Anti-Jamming Message-Driven Frequency Hopping: Part II — Capacity Analysis Under Disguised Jamming

Lei Zhang Tongtong Li

***Abstract*—This is part II of a two-part paper that explores efficient anti-jamming system design based on message-driven frequency hopping (MDFH). In Part I, we point out that under disguised jamming, where the jammer mimics the authorized signal, MDFH experiences considerable performance losses like other wireless systems. To overcome this limitation, we propose an anti-jamming MDFH scheme (AJ-MDFH), which enhances the jamming resistance of MDFH by enabling shared randomness between the transmitter and the receiver using an AES generated ID sequence transmitted along the information stream. In part II, using the arbitrarily varying channel (AVC) model, we analyze the capacity of MDFH and AJ-MDFH under disguised jamming. We show that under the worst case disguised jamming, as long as the secure ID sequence is unavailable to the jammer (which is ensured by AES), the AVC corresponding to AJ-MDFH is nonsymmetrizable. This implies that the deterministic capacity of AJ-MDFH with respect to the average probability of error is positive. On the other hand, due to lack of shared randomness, the AVC corresponding to MDFH is symmetric, resulting in zero deterministic capacity. We further calculate the capacity of AJ-MDFH and show that it converges as the ID constellation size goes to infinity.**

I. Introduction

This is part II of an exploration of jamming mitigation techniques based on message-driven frequency hopping (MDFH) [1], [2], a highly efficient spread spectrum system. The basic idea of MDFH is that part of the information message acts as the PN sequence for carrier frequency selection at the transmitter. Transmission through hopping frequency control adds another dimension to the signal space, and the resulted coding gain can increase the system spectral efficiency significantly. In Part I [2], we pointed out that MDFH is sensitive to disguised jamming, where the jammer mimics the signal of the legal user. Performance losses occur since it is difficult for the MDFH receiver to distinguish the authorized signal from disguised jamming. To overcome this limitation, we proposed the anti-jamming MDFH (AJ-MDFH) scheme. The idea is to insert some secure signal identification (ID) information during the transmission process. The ID information can be regenerated at the receiver based on the pre-shared secret, and then be used for signal detection and extraction.

We further explored ID constellation design and its impact on the performance of AJ-MDFH. It was observed that constant modulus constellation would result in minimum probability of error under noise jamming, as the signal power is always equal to the maximal signal power available. Under the worst case disguised jamming, in which the jamming mimics the ID symbols of the legal user (referred to as ID jamming [2]), we showed that for ideal noise-free systems, increasing the ID constellation size can increase the ID uncertainty, and hence reduce the probability of error. In this case, the ideal constellation size is $M = \infty$. However, when noise is present, we proved that the detection error probability under ID jamming converges as M goes to infinity. This result justifies the use of practical, finite size constellations in AJ-MDFH.

In this paper (Part II), we analyze the capacity of MDFH and AJ-MDFH under disguised jamming. Both MDFH and AJ-MDFH are modeled as arbitrarily varying channels (AVCs) [3]–[8], which is characterized as $W : \mathcal{X} \times \mathcal{J} \to \mathcal{S}$, where $\mathcal{X}$ is the transmitted signal space, $\mathcal{J}$ is the jamming space and $\mathcal{S}$ is the estimated information space. For any $\mathbf{x} \in \mathcal{X}$, $\mathbf{J} \in \mathcal{J}$ and $\mathbf{s} \in \mathcal{S}$, $W(\mathbf{s}|\mathbf{x}, \mathbf{J})$ denotes the conditional probability that $\mathbf{s}$ is detected at the receiver, given that $\mathbf{x}$ is the transmitted signal and $\mathbf{J}$ is the jamming. If $\mathcal{J} = \mathcal{X}$ and $W(\mathbf{s}|\mathbf{x}, \mathbf{J}) = W(\mathbf{s}|\mathbf{J}, \mathbf{x})$ for any $\mathbf{x}, \mathbf{J} \in \mathcal{X}, \mathbf{s} \in \mathcal{S}$, the AVC is said to have a *symmetric kernel* [9]. Define $\hat{W} : \mathcal{X} \times \mathcal{X} \to \mathcal{S}$ by $\hat{W}(\mathbf{s}|\mathbf{x}, \mathbf{J}) \triangleq \sum_{\mathbf{y} \in \mathcal{Y}} \pi(\mathbf{y}|\mathbf{J}) W(\mathbf{s}|\mathbf{x}, \mathbf{y})$, where $\pi : \mathcal{X} \to \mathcal{Y}$ is a probability matrix, and $\mathcal{Y} \subseteq \mathcal{J}$. If there exists a π such that $\hat{W}(\mathbf{s}|\mathbf{x}, \mathbf{J}) = \hat{W}(\mathbf{s}|\mathbf{J}, \mathbf{x}), \quad \forall \mathbf{x}, \mathbf{J} \in \mathcal{X}, \ \forall \mathbf{s} \in \mathcal{S}$, then W is said to be *symmetrizable*. The deterministic code[1] capacity of an AVC for the average probability of error is positive iff the AVC is nonsymmetrizable [6], [7], [9], [10].

The main contributions of this paper (Part II) can be summarized as follows:

- Under the worst case disguised jamming, the AVC corresponding to MDFH has symmetric kernel, which implies that the deterministic code capacity of MDFH under the worst case disguised jamming is zero. This is due to the existence of *symmetricity between the disguised jamming and the authorized signal*, which makes it impossible for the receiver to distinguish the authorized signal from jamming.
- For AJ-MDFH, under the worst case disguised jamming - ID jamming, we prove that: as long as the ID sequence is unavailable to the jammer, the AVC corresponding to AJ-MDFH is *nonsymmetrizable*. Note that the secure ID

Lei Zhang is with Marvell Semiconductor Inc., 5488 Marvell Ln, Santa Clara, CA 95054, USA. (email: lei@marvell.com).

Tongtong Li is with the Department of ECE, Michigan State University, East Lansing, MI 48824, USA. (email:tongli@egr.msu.edu)

[1]A deterministic (n, k) code means that each k-bit data word is mapped to a unique n-bit codeword.

sequence in AJ-MDFH is generated using AES [11], [12], to symmetrize AJ-MDFH is equivalent to break AES, which is computationally infeasible in practical systems as AES has been proven to be secure under all existing attacks. That is, the AVC corresponding to AJ-MDFH is computationally infeasible to be symmetrized. This result ensures that AJ-MDFH has positive capacity under ID jamming.

- We derive the capacity of AJ-MDFH under ID jamming, for which the mutual information is maximized over all possible input probability distributions and minimized with respect to all possible jamming distributions. We show that the capacity converges as the constellation size M goes to infinity. It is observed that: (i) Under reasonable SNR levels ($\geq$ 10dB, for example), the capacity of AJ-MDFH under ID jamming is close to the jamming-free case, and it outperforms the conventional FH system by big margins; (ii) For AJ-MDFH, since the information bits are transmitted through hopping frequency control, it is very robust to additive noise.

This paper is organized as follows. A brief system description for MDFH and AJ-MDFH is provided in Section II. The capacity of MDFH and AJ-MDFH under disguised jamming is analyzed in Section III and Section IV, respectively. We conclude in Section V. The main notations used in the paper is summarized in Table I.

TABLE I
MAIN NOTATIONS IN PART II

Symbol	Definition
s, $\mathbf{x}$, $\mathcal{X}$	Signal symbol, vector, and vector space
b, $\mathbf{J}$, $\mathcal{J}$	Jamming symbol, vector, and vector space
$\boldsymbol{\alpha}$	Indicator vector for the presence of transmitted signal
$\boldsymbol{\beta}$	Indicator vector for the presence of jamming
$W_0 : \mathcal{X} \times \mathcal{J} \to \mathcal{X}$	Probability matrix of the AVC model for MDFH
$W : \mathcal{X} \times \mathcal{J} \to \mathcal{X}$	Probability matrix of the AVC model for AJ-MDFH
$\mathcal{I}_c$	Set of channel indexes: $\{1, \cdots, N_c\}$
$\mathcal{P}(\mathcal{I}_c)$	Set of all probability distributions on $\mathcal{I}_c$
C	Channel capacity

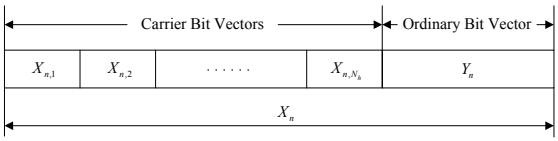
II. A BRIEF REVIEW OF MDFH AND AJ-MDFH

A. MDFH

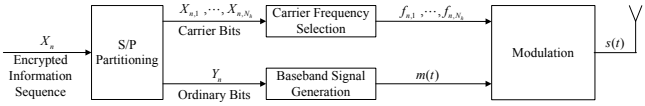
The basic idea of MDFH is that part of the message acts as the PN sequence for carrier frequency selection at the transmitter. More specifically, selection of carrier frequencies is directly determined by the encrypted information stream rather than by a pre-selected pseudo-random sequence as in the conventional FH.

