CDMA System Design and Capacity Analysis under Disguised Jamming

Tianlong Song, Kai Zhou, and Tongtong Li

***Abstract*—This paper considers robust CDMA system design and capacity analysis under disguised jamming, where the jammer generates a fake signal using the same spreading code, constellation and pulse shaping filter as that of the authorized signal. Unlike Gaussian jamming, which is destructive only when jamming is dominant, disguised jamming can be devastating even if the jamming power is comparable to the signal power. In this paper, *first*, we analyze the performance of conventional CDMA under disguised jamming, and show that due to the symmetricity between the authorized signal and the jamming interference, the receiver cannot really distinguish the authorized signal from jamming, leading to complete communication failure. *Second*, we propose to combat disguised jamming using secure scrambling. Instead of using conventional scrambling codes, we apply advanced encryption standard (AES) to generate the security-enhanced scrambling codes. Theoretical analysis based on the arbitrarily varying channel (AVC) model shows that: the capacity of conventional CDMA without secure scrambling under disguised jamming is actually zero; however, secure scrambling can break the symmetricity between the authorized signal and the jamming interference, and hence ensures positive channel capacity under disguised jamming. Numerical examples are provided to demonstrate the effectiveness of secure scrambling in combating disguised jamming.**

***Index Terms*—CDMA, physical layer security, disguised jamming, secure scrambling, capacity analysis.**

I. Introduction

ALONG with the advances in user reconfigurable devices, anti-jamming system design and analysis are getting more attentions from the research community [1]–[7]. Traditionally, the anti-jamming systems are mainly based on spread spectrum techniques. The spread spectrum systems, including code division multiple access (CDMA) and frequency hopping (FH), were originally developed for secure communications in military applications. Both CDMA and FH systems possess anti-jamming and anti-interception features by exploiting frequency diversity over large spectrum. Under hostile environments, CDMA is one of the most effective approaches to ensure secure communications under eavesdropping, malicious jamming attacks or intended electronic interference [8], [9].

In CDMA, each user is assigned a specific pseudo-random code (also known as the signature waveform) to spread its signal over a bandwidth N times larger. Due to the processing gain resulted from the spread spectrum technique, CDMA is especially robust under narrowband jamming and works well under low SNR levels [10]. Hidden within the noise floor, CDMA signals are difficult to be detected, and cannot be recovered unless the user signature is known at the receiver. For these reasons, CDMA has been widely used in both civilian and military applications. For example, CDMA has been used in 3GPP UMTS systems [11], and adopted in high speed packet access (HSPA) systems; it is also serving as an active solution in the navigation systems, including the GPS system [12] developed by the United States, the Compass system developed by China, and the Galileo system developed by Europe.

In this paper, we consider CDMA system design and capacity analysis under hostile jamming. For a long time, hostile jamming has generally been modeled as Gaussian noise, and people believe that the impact of jamming on the channel capacity can be characterized as $C = B\log_2(1 + \frac{P_s}{P_J+P_n})$. This implies that only strong jamming is really harmful. However, recent research [13]–[21] has found that: disguised jamming, which mimics the characteristics of the authorized user's signal, can paralyze the communication system with a power level close to that of the authorized user's signal. As a result of the wide spread of advanced wireless devices, once the authorized user's signature waveform is captured, disguised jamming may be launched using a portable user reconfigurable intelligent device.

Does CDMA also suffer from disguised jamming? The answer largely relies on the security of the PN sequence. For CDMA, the spreading code of each user is obtained through the modulo 2 sum of the Walsh code and the long code, and thus is varying in every symbol period. However, according to the Berlekamp-Massey algorithm [22], for a sequence generated from an n-stage linear feedback shift register, the characteristic polynomial and the entire sequence can be reconstructed if an eavesdropper can intercept a $2n$-bit sequence segment. Note that the characteristic polynomial is generally available to the public, then PN sequence can be recovered if an n-bit sequence segment is intercepted. That is, it is possible to break the PN sequence used in the conventional CDMA systems in real time with today's high speed computing techniques [23]. Once the PN sequence is recovered or broken, the jammer can generate a fake signal using the same spreading code, constellation and pulse shaping filter as that of the authorized signal. This is the *disguised jamming* for CDMA. As can be seen, it has become a serious threat to practical CDMA systems.

This work was supported in part by the NSF under Grants CNS-1217206 and ECCS-1232109.

T. Song, K. Zhou and T. Li are with the Department of Electrical and Computer Engineering, College of Engineering, Michigan State University, East Lansing, MI 48824 USA (e-mail: {songtia6, zhoukai}@msu.edu, tongli@egr.msu.edu).

In this paper, we first analyze the performance of the conventional CDMA systems under disguised jamming, and show that due to the symmetricity between the authorized signal and the jamming interference, the receiver cannot really distinguish the authorized signal from jamming, leading to complete communication failure. Then we propose to combat disguised jamming using secure scrambling. More specifically, instead of using conventional scrambling codes, we apply advanced encryption standard (AES) to generate the security-enhanced scrambling codes. Its security is guaranteed by AES, which is has been proved to be secure under all known attacks [24]. Assuming ideal synchronization between the authorized user and the jammer, we prove that: the capacity of the conventional CDMA without secure scrambling under disguised jamming is actually zero; however, the capacity can be significantly increased when CDMA systems are protected using secure scrambling. The underlying argument is that: the secure scrambling process results in security-enhanced PN codes which are intractable for the malicious user; hence it breaks the symmetricity between the authorized user and the jammer, and ensures positive transmission capacity under disguised jamming.

To the best of our knowledge, we are the first to analyze the capacity of CDMA systems under disguised jamming, in addition to Gaussian noise-like jamming. It is found that: CDMA communication could fail completely under disguised jamming, which is easy to launch (e.g., using a portable, user reconfigurable device), but difficult to detect due to the similarity between the authorized signal and the jamming. For this reason, we propose an AES-based secure scrambling scheme to combat disguised jamming for CDMA systems. The main contributions of this paper can be summarized as:

- We analyze the performance of conventional CDMA under disguised jamming using the arbitrarily varying channel (AVC) model, and show that due to the symmetricity between the authorized signal and the jamming interference, the receiver cannot really distinguish the authorized signal from jamming, leading to complete communication failure. More specifically, the capacity of the conventional CDMA without secure scrambling under disguised jamming is actually proved to be zero.
- We propose a secure scrambling scheme to combat disguised jamming for CDMA systems, and using the AVC model, we prove that it ensures positive capacity under disguised jamming. More specifically, instead of using conventional scrambling codes, we apply AES to generate the security enhanced scrambling codes. It is shown that: due to the shared secure randomness between the transmitter and receiver, the symmetricity between the authorized signal and the jamming interference is broken. In fact, the AVC kernel corresponding to CDMA systems with secure scrambling is not only nonsymmetric but also nonsymmetrizable, and therefore ensures positive channel capacity under disguised jamming. In the paper, we further estimate the capacity and error probability of CDMA systems with secure scrambling under disguised jamming.

Simulation results are provided to demonstrate the effectiveness of secure scrambling in combating disguised jamming.

The rest of the paper is organized as follows. The system model and problem formulation are described in Section II. The secure scrambling scheme is elaborated in Section III. Analytical capacity and error probability analysis for CDMA systems with and without secure scrambling is presented in Section IV. Numerical evaluation is provided in Section V and we conclude in Section VI.

II. System Model and Problem Identification

A. System Model

We consider an individual user in a typical CDMA system. Assuming the processing gain is N, namely, there are N chips per symbol. Let

$$\mathbf{c} = [c_0, c_1, ..., c_{N-1}] \tag{1}$$

denote the spreading code, in which $c_n = \pm 1, \ \forall n$. In the isolated pulse case, the general baseband signal of the spreading sequence can be represented as

$$c(t) = \sum_{n=0}^{N-1} c_n \, g(t - nT_c), \tag{2}$$

where $g(t)$ is the pulse shaping filter, T_c the chip period, and we assume

$$\frac{1}{T} \int_0^T c^2(t) dt = 1, \tag{3}$$

where $T = NT_c$ is the symbol period.

Let Ω be the constellation, and $u_k \in \Omega$ the kth symbol to be transmitted. The spread chip-rate signal can be expressed as

$$q_n = u_k \, c_{n-kN}, \tag{4}$$

where $k = \lfloor \frac{n}{N} \rfloor$. The successive scrambling process is achieved by

$$z_n = q_n \, e_n = u_k \, c_{n-kN} \, e_n, \tag{5}$$

where $e_n = \pm 1$ is a pseudorandom chip-rate scrambling sequence. After pulse shaping, the transmitted signal would then be

$$s(t) = \sum_{n=-\infty}^{\infty} u_k \, c_{n-kN} \, e_n \, g(t - nT_c). \tag{6}$$

Note that c_n, e_n and $g(t)$ are real-valued, while u_k can be complex depending on the constellation Ω.

For an AWGN channel, the received signal can be written as

$$y(t) = s(t) + n(t) = \sum_{n=-\infty}^{\infty} u_k \, c_{n-kN} \, e_n \, g(t - nT_c) + n(t), \tag{7}$$

where $n(t)$ is the white Gaussian noise.

