of h can be expressed as:

$$\begin{aligned}\gamma&=\frac{E[(\hat{R}_i-\mu)(\hat{R}_{i+h}-\mu)]}{\sqrt{Var(\hat{R}_i)}\sqrt{Var(\hat{R}_{i+h})}}=\frac{E[(X^2-\mu)(Y^2-\mu)]}{Var(\hat{R})}\\&=\frac{\|k\|_2^4\rho_i^2\delta_s^4}{(\|k\|_2^2\delta_s^2+\delta_n^2)^2}=\frac{\rho_i^2}{(1+10^{-\frac{\varsigma_2}{10}})^2}\end{aligned} \tag{10}$$

where $\|k\|_2$ denotes 2-norm and SNR is defined as $\varsigma_2=10\lg(\frac{\|k\|_2^2\delta_s^2}{\delta_n^2})$

3.3.3 SAC value analysis in a time-varying multipath channel

In this section, a fading channel with Doppler shift is considered.

$$\begin{aligned} r(t) &= k(t) \otimes s(t) + \lambda(t) \\ &= \sum_{l=1}^{L} k_l(t+\tau_k)\, s(t+\tau_k) + \lambda(t) \end{aligned} \tag{11}$$

where $k(t)=\{k_l(t), l=1,...L\} \sim N(0, \delta_{k,l}^2)$ is a vector of Rayleigh fading path gains variables [13]. The autocorrelation function is:

$$E(k_l(t)k_l(t+\tau)) = \delta_{k,l}^2 J_0(2\pi f_d \tau) \tag{12}$$

and the cross-correlation function is :

$$E(k_l(t)k_j(t+\tau)) = 0 (k \neq j) \tag{13}$$

The SAC value for r with a lag of h can be expressed as:

$$\begin{aligned} \gamma &= \frac{E[(\hat{R}_i - \mu)(\hat{R}_{i+h} - \mu)]}{\sqrt{Var(\hat{R}_i)}\sqrt{Var(\hat{R}_{i+h})}} = \frac{E[(X^2 - \mu)(Y^2 - \mu)]}{Var(\hat{R})} \\ &= \frac{\rho_i^2 \delta_s^4 (\sum_{l=1}^{L} \delta_{k,l}^2)^2 J_0^2(2\pi f_d T_b)}{(\delta_s^2 \sum_{l=1}^{L} \delta_{k,l}^2 + \delta_n^2)^2} = \frac{J_0^2(2\pi f_d T_b)\rho_i^2}{(1+10^{-\frac{\varsigma_3}{10}})^2} \end{aligned} \tag{14}$$

where $J_0(\cdot)$ is zero-order Bessel function of the first kind; f_d is the maximum Doppler shift; T_b is bit interval time and SNR is defined as $\varsigma_3 = 10\lg(\frac{\delta_s^2 \sum_{l=1}^{L} \delta_{k,l}^2}{\delta_n^2})$.

3.4 detection scheme

For the time-domain signal of the measured sample, we develop a detection scheme based on the SAC characteristic. **Fig. 4** shows the normal probability plot of the received CJND signal in the AWGN, time-invariant multipath channel, time-varying multipath channel (channel A) and TGn-B channel. The Doppler frequency domain of channel A is 100 Hz, path delays and path gains are $[0, 3.8, 7.2, 11]*10^{-6} s$ and $[0, -10/3, -20/3, -10]$dB, respectively.

Gaussian noise is applied as a carrier signal in the CJND scheme. In the AWGN and time-invariant multipath channel, the received time-domain sequence obeys Gaussian distribution. By contrast, the received sequence does not obey Gaussian distribution in the time-varying multipath channel, as shown in **Fig. 4**. When the channel environment between the detector and the transmitter is complex, the time-domain distribution for the received signal will no longer satisfy the Gaussian distribution.