Let N_c be the total number of available channels, with $\{f_1, f_2, \cdots, f_{N_c}\}$ being the set of all available carrier frequencies. The number of bits required to specify an individual channel is $B_c = \lfloor \log_2 N_c \rfloor$, where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x. Without loss of generality, we assume that $N_c = 2^{B_c}$. Let Ω be the selected constellation of size M, and denote $B_s = \log_2 M$ bits. Let T_s and T_h denote the symbol period and the hop duration, respectively, then the number of hops per symbol period is given by $N_h = \frac{T_s}{T_h}$.

The transmitter structure of MDFH is shown in Fig. 1. The *encrypted* information stream is divided into blocks of



(a) Information block structure



(b) Transmitter

Fig. 1. MDFH transmitter.

length $L \triangleq N_h B_c + B_s$. Each block is parsed into $N_h B_c$ *carrier bits* and B_s *ordinary bits*. The carrier bits determine the hopping frequencies, and the ordinary bits are mapped to a symbol in Ω and transmitted through the channels identified by the carrier bits. The structure of the nth block is $X_n = [X_{n,1}, X_{n,2}, \cdots, X_{n,N_h}, Y_n]$. Let $f_{n,l}$ be the carrier frequency corresponding to $X_{n,l}$, $l \in \{1, \cdots, N_h\}$, s_n the symbol corresponding to ordinary bit vector Y_n, and $g(t)$ the pulse shaping filter. For the mth hopping period $[mT_h, (m+1)T_h]$ with $m = nN_h + l$, the transmitted signal can be represented as

$$s(t) = \sqrt{2} Re \left\{ \sum_{i=1}^{N_c} \alpha_{i,m} s_n g(t - mT_h) e^{j2\pi f_i t} \right\}, \quad (1)$$

where $\alpha_{i,m} = 1$ if $f_{X_{n,l}} = f_i$, and $\alpha_{i,m} = 0$ otherwise.

Let $s(t)$, $J(t)$ and $n(t)$ denote the signal, the jamming interference and the noise, respectively. For AWGN channels, the received signal can be represented as

$$r(t) = s(t) + J(t) + n(t). \quad (2)$$

We assume that $s(t), J(t)$ and $n(t)$ are independent of each other. Feeding $r(t)$ into a bank of N_c bandpass filters, each centered at f_i ($i = 1, 2, \cdots, N_c$), the output of the ith ideal bandpass filter $\mathrm{f}_i(t)$ is $r_i(t) = \mathrm{f}_i(t) * r(t)$. For demodulation, $r_i(t)$ is first shifted back to the baseband, and then passed through a matched filter. At the mth hopping period, for $i = 1, \cdots, N_c$, the sampled matched filter output corresponds to channel i can be expressed as

$$r_{i,m} = \alpha_{i,m} s_n + \beta_{i,m} J_{i,m} + n_{i,m}, \quad (3)$$

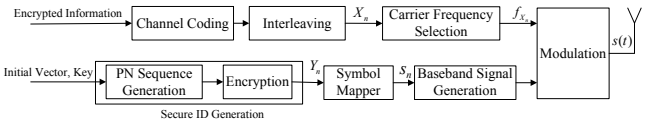
where $s_n, J_{i,m}$ and $n_{i,m}$ correspond to the signal symbol, the jamming interference and the noise, respectively; $\alpha_{i,m}, \beta_{i,m} \in \{0, 1\}$ are binary indicators for the presence of signal and jamming over channel i at the mth hopping period, respectively. Note that the user's information is carried in both $\alpha_{i,m}$ and s_n. For notation simplicity, without loss of generality, we omit the subscript m and n in (3). That is, for a particular hopping period, (3) is reduced to:

$$r_i = \alpha_i s + \beta_i J_i + n_i, \quad i = 1, \cdots, N_c. \quad (4)$$

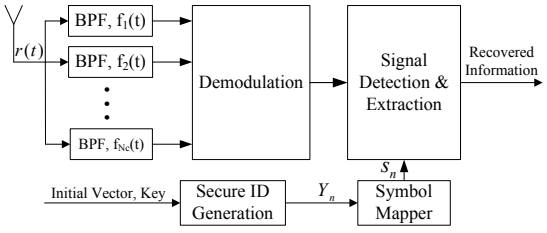
The carrier bits and the ordinary bits can then be estimated from r_i [2].

B. AJ-MDFH

AJ-MDFH was proposed to improve the capacity of MDFH under disguised jamming by adding shared randomness between the transmitter and the receiver. This is achieved by replacing the ordinary bits in MDFH with secure identification (ID) information during the transmission process.



(a) Transmitter structure



(b) Receiver structure

Fig. 2. Transmitter and receiver structure of AJ-MDFH.

The system structure of AJ-MDFH is illustrated in Figure 2. Each user is assigned a secure ID sequence. For each hopping period, AJ-MDFH can also be characterized by (4), except that s is now the ID symbol instead of the signal symbol. *It should be noted that: to prevent impersonate ID attack, the ID symbol is refreshed at each hopping period.* For AJ-MDFH, the user's information is only carried in α_i. Recall that for AJ-MDFH, the ML receiver reduces to a normalized minimum distance receiver [2]. Define $P_i = E\{\|r_i\|^2\}$, and

$$Z_i = \frac{\|r_i - s\|}{\sqrt{P_i}}. \tag{5}$$

Let $\mathcal{I}_c = \{1, \cdots, N_c\}$. Assuming $\alpha_i = \delta(k-i)$ for some $k \in \mathcal{I}_c$, at the receiver, k is then estimated as $\hat{k} = \arg\min_{i \in \mathcal{I}_c} Z_i$.

For more efficient spectrum usage, the system can be extended to multi-carrier AJ-MDFH (MC-AJ-MDFH). The idea is to split all the N_c channels into N_g non-overlapping subgroups, and each carrier hops within the assigned subgroup based on the AJ-MDFH scheme [2].

III. Capacity of MDFH under Disguised Jamming

In this section, we will show that for MDFH, due to the fact that there is no shared secret between the transmitter and the receiver, when the constellation Ω and the pulse shaping filter $g(t)$ are known to the jammer, the capacity of MDFH under the worst case disguised jamming is actually zero.

Following (4), let $\mathbf{r} = (r_1, \ldots, r_{N_c})$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{N_c})$, $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_{N_c})$, $\mathbf{J}' = (J_1, \cdots, J_{N_c})$ and $\mathbf{n} = (n_1, \ldots, n_{N_c})$, the MDFH system under hostile jamming can be modeled as:

$$\mathbf{r} = \boldsymbol{\alpha} s + \boldsymbol{\beta} \cdot \mathbf{J}' + \mathbf{n}. \tag{6}$$

Note that in MDFH, the information is contained in both $\boldsymbol{\alpha}$ and s. Define $\mathbf{x} = \boldsymbol{\alpha} s$, $\mathbf{J} = \boldsymbol{\beta} \cdot \mathbf{J}'$, then we have

$$\mathbf{r} = \mathbf{x} + \mathbf{J} + \mathbf{n}. \tag{7}$$

Let $\mathcal{A} = \{\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{N_c}) | \alpha_i \text{ is 0 or 1, and } \sum_{i=1}^{N_c} \alpha_i = 1\}$. Define $\mathcal{X} = \{\boldsymbol{\alpha} s | \boldsymbol{\alpha} \in \mathcal{A}, s \in \Omega\}$ be the set of all possible information signal $\mathbf{x}$, and $\mathcal{J} = \{\mathbf{J} = (\beta_1 J_1, \cdots, \beta_{N_c} J_{N_c}) | J_i \in \Omega_J, \beta_i = 0 \text{ or } 1, i = 1, \cdots, N_c\}$, where Ω_J is the set of all possible jamming symbols. Let $\hat{\mathbf{x}}$ be the estimated version of $\mathbf{x}$ at the receiver, and $W_0(\hat{\mathbf{x}}|\mathbf{x}, \mathbf{J})$ the conditional probability that $\hat{\mathbf{x}}$ is estimated at the receiver given that the signal is $\mathbf{x}$, and the jamming is $\mathbf{J}$. The jammed MDFH system can be modeled as an arbitrarily varying channel (AVC) characterized by the probability matrix

$$W_0 : \mathcal{X} \times \mathcal{J} \to \mathcal{X}, \tag{8}$$

with

$$W_0(\hat{\mathbf{x}}|\mathbf{x}, \mathbf{J}) \geq 0, \qquad \hat{\mathbf{x}}, \mathbf{x} \in \mathcal{X}, \mathbf{J} \in \mathcal{J}, \tag{9}$$

$$\sum_{\hat{\mathbf{x}} \in \mathcal{X}} W_0(\hat{\mathbf{x}}|\mathbf{x}, \mathbf{J}) = 1, \quad \mathbf{x} \in \mathcal{X}, \mathbf{J} \in \mathcal{J}. \tag{10}$$

W_0 is called the kernel of the AVC.