To recover the transmitted symbols, the CDMA receiver first descrambles the received signal by multiplying a locally generated and synchronized copy of the scrambling sequence, e_n. Afterwards, the received signal will be reduced to

$$y(t) = \sum_{n=-\infty}^{\infty} u_k \, c_{n-kN} \, g(t - nT_c) + n(t). \tag{8}$$

Without loss of generality, we consider the recovery of the symbol indexed by $k = 0$ and omit the subscript k in u_k. The corresponding signal of interest would be constrained within $t = [0, T)$, and following the definition in (2), we have

$$r(t) = \sum_{n=0}^{N-1} u\, c_n\, g(t - nT_c) + n(t) = u\, c(t) + n(t). \quad (9)$$

Performing the despreading process, and following (3), the CDMA receiver estimates the transmitted symbol as

$$\hat{u} = \frac{1}{T}\int_0^T r(t)c(t)dt = u + \frac{1}{T}\int_0^T n(t)c(t)dt. \quad (10)$$

We can observe from the process above that it is impossible to recover the transmitted symbols without knowing the user's spreading code and scrambling code. This is known as a *built-in security* feature of the CDMA systems. In the following subsection, we will discuss the security level of several typical CDMA systems, and show that: disguised jamming, which mimics the authorized signal, can severely jeopardize the CDMA systems, and in the worst case, leads to complete communication failure.

B. Problem Identification

Since the spreading codes are generally short and easy to generate, the physical layer built-in security of typical CDMA systems mainly relies on the long pseudorandom scrambling sequence, also known as long code, e.g., in IS-95, 3GPP as well as the military GPS. However, it was shown in [23] that the long scrambling codes used by IS-95 or 3GPP UMTS can be cracked with reasonably high computational complexity. In fact, the maximum complexity to recover the long scrambling codes in IS-95 and 3GPP UMTS is only $O(2^{42})$ and $O(2^{36})$ [23], respectively. As another example, the civilian GPS even makes its codes public to attract potential users for global competitiveness.

The weakly secured or even public spreading/scrambling codes leave considerable room for malicious users to launch disguised jamming [14], [15], [17] towards the authorized signal. The jammer can mimic the authorized signal by generating fake symbols over the cracked or already known codes. With complete knowledge of the code information and the pulse shaping filter, the jammer can launch disguised jamming, which has the similar characteristics as the authorized signal, except that the fake symbol can only be randomly chosen out of Ω. Moreover, there may be small timing and amplitude differences between the authorized signal and the disguised jamming due to non-ideal estimation at the jammer side.

Let $v \in \Omega$ denote the fake symbol, τ the small timing difference, and γ the amplitude ratio of the disguised jamming to the authorized signal. Then, the disguised jamming can be modeled as

$$j(t) = v\,\gamma\, c(t - \tau). \quad (11)$$

Taking both the noise and disguised jamming into account, and following (9), the received signal can be written as

$$r(t) = s(t) + j(t) + n(t) = u\, c(t) + v\,\gamma\, c(t - \tau) + n(t), \quad (12)$$

where $n(t)$ is the noise.

An important observation is that: *the conventional CDMA receiver in (10) would fail under disguised jamming.* In fact, replacing the received signal $r(t)$ in (10) with (12), and following (3), we have

$$\hat{u} = u + v\gamma\frac{1}{T}\int_0^T c(t-\tau)c(t)dt + \frac{1}{T}\int_0^T n(t)c(t)dt. \quad (13)$$

As can be seen, the symbol estimation would be considerably influenced by the second term in the RHS of (13), which is introduced by disguised jamming, especially when τ is small (e.g., $|\tau| < T_c$) and $\gamma \approx 1$. In the worst case, when $\tau = 0$ and $\gamma = 1$, (13) is reduced to a very simple form:

$$\hat{u} = u + v + \frac{1}{T}\int_0^T n(t)c(t)dt. \quad (14)$$

We can now apply the error probability analysis result in [17], in which it was shown that in this case, the probability of symbol error, $\mathcal{P}_s$, would be lower bounded by

$$\mathcal{P}_s \geq \frac{M-1}{2M}, \quad (15)$$

where M is the constellation size of Ω. An intuitive explanation is that: if the authorized symbol "u" and the fake one "v" are distinct, the receiver would have to guess between them as indicated in (14). Note that: (i) the error probability of a random guess between two symbols is $\frac{1}{2}$; (ii) the two symbols randomly and independently selected out of Ω by the authorized transmitter and disguised jammer differ with a probability of $\frac{M-1}{M}$. Combining (i) and (ii), it then follows that $\mathcal{P}_s \geq \frac{M-1}{2M}$.

The lower bound in (15) sets up a limit for the error probability performance of CDMA systems under the worst-case disguised jamming (i.e., $\tau = 0$ and $\gamma = 1$), which implies that the CDMA communication is completely paralyzed.

When the timing and amplitude differences between the authorized signal and the disguised jamming are not too small, that is, the disguised jamming is not the worst, then it is possible to mitigate the jamming considerably by exploiting these differences in the receiver design (see Appendix A). However, when these differences get too small, then it is difficult for the receiver to distinguish the authorized signal from the jamming due to the symmetricity between them.

To address this issue, we propose to combat disguised jamming using secure scrambling, which essentially enhances the security of the scrambling codes and hence breaks the symmetricity between the authorized user and the jammer.

III. Jamming Mitigation with Secure Scrambling

As can be seen in Section II, the physical layer security of most CDMA systems largely relies on the scrambling process. To prevent disguised jamming in CDMA systems, we propose to generate the scrambling sequence using the advanced encryption standard (AES), also known as Rijndael.

A. AES-based Secure Scrambling

Rijndael was identified as the new AES in October 2, 2000. Rijndael's combination of security, performance, efficiency, ease of implementation, and flexibility make it an appropriate selection for the AES. Rijndael is a good performer in both hardware and software across a wide range of computing environments. Its low memory requirements make it very well suited for restricted-space environments such as mobile handset to achieve excellent performance. More details on AES can be found in [25].

The proposed secure scrambling scheme aims to increase the physical layer built-in security of CDMA systems and prevent exhaustive key search attack, while minimizing the changes required to the existing standards. As shown in Fig. 1, the secure scrambling sequence is generated through two steps: first, generate a pseudo-noise (PN) sequence, then encrypt the sequence with the AES algorithm. More specifically, a PN sequence is first generated using a PN sequence generator with a secure initialization vector (IV), where the PN sequence generator is typically a linear feedback shift register (LFSR) or Gold sequence generator; subsequently the PN sequence is encrypted by the AES algorithm block by block secured by a secret encryption key, which is shared between the legitimate communication parties.

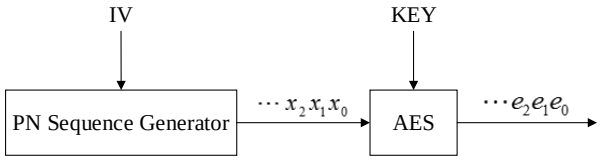


Fig. 1. Secure scrambling sequence generation.

The secure scrambling process can be summarized as follows:

1) The communication parties share a common initial vector (IV) for the PN sequence generator and an L-bit (L=128, 192, or 256) common secret encryption key;
2) The long scrambling sequence is generated through encryption of a particular segment of the sequence generated from the PN sequence generator using the shared secret key;
3) The scrambling process is realized by adding the scrambling sequence to the chip-rate spread signal.

B. Security Analysis

To eavesdrop the transmitted data or launch disguised jamming, the malicious user has to intercept the secure scrambling sequence used by the legitimate users. Hence, the security of the proposed scrambling process lies in how difficult it is to crack the encrypted scrambling sequence. In this subsection, we use data encryption standard (DES) [26] as a benchmark to evaluate the security of the proposed secure scrambling, which is essentially ensured by AES. We compare the number of possible keys of AES, DES and that of the typical CDMA scrambling sequences. The number of keys determines the effort required to crack the cryptosystem by trying all possible keys.

The most important reason for DES to be replaced by AES is that it is becoming possible to crack DES through exhaustive key search. Single DES uses 56-bit encryption key, which means that there are approximately 7.2×10^{16} possible DES keys. In the late 1990s, specialized "DES cracker" machines were built and they could recover a DES key after a few hours. In other words, by trying all possible keys, the hardware could determine which key was used to encrypt a message. Compared with DES, IS-95 has only 42-bit shared secret (approximately 4.4×10^{12} possible keys), and 3GPP UMTS has even lower security with 36-bit shared secret (approximately 6.9×10^{10} possible keys). This makes it possible to break these low-security scrambling sequences almost in real time through exhaustive key search.

On the other hand, AES specifies three key sizes: 128, 192, and 256 bits. In decimal terms, this means that approximately there are

1) 3.4×10^{38} possible 128-bit keys;
2) 6.2×10^{57} possible 192-bit keys;
3) 1.1×10^{77} possible 256-bit keys.

Thus, if we choose $L = 128$, then there are on the order of 10^{21} times more AES 128-bit keys than DES 56-bit keys. Assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{56} keys per second), as we can see, this is a very ambitious assumption and far from what we can do today, then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key.