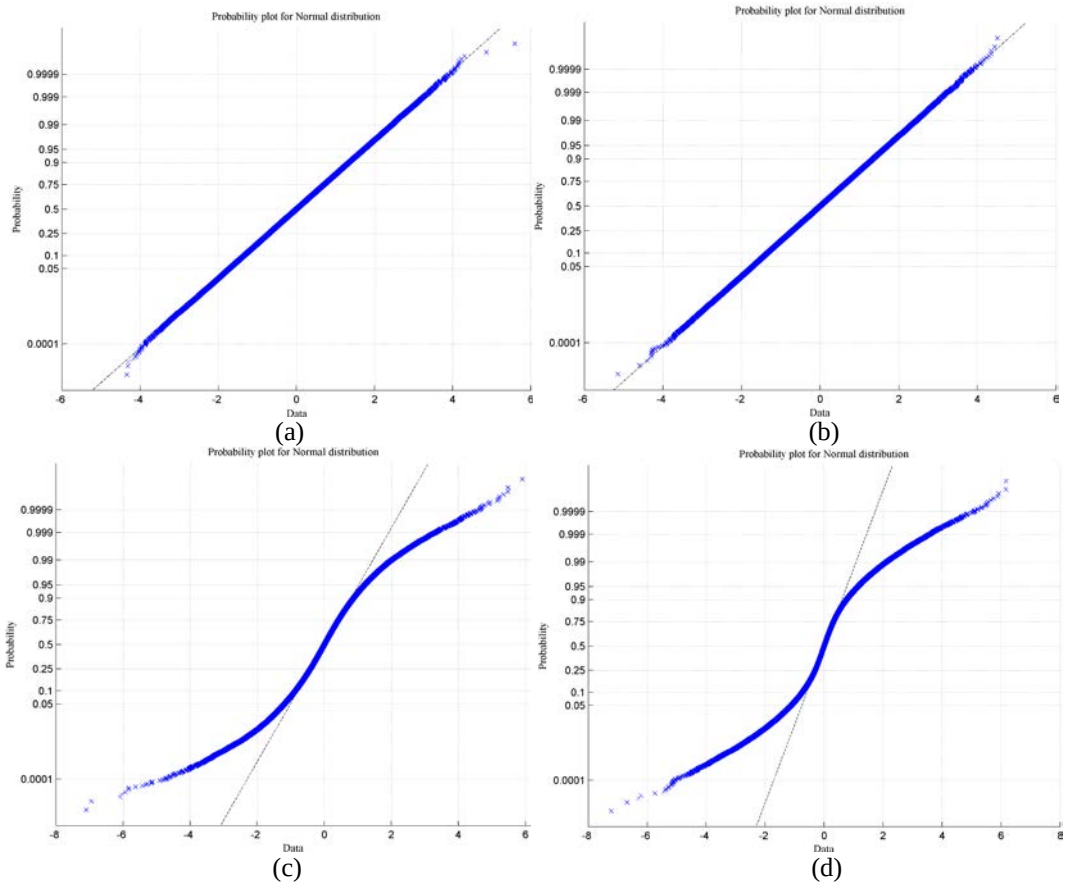


Fig. 4. Normal probability plot for the received signal with SNR $\varsigma = 10dB$
(a) AWGN channel (b) time-invariant multipath channel, where channel gain
$k = [0.8771, 0, 0.1754, -0.2631, 0, 0.0877, -0.3508]$
(c) time-varying multipath channel A (d) time-varying multipath channel B (TGn-B)

For the standard Gaussian sequence, the SAC value with offset is close to zero. In section 3.3, although the signals received in AWGN and time-invariant multipath channels obey Gaussian distribution in time domain, the SAC value with a lag of h is significantly higher than zero when h is equal to the length of symbol. For the received signal in the time-varying multipath channel, the received signal does not obey Gaussian distribution, and the SAC value will be significantly greater than 0. We take advantage of the SAC characteristic to make comparisons between CJND and legitimate traffic.

For the measured sample, we calculate the SAC value under different offsets. At the same time, we calculate the SAC value for the Gaussian sequence under different offsets and count maximum value as the detection threshold. If the maximum SAC value for the measured sample is higher than the detection threshold, we believe that the measured sample comes from CJND covert channel. Otherwise, it is judged to be the standard Gaussian signal.

4. Simulation and analysis

The purpose of detection is to distinguish CJND covert traffic from legitimate traffic. In this part, we use a series of simulations to verify the effectiveness of our proposed scheme. The

focus of the simulation is to examine the influence of correlation coefficient, detection window size, and sampling length under different channel models. Furthermore, We test the effect of the synchronization error on our detection scheme.