Under the worst case single band disguised jamming,

$$\mathcal{J} = \{\boldsymbol{\beta} b | \boldsymbol{\beta} \in \mathcal{A}, b \in \Omega\} = \mathcal{X}. \tag{11}$$

That is, the jamming and the information signal are fully symmetric. Note that in MDFH, no shared randomness is exploited for signal detection at the receiver, the recovery of $\mathbf{x}$ is fully based on $\mathbf{r}$, we further have

$$W_0(\hat{\mathbf{x}}|\mathbf{x}, \mathbf{J}) = W_0(\hat{\mathbf{x}}|\mathbf{J}, \mathbf{x}). \tag{12}$$

This implies that the kernel of the AVC corresponding to MDFH, W_0, is symmetric.

In [9], it has been proved that the deterministic capacity (i.e., the largest rate achieved with deterministic codes) of an AVC with symmetric kernel is zero. Therefore, we have the result below.

***Proposition** 1:* The deterministic capacity of MDFH under the worst case single band disguised jamming is zero.

IV. Capacity of AJ-MDFH under Disguised Jamming

In this section, first, we will show that due to the shared randomness introduced by the secure ID sequence, the AVC kernel corresponding to AJ-MDFH is nonsymmetrizable even under the worst case disguised jamming - ID jamming. We will further derive the capacity of AJ-MDFH under ID jamming.

A. AVC Symmetricity Analysis

Recall that for AJ-MDFH,

$$\mathbf{r} = \boldsymbol{\alpha} s + \mathbf{J} + \mathbf{n}. \tag{13}$$

Under the worse case single band disguised jamming, $\mathbf{J} \in \mathcal{X}$, and can be represented as $\mathbf{J} = \boldsymbol{\beta} b$ for some $\boldsymbol{\beta} \in \mathcal{A}$ and $b \in \Omega$. Note that the information is only transmitted through $\boldsymbol{\alpha}$, the AVC corresponding to AJ-MDFH can be characterized by the probability matrix

$$W : \mathcal{X} \times \mathcal{X} \to \mathcal{A}, \tag{14}$$

with

$$W(\hat{\boldsymbol{\alpha}}|\mathbf{x},\mathbf{J}) \geq 0, \mathbf{x}=\boldsymbol{\alpha}s \in \mathcal{X}, \mathbf{J}=\boldsymbol{\beta}b \in \mathcal{X}, \hat{\boldsymbol{\alpha}}, \boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{A},$$
$$\sum_{\hat{\boldsymbol{\alpha}} \in \mathcal{A}} W(\hat{\boldsymbol{\alpha}}|\mathbf{x},\mathbf{J}) = 1, \forall\ (\mathbf{x},\mathbf{J}) \in \mathcal{X}^2. \quad (15)$$

Here $\hat{\boldsymbol{\alpha}}$ is the estimated version of $\boldsymbol{\alpha}$. In this section, we will first prove that: *under reasonable SNR levels, the kernel W defined in (14)-(15) is nonsymmetric*. Then prove a stronger result: *W is actually nonsymmetrizable*.

For AJ-MDFH, W is symmetric if and only if

$$W(\hat{\boldsymbol{\alpha}}|\mathbf{x},\mathbf{J}) = W(\hat{\boldsymbol{\alpha}}|\mathbf{J},\mathbf{x}),\ \forall \mathbf{x},\mathbf{J} \in \mathcal{X},\ \forall \hat{\boldsymbol{\alpha}} \in \mathcal{A}. \quad (16)$$

To prove that W is nonsymmetric, we need to show that there always exists some $\mathbf{x},\mathbf{J}$ and $\hat{\boldsymbol{\alpha}}$, such that the equality above does not hold. Following the discussion on ID constellation design in Part I [2], we assume that Ω is a PSK constellation with power P_s, and define a mapping $v: \mathcal{I}_c \to \mathcal{A}$ as

$$v(k) = \boldsymbol{\alpha} \text{ if } \alpha_i = \delta(k-i), \forall i \in \mathcal{I}_c. \quad (17)$$

Lemma 1: Suppose X, Y are independent continuous random variables. If $Z_1, \cdots, Z_N$ are i.i.d. continuous random variables, which are also independent of X, Y, then

$$\begin{aligned} & Pr\{X < Y \text{ and } X < Z_i, \forall 1 \leq i \leq N\} \\ \geq\ & Pr\{X < Y\} - NPr\{X \geq Z_{i_0}\}, \end{aligned} \quad (18)$$

for any fixed $1 \leq i_0 \leq N$.

Proof: Let $\mathcal{A} = \{X < Y\}$, $\mathcal{B} = \{X < Z_i, \forall 1 \leq i \leq N\}$, and $\bar{\mathcal{B}}$ being the complement of $\mathcal{B}$. Then the inequality (18) follows from the fact that $Pr\{\bar{\mathcal{B}}\} \geq \sum_{i=1}^{N} Pr\{X \geq Z_i\} = NPr\{X \geq Z_{i_0}\}$ for any fixed $1 \leq i_0 \leq N$, and $Pr\{\mathcal{A} \bigcap \mathcal{B}\} = Pr\{\mathcal{A}\} - Pr\{\mathcal{A} \bigcap \bar{\mathcal{B}}\} \geq Pr\{\mathcal{A}\} - Pr\{\bar{\mathcal{B}}\}$. ■

Proposition 2: Assuming Ω is a PSK constellation with power P_s. Let $\mathbf{x} = \boldsymbol{\alpha}s$, $\mathbf{J} = \boldsymbol{\beta}b$, where $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{A}$, $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$, and $s, b \in \Omega$, then

$$W(\boldsymbol{\alpha}|\mathbf{x},\mathbf{J}) \geq 1 - \frac{1}{2} e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} - \epsilon, \quad (19)$$

where $\epsilon = \frac{N_c-2}{\gamma+2} \exp\{-\frac{\gamma(\gamma+1)}{\gamma+2}\}$ with $\gamma = \frac{P_s}{\sigma_n^2}$ denoting the SNR.

Proof: Let $\boldsymbol{\alpha} = v(k)$ and $\boldsymbol{\beta} = v(j)$. When $\boldsymbol{\beta} \neq \boldsymbol{\alpha}$, we have $j \neq k$ and

$$\begin{aligned} & W(\boldsymbol{\alpha}|\mathbf{x},\mathbf{J}) \\ =\ & W(\boldsymbol{\alpha}|\boldsymbol{\alpha}s, \boldsymbol{\beta}b) \\ =\ & Pr\{Z_k < Z_j \text{ and } Z_k < Z_i, \forall i \in \mathcal{I}_c, i \neq j,k|\mathbf{x},\mathbf{J}\}. \end{aligned} \quad (20)$$

From Lemma 1, we have: for any fixed $i_0 \in \mathcal{I}_c, i_0 \neq k, j$,

$$\begin{aligned} W(\boldsymbol{\alpha}|\mathbf{x},\mathbf{J}) \ \geq\ & Pr\{Z_k < Z_j|\mathbf{x},\mathbf{J}\} \\ & -(N_c-2)Pr\{Z_k \geq Z_{i_0}|\mathbf{x},\mathbf{J}\}. \end{aligned} \quad (21)$$

For any $i \in \mathcal{I}_c$, it follows from (4) and (5) that the received signal r_i and the corresponding metric Z_i can be written as

$$r_i = \begin{cases} s+n_k, & i=k, \\ b+n_j, & i=j, \\ n_i, & i \neq j,k, \end{cases} \quad Z_i = \begin{cases} \frac{\|n_k\|}{\sqrt{P_s+\sigma_n^2}}, & i=k, \\ \frac{\|b-s+n_j\|}{\sqrt{P_s+\sigma_n^2}}, & i=j, \\ \frac{\|n_i-s\|}{\sigma_n}, & i \neq j,k. \end{cases} \quad (22)$$