Security measurement through the number of all possible keys is based on the assumption that the attacker has no easy access to the secret encryption key, therefore, the attacker has to perform an exhaustive key search in order to break the system. As is well known, the security of AES is based on the infeasible complexity in recovering the encryption key. Currently, no weakness has been detected for AES, thus, exhaustive key search is still being recognized as the most effective method in recovering the encryption key and breaking the cryptosystem. Based on the evaluation above, as long as the encryption key is kept secret, it is impossible for the malicious user to recover the scrambling sequence, and thus disguised jamming can hardly be launched. In this case, the best jamming strategy for the malicious user would be distributing its total available power uniformly on the spread spectrum by randomly generating a PN sequence as the scrambling sequence [27].

As will be seen in Section IV, under the condition that the jammer has comparable power as the authorized user, the harm of this kind of jamming without knowing the secure scrambling sequence will actually become trivial.

IV. Capacity Analysis of CDMA Systems with and without Secure Scrambling under Disguised Jamming

Without secure scrambling, the jammer can launch disguised jamming towards the CDMA systems by exploiting

the known code information and mimicking the authorized signal. In this case, it has been shown in Section II-B that the error probability of the symbol transmission is lower bounded by $\frac{M-1}{2M}$, where M is the constellation size. In this section, by applying the arbitrarily varying channel (AVC) model, we will show that: due to the symmetricity between the authorized signal and jamming interference, the capacity of the traditional CDMA system (i.e., without secure scrambling) under worst disguised jamming is actually zero; on the other hand, with secure scrambling, the shared secure randomness between the transmitter and the receiver breaks the symmetricity between the authorized signal and jamming, and hence ensures positive capacity under worst disguised jamming.

A. Revisit of the AVC Model

Before proceeding to the analysis of any specific systems, we first briefly revisit the general AVC model and some well-known results corresponding to it. An AVC channel model is generally characterized using a kernel $W : \mathcal{S} \times \mathcal{J} \to \mathcal{Y}$, where $\mathcal{S}$ is the transmitted signal space, $\mathcal{J}$ is the jamming space (i.e., the jamming is viewed as the arbitrarily varying channel states) and $\mathcal{Y}$ is the estimated signal space. For any $\mathbf{s} \in \mathcal{S}$, $\mathbf{j} \in \mathcal{J}$ and $\mathbf{y} \in \mathcal{Y}$, $W(\mathbf{y}|\mathbf{s},\mathbf{j})$ denotes the conditional probability that $\mathbf{y}$ is detected at the receiver, given that $\mathbf{s}$ is the transmitted signal and $\mathbf{j}$ the jamming.

***Definition* 1** ([18])**.** *The AVC is said to have a symmetric kernel, if $\mathcal{S} = \mathcal{J}$ and $W(\boldsymbol{y}|\boldsymbol{s},\boldsymbol{j}) = W(\boldsymbol{y}|\boldsymbol{j},\boldsymbol{s})$ for any $\boldsymbol{s},\boldsymbol{j} \in \mathcal{S}, \boldsymbol{y} \in \mathcal{Y}$.*

***Definition* 2** ([18])**.** *Define $\hat{W} : \mathcal{S} \times \mathcal{S} \to \mathcal{Y}$ by $\hat{W}(\boldsymbol{y}|\boldsymbol{s},\boldsymbol{s}') \triangleq \sum_{\boldsymbol{j}\in\mathcal{J}'} \pi(\boldsymbol{j}|\boldsymbol{s}')W(\boldsymbol{y}|\boldsymbol{s},\boldsymbol{j})$, where $\pi : \mathcal{S} \to \mathcal{J}'$ is a probability matrix and $\mathcal{J}' \subseteq \mathcal{J}$. If there exists a $\pi : \mathcal{S} \to \mathcal{J}'$ such that $\hat{W}(\boldsymbol{y}|\boldsymbol{s},\boldsymbol{s}') = \hat{W}(\boldsymbol{y}|\boldsymbol{s}',\boldsymbol{s})$, $\forall \boldsymbol{s},\boldsymbol{s}' \in \mathcal{S}, \forall \boldsymbol{y} \in \mathcal{Y}$, then W is said to be symmetrizable.*

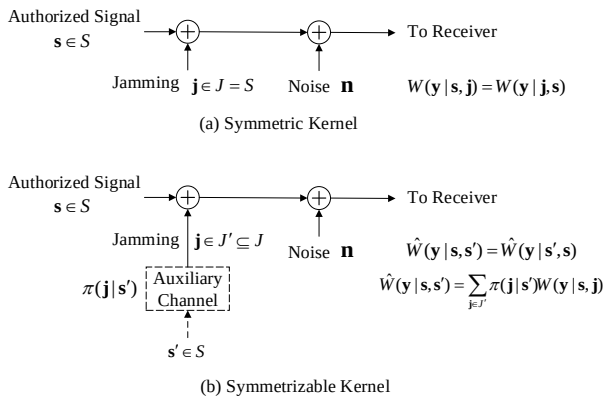


Fig. 2. An illustration of symmetric and symmetrizable AVC kernels.

To help elaborate the physical meaning of these concepts, symmetric and symmetrizable AVC kernels are depicted in Fig. 2. In an AVC with a symmetric kernel, jamming is generated from exactly the same signal space as that of the authorized signal. Even if the roles of the authorized signal and the jamming are switched, the receiver cannot detect any differences, i.e., $W(\mathbf{y}|\mathbf{s},\mathbf{j}) = W(\mathbf{y}|\mathbf{j},\mathbf{s})$. In an AVC with a symmetrizable kernel, jamming is generated or can be viewed as: the jammer excites the main channel via an auxiliary channel $\pi : \mathcal{S} \to \mathcal{J}$, where π is essentially a probability matrix. More specifically, the input of the auxiliary channel comes from exactly the same signal space as that of the authorized signal, and it is transformed by the auxiliary channel and then imposed to the main channel. An AVC kernel is said to be symmetrizable, if there exist an auxiliary channel π, such that even if we switch the authorized signal and the input signal of the auxiliary channel, the receiver cannot tell any differences, i.e., $\hat{W}(\mathbf{y}|\mathbf{s},\mathbf{s}') = \hat{W}(\mathbf{y}|\mathbf{s}',\mathbf{s})$ with $\hat{W}(\mathbf{y}|\mathbf{s},\mathbf{s}') \triangleq \sum_{\mathbf{j}\in\mathcal{J}'} \pi(\mathbf{j}|\mathbf{s}')W(\mathbf{y}|\mathbf{s},\mathbf{j})$. In both cases, the receiver will be confused by the disguised jamming (either generated directly or via an auxiliary channel), which is indistinguishable from the authorized signal. An interesting observation is that: for an AVC kernel, being symmetric is actually a special case of being symmetrizable, where the output of the auxiliary channel equals its input.

***Remark* 1.** *In Definition 2, $\mathcal{J}'$ can be any finite subset of $\mathcal{J}$. Note that the probability matrix $\pi : \mathcal{S} \to \mathcal{J}'$ can be viewed as a special case of $\pi : \mathcal{S} \to \mathcal{J}$ with zero entries corresponding to the elements that are in $\mathcal{J}$ but not in $\mathcal{J}'$, i.e., $\pi(\boldsymbol{j}|\boldsymbol{s}') = 0$, $\forall \boldsymbol{s}' \in \mathcal{J}\backslash\mathcal{J}'$. Hence, in addressing the existence of the probability matrix, we will hereinafter focus on the case associating to the full set, namely, $\pi : \mathcal{S} \to \mathcal{J}$.*

Concerning the capacity of the AVC channel, it was shown in [18] that: *the deterministic code capacity*[1] *of an AVC for the average probability of error is positive if and only if the AVC is neither symmetric nor symmetrizable.*

Next we will analyze the CDMA systems with and without secure scrambling under disguised jamming, by applying the AVC model.

B. Capacity of CDMA Systems without Secure Scrambling under Disguised Jamming

Without secure scrambling, the codes employed by the authorized user can be regenerated by the jammer, and disguised jamming can thus be generated by applying the same codes but with a fake symbol. If we denote the fake symbol by $v \in \Omega$, in an isolated symbol period, the chip-rate disguised jamming can be represented as

$$\mathbf{j} = v\mathbf{c} = [vc_0, vc_1, ..., vc_{N-1}], \tag{16}$$

where $\mathbf{c} = [c_0, c_1, ..., c_{N-1}]$ is the spreading code, and $v \in \Omega$ the fake symbol. The authorized signal can similarly be written as

$$\mathbf{s} = u\mathbf{c} = [uc_0, uc_1, ..., uc_{N-1}], \tag{17}$$

where $u \in \Omega$ is the authorized symbol. Taking both the noise and jamming into account, the received chip-rate signal can be written as

$$\mathbf{r} = \mathbf{s} + \mathbf{j} + \mathbf{n}, \tag{18}$$

[1]A deterministic code capacity is defined by the capacity that can be achieved by a communication system, when it applies only one code pattern during the information transmission. In other words, the coding scheme is deterministic and can be readily repeated by other users [18].

in which $\mathbf{n} = [n_0, n_1, ..., n_{N-1}]$ and $\mathbf{r} = [r_0, r_1, ..., r_{N-1}]$ denote the AWGN noise vector and received signal vector, respectively.