4.1 Simulation setup

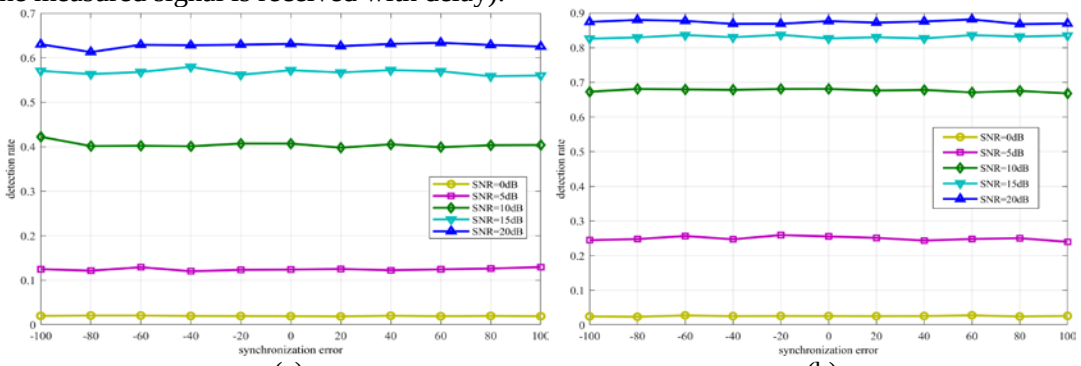
The simulation experiment in this paper is based on four different communication channel models. In the first scenario, which is an AWGN channel, we only consider the influence of white Gaussian noise. In the second scenario, which is a time-invariant multipath channel, we consider a frequency-flat Rayleigh fading channel without Doppler shift with $k=[0.8771,0,0.1754,-0.2631,0,0.0877,-0.3508]$. In the third scenario, which is a time-varying multipath channel, a frequency-selective with Doppler shift channel is considered to test our detection scheme. Where, the maximum Doppler shift $f_d=100Hz$, bit interval time $T_b=10^{-4}s$, path delay is $[0,3.8,7.2,11]*10^{-6}s$, and the path gain of the frequency-selective channel is $[0,-10/3,-20/3,-10]$db . In the following paragraphs, we refer to this time-varying multipath channel as channel A. Finally, we consider a TGn-B channel (another frequency-selective with Doppler shift channel) to test the detection scheme. In our simulation, the normalized power of the transmitted signal $\delta_s=1$ and a number of 10^5 trials are used.

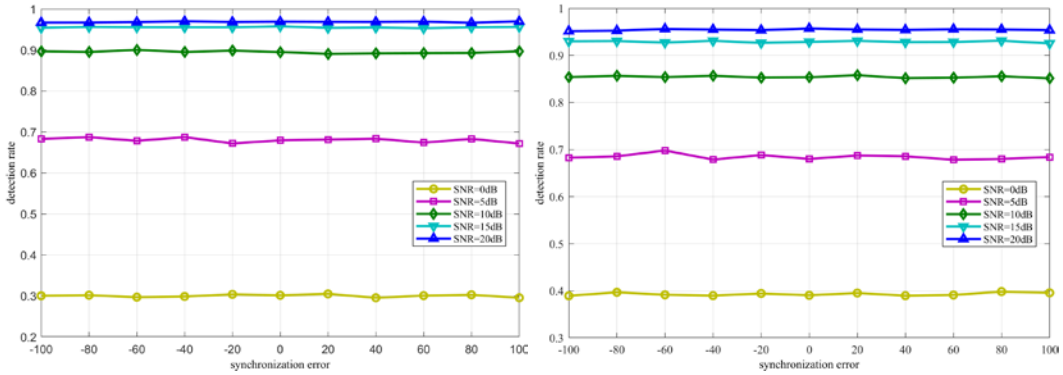
4.2 Detection simulation result

In this section, four parts of the simulation are introduced in detail: the detection with synchronization error; the detection with different correlation coefficients; the detection with different window sizes and the detection with different sampling lengths. All these simulations are tested in four different channel models. The detection rate is defined as $\frac{m}{M}$, where, M is the number of detection window for the measured sequence, m is the number of detection window judged to be covert channels.