Then, $Pr\{Z_k < Z_j|\mathbf{x},\mathbf{J}\} = Pr\{\|n_k\| < \|b-s+n_j\||\mathbf{x},\mathbf{J}\}$. For any $s, b \in \Omega$, both n_k and $b-s+n_j$ are circularly symmetric complex Gaussian random variables with $n_k \sim \mathcal{CN}(0, \sigma_n^2)$ and $b-s+n_j \sim \mathcal{CN}(b-s, \sigma_n^2)$. Then $Pr\{Z_k < Z_j|\mathbf{x},\mathbf{J}\}$ can be calculated as (see [13], page 49)

$$Pr\{Z_k < Z_j|\mathbf{x},\mathbf{J}\} = 1 - \frac{1}{2} e^{-\frac{\|b-s\|^2}{2\sigma_n^2}}. \quad (23)$$

Similarly, for any fixed $i_0 \in \mathcal{I}_c, i_0 \neq k, j$, we have $\frac{n_k}{\sqrt{P_s+\sigma_n^2}} \sim \mathcal{CN}(0, \frac{\sigma_n^2}{P_s+\sigma_n^2})$, $\frac{n_{i_0}-s}{\sigma_n} \sim \mathcal{CN}(-\frac{s}{\sigma_n}, 1)$ and

$$\begin{aligned} Pr\{Z_k \geq Z_{i_0}|\mathbf{x},\mathbf{J}\} &= Pr\{\frac{\|n_k\|}{\sqrt{P_s+\sigma_n^2}} \geq \frac{\|n_{i_0}-s\|}{\sigma_n}\} \\ &= \frac{1}{\gamma+2} e^{-\frac{\gamma(\gamma+1)}{\gamma+2}}, \end{aligned} \quad (24)$$

where $\gamma = \frac{P_s}{\sigma_n^2}$. It then follows from (21) - (24) that

$$W(\boldsymbol{\alpha}|\mathbf{x},\mathbf{J}) \geq 1 - \frac{1}{2} e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} - \epsilon. \quad (25)$$

■

Note that ϵ is determined by the SNR γ as well as the number of channels N_c. When $SNR \geq 10$dB and $N_c = 512$, for example, $\epsilon \leq 0.004$.

Theorem 1: Assuming Ω is a PSK constellation with power P_s. Let $\mathbf{x} = \boldsymbol{\alpha}s$, $\mathbf{J} = \boldsymbol{\beta}b$, where $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{A}$, $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$, and $s, b \in \Omega$, $s \neq b$. Let $\gamma = \frac{P_s}{\sigma_n^2}$ and $\epsilon = \frac{N_c-2}{\gamma+2} \exp\{-\frac{\gamma(\gamma+1)}{\gamma+2}\}$, then

$$W(\boldsymbol{\alpha}|\mathbf{x},\mathbf{J}) - W(\boldsymbol{\alpha}|\mathbf{J},\mathbf{x}) \geq 1 - e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} - 2\epsilon. \quad (26)$$

Proof: Following Proposition 2, we have

$$W(\boldsymbol{\beta}|\mathbf{J},\mathbf{x}) \geq 1 - \frac{1}{2} e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} - \epsilon. \quad (27)$$

An upper bound for $W(\boldsymbol{\alpha}|\mathbf{J},\mathbf{x})$ can be derived as

$$\begin{aligned} W(\boldsymbol{\alpha}|\mathbf{J},\mathbf{x}) &= 1 - W(\boldsymbol{\beta}|\mathbf{J},\mathbf{x}) - \sum_{\hat{\boldsymbol{\alpha}} \neq \boldsymbol{\alpha}, \boldsymbol{\beta}} W(\hat{\boldsymbol{\alpha}}|\mathbf{J},\mathbf{x}) \\ &\leq 1 - W(\boldsymbol{\beta}|\mathbf{J},\mathbf{x}) \\ &\leq \frac{1}{2} e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} + \epsilon. \end{aligned} \quad (28)$$

It then follows form (19) and (28) that

$$W(\boldsymbol{\alpha}|\mathbf{x},\mathbf{J}) - W(\boldsymbol{\alpha}|\mathbf{J},\mathbf{x}) \geq 1 - e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} - 2\epsilon. \quad (29)$$

■

Proposition 3: Assuming Ω is a PSK constellation with power P_s. Let $\mathbf{x} = \boldsymbol{\alpha}s$, $\mathbf{J} = \boldsymbol{\beta}b$, where $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{A}$, $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$, and $s, b \in \Omega$, $s \neq b$, then

$$W(\boldsymbol{\alpha}|\mathbf{x},\mathbf{J}) > W(\boldsymbol{\alpha}|\mathbf{J},\mathbf{x}), \quad (30)$$

whenever $\frac{\|b-s\|^2}{\sigma_n^2} > 2\ln\frac{1}{1-2\epsilon}$.

This result follows directly from Theorem 1. It implies that as long as s and b are "distinguishable" under the additive noise, the channel symmetricity between the jammer and the legal user is broken, and this increases the probability of correct decision.

Consider $\mathcal{J} = \mathcal{X}$. Define $\hat{W} : \mathcal{X} \times \mathcal{X} \to \mathcal{A}$ by

$$\hat{W}(\hat{\boldsymbol{\alpha}}|\mathbf{x}, \mathbf{J}) \triangleq \sum_{\mathbf{y} \in \mathcal{Y}} \pi(\mathbf{y}|\mathbf{J}) W(\hat{\boldsymbol{\alpha}}|\mathbf{x}, \mathbf{y}), \tag{31}$$

where $\pi : \mathcal{X} \to \mathcal{Y}$ is a probability matrix, and $\mathcal{Y} \subseteq \mathcal{X}$. If there exists a π such that

$$\hat{W}(\hat{\boldsymbol{\alpha}}|\mathbf{x}, \mathbf{J}) = \hat{W}(\hat{\boldsymbol{\alpha}}|\mathbf{J}, \mathbf{x}), \quad \forall \mathbf{x}, \mathbf{J} \in \mathcal{X}, \ \forall \hat{\boldsymbol{\alpha}} \in \mathcal{A}, \tag{32}$$

then W is said to be *symmetrizable*. Next, we will show that under ID jamming, as long as the ID sequence is unavailable to the jammer, the AVC corresponding to AJ-MDFH is not only nonsymmetric, but also *nonsymmetrizable*.

Note that any probability matrix $\pi : \mathcal{X} \to \mathcal{Y}$ with $\mathcal{Y} \subseteq \mathcal{X}$ can be represented with $\pi : \mathcal{X} \to \mathcal{X}$, as long as we set $\pi(\mathbf{y}|\mathbf{x}) = 0$ for any $\mathbf{x} \in \mathcal{X}, \mathbf{y} \in \mathcal{X} \setminus \mathcal{Y}$. In other words, For any $\mathbf{x}, \mathbf{y} \in \mathcal{X}$, we assume $0 \leq \pi(\mathbf{y}|\mathbf{x}) \leq 1$. Here the value 1 corresponds to the case that $\mathcal{Y}$ is a single item subset; the value 0 excludes certain points in $\mathcal{X}$, and results in the case that $\mathcal{Y}$ is a proper subset of $\mathcal{X}$. Without loss of generality, in the following, we only consider $\pi : \mathcal{X} \to \mathcal{X}$ under the assumption that $0 \leq \pi(\mathbf{y}|\mathbf{x}) \leq 1$ for any $\mathbf{x}, \mathbf{y} \in \mathcal{X}$.

***Theorem** 2:* Assuming Ω is an M-PSK constellation with power P_s. Let $\gamma = \frac{P_s}{\sigma_n^2}$, $\epsilon = \frac{N_c - 2}{\gamma + 2} \exp\{-\frac{\gamma(\gamma+1)}{\gamma+2}\}$ and $d_{\min} = \min_{s_1, s_2 \in \Omega, s_1 \neq s_2} \|s_1 - s_2\|$. Let $f(x) = \frac{1}{x+2} \exp\{-\frac{x(x+1)}{x+2}\}$. For $N_c > 2$ and $M > 2$, under the conditions that

$$\begin{aligned} \gamma &> f^{-1}\left(\frac{1}{2N_c}\right) \text{ and,} \\ \frac{d_{\min}^2}{\sigma_n^2} &> \max\left(\frac{2\sqrt{\ln N_c}}{\sqrt{2}\gamma - \sqrt{\ln N_c}}, 2\ln\frac{1}{1-2\epsilon}\right), \end{aligned} \tag{33}$$

the kernel W for the AVC corresponding to AJ-MDFH is **nonsymmetrizable**.