Define the authorized signal space as $\mathcal{S} = \{u\mathbf{c}|u \in \Omega\}$, where $\mathbf{c} = [c_0, c_1, ..., c_{N-1}]$ is the spreading code. It follows immediately that the disguised jamming space

$$\mathcal{J} = \{v\mathbf{c}|v \in \Omega\} = \mathcal{S}. \tag{19}$$

Let $\hat{u} \in \Omega$ be the estimated version of the authorized symbol "u" at the receiver, and $W_0(\hat{u}|\mathbf{s}, \mathbf{j})$ the conditional probability that $\hat{u}$ is estimated given that the authorized signal is $\mathbf{s} \in \mathcal{S}$, and the disguised jamming is $\mathbf{j} \in \mathcal{S}$. Thus, the CDMA system under disguised jamming can be modeled as an AVC channel characterized by the probability matrix

$$W_0 : \mathcal{S} \times \mathcal{S} \to \Omega, \tag{20}$$

where W_0 is the kernel of the AVC.

As indicated in (19), the jamming and the authorized signal are fully symmetric as they are generated from exactly the same space $\mathcal{S}$. Note that the recovery of the authorized symbol is completely based on $\mathbf{r}$ in (18), so we further have

$$W_0(\hat{u}|\mathbf{s}, \mathbf{j}) = W_0(\hat{u}|\mathbf{j}, \mathbf{s}). \tag{21}$$

Combining (19) and (21), and following Definition 1, we have the proposition below.

***Proposition* 1.** *Under disguised jamming, the kernel of the AVC corresponding to a CDMA system without secure scrambling, W_0, is symmetric.*

The symmetricity of the AVC kernel explains why the error probability of the symbol transmission in CDMA systems without secure scrambling is lower bounded under disguised jamming, as indicated in (15). Applying the result in [18] that the deterministic code capacity of an AVC with a symmetric or symmetrizable kernel is zero, the proposition below follows immediately.

***Proposition* 2.** *Under disguised jamming, the deterministic code capacity of a CDMA system without secure scrambling is zero.*

C. Symmetricity Analysis of CDMA Systems with Secure Scrambling under Disguised Jamming

From the discussions above, it can be seen that disguised jamming is destructive to CDMA systems without secure scrambling, as zero capacity implies a complete failure in information transmission. In what follows, we will show how secure scrambling breaks the symmetricity between the authorized signal and jamming interference, and evaluate the resulted performance gain in terms of error probability and capacity.

When the code information of the authorized user is securely hidden from the jammer by the proposed secure scrambling scheme, the best strategy for the jammer would be distributing its total available power uniformly over the entire spectrum, since CDMA systems are well known to be resistant to narrowband jamming. To this end, the jammer can spread its power by using a randomly generated spreading sequence. More specifically, if we define $\mathcal{D} = \{[d_0, d_1, ..., d_{N-1}]|d_n = \pm 1, \ \forall n\}$, and denote the randomly generated spreading sequence by $\mathbf{d} \in \mathcal{D}$, the chip-rate jamming sequence can be represented as

$$\mathbf{j} = v\mathbf{d} = [vd_0, vd_1, ..., vd_{N-1}], \tag{22}$$

where $v \in \Omega$ is the fake symbol. The jamming space now becomes

$$\mathcal{J} = \{v\mathbf{d}|v \in \Omega, \mathbf{d} \in \mathcal{D}\}. \tag{23}$$

We can see that without the code information $\mathbf{c}$, the jamming, $\mathbf{j}$, can only be generated from a space much larger than the authorized signal space. More specifically, $\mathcal{J} \supset \mathcal{S}$. For any $\mathbf{j} \in \mathcal{J}$, the probability that $\mathbf{j} \in \mathcal{S}$ (i.e., the jamming falls into the authorized signal space by coincidentally repeating the authorized code $\mathbf{c}$ or its negative) is $\frac{1}{2^{N-1}}$, which approaches zero when N is reasonably large.

With the jamming space $\mathcal{J}$ as defined in (23), the AVC corresponding to the CDMA system with secure scrambling can be characterized by

$$W : \mathcal{S} \times \mathcal{J} \to \Omega. \tag{24}$$

Based on the discussion above, $\mathcal{J} \neq \mathcal{S}$. That is, the jamming and the authorized signal are no longer symmetric. Following Definition 1, we have the proposition below.

***Proposition* 3.** *Under disguised jamming, the kernel of the AVC corresponding to a CDMA system with secure scrambling, W, is nonsymmetric.*

Next, we will prove a stronger result: *W is actually nonsymmetrizable*. According to Definition 2, we need to show that for any probability matrix $\pi : \mathcal{S} \to \mathcal{J}$, there exists some $\mathbf{s}_0, \mathbf{s}_0' \in \mathcal{S}$ and $\hat{u}_0 \in \Omega$, such that

$$\hat{W}(\hat{u}_0|\mathbf{s}_0, \mathbf{s}_0') \neq \hat{W}(\hat{u}_0|\mathbf{s}_0', \mathbf{s}_0), \tag{25}$$

where $\hat{W}(\hat{u}|\mathbf{s}, \mathbf{s}') \triangleq \sum_{\mathbf{j} \in \mathcal{J}} \pi(\mathbf{j}|\mathbf{s}')W(\hat{u}|\mathbf{s}, \mathbf{j})$. To prove it, we present three lemmas first.

***Lemma* 1.** *In a complex plane, there are two pairs of symmetric points, (u_1, u_2) and (v_1, v_2), which share the same axis of symmetry. Suppose u_1 and v_1 are located on one side of the axis of symmetry, while u_2 and v_2 reside on the other side. For any point p, if $|p-u_1| \leq |p-u_2|$, then $|p-v_1| \leq |p-v_2|$, where the equality holds if and only if $|p-u_1| = |p-u_2|$.*

Proof: From $|p-u_1| \leq |p-u_2|$, we know that p is either on the same side with u_1 or exactly on the axis of symmetry. If p is on the same side with u_1, i.e., $|p-u_1| < |p-u_2|$, since u_1 and v_1 are on the same side, hence p and v_1 are on the same side. Since v_2 is on the other side, it follows immediately that $|p-v_1| < |p-v_2|$. If p is exactly on the axis of symmetry, i.e., $|p-u_1| = |p-u_2|$, then $|p-v_1| = |p-v_2|$. Similarly, if $|p-v_1| = |p-v_2|$, then $|p-u_1| = |p-u_2|$. ■

Define $R(u)$ as the region of detection for symbol $u \in \Omega$ in the complex plane, which means that any received symbol located in this region will be decided as "u" by a minimum distance detector. That is, for any point $p \in R(u)$, any symbol $v \in \Omega$ and $v \neq u$, we always have $|p-u| < |p-v|$.

Furthermore, for a pair of symmetric symbols from a symmetric constellation[2], $(u, -u)$, their regions of detection, $R(u)$ and $R(-u)$, are said to be *axial symmetric*, if for any point $p \in R(u)$, there always exists a point $M(p) \in R(-u)$, such that $(p, M(p))$ and $(u, -u)$ share the same axis of symmetry. Such a point, $M(p)$, is called the *symmetric point* of p with respect to the axis of symmetry for $(u, -u)$. The shaded areas of Fig. 3 illustrate the regions of detection for two symmetric symbols, which are axial symmetric with respect to the axis of symmetry given in the figure.

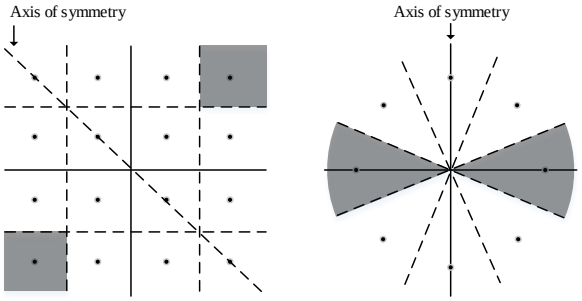


Fig. 3. Illustration of symmetric symbols with axial symmetric regions of detection.

***Lemma* 2.** *Assume the received symbol is $r = u+z+n$, where $u \in \Omega$ is the transmitted symbol, z a fixed complex deviation with $|z| \leq |u|$, and $n \sim \mathcal{CN}\left(0, \sigma^2\right)$ the complex Gaussian noise. If the regions of detection, $R(u)$ and $R(-u)$, are axial symmetric, then we have $W(u|u, z) \geq W(-u|u, z)$, where the equality holds if and only if $z = -u$.*

Proof: For the received symbol $r = u + z + n$, where "u" is the transmitted symbol, "z" is the fixed deviation and $n \sim \mathcal{CN}\left(0, \sigma^2\right)$, r follows a complex Gaussian distribution, $r \sim \mathcal{CN}\left(u + z, \sigma^2\right)$. Hence, the conditional probability that the received symbol will be decided as "u" given that the actually transmitted symbol is "u" and the fixed deviation is "z" can be calculated as

$$W(u|u, z) = \int_{r \in R(u)} f_R(r) dr, \tag{26}$$

where $f_R(r) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left\{-\frac{|r-(u+z)|^2}{2\sigma^2}\right\}$ is the probability density function of r. Similarly, the probability that the received symbol will be decided as "$-u$" given that the actually transmitted symbol is "u" and the fixed deviation is "z" can be calculated as

$$W(-u|u, z) = \int_{r \in R(-u)} f_R(r) dr = \int_{r \in R(u)} f_R(M(r)) dr. \tag{27}$$

Note that the two regions of detection, $R(u)$ and $R(-u)$, are axial symmetric, and $M(r)$ is the symmetric point of r with respect to the axis of symmetry for $(u, -u)$.