4.2.1 Simulation result with the different synchronization errors

In this section, we test the effect of synchronization error on the detection results. In the wireless communication scenario, especially in the detection process, it is difficult to achieve perfect synchronization. **Fig. 5** shows the detection results in four different simulation channel models with the synchronization error (negative synchronization error indicates that the measured signal sequence is received in advance, and positive synchronization indicates that the measured signal is received with delay).





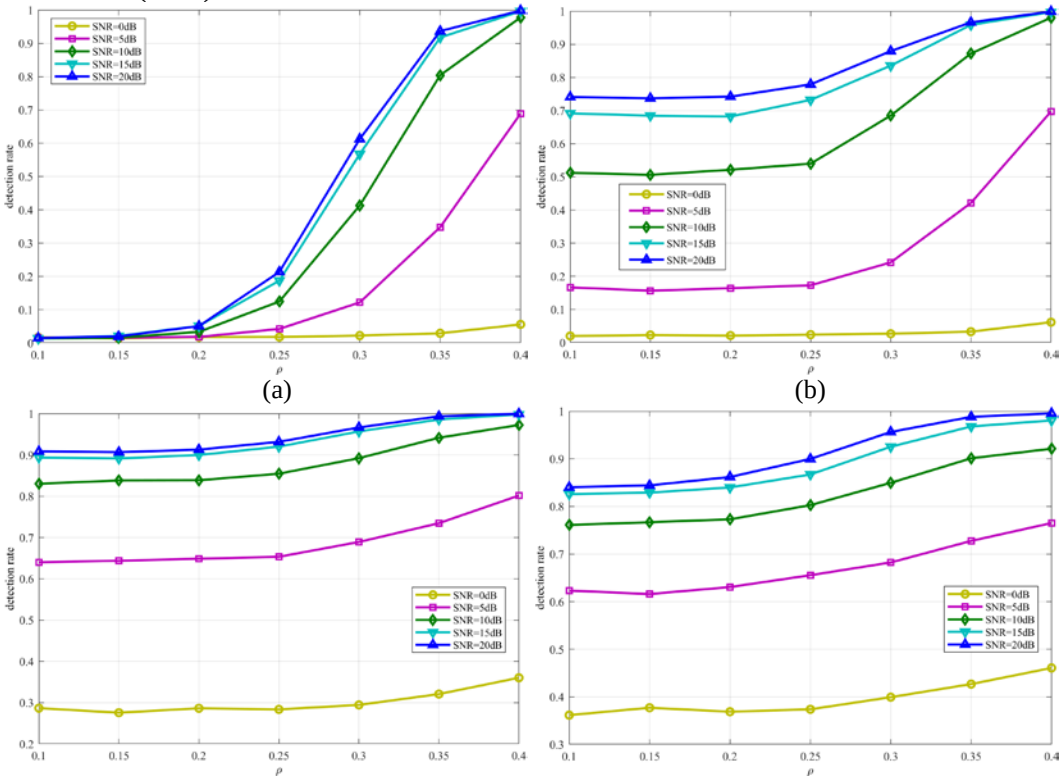
(c) (d)

Fig. 5. The detection rate for CJND received signal with synchronization error (ρ=0.3 , N=100)
(a) AWGN channel (b) time-invariant multipath channel (c) channel A (d) TGn-B channel

Since the synchronization error does not affect the sequence correlation, synchronization error does not affect the detection rate, regardless of whether it is earlier or later than perfect synchronization, as shown in **Fig. 5**. In the following detection simulation, the signals received by the detector are accurately synchronized.

4.2.2 Simulation result with the different correlation coefficient

In the process of CJND communication, the correlation coefficient ρ will directly affect the bit error rate (BER) of covert communication.



(a) (b)

(c) (d)

Fig. 6. The detection rate for CJND received signal with different correlation coefficient
(a) AWGN channel (b) time-invariant multipath channel (c) channel A (d) TGn-B channel

In this paper, the covert channel detection is achieved by using the SAC characteristic. The relationship between the detection rate for the CJND communication and correlation coefficient in different SNRs is shown in **Fig. 6**. In this simulation, the sampling length for CJND communication is 100 and the window size is 3000.