We are going to show that for any probability matrix π, there exists some $\hat{\boldsymbol{\alpha}}_0 \in \mathcal{A}$, and $\mathbf{x}_0, \mathbf{J}_0 \in \mathcal{X}$, such that

$$\hat{W}(\hat{\boldsymbol{\alpha}}_0|\mathbf{x}_0, \mathbf{J}_0) \neq \hat{W}(\hat{\boldsymbol{\alpha}}_0|\mathbf{J}_0, \mathbf{x}_0). \tag{34}$$

To prove this result, we need the two Lemmas below.

***Lemma** 2:* Assuming $N_c > 2$, $M > 2$. For any given $\pi : \mathcal{X} \to \mathcal{X}$, there exists a pair $\mathbf{x}_0 = \boldsymbol{\alpha} s$ and $\mathbf{J}_0 = \boldsymbol{\beta} b$, $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{A}$, $s, b \in \Omega$, such that $\boldsymbol{\beta} \neq \boldsymbol{\alpha}, b \neq s$ and $\pi(-\mathbf{x}_0|\mathbf{J}_0) + \pi(\boldsymbol{\beta} s|\mathbf{J}_0) < 1$.

Proof: Suppose for all $\mathbf{x} = \tilde{\boldsymbol{\alpha}}\tilde{s}$ and $\mathbf{J} = \tilde{\boldsymbol{\beta}}\tilde{b}$ with $\tilde{\boldsymbol{\beta}} \neq \tilde{\boldsymbol{\alpha}}, \tilde{b} \neq \tilde{s}$, the equality $\pi(-\mathbf{x}|\mathbf{J}) + \pi(\tilde{\boldsymbol{\beta}}\tilde{s}|\mathbf{J}) = 1$ holds. For $N_c > 2$ and $M > 2$, consider $\mathbf{x}_0 = \boldsymbol{\alpha} s$, $\mathbf{J}_0 = \boldsymbol{\beta} b$ with $\boldsymbol{\beta} \neq \boldsymbol{\alpha}, b \neq s$ and any $\mathbf{x}_1 = \boldsymbol{\lambda} c$, $\boldsymbol{\lambda} \in \mathcal{A}$, $c \in \Omega$ with $\boldsymbol{\lambda} \neq \boldsymbol{\alpha}, \boldsymbol{\beta}$ and $c \neq b, s$. On one hand, $\pi(-\mathbf{x}_0|\mathbf{J}_0) + \pi(\boldsymbol{\beta} s|\mathbf{J}_0) = 1$, which implies that $\mathbf{J}_0$ can only be mapped to $-\mathbf{x}_0$ and $\boldsymbol{\beta} s$. On the other hand, we also have $\pi(-\mathbf{x}_1|\mathbf{J}_0) + \pi(\boldsymbol{\beta} c|\mathbf{J}_0) = 1$, which implies that $\mathbf{J}_0$ can only be mapped to $-\mathbf{x}_1$ and $\boldsymbol{\beta} c$. Since $\mathbf{x}_1 \neq \mathbf{x}_0$ and $\boldsymbol{\beta} c \neq \boldsymbol{\beta} s$, this is a contradiction. Hence, we can always find a pair $\mathbf{x}_0$ and $\mathbf{J}_0$ such that $\pi(-\mathbf{x}_0|\mathbf{J}_0) + \pi(\boldsymbol{\beta} s|\mathbf{J}_0) < 1$. ■

With the same notations as in Lemma 2, we have:

***Lemma** 3:* $\mathcal{X}$ can be partitioned into six subsets with respect to $\mathbf{x}_0 = \boldsymbol{\alpha} s$ as $\mathcal{X} = \cup_{i=1}^6 \mathcal{X}_i$, where

$$\begin{aligned} \mathcal{X}_1 &\triangleq \{\boldsymbol{\alpha}(-s)\}, \ \mathcal{X}_2 \triangleq \{\boldsymbol{\alpha} s_0 | s_0 \in \Omega, s_0 \neq -s\}, \\ \mathcal{X}_3 &\triangleq \{\boldsymbol{\beta} s\}, \ \mathcal{X}_4 \triangleq \{\boldsymbol{\beta} s_0 | s_0 \in \Omega, s_0 \neq s\} \\ \mathcal{X}_5 &\triangleq \{\boldsymbol{\alpha}_0 s | \boldsymbol{\alpha}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}\}, \\ \mathcal{X}_6 &\triangleq \{\boldsymbol{\alpha}_0 s_0 | \boldsymbol{\alpha}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}, s_0 \neq s\}. \end{aligned} \tag{35}$$

Under the conditions that $\gamma > f^{-1}(\frac{1}{2N_c})$ and $\frac{d_{\min}^2}{\sigma_n^2} > \max(\frac{2\sqrt{\ln N_c}}{\sqrt{2}\gamma - \sqrt{\ln N_c}}, 2\ln\frac{1}{1-2\epsilon})$,

$$W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) = W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}), \quad \forall \mathbf{y} \in \mathcal{X}_i, i = 1, 3. \tag{36}$$

$$W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) > 0, \quad \forall \mathbf{y} \in \mathcal{X}_i, i = 2, 4, 5, 6. \tag{37}$$

Proof: See Appendix A. ■

Proof of Theorem 2: Following Lemma 2, we pick $\mathbf{x}_0$, $\mathbf{J}_0$ such that $\boldsymbol{\beta} \neq \boldsymbol{\alpha}, b \neq s$ and $\pi(-\mathbf{x}_0|\mathbf{J}_0) + \pi(\boldsymbol{\beta} s|\mathbf{J}_0) < 1$. We will prove that $\hat{W}(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{J}_0) = \hat{W}(\boldsymbol{\alpha}|\mathbf{J}_0, \mathbf{x}_0)$ and $\hat{W}(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{J}_0) = \hat{W}(\boldsymbol{\beta}|\mathbf{J}_0, \mathbf{x}_0)$ cannot hold simultaneously, by showing that

$$\hat{W}(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{J}_0) - \hat{W}(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{J}_0) > \hat{W}(\boldsymbol{\alpha}|\mathbf{J}_0, \mathbf{x}_0) - \hat{W}(\boldsymbol{\beta}|\mathbf{J}_0, \mathbf{x}_0). \tag{38}$$

By Lemma 3, $\mathcal{X} = \cup_{i=1}^6 \mathcal{X}_i$. For any $\hat{\boldsymbol{\alpha}}_0 \in \mathcal{A}$, we have

$$\hat{W}(\hat{\boldsymbol{\alpha}}_0|\mathbf{x}_0, \mathbf{J}_0) = \sum_{i=1}^6 \sum_{\mathbf{y} \in \mathcal{X}_i} \pi(\mathbf{y}|\mathbf{J}_0) W(\hat{\boldsymbol{\alpha}}_0|\mathbf{x}_0, \mathbf{y}). \tag{39}$$

It then follows from (36) - (37) that

$$\begin{aligned} &\hat{W}(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{J}_0) - \hat{W}(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{J}_0) \\ = &\sum_{\substack{i=2, \\ i \neq 3}}^6 \sum_{\mathbf{y} \in \mathcal{X}_i} [W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y})] \pi(\mathbf{y}|\mathbf{J}_0) \geq 0, \end{aligned} \tag{40}$$

with the equality holds if and only if $\sum_{\substack{i=2, \\ i \neq 3}}^6 \sum_{\mathbf{y} \in \mathcal{X}_i} \pi(\mathbf{y}|\mathbf{J}_0) = 0$, i.e., $\pi(-\mathbf{x}_0|\mathbf{J}_0) + \pi(\boldsymbol{\beta} s|\mathbf{J}_0) = 1$. Recall that we pick $\mathbf{x}_0$, $\mathbf{J}_0$ such that $\boldsymbol{\beta} \neq \boldsymbol{\alpha}, b \neq s$ and $\pi(-\mathbf{x}_0|\mathbf{J}_0) + \pi(\boldsymbol{\beta} s|\mathbf{J}_0) < 1$. Therefore,

$$\hat{W}(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{J}_0) - \hat{W}(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{J}_0) > 0. \tag{41}$$