[2]A constellation Ω is said to be symmetric, if for any $u \in \Omega$, we always have $-u \in \Omega$. For maximum power efficiency, traditional constellations in use are generally symmetric, e.g., PSK and QAM.

Let $p = u + z$, $u_1 = u$ and $u_2 = -u$. Since $|z| \leq |u|$,

$$|p - u_1| - |p - u_2| = |z| - |2u + z| \leq 0, \tag{28}$$

where the equality holds if and only if $z = -u$. For any $r \in R(u)$, r must be on the same side with $u_1 = u$ relative to the axis of symmetry for $(u, -u)$, and $M(r)$ must be on the same side with $u_2 = -u$, as illustrated in Fig. 3. Applying Lemma 1, for any $r \in R(u)$, it follows from (28) that

$$|p-r|-|p-M(r)| = |r-(u+z)|-|M(r)-(u+z)| \leq 0, \tag{29}$$

where the equality holds if and only if $z = -u$. Thus, we have

$$\begin{aligned} & W(u|u, z) - W(-u|u, z) \\ &= \int_{r \in R(u)} [f_R(r) - f_R(M(r))] dr \\ &= \int_{r \in R(u)} \frac{1}{\sqrt{2\pi}\sigma} \left[\exp\left\{-\frac{|r-(u+z)|^2}{2\sigma^2}\right\}\right. \\ &\qquad \left. - \exp\left\{-\frac{|M(r)-(u+z)|^2}{2\sigma^2}\right\}\right] dr. \end{aligned} \tag{30}$$

Applying (29) to (30), we have

$$W(u|u, z) - W(-u|u, z) \geq 0, \tag{31}$$

where the equality holds if and only if $z = -u$. ■

***Lemma* 3.** *Assume the received signal is $\boldsymbol{r} = \boldsymbol{s} + \boldsymbol{j} + \boldsymbol{n}$, where $\boldsymbol{s} = u\boldsymbol{c}$ is the signal vector with $u \in \Omega$ as the transmitted symbol and $\boldsymbol{c}$ as the spreading code, $\boldsymbol{j} \in \mathcal{J} = \{v\boldsymbol{d} | v \in \Omega, \boldsymbol{d} \in \mathcal{D}\}$ is the jamming vector, and $\boldsymbol{n}$ is the noise vector. If the regions of detection, $R(u)$ and $R(-u)$, are axial symmetric, and $|u| \geq |v|$, $\forall v \in \Omega$, then we have $W(u|\boldsymbol{s},\boldsymbol{j}) \geq W(-u|\boldsymbol{s},\boldsymbol{j})$, where the equality holds if and only if $\boldsymbol{j} = -\boldsymbol{s}$.*

Proof: With $\mathbf{r} = \mathbf{s} + \mathbf{j} + \mathbf{n}$, the despread signal at the receiver would be

$$r = \frac{1}{N} \sum_{n=0}^{N-1} r_n c_n = u + \frac{v}{N} \sum_{n=0}^{N-1} c_n d_n + \frac{1}{N} \sum_{n=0}^{N-1} c_n n_n. \tag{32}$$

Let $z = \frac{v}{N} \sum_{n=0}^{N-1} c_n d_n$ and $n = \frac{1}{N} \sum_{n=0}^{N-1} c_n n_n$. Note that for all n, $c_n = \pm 1$, so the despread noise n would follow a complex Gaussian distribution, i.e., $n \sim \mathcal{CN}(0, \frac{\sigma_n^2}{N})$, where σ_n^2 is the original noise power before despreading. Hence, the recovered symbol, $r = u + z + n$, is actually the transmitted symbol "u" distorted by a fixed deviation z and a complex Gaussian noise n.

Since $|v| \leq |u|$, and for all n, $c_n = \pm 1$, $d_n = \pm 1$, we know that $|z| = |\frac{v}{N} \sum_{n=0}^{N-1} c_n d_n| \leq |u|$. Applying Lemma 2, we have $W(u|u, z) \geq W(-u|u, z)$, where the equality holds if and only if $z = \frac{v}{N} \sum_{n=0}^{N-1} c_n d_n = -u$. We then prove that $z = -u$ is equivalent to $\mathbf{j} = -\mathbf{s}$. On one hand, if $z = -u$, then $|z| = |u|$. Considering $|v| \leq |u|$ and $|\frac{1}{N} \sum_{n=0}^{N-1} c_n d_n| \leq 1$, we must have $|v| = |u|$ and $|\frac{1}{N} \sum_{n=0}^{N-1} c_n d_n| = 1$. There are only two cases that satisfy $z = -u$: (i) $v = -u$ and $d_n = c_n$, $\forall n$; (ii) $v = u$ and $d_n = -c_n$, $\forall n$. Both cases lead to $\mathbf{j} = v\mathbf{d} = -u\mathbf{c} = -\mathbf{s}$. On the other hand, if $\mathbf{j} = -\mathbf{s}$, then it leads to the same two cases as above, both of which satisfy $z = -u$.

Due to the equivalence between the signals before and after despreading as shown in (32), we have $W(u|u, z) = W(u|\mathbf{s}, \mathbf{j})$

and $W(-u|u,z) = W(-u|\mathbf{s},\mathbf{j})$. It then follows immediately that $W(u|\mathbf{s},\mathbf{j}) \geq W(-u|\mathbf{s},\mathbf{j})$, where the equality holds if and only if $\mathbf{j} = -\mathbf{s}$. ■

***Proposition* 4.** *Under disguised jamming, the kernel of the AVC corresponding to a CDMA system with secure scrambling, W, is nonsymmetrizable.*

Proof: We will show that for any probability matrix $\pi : \mathcal{S} \to \mathcal{J}$, there exists some $\mathbf{s}_0, \mathbf{s}_0' \in \mathcal{S}$ and $\hat{u}_0 \in \Omega$, such that

$$\hat{W}(\hat{u}_0|\mathbf{s}_0,\mathbf{s}_0') \neq \hat{W}(\hat{u}_0|\mathbf{s}_0',\mathbf{s}_0), \tag{33}$$

where $\hat{W}(\hat{u}|\mathbf{s},\mathbf{s}') \triangleq \sum_{\mathbf{j}\in\mathcal{J}} \pi(\mathbf{j}|\mathbf{s}')W(\hat{u}|\mathbf{s},\mathbf{j})$. To this end, we pick $\mathbf{s}_0 = u\mathbf{c}$, $\mathbf{s}_0' = -u\mathbf{c}$, $\hat{u}_1 = u$ and $\hat{u}_2 = -u$. Note that "u" is picked such that $R(u)$ and $R(-u)$ are axial symmetric, and $|u| \geq |v|$, $\forall v \in \Omega$, as illustrated in Fig. 3. We will prove that $\hat{W}(\hat{u}_1|\mathbf{s}_0,\mathbf{s}_0') = \hat{W}(\hat{u}_1|\mathbf{s}_0',\mathbf{s}_0)$ and $\hat{W}(\hat{u}_2|\mathbf{s}_0,\mathbf{s}_0') = \hat{W}(\hat{u}_2|\mathbf{s}_0',\mathbf{s}_0)$ cannot hold simultaneously, by showing that

$$\hat{W}(\hat{u}_1|\mathbf{s}_0,\mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0,\mathbf{s}_0') > \hat{W}(\hat{u}_1|\mathbf{s}_0',\mathbf{s}_0) - \hat{W}(\hat{u}_2|\mathbf{s}_0',\mathbf{s}_0). \tag{34}$$

Following the definition of $\hat{W}$, we have

$$\begin{aligned} &\hat{W}(\hat{u}_1|\mathbf{s}_0,\mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0,\mathbf{s}_0') \\ =&\sum_{\mathbf{j}\in\mathcal{J}} \pi(\mathbf{j}|\mathbf{s}_0')W(\hat{u}_1|\mathbf{s}_0,\mathbf{j}) - \sum_{\mathbf{j}\in\mathcal{J}} \pi(\mathbf{j}|\mathbf{s}_0')W(\hat{u}_2|\mathbf{s}_0,\mathbf{j}) \\ =&\sum_{\mathbf{j}\in\mathcal{J}} \pi(\mathbf{j}|\mathbf{s}_0')[W(\hat{u}_1|\mathbf{s}_0,\mathbf{j}) - W(\hat{u}_2|\mathbf{s}_0,\mathbf{j})]. \end{aligned} \tag{35}$$