Since the SAC value has a positive correlation with the correlation coefficient ρ, it can be seen that the detection rate increases, when the correlation coefficient ρ increases. Moreover, when the SNR>10dB, when the correlation coefficient ρ is relatively large (e.g. 0.4), the performance of the detection rate tends to saturation. For the AWGN channel, when the SNR and window size are constant, the correlation coefficient ρ is the only factor that affects the detection rate. For the time-invariant multipath channel, the Multipath channel will affect the SAC value besides the correlation coefficient. By contrast, for the time-varying multipath channel, in addition to the correlation coefficient, channel fading and Doppler frequency shifts will affect the SAC value. Compared **Fig. 6**(a),(b), (c), and (d), it can be seen that the correlation coefficient has the greatest influence on the detection rate for the AWGN channel, followed by time-invariant multipath channel and time-varying multipath channel.

4.2.3 Simulation result with the different window size

In this section, we focus on the relationship between the detection rate and detection window size. The length of the detection window will have an impact on SAC value. As the length of the detection window increases, the estimation of SAC value is more accurate and closer to ρ^2, as shown in **Fig. 7**.

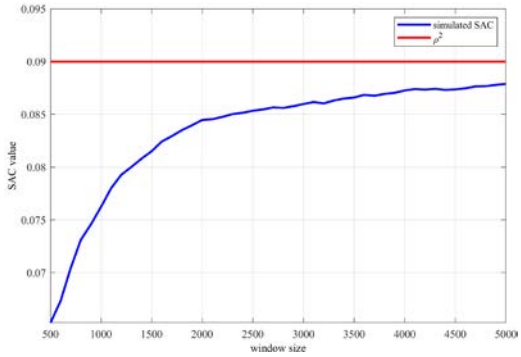
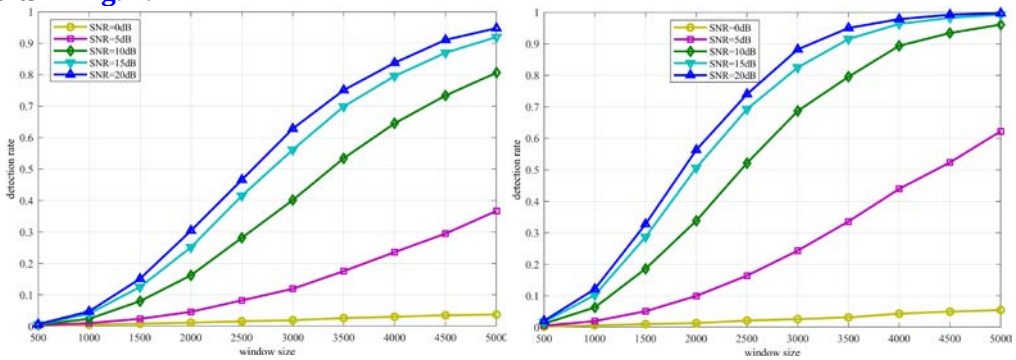


Fig. 7. Simulated and theoretical SAC value with ρ=0.3, N=100 and different window size

Fig. 8 shows the relationship between the detection rate and detection window under different channel models and SNRs. The simulation results are consistent with the theoretical results in **Fig. 7**.



(a) (b)

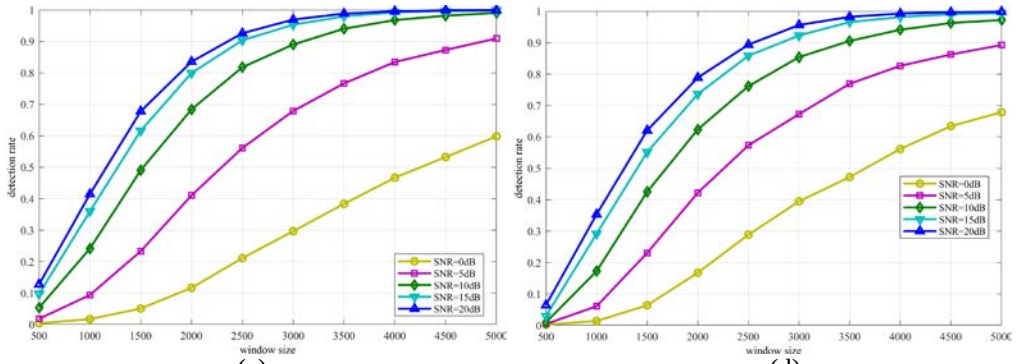


Fig. 8. The detection rate for CJND received signal with different window size
(a) AWGN channel (b) time-invariant multipath channel (c) channel A (d) TGn-B channel

With the increase of the detection window, our detection scheme has a higher detection rate. By comparing **Fig. 8(c)** and **Fig. 8(d)**, the relationship between the detection rate and detection window is similar under the same type of simulation channel (time-varying multipath channel).