Similarly, $\mathcal{X}$ can be partitioned into six subsets with respect to $\mathbf{J}_0 = \boldsymbol{\beta} b$, defined as

$$\begin{aligned} &\mathcal{J}_1 \triangleq \{\boldsymbol{\beta}(-b)\}, \ \mathcal{J}_2 \triangleq \{\boldsymbol{\beta} b_0 | b_0 \in \Omega, b_0 \neq -b\}, \\ &\mathcal{J}_3 \triangleq \{\boldsymbol{\alpha} b\}, \mathcal{J}_4 \triangleq \{\boldsymbol{\alpha} b_0 | b_0 \in \Omega, b_0 \neq b\} \\ &\mathcal{J}_5 \triangleq \{\boldsymbol{\beta}_0 b | \boldsymbol{\beta}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}\}, \mathcal{J}_6 \triangleq \{\boldsymbol{\beta}_0 b_0 | \boldsymbol{\beta}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}, b_0 \neq b\}, \end{aligned} \tag{42}$$

thus

$$\hat{W}(\hat{\boldsymbol{\alpha}}_0|\mathbf{J}_0, \mathbf{x}_0) = \sum_{i=1}^6 \sum_{\mathbf{y} \in \mathcal{J}_i} \pi(\mathbf{y}|\mathbf{x}_0) W(\hat{\boldsymbol{\alpha}}_0|\mathbf{J}_0, \mathbf{y}). \tag{43}$$

Then we have

$$\begin{aligned} &\hat{W}(\boldsymbol{\alpha}|\mathbf{J}_0, \mathbf{x}_0) - \hat{W}(\boldsymbol{\beta}|\mathbf{J}_0, \mathbf{x}_0) \\ = &\sum_{\substack{i=2, \\ i \neq 3}}^6 \sum_{\mathbf{y} \in \mathcal{J}_i} [W(\boldsymbol{\alpha}|\mathbf{J}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{J}_0, \mathbf{y})] \pi(\mathbf{y}|\mathbf{x}_0). \end{aligned} \tag{44}$$

Moreover, under the same conditions as in previous case,

$$\hat{W}(\boldsymbol{\alpha}|\mathbf{J}_0,\mathbf{x}_0)-\hat{W}(\boldsymbol{\beta}|\mathbf{J}_0,\mathbf{x}_0)\leq 0. \tag{45}$$

Therefore, we can see that (38) holds, which implies that $\hat{W}(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{J}_0) = \hat{W}(\boldsymbol{\alpha}|\mathbf{J}_0,\mathbf{x}_0)$ and $\hat{W}(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{J}_0) = \hat{W}(\boldsymbol{\beta}|\mathbf{J}_0,\mathbf{x}_0)$ cannot hold simultaneously. □

Note that the secure ID in AJ-MDFH is generated using AES, to symmetrize AJ-MDFH is thus equivalent to break AES, which is computationally infeasible in practical systems. That is, the AVC corresponding to AJ-MDFH is computationally infeasible to be symmetrized. This result ensures that when the ID sequence is unknown to the jammer, the deterministic capacity of AJ-MDFH is positive, and equal to the random code capacity [7], [9].

B. Capacity Calculation

Note that in AJ-MDFH, the message information is only transmitted through the carrier bits. Consider $\mathbf{x}=\boldsymbol{\alpha}s$ where $s\in\Omega$ and $\boldsymbol{\alpha}=(\alpha_1,\cdots,\alpha_{N_c})\in\mathcal{A}$. Let i_S and i_J be the signal channel index and jamming channel index, respectively, and $\hat{i}_S$ the detected signal channel index at the receiver. For capacity derivation, define

$$W_1(\hat{k}|k,j)\triangleq Pr\{\hat{i}_S=\hat{k}|i_S=k,i_J=j\}. \tag{46}$$

Let $\mathbf{x}=\boldsymbol{\alpha}s$, $\mathbf{J}=\boldsymbol{\beta}b$ with $\boldsymbol{\alpha}=v(k)$, $\boldsymbol{\beta}=v(j)$. Let $\hat{\boldsymbol{\alpha}}=v(\hat{k})$, and assuming s and b are uniformly distributed over Ω, then the relationship between W_1 and W can be characterized as

$$W_1(\hat{k}|k,j)=\frac{1}{|\Omega|^2}\sum_{s\in\Omega}\sum_{b\in\Omega}W(\hat{\boldsymbol{\alpha}}|\mathbf{x}=\boldsymbol{\alpha}s,\mathbf{J}=\boldsymbol{\beta}b). \tag{47}$$

The detailed representation of W_1 is provided in Appendix B, where we prove that W_1 has the following properties:

(P1): $W_1(k|k,k) = W_1(k_0|k_0,k_0)$ and $W_1(i|k,k) = W_1(i_0|k_0,k_0)$ for any $i,k,i_0,k_0\in\mathcal{I}_c, i\neq k, i_0\neq k_0$.

(P2): $W_1(k|k,j) = W_1(k_0|k_0,j_0)$, $W_1(j|k,j) = W_1(j_0|k_0,j_0)$ and $W_1(i|k,j) = W_1(i_0|k_0,j_0)$ for any $i,j,k,i_0,j_0,k_0\in\mathcal{I}_c$, $j\neq k, i\neq j,k, j_0\neq k_0, i_0\neq j_0,k_0$.

Denote the set of all probability distributions on $\mathcal{I}_c$ as $\mathcal{P}(\mathcal{I}_c)$. Let P and ζ denote the probability distribution associated with i_S and i_J, respectively. $P,\zeta\in\mathcal{P}(\mathcal{I}_c)$. Let W_ζ denote the averaged probability matrix for a given ζ

$$\begin{aligned}W_\zeta(\hat{k}|k) &= W_\zeta(\hat{i}_S=\hat{k}|i_S=k)\\ &= \sum_{j\in\mathcal{I}_c}W_1(\hat{k}|k,j)\zeta(i_J=j).\end{aligned} \tag{48}$$

Let $I(P,W_\zeta)$ denote the mutual information [7] between the input and the output for the AJ-MDFH channel, defined as

$$I(P,W_\zeta)\triangleq\sum_{\hat{k}\in\mathcal{I}_c}\sum_{k\in\mathcal{I}_c}P(i_S=k)W_\zeta(\hat{k}|k)\log\frac{W_\zeta(\hat{k}|k)}{(PW)_\zeta(\hat{k})}, \tag{49}$$

where $(PW)_\zeta(\hat{k})=\sum_{k'\in\mathcal{I}_c}W_\zeta(\hat{k}|k')P(k')$. Following Theorem 2, the AVC corresponding to AJ-MDFH is nonsymmetrizable. Its channel capacity for the average error probability is positive and can be calculated as [6], [10]

$$C=\max_{P\in\mathcal{P}(\mathcal{I}_c)}\min_{\zeta\in\mathcal{P}(\mathcal{I}_c)}I(P,W_\zeta)=\min_{\zeta\in\mathcal{P}(\mathcal{I}_c)}\max_{P\in\mathcal{P}(\mathcal{I}_c)}I(P,W_\zeta). \tag{50}$$

It can be observed from (50) that the legal user tries to choose P to maximize the mutual information, while the jammer tries to minimize it by choosing an appropriate ζ. Let $(P,\zeta)\in\mathcal{P}(\mathcal{I}_c)\times\mathcal{P}(\mathcal{I}_c)$ be a pair of mixed strategy chosen by the user and the jammer. The capacity can be achieved when a pair of saddle point strategy (P^*,ζ^*) are chosen, which can be characterized by the following two inequalities for all $(P,\zeta)\in\mathcal{P}(\mathcal{I}_c)\times\mathcal{P}(\mathcal{I}_c)$ [14]–[17]:

$$I(P,W_{\zeta^*})\leq I(P^*,W_{\zeta^*})\leq I(P^*,W_\zeta). \tag{51}$$

Following the same argument as in [18], it can be shown that:

Lemma 4: In an AJ-MDFH channel, the saddle point strategy pair can be reached when both P and ζ are uniform distributions over $\mathcal{I}_c$. That is,

$$P^*(k)=\begin{cases}\frac{1}{N_c}, & k\in\mathcal{I}_c,\\ 0, & \text{otherwise},\end{cases}\qquad \zeta^*(j)=\begin{cases}\frac{1}{N_c}, & j\in\mathcal{I}_c,\\ 0, & \text{otherwise}.\end{cases} \tag{52}$$

In AJ-MDFH, when the jammer chooses the strategy ζ^* as in (52), the averaged probability matrix can be calculated as

$$W_{\zeta^*}(\hat{k}|k)=\sum_{j=1}^{N_c}W_1(\hat{k}|k,j)\zeta^*(j). \tag{53}$$

(i) When $\hat{k}=k$, (53) can be expanded as

$$W_{\zeta^*}(\hat{k}|k)=W_1(k|k,k)\zeta^*(k)+\sum_{j\in\mathcal{I}_c,j\neq k}W_1(k|k,j)\zeta^*(j). \tag{54}$$

Following the properties **(P1)** and **(P2)** of W_1, we have $W_{\zeta^*}(\hat{k}|k)=\frac{1}{N_c}W_1(k_0|k_0,k_0)+\frac{N_c-1}{N_c}W_1(k_0|k_0,j_0)$, for any fixed $j_0,k_0\in\mathcal{I}_c, j_0\neq k_0$.