Note that $W(\hat{u}_1|\mathbf{s}_0,\mathbf{j})$ and $W(\hat{u}_2|\mathbf{s}_0,\mathbf{j})$ denote the probabilities that the received symbol is decided as $\hat{u}_1 = u$ and $\hat{u}_2 = -u$, respectively, given that the transmitted signal is $\mathbf{s}_0$ and the jamming is $\mathbf{j}$. Applying Lemma 3, we have

$$W(\hat{u}_1|\mathbf{s}_0,\mathbf{j}) \geq W(\hat{u}_2|\mathbf{s}_0,\mathbf{j}), \tag{36}$$

where the equality holds if and only if $\mathbf{j} = -\mathbf{s}_0$. Substituting (36) into (35), it follows immediately that

$$\hat{W}(\hat{u}_1|\mathbf{s}_0,\mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0,\mathbf{s}_0') \geq 0, \tag{37}$$

where the equality holds if and only if $\pi(\mathbf{j}|\mathbf{s}_0') = 0$, $\forall \mathbf{j} \neq -\mathbf{s}_0$. This means that $\hat{W}(\hat{u}_1|\mathbf{s}_0,\mathbf{s}_0') = \hat{W}(\hat{u}_2|\mathbf{s}_0,\mathbf{s}_0')$ occurs only when the jammer can *always* generate the jamming exactly as the opposite to the authorized signal, which is impossible since the jammer has no knowledge how the spreading sequence $\mathbf{c}$ is encrypted and changes at each symbol period. Based on the observation above, we further have

$$\hat{W}(\hat{u}_1|\mathbf{s}_0,\mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0,\mathbf{s}_0') > 0. \tag{38}$$

Applying the same methodology, we can show that

$$\hat{W}(\hat{u}_1|\mathbf{s}_0',\mathbf{s}_0) - \hat{W}(\hat{u}_2|\mathbf{s}_0',\mathbf{s}_0) < 0. \tag{39}$$

Combining (38) and (39), we have

$$\hat{W}(\hat{u}_1|\mathbf{s}_0,\mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0,\mathbf{s}_0') > \hat{W}(\hat{u}_1|\mathbf{s}_0',\mathbf{s}_0) - \hat{W}(\hat{u}_2|\mathbf{s}_0',\mathbf{s}_0), \tag{40}$$

which shows that $\hat{W}(\hat{u}_1|\mathbf{s}_0,\mathbf{s}_0') = \hat{W}(\hat{u}_1|\mathbf{s}_0',\mathbf{s}_0)$ and $\hat{W}(\hat{u}_2|\mathbf{s}_0,\mathbf{s}_0') = \hat{W}(\hat{u}_2|\mathbf{s}_0',\mathbf{s}_0)$ cannot hold simultaneously. ■

Since the kernel corresponding to a CDMA system with secure scrambling under disguised jamming, W, is neither symmetric (Proposition 3) nor symmetrizable (Proposition 4), we have the proposition below.

***Proposition* 5.** *Under disguised jamming, the deterministic code capacity of a CDMA system with secure scrambling is not zero.*

Discussions: Proposition 4 shows that the kernel of the AVC corresponding to a CDMA system with secure scrambling is nonsymmetrizable, except when the jammer can always generate the jamming as exactly as the opposite to the authorized signal. However, this is computationally impossible, since it is equivalent to break AES applied in secure scrambling, which has been proved to be secure under all known attacks.

An aggressive jammer can probably launch jamming consisting of multiple spreading codes, in order to increase the probability that one of its applied codes coincides with the one applied by the authorized user. When the number of spreading codes covered by the jammer is small, the harm to the authorized communication would be negligible. While using multiple spreading codes produces more effective jamming, the power consumption can be forbiddingly high. However, it does indicate that: when the user information (including both symbol and codes) is unknown, the most effective jamming is still Gaussian [28], resulting from accumulation of a large number of spreading codes and the central limit theorem (CLT).

D. Capacity Estimation of CDMA Systems with Secure Scrambling under Disguised Jamming

So far we have shown that: in CDMA systems with secure scrambling, the symmetricity between the authorized signal and the disguised jamming is broken, and hence the capacity is no longer zero. A natural question is: what is the capacity then? Although it is difficult to derive a modulation-specific capacity, we manage to provide a general analysis on the capacity by applying the Shannon Formula as stated below. For particular modulation schemes like QAM and PSK, the error probabilities of symbol transmission will also be provided.

Recall that at the receiver, the despread symbol under disguised jamming can be calculated as

$$r = \frac{1}{N}\sum_{n=0}^{N-1} r_n c_n = u + \frac{v}{N}\sum_{n=0}^{N-1} c_n d_n + \frac{1}{N}\sum_{n=0}^{N-1} c_n n_n. \tag{41}$$

Note that for all n, $c_n = \pm 1$ are constant, while $d_n = \pm 1$ are statistically independent and identically distributed (i.i.d.) binary random variables with zero mean and variance 1. Applying the central limit theorem (CLT), $\frac{1}{N}\sum_{n=0}^{N-1} c_n d_n$ would follow a complex Gaussian distribution with zero mean and variance $\frac{1}{N}$, i.e.,

$$\frac{1}{N}\sum_{n=0}^{N-1} c_n d_n \sim \mathcal{CN}\left(0, \frac{1}{N}\right). \tag{42}$$

Similarly, we have

$$\frac{1}{N}\sum_{n=0}^{N-1} c_n n_n \sim \mathcal{CN}\left(0, \frac{\sigma_n^2}{N}\right), \tag{43}$$

where σ_n^2 is the original noise power before despreading. It then follows that r is also a complex Gaussian variable, whose distribution can be characterized by

$$r \sim \mathcal{CN}\left(u, \frac{|v|^2}{N} + \frac{\sigma_n^2}{N}\right), \tag{44}$$

which implies that for an arbitrary transmitted symbol $u \in \Omega$ and an arbitrary fake symbol $v \in \Omega$ in (41), the received symbol is actually the transmitted symbol "u" contaminated by a complex Gaussian noise, $n \sim \mathcal{CN}\left(0, \frac{|v|^2}{N} + \frac{\sigma_n^2}{N}\right)$.

Let σ_s^2 denote the average symbol power, namely, $\mathcal{E}\{|u|^2\} = \sigma_s^2$, where $u \in \Omega$. Based on (44), for a specific fake symbol $v \in \Omega$, the corresponding signal-to-jamming-and-noise ratio (SJNR) can be calculated as

$$\gamma(v) = \frac{\sigma_s^2}{|v|^2/N + \sigma_n^2/N} = \frac{N\sigma_s^2}{|v|^2 + \sigma_n^2}. \tag{45}$$

The symbol error probability largely depends on the employed constellation Ω. However, with SJNR available, and considering all possible $v \in \Omega$, the average symbol error probability can be calculated as

$$\mathcal{P}_s = \frac{1}{|\Omega|}\sum_{v\in\Omega}\mathcal{P}_\Omega(\gamma(v)) = \frac{1}{|\Omega|}\sum_{v\in\Omega}\mathcal{P}_\Omega\left(\frac{N\sigma_s^2}{|v|^2+\sigma_n^2}\right), \tag{46}$$

where $|\Omega|$ denotes the constellation size, and $\mathcal{P}_\Omega(\cdot)$ is readily available in [29, eqn. (5.2-78) & (5.2-79), page 278] for QAM and [29, eqn. (5.2-56), page 268] for PSK, respectively.

To estimate the capacity, a CDMA system which operates over a spectrum of B Hz can be equivalently viewed as a narrowband transmission with a bandwidth of $\frac{B}{N}$, while simultaneously having its SJNR level increased to (45) as a result of the processing gain. Hence, the capacity can be estimated as

$$\begin{aligned} C &= \frac{B}{N}\frac{1}{|\Omega|}\sum_{v\in\Omega}\log_2(1+\gamma(v)) \\ &= \frac{B}{N}\frac{1}{|\Omega|}\sum_{v\in\Omega}\log_2\left(1+\frac{N\sigma_s^2}{|v|^2+\sigma_n^2}\right). \end{aligned} \tag{47}$$

For clarity, we summarize the analysis above in Table I. It can be seen that: (i) Compared with the lower-bounded error probability for CDMA without secure scrambling, the symbol error probability of a CDMA system under disguised jamming can be decreased significantly using the secure scrambling scheme, especially when the processing gain, N, is large; (ii) With secure scrambling, the capacity of a CDMA system will no longer be zero.

Overall, we would like to point out that: based on the shared secret between the authorized transmitter and receiver, secure scrambling enhances the randomness in the CDMA spreading process and makes it forbiddingly difficult for the malicious user to launch disguised jamming. Our results echo the observations in [13], [17]–[20], where random coding is viewed as a promising solution in combating disguised jamming.

TABLE I
COMPARISON OF CDMA SYSTEMS WITH AND WITHOUT SECURE SCRAMBLING (S.S.) UNDER DISGUISED JAMMING.

	Without S.S.	With S.S.
Symmetric	Yes	No
Symmetrizable	N/A	No
SJNR	N/A	$\frac{N\sigma_s^2}{\lvert v\rvert^2+\sigma_n^2},\ v\in\Omega$
Error Probability	$\geq \frac{M-1}{2M}$	$\frac{1}{\lvert\Omega\rvert}\sum_{v\in\Omega}\mathcal{P}_\Omega\left(\frac{N\sigma_s^2}{\lvert v\rvert^2+\sigma_n^2}\right)$
Capacity	0	$\frac{B}{N}\frac{1}{\lvert\Omega\rvert}\sum_{v\in\Omega}\log_2\left(1+\frac{N\sigma_s^2}{\lvert v\rvert^2+\sigma_n^2}\right)$

V. NUMERICAL RESULTS

In this section, we demonstrate the effectiveness of secure scrambling in combating disguised jamming for CDMA systems. In what follows, we assume AWGN channels. We adopt Walsh codes with a processing gain of $N = 64$ as the spreading codes, and apply 16-QAM modulation.