4.2.4 Simulation result with the different sampling length

Through theoretical analysis, for the transmitted sequence of the CJND scheme, the value corresponding to SAC is only related to ρ ($SAC = \rho^2$). In the simulation process, the sampling length in the CJND scheme will have an impact on SAC value. In this section, the influence of symbol length on SAC is analyzed through the simulation experiment, and the detection rate of our detection scheme for the CJND covert channel with different sampling lengths is obtained through simulation.

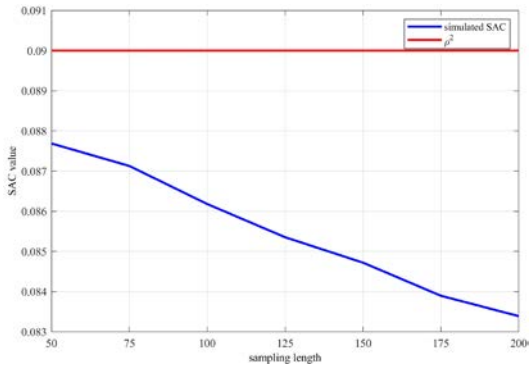


Fig. 9. Simulated and theoretical SAC value with ρ=0.3 and different sampling length

For the CJND scheme, increasing the sampling length can improve the accuracy of information transmission, but at the expense of bit transmission rate. In the process of our detection scheme, **Fig. 9** shows the relationship between SAC value and sampling length, as the sampling length increases, the corresponding SAC value decreases slightly under the same detection window size.