(ii) When $\hat{k}\neq k$, (53) can be expanded as

$$\begin{aligned}W_{\zeta^*}(\hat{k}|k) &= W_1(\hat{k}|k,k)\zeta^*(k)+W_1(\hat{k}|k,\hat{k})\zeta^*(\hat{k})\\ &\quad+\sum_{j\in\mathcal{I}_c,j\neq\hat{k},k}W_1(\hat{k}|k,j)\zeta^*(j).\end{aligned} \tag{55}$$

Following the properties **(P1)** and **(P2)** of W_1, we have $W_{\zeta^*}(\hat{k}|k) = \frac{1}{N_c}W_1(\hat{k}_0|k_0,k_0)+\frac{1}{N_c}W_1(\hat{k}_0|k_0,\hat{k}_0)+\frac{N_c-2}{N_c}W_1(\hat{k}_0|k_0,j_0)$, for any fixed $\hat{k}_0,k_0,j_0\in\mathcal{I}_c,\hat{k}_0\neq k_0,j_0\neq\hat{k}_0,k_0$. Define $w_1\triangleq W_{\zeta^*}(k|k)$ and $w_2\triangleq W_{\zeta^*}(\hat{k}|k),\hat{k}\neq k$, then W_{ζ^*} can be obtained as

$$\begin{aligned}W_{\zeta^*} &= \begin{pmatrix}W_{\zeta^*}(1|1) & W_{\zeta^*}(2|1) & \cdots & W_{\zeta^*}(N_c|1)\\ W_{\zeta^*}(1|2) & W_{\zeta^*}(2|2) & \cdots & W_{\zeta^*}(N_c|2)\\ \vdots & \vdots & \ddots & \vdots\\ W_{\zeta^*}(1|N_c) & W_{\zeta^*}(2|N_c) & \cdots & W_{\zeta^*}(N_c|N_c)\end{pmatrix}\\ &= \begin{pmatrix}w_1 & w_2 & \cdots & w_2\\ w_2 & w_1 & \cdots & w_2\\ \vdots & \vdots & \ddots & \vdots\\ w_2 & w_2 & \cdots & w_1\end{pmatrix}_{N_c\times N_c}.\end{aligned} \tag{56}$$

Due to the special structure of matrix W_{ζ^*}, we have: for any $\hat{k}, k' \in \mathcal{I}_c$, $\sum_{k' \in \mathcal{I}_c} W_{\zeta^*}(\hat{k}|k') = \sum_{\hat{k} \in \mathcal{I}_c} W_{\zeta^*}(\hat{k}|k') = 1$, and

$$(P^*W)_{\zeta^*}(\hat{k}) = \sum_{k' \in \mathcal{I}_c} W_{\zeta^*}(\hat{k}|k')P^*(k') = \frac{1}{N_c}. \quad (57)$$

Therefore, the capacity can be calculated as:

$$\begin{aligned} C &= I(P^*, W_{\zeta^*}) \\ &= \sum_{\hat{k} \in \mathcal{I}_c} \sum_{k \in \mathcal{I}_c} \frac{1}{N_c} W_{\zeta^*}(\hat{k}|k) \log \frac{W_{\zeta^*}(\hat{k}|k)}{\frac{1}{N_c}} \\ &= \sum_{\hat{k} \in \mathcal{I}_c} \sum_{k \in \mathcal{I}_c} \frac{1}{N_c} W_{\zeta^*}(\hat{k}|k) \log N_c \\ &\quad + \sum_{\hat{k} \in \mathcal{I}_c} \sum_{k \in \mathcal{I}_c} \frac{1}{N_c} W_{\zeta^*}(\hat{k}|k) \log W_{\zeta^*}(\hat{k}|k) \\ &= \log N_c + \sum_{\hat{k}=1}^{N_c} W_{\zeta^*}(\hat{k}|1) \log W_{\zeta^*}(\hat{k}|1) \\ &= \log N_c + w_1 \log w_1 + (N_c - 1) w_2 \log w_2. \quad (58) \end{aligned}$$

Following the discussions above, we have

***Theorem** 3:* Assuming Ω is an M-PSK constellation with power P_s. Under the worst case single band disguised jamming, the channel capacity of AJ-MDFH system is a function of M, N_c and $\frac{P_s}{\sigma_n^2}$ of the form $C = C\left(M, N_c, \frac{P_s}{\sigma_n^2}\right)$. As M approaches infinity, C converges to

$$\bar{C} = \log N_c + \bar{w}_1 \log \bar{w}_1 + (N_c - 1)\bar{w}_2 \log \bar{w}_2, \quad (59)$$

where $\bar{w}_1 = \lim_{M \to \infty} w_1$ and $\bar{w}_2 = \lim_{M \to \infty} w_2$.

The convergence result follows from similar argument as in the proof of Theorem 1 in Part I. Our analysis in this section can be extended to MC-AJ-MDFH, which is a secure combination of several collision-free single carrier AJ-MDFH systems. The capacity of MC-AJ-MDFH can be obtained as

$$C_{MC} = \sum_{m=1}^{N_g} C_m, \quad (60)$$

where N_g is the number of carriers, and C_m is the capacity of the m-th carrier.

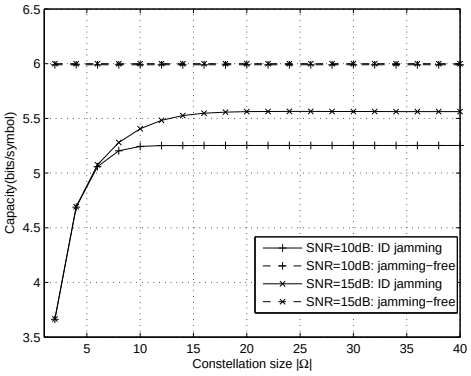


Fig. 3. AJ-MDFH capacity under the worst case single band disguised jamming (ID jamming) for different PSK constellation size. $N_c = 64$.

Theorem 3 is illustrated in Fig. 3, where we can see that: under reasonable SNR levels ($\geq$ 10dB, for example), the capacity limit $\bar{C}$ is close to the corresponding jamming-free case indicated by the dashed line. Figure 4 compares the capacity of MC-AJ-MDFH and frequency hopping multiple access (FHMA) system in [19], [20]. It can be observed that due to the collision-free design and the use of ID sequence, under disguised jamming, MC-AJ-MDFH can effectively support much more users than FHMA.

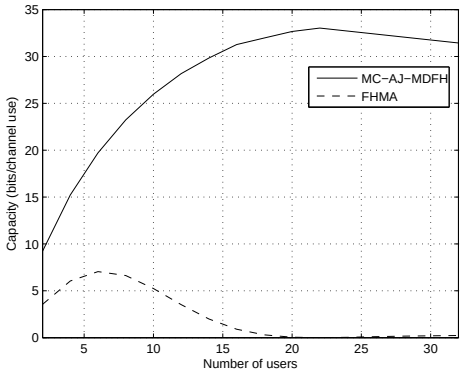


Fig. 4. Capacity of MC-AJ-MDFH and FHMA under the worst case single band disguised jamming. $N_c = 64$, $SNR = 10$dB. Here, per channel use means the total bandwidth of all used channels over one hopping period.

V. Conclusions

In this paper, we analyzed the capacity of MDFH and AJ-MDFH under disguised jamming. We proved that: under the worst case disguised jamming, (i) For MDFH, the corresponding AVC is symmetric, which implies that the deterministic capacity of MDFH is zero; (ii) For AJ-MDFH, due to shared randomness between the transmitter and the receiver provided by the secure ID sequence, the corresponding AVC is nonsymmetrizable, which implies that the deterministic capacity of AJ-MDFH is positive, and equal to the random code capacity. We calculated the capacity of AJ-MDFH and showed that it converges as the ID constellation size goes to infinity. This echoes our result in part I, where we showed that the probability of error of AJ-MDFH converges as the ID constellation size goes to infinity. From this paper, we can see that shared secure randomness between the transmitter and the receiver plays a critical role in anti-jamming system design. Designing of more efficient and robust jamming resistant systems remains an open and interesting topic.