The symbol error rates (SERs) of CDMA systems are shown in Fig. 4 associating with the following four conditions: (a) jamming-free case as the benchmark; (b) under disguised jamming but without secure scrambling; (c) under disguised jamming and with secure scrambling; (d) the theoretical result for the case in (c) as a verification.

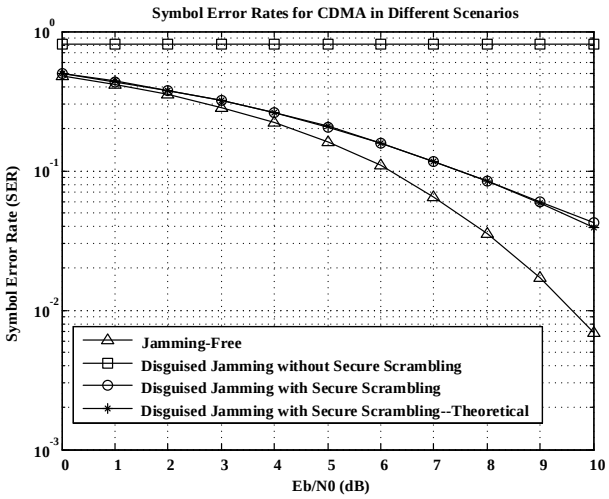


Fig. 4. Symbol error rates (SERs) for CDMA in Different Scenarios.

In Fig. 4, it is observed that: (i) Without secure scrambling, the symbol error rate of CDMA communication under disguised jamming maintains at a very high level no matter how high the SNR is, which shows that the CDMA communication is severely paralyzed by disguised jamming; (ii) The secure scrambling scheme significantly improves the performance of CDMA communication under disguised jamming, where the SER curve matches the theoretical result as indicated in (46) as well; (iii) The SER curve using secure scrambling under disguised jamming is quite close to that of the jamming-free case, and it can be expected that the gap will become even smaller if we have a larger processing gain N.

VI. Conclusions

In this paper, we analyzed the impact of disguised jamming on conventional CDMA systems, and developed an effective approach to combat disguised jamming using secure scrambling. Instead of using conventional scrambling codes, we applied advanced encryption standard (AES) to generate the security-enhanced scrambling codes. Theoretical analysis shows that: the capacity of the conventional CDMA systems without secure scrambling under disguised jamming is actually zero; however, secure scrambling can break the symmetricity between the authorized signal and the jamming interference, and ensures positive channel capacity under disguised jamming. Numerical examples were provided to demonstrate the effectiveness of secure scrambling in combating disguised jamming.

Appendix A
Disguised Jamming Mitigation Exploiting Timing and Amplitude Differences Between the Authorized User and the Jammer

For CDMA systems with public or easily accessed codes, disguised jamming can hardly be prevented. However, the disguised jammer may not be able to capture the exact timing and amplitude information of the authorized signal. In this appendix, we will show that: when the timing and amplitude differences between the authorized signal and the disguised jamming are not too small, it is possible to improve the system performance through robust receiver design. It should also be pointed out that when these differences get too small, enhancing the shared secure randomness between the authorized transmitter and receiver would be the only option.

In the following, we try to estimate the jamming parameters as well as the authorized symbol using the minimum mean square error (MMSE) criterion. Unlike traditional MSE between the received signal and transmitted signal, the MSE here is calculated between the received signal and jammed signal, which is the sum of the authorized signal and the disguised jamming.

Following (6)-(7), the aforementioned MSE can be calculated as

$$\begin{aligned}
&J(u,v,\tau,\gamma)\\
=&\frac{1}{T}\int_0^T |r(t)-s(t)-j(t)|^2dt\\
=&\frac{1}{T}\int_0^T |r(t)-u\,c(t)-v\,\gamma\,c(t-\tau)|^2dt\\
=&\frac{1}{T}\int_0^T |r(t)-u\,c(t)|^2dt-\frac{\gamma v^*}{T}\int_0^T [r(t)-u\,c(t)]c(t-\tau)dt\\
-&\frac{\gamma v}{T}\int_0^T [r(t)-u\,c(t)]^*c(t-\tau)dt+\frac{\gamma^2|v|^2}{T}\int_0^T c^2(t-\tau)dt,
\end{aligned} \tag{48}$$

where $(\cdot)^*$ denotes the complex conjugate. Since $c(t)$ is T-periodic, following (3), we have $\frac{1}{T}\int_0^T c^2(t-\tau)dt = \frac{1}{T}\int_0^T c^2(t)dt = 1$. If we further denote

$$A(u,\tau)=\frac{1}{T}\int_0^T [r(t)-u\,c(t)]c(t-\tau)dt, \tag{49}$$

the MSE can be rewritten as

$$\begin{aligned}
J(u,v,\tau,\gamma)=&\frac{1}{T}\int_0^T |r(t)-u\,c(t)|^2dt\\
&-\gamma v^*A(u,\tau)-\gamma vA^*(u,\tau)+\gamma^2|v|^2.
\end{aligned} \tag{50}$$

Thus, the problem can be formulated as minimizing (50) by finding the optimal u, v, τ and γ, i.e.,

$$\{\hat{u},\hat{v},\hat{\tau},\hat{\gamma}\}=\arg\min_{u,v,\tau,\gamma} J(u,v,\tau,\gamma). \tag{51}$$

To minimize (50), one necessary condition is that its partial derivatives regarding v and γ are zero. Note that when z is a complex variable, we have $\frac{\partial z}{\partial z}=0$, $\frac{\partial z^*}{\partial z}=2$ and $\frac{\partial |z|^2}{\partial z}=2z$. Hence,

$$\begin{cases}
\dfrac{\partial J}{\partial v}=-2\gamma A(u,\tau)+2\gamma^2 v=0, & \text{(52a)}\\
\dfrac{\partial J}{\partial \gamma}=-v^*A(u,\tau)-vA^*(u,\tau)+2\gamma|v|^2=0, & \text{(52b)}
\end{cases}$$

from which we can get

$$\gamma=\frac{A(u,\tau)}{v}=\frac{A^*(u,\tau)}{v^*}. \tag{53}$$

Substituting (53) into (50), the MSE can be reduced to

$$J=\frac{1}{T}\int_0^T |r(t)-u\,c(t)|^2dt-|A(u,\tau)|^2, \tag{54}$$

which is a function depending only on u and τ.

In numerical solution search, limited by the time resolution, τ becomes discrete and thus has only finite possible values with $|\tau|<T_c$. In this way, an exhaustive search[3] on τ and u would be feasible and also an effective approach to minimize (54). Let $\hat{u}$ and $\hat{\tau}$ be the solution pair that minimizes (54), following (53), the amplitude ratio can be estimated as

$$\hat{\gamma}=\frac{|A(\hat{u},\hat{\tau})|}{|v|}. \tag{55}$$

For a constant-modulus constellation (e.g., PSK), $|v|$ is readily available since it holds constant for all $v\in\Omega$. For non-constant-modulus constellation, the amplitude ratio cannot be exactly drawn. This is because that from (53), we can only determine $\hat{v}\hat{\gamma}=A(\hat{u},\hat{\tau})$, which cannot yield a specific $\hat{\gamma}$ when the amplitude of the jamming symbol is not specifically available. However, in this case, we can obtain a range for $\hat{\gamma}$. More specifically, if $B_1\le|v|\le B_2$ for $v\in\Omega$, then we have

$$\frac{|A(\hat{u},\hat{\tau})|}{B_2}\le\hat{\gamma}\le\frac{|A(\hat{u},\hat{\tau})|}{B_1}. \tag{56}$$

Although disguised jamming and multipath variations [30], [31] (i.e., delayed and scaled signals) have similar characteristics, they have the following major differences: (1) Multipath signals always contain the same symbol as the primary signal (which is the signal going through the line-of-sight path), while the symbol carried by disguised jamming is chosen independently from the authorized signal; (2) Multipath signals

[3]Generally it would be sufficient to perform an exhaustive search for regular time resolution with a practical sampling rate; however, for high time resolution, we suggest the usage of state-of-the-art iterative optimization methods, e.g., Newton's method.

are generally much weaker than the primary signal, while disguised jamming maintains a similar power level as the authorized signal; (3) Multipath signals always arrive at the receiver after the primary signal, while disguised jamming can have either a leading or lagging phase compared with the authorized signal.

The effectiveness of the proposed receiver design in improving BER performance is demonstrated using numerical examples. In the simulation, we adopt the settings as in civilian GPS, where BPSK modulation is applied and the spreading code is a Gold sequence with a processing gain $N = 1023$. Note that the civilian GPS has public spreading codes, and it is exactly one of the scenarios where the robust receiver design is needed in order to avoid hiding the codes. The amplitude ratio γ is set to 1, and we compare the performance of a conventional receiver with that of the proposed receiver in Fig. 5.