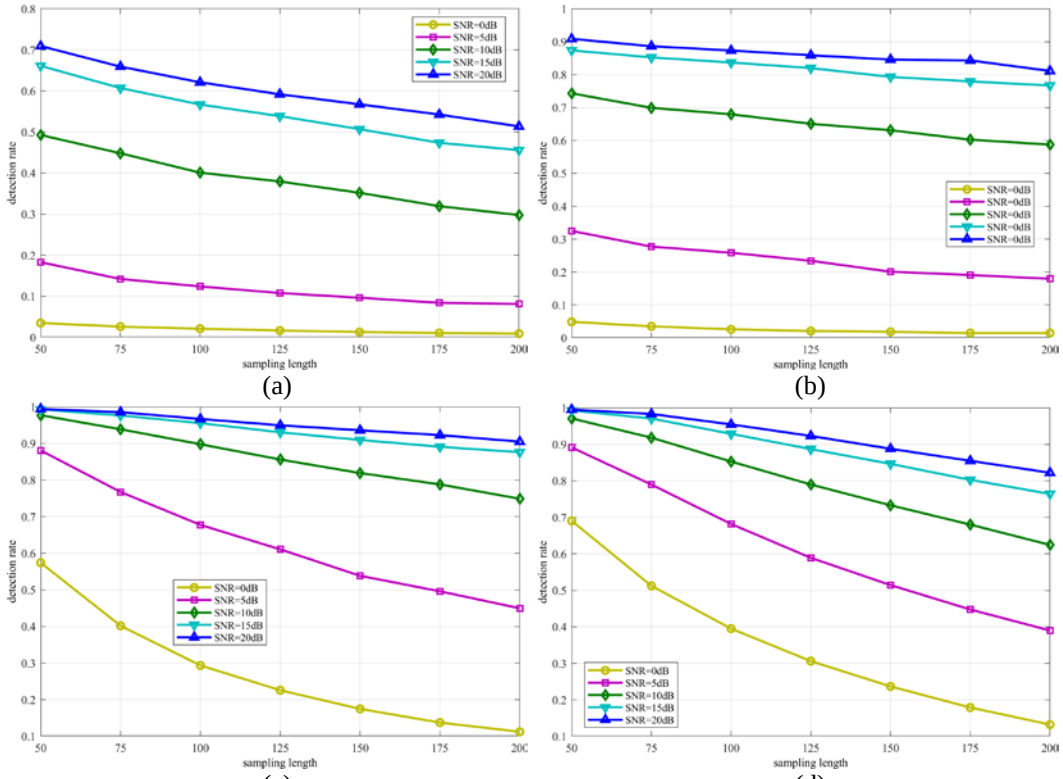


Fig. 10. The relationship between detection rate and sampling length
(a) AWGN channel (b) time-invariant multipath channel (c) channel A (d) TGn-B channel

Fig. 10 shows the relationship between the detection rate and sampling length. As the symbol length affects SAC value, the detection rate decreases with the increase of the sampling length. Compared to **Fig. 10** (c) and (d), it can be seen that the detection rate has similar variation characteristics with the sampling length in the same type of simulation channel model.

5. Conclusion

In this paper, we proposed a wireless covert channel detection scheme based on the SAC characteristic for detecting the CJND scheme. We analyzed the SAC values at the detection end under different channel models and find that when the offset is equal to the length of the code symbol, the SAC values will show obvious peak. Since there is a synchronization error in the detection end, the SAC characteristic between the sequences is not affected. Through simulation observation, the synchronization error at the detection end has no impact on the detection result. At the same time, it was found through simulation experiments that the SAC value and detection rate increase with the increase of detection window size and correlation coefficient, and the decrease of sampling length. However, in this paper, through the scheme proposed in this article, we can only judge whether the measured sample is a CJND sample, but we cannot perform further analysis on this sample. In the subsequent research, we will estimate the characteristic coefficients of the measured sample, such as symbol length and correlation coefficient.

References

[1] E. Casey, "Investigating sophisticated security breaches," *Communications of the ACM*, vol. 49, no. 2, pp. 48-55, February, 2006. Article (CrossRef Link)

[2] D. Xiao, J. Liang, Q. Ma, Y. Xiang, and Y. Zhang, "High capacity data hiding in encrypted image based on compressive sensing for nonequivalent resources," *Computers, Materials & Continua*, vol. 58, no. 1, pp. 1-13, 2019. Article (CrossRef Link)

[3] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, "Model-based covert timing channels: Automated modeling and evasion," in *Proc. of International Workshop on Recent Advances in Intrusion Detection*, vol. 5230, pp. 211-230, 2008. Article (CrossRef Link)

[4] K. Kothari and M. Wright, "Mimic: An active covert channel that evades regularity-based detection," *Computer Networks*, vol. 57, no. 3, pp. 647-657, February, 2013. Article (CrossRef Link)

[5] 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, April, 2011. Article (CrossRef Link)

[6] G. Liu, J. Zhai, and Y. Dai, "Network covert timing channel with distribution matching," *Telecommunication Systems*, vol. 49, no. 2, pp. 199-205, 2012. Article (CrossRef Link)

[7] A. Mileva and B. Panajotov, "Covert channels in TCP/IP protocol stack-extended version," *Open Computer Science*, vol. 4, no. 2, pp. 45-66, June, 2014. Article (CrossRef Link)

[8] I. Grabska and K. Szczypiorski, "Steganography in long term evolution systems," in *Proc. of 2014 IEEE Security and Privacy Workshops*, pp. 92-99, May, 2014. Article (CrossRef Link)

[9] K. Szczypiorski and W. Mazurczyk, "Hiding data in OFDM symbols of IEEE 802.11 networks," in *Proc. of 2010 International Conference on Multimedia Information Networking and Security*, pp. 835-840, November, 2010. Article (CrossRef Link)

[10] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 3, pp. 44-57, 2007. Article (CrossRef Link)

[11] J. Classen, M. Schulz, and M. Hollick, "Practical covert channels for WiFi systems," in *Proc. of 2015 IEEE Conference on Communications and Network Security (CNS)*, pp. 209-217, September, 2015. Article (CrossRef Link)