Acknowledgement

This work was supported in part by the National Science Foundation under grants CNS-0746811, CNS-1117831, CNS-1217206, and CNS-1232109.

Appendix A
Proof of Lemma 3

Proof of Lemma 3: Note that $\mathcal{X}$ can be partitioned into six subsets with respect to $\mathbf{x}_0 = \boldsymbol{\alpha} s$. Define $\mathcal{B}_1 \triangleq \{\boldsymbol{\alpha}\tilde{s} | \tilde{s} \in \Omega\}$,

$\mathcal{B}_2 \triangleq \{\boldsymbol{\beta}\tilde{s}|\tilde{s} \in \Omega\}$ and $\mathcal{B}_3 \triangleq \{\boldsymbol{\alpha}_0\tilde{s}|\tilde{s} \in \Omega, \boldsymbol{\alpha}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}\}$. We have $\mathcal{X} = \cup_{i=1}^{3}\mathcal{B}_i$. It follows from the definition of subset $\mathcal{X}_i$ in (35) that $\mathcal{B}_1 = \mathcal{X}_1 \cup \mathcal{X}_2$, $\mathcal{B}_2 = \mathcal{X}_3 \cup \mathcal{X}_4$, $\mathcal{B}_3 = \mathcal{X}_5 \cup \mathcal{X}_6$, and $\mathcal{X} = \cup_{i=1}^{6}\mathcal{X}_i$.

(i) We consider the cases where $\mathbf{y} \in \mathcal{X}_i, i = 1, 3$. When $\mathbf{y} \in \mathcal{X}_1$ ($\mathbf{y} = -\mathbf{x}_0$), the jamming cancels the true signal, and the received signal contains only noise, resulting in $W(\hat{\boldsymbol{\alpha}}_0|\mathbf{x}_0, -\mathbf{x}_0) = \frac{1}{N_c}, \forall \hat{\boldsymbol{\alpha}}_0 \in \mathcal{A}$. When $\mathbf{y} \in \mathcal{X}_3$ ($\mathbf{y} = \boldsymbol{\beta}s$), the jamming has the same ID symbol as the true signal, and the receiver cannot distinguish between the two, resulting in $W(\boldsymbol{\alpha}|\mathbf{x}_0, \boldsymbol{\beta}s) = W(\boldsymbol{\beta}|\mathbf{x}_0, \boldsymbol{\beta}s)$. Hence, $W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) = W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y})$ holds in both cases.

(ii) When $\mathbf{y} \in \mathcal{X}_2$, we have $\mathbf{y} = \boldsymbol{\alpha}s_0$ where $s_0 \in \Omega, s_0 \neq -s$. Assuming $\boldsymbol{\alpha} = v(k)$,

$$\begin{aligned} W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) &= Pr\{Z_k < Z_i, \forall i \in \mathcal{I}_c, i \neq k|\mathbf{x}_0, \mathbf{y}\} \\ &\geq 1 - \sum_{i \neq k} Pr\{Z_k \geq Z_i|\mathbf{x}_0, \mathbf{y}\} \\ &= 1 - (N_c - 1)Pr\{Z_k \geq Z_{i_0}|\mathbf{x}_0, \mathbf{y}\}, \quad (61) \end{aligned}$$

for any fixed $i_0 \neq k$. Since $s_0 \neq -s$, it follows from the results in [13] that

$$\begin{aligned} & Pr\{Z_k \geq Z_{i_0}|\mathbf{x}_0, \mathbf{y}\} \\ = \; & Q_1(\sqrt{C}, \sqrt{D}) - \frac{\|s + s_0\|^2 + \sigma_n^2}{\|s + s_0\|^2 + 2\sigma_n^2} e^{-\frac{C+D}{2}} I_0(\sqrt{CD}) \\ < \; & Q_1(\sqrt{C}, \sqrt{D}), \quad (62) \end{aligned}$$

where $C = \frac{2P_s}{\|s+s_0\|^2+2\sigma_n^2}$ and $D = \frac{2P_s(\|s+s_0\|^2+\sigma_n^2)}{\sigma_n^2(\|s+s_0\|^2+2\sigma_n^2)}$. Since $D > C$, $Pr\{Z_k \geq Z_{i_0}|\mathbf{x}_0, \mathbf{y}\} \leq e^{-\frac{(D-C)^2}{2}}$ [21]. It then follows from (61) and $\|s+s_0\| \geq d_{\min}$ that $W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) > 1 - (N_c - 1)\exp[-2(\frac{\gamma d_{\min}^2}{d_{\min}^2+2\sigma_n^2})^2]$, and $W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) = \frac{1}{N_c-1}[1 - W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y})] < \exp[-2(\frac{\gamma d_{\min}^2}{d_{\min}^2+2\sigma_n^2})^2]$. Hence, we have $W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) > 1 - N_c\exp[-2(\frac{\gamma d_{\min}^2}{d_{\min}^2+2\sigma_n^2})^2]$, which implies that under the conditions

$$\gamma > \sqrt{\frac{1}{2}\ln N_c} \text{ and } \frac{d_{\min}^2}{\sigma_n^2} > \frac{2\sqrt{\ln N_c}}{\sqrt{2}\gamma - \sqrt{\ln N_c}}, \quad (63)$$

$W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) > 0$.

(iii) When $\mathbf{y} \in \mathcal{X}_4$, we have $\mathbf{y} = \boldsymbol{\beta}s_0$ where $s_0 \in \Omega, s_0 \neq s$. Note that $W(\boldsymbol{\alpha}|\mathbf{y}, \mathbf{x}_0) = W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y})$. Since $\|s_0 - s\| \geq d_{\min}$, it follows from Theorem 1 that $W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) \geq 1 - e^{-\frac{d_{\min}^2}{2\sigma_n^2}} - 2\epsilon$. Therefore, under the conditions

$$\epsilon < \frac{1}{2} \text{ and } \frac{d_{\min}^2}{\sigma_n^2} > 2\ln\frac{1}{1-2\epsilon}, \quad (64)$$

$W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) > 0$.

(iv) When $\mathbf{y} \in \mathcal{X}_5$, we have $\mathbf{y} = \boldsymbol{\alpha}_0 s$ where $\boldsymbol{\alpha}_0 \in \mathcal{A}, \boldsymbol{\alpha}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}$. It follows from Proposition 2 that $W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) \geq \frac{1}{2} - \epsilon$. Note that $W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) = W(\boldsymbol{\alpha}_0|\mathbf{x}_0, \mathbf{y})$, we have $W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) = \frac{1}{N_c-2}[1 - 2W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y})] \leq \frac{2\epsilon}{N_c-2}$. Hence, we have $W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) \geq \frac{1}{2} - \frac{N_c\epsilon}{N_c-2}$. Under the condition

$$\epsilon < \frac{N_c - 2}{2N_c}, \quad (65)$$

$W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) > 0$.

(v) When $\mathbf{y} \in \mathcal{X}_6$, we have $\mathbf{y} = \boldsymbol{\alpha}_0 s_0$ where $\boldsymbol{\alpha}_0 \in \mathcal{A}, \boldsymbol{\alpha}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}$ and $s_0 \in \Omega, s_0 \neq s$. It follows from Proposition 2 that $W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) \geq 1 - \frac{1}{2}e^{-\frac{\|s_0-s\|^2}{2\sigma_n^2}} - \epsilon$. Assuming $\boldsymbol{\alpha} = v(k)$ and $\boldsymbol{\alpha}_0 = v(k_0)$, it follows from Lemma 1 that $W(\boldsymbol{\alpha}_0|\mathbf{x}_0, \mathbf{y}) \geq Pr\{Z_{k_0} < Z_k|\mathbf{x}_0, \mathbf{y}\} - (N_c - 2)Pr\{Z_{k_0} \geq Z_{i_0}|\mathbf{x}_0, \mathbf{y}\} = \frac{1}{2}e^{-\frac{\|s_0-s\|^2}{2\sigma_n^2}} - \epsilon$. Then we have $W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) = \frac{1}{N_c-2}[1 - W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\alpha}_0|\mathbf{x}_0, \mathbf{y})] \leq \frac{2\epsilon}{N_c-2}$. Hence, we have $W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) \geq 1 - \frac{1}{2}e^{-\frac{d_{\min}^2}{2\sigma_n^2}} - \frac{N_c\epsilon}{N_c-2}$, which implies that under the conditions

$$\epsilon < \frac{N_c - 2}{N_c} \text{ and } \frac{d_{\min}^2}{\sigma_n^2} > -