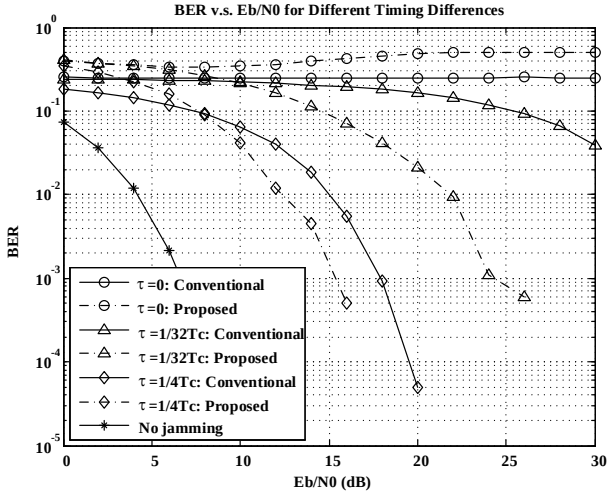


Fig. 5. BER v.s. Eb/N0 for different timing differences.

It is observed that: (i) Comparing with the jamming-free case, the BER performance is severely degraded by the disguised jamming, especially when the timing difference τ is small; (ii) For essentially nonzero timing differences, the BER is decreased significantly by the proposed CDMA receiver with reasonable SNRs; (iii) For the worst disguised jamming with zero timing difference, the proposed receiver design cannot help at all, in which case we should consider using secure scrambling to break the symmetricity.

APPENDIX B
FEASIBILITY ANALYSIS OF AES-BASED SECURE SCRAMBLING

The AES algorithm is one of the block ciphers that can be implemented in different operational modes to generate stream data [32]. High-throughput (3.84 Gbps and higher) AES chips can be found in [33], [34]. In [35], an experiment was performed to measure the AES algorithm performance, where several file sizes from 100 KB to 50 MB were encrypted using a laptop with 2.99 GHz CPU and 2 GB RAM. Based on the results of the experiment, when the AES operates in the cipher feedback (CFB) mode, 554 bytes can be encrypted using 256-bit AES algorithm in 77.3 μs, which is equivalently as high as 57 Mbps. Comparing with the chip rates of regular CDMA systems which are typically below 10 Mbps, the existing hardware would be more than adequate in performing a real-time AES-based secure scrambling sequence generation.

REFERENCES

[1] S. Barbarossa and A. Scaglione, "Adaptive time-varying cancellation of wideband interferences in spread-spectrum communications based on time-frequency distributions," *IEEE Trans. Signal Processing*, vol. 47, no. 4, pp. 957–965, Apr 1999.

[2] S. Aromaa, P. Henttu, and M. Juntti, "Transform-selective interference suppression algorithm for spread-spectrum communications," *IEEE Signal Processing Lett.*, vol. 12, no. 1, pp. 49–51, Jan 2005.

[3] Y. Wu, B. Wang, K. Liu, and T. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE J. Select. Areas Commun.*, vol. 30, no. 1, pp. 4–15, January 2012.

[4] A. Garnaev, Y. Hayel, and E. Altman, "A bayesian jamming game in an OFDM wireless network," in *10th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, May 2012, pp. 41–48.

[5] C. Shahriar, M. La Pan, M. Lichtman, T. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. Reed, "PHY-layer resiliency in OFDM communications: A tutorial," *IEEE Communications Surveys Tutorials*, vol. 17, no. 1, pp. 292–314, Firstquarter 2015.

[6] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Jamming resilient communication using MIMO interference cancellation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1486–1499, July 2016.

[7] A. Garnaev, Y. Liu, and W. Trappe, "Anti-jamming strategy versus a low-power jamming attack when intelligence of adversary's attack type is unknown," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 2, no. 1, pp. 49–56, March 2016.

[8] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum communications–a tutorial," *IEEE Trans. Wireless Commun.*, vol. 30, no. 5, pp. 855–884, May 1982.

[9] R. Nikjah and N. C. Beaulieu, "On antijamming in general cdma systems-part i: multiuser capacity analysis," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1646–1655, May 2008.

[10] C.-L. Wang and K.-M. Wu, "A new narrowband interference suppression scheme for spread-spectrum CDMA communications," *IEEE Trans. Signal Processing*, vol. 49, no. 11, pp. 2832–2838, Nov 2001.

[11] H. Holma and A. Toskala, *WCDMA for UMTS: HSPA Evolution and LTE*. New York, NY, USA: John Wiley & Sons, Inc., 2007.

[12] E. Kaplan, *Understanding GPS - Principles and applications*, 2nd ed. Artech House, December 2005.

[13] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2148–2177, 1998.

[14] M. Medard, "Capacity of correlated jamming channels," in *Allerton Conference on Communications, Computing and Control*, 1997.

[15] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping-part I: System design," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 70 –79, Jan. 2013.

[16] L. Zhang and T. Li, "Anti-jamming message-driven frequency hopping-part II: Capacity analysis under disguised jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 80 –88, Jan. 2013.

[17] T. Ericson, "The noncooperative binary adder channel," *IEEE Trans. Inform. Theory*, vol. 32, no. 3, pp. 365–374, 1986.

[18] ——, "Exponential error bounds for random codes in the arbitrarily varying channel," *IEEE Trans. Inform. Theory*, vol. 31, no. 1, pp. 42–48, 1985.

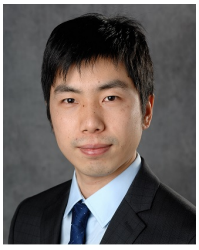
[19] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Z. Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 44, no. 2, pp. 159–175, 1978.

[20] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacities of certain channel classes under random coding," *The Annals of Mathematical Statistics*, vol. 31, no. 3, pp. pp. 558–567, 1960.

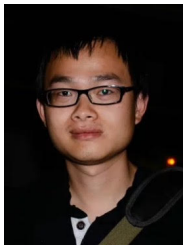
[21] T. Song, Z. Fang, J. Ren, and T. Li, "Precoding for OFDM under disguised jamming," in *2014 IEEE Global Communications Conference*, Dec 2014, pp. 3958–3963.

[22] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. 15, no. 1, pp. 122–127, Jan 1969.

[23] T. Li, Q. Ling, and J. Ren, "Physical layer built-in security analysis and enhancement algorithms for CDMA systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, no. 1, p. 083589, 2007.
[24] W. Burr, "Selecting the advanced encryption standard," *IEEE Security Privacy*, vol. 1, no. 2, pp. 43–52, 2003.
[25] *Advanced Encryption Standard*, ser. FIPS-197, National Institute of Standards and Technology Std., Nov. 2001. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[26] *Data Encryption Standard*, ser. FIPS-46-3, National Institute of Standards and Technology Std., Oct. 1999. [Online]. Available: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
[27] A. J. Viterbi, *CDMA: Principles of Spread Spectrum Communication*. Redwood City, CA, USA: Addison Wesley Longman Publishing Co., Inc., 1995.
[28] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. Inform. Theory*, vol. 29, no. 1, pp. 152–157, Jan 1983.
[29] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2000.
[30] M. Sahmoudi and M. Amin, "Fast iterative maximum-likelihood algorithm (FIMLA) for multipath mitigation in the next generation of GNSS receivers," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4362–4374, November 2008.
[31] Z. Xu and P. Liu, "Code-constrained blind detection of CDMA signals in multipath channels," *IEEE Signal Processing Lett.*, vol. 9, no. 12, pp. 389–392, Dec 2002.
[32] T. Good and M. Benaissa, "AES as stream cipher on a small FPGA," in *Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE International Symposium on*, May 2006, pp. 4 pp.–.
[33] A. Hodjat, D. D. Hwang, B. Lai, K. Tiri, and I. Verbauwhede, "A 3.84 Gbits/s AES crypto coprocessor with modes of operation in a 0.18-μm CMOS technology," in *Proceedings of the 15th ACM Great Lakes Symposium on VLSI*, ser. GLSVLSI '05. New York, NY, USA: ACM, 2005, pp. 60–63. [Online]. Available: http://doi.acm.org/10.1145/1057661.1057677
[34] S.-Y. Lin and C.-T. Huang, "A high-throughput low-power AES cipher for network applications," in *Design Automation Conference, 2007. ASP-DAC '07. Asia and South Pacific*, Jan 2007, pp. 595–600.
[35] N. Singhal and J.P.S.Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 1, no. 3, pp. 259–263, Jul 2011.



Tianlong Song received the B.S. degree in Communication Engineering from Beijing University of Chemical Technology, Beijing, China, in 2009, the M.S. degree in Information and Communication Engineering from Beihang University, Beijing, China, in 2012, and the Ph.D. degree in Electrical and Computer Engineering from Michigan State University, East Lansing, MI, United States, in 2016, respectively. His research interests lie in the areas of efficient and secure communications, brain neuroimaging data mining, and artificial intelligence.



Kai Zhou received the B.S. degree in Electrical Engineering from Shanghai Jiao Tong University, China in 2013. He is currently working towards the Ph.D. degree in Electrical and Computer Engineering in Michigan State University. His research interests include cryptography, security & privacy, cloud computing and secure communication. He is a student member of the IEEE.

Tongtong Li received her Ph.D. degree in Electrical Engineering in 2000 from Auburn University. She is currently an Associate Professor in the Department of Electrical and Computer Engineering at Michigan State University. Her research interests fall into the areas of communication system design and networking, wireless security, and statistical signal processing, with applications in computational neuroscience. Dr. Li is currently serving as an Associate Editor for IEEE Transactions on Signal Processing. She is a recipient of the National Science Foundation (NSF) CAREER Award and a senior member of the IEEE.