[12] P. Cao, W. Liu, G. Liu, X. Ji, J. Zhai, and Y. Dai, "A wireless covert channel based on constellation shaping modulation," *Security and Communication Networks*, vol. 2018, January, 2018. Article (CrossRef Link)

[13] Z.-J. Xu, Y. Gong, K. Wang, W.-D. Lu, and J.-Y. Hua, "Covert digital communication systems based on joint normal distribution," *IET Communications*, vol. 11, no. 8, pp. 1282-1290, 2017. Article (CrossRef Link)

[14] Y. Wang, Y. Cao, L. Zhang, H. Zhang, R. Ohriniuc, G. Wang, et al., "YATA: Yet Another Proposal for Traffic Analysis and Anomaly Detection," *CMC-Computers, Materials & Continua*, vol. 60, no. 3, pp. 1171-1187, 2019. Article (CrossRef Link)

[15] P. Peng, P. Ning, and D. S. Reeves, "On the secrecy of timing-based active watermarking trace-back techniques," in *Proc. of 2006 IEEE Symposium on Security and Privacy (S&P'06)*, pp. 334-349, May, 2006. Article (CrossRef Link)

[16] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert timing channels: design and detection," in *Proc. of the 11th ACM conference on Computer and communications security*, pp. 178-187, October, 2004. Article (CrossRef Link)

[17] G. Shah, A. Molina, and M. Blaze, "Keyboards and Covert Channels," in *Proc. of USENIX Security Symposium*, vol. 15, pp. 59-75, July, 2006. Article (CrossRef Link)

[18] S. Gianvecchio and H. Wang, "An entropy-based approach to detecting covert timing channels," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 785-797, 2011. Article (CrossRef Link)

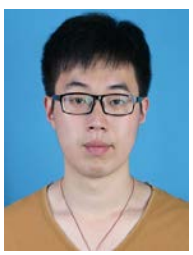
[19] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, "Secret agent radio: Covert communication through dirty constellations," in *Proc. of International Workshop on Information Hiding*, vol. 7692, pp. 160-175, 2012. Article (CrossRef Link)
[20] M. E. Çek and F. Savaci, "Stable non-Gaussian noise parameter modulation in digital communication," *Electronics Letters*, vol. 45, no. 24, pp. 1256-1257, 2009. Article (CrossRef Link)

Shuhua Huang received the B.S. degree in automation from the Nanjing University of Science and Technology, Nanjing, P.R. China, in 2015. He is currently a Ph.D. candidate with the Nanjing University of Science and Technology, Nanjing. His research interests include detection of wireless covert communication and network security.

Weiwei Liu received the B.S. degree in automation and the Ph.D. degree in control science and engineering from the Nanjing University of Science and Technology, Nanjing, in 2010 and 2015, respectively. From 2014 to 2015, he was a Visiting Scholar with the Department of Computer Science, University of California at Davis, Davis, CA, USA. He is currently an Associate Professor with the School of Automation, Nanjing University of Science and Technology. His research interests include multimedia signal processing and network traffic analysis. He has published over 30 articles in these areas, including the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and Annals of Telecommunications. He is an active Reviewer of several journals, including Digital Signal Processing and Security and Communication Networks.

Guangjie Liu received the B.S. degree in electrical and computer engineering and the Ph.D. degree in control science and engineering from the Nanjing University of Science and Technology, Nanjing, in 2002 and 2007, respectively. He is currently an Associate Professor with the School of Automation, Nanjing University of Science and Technology. His research interests are multimedia systems and deep learning.

Yuewei Dai received the B.S. and M.S. degrees in system engineering from the East China Institute of Technology, Nanjing, P.R. China, in 1984 and 1987, respectively, and the Ph.D. degree in control science and engineering from the Nanjing University of Science and Technology, in 2002. He is currently a professor with the School of Automation, Nanjing University of Science and Technology. His research interests are in multimedia security, system engineering theory, and network security.



Wen Tian received the B.S. degree in physics from Changsha University of Science and Technology, Changsha, P.R. China, in 2014 and the M.S. degree in control theory and control engineering from the Jiangsu University of Science and Technology, Zhenjiang, P.R. China, in 2017. He is currently a Ph.D. candidate with the Nanjing University of Science and Technology, Nanjing, P.R. China. His research interests include cyber–physical systems and network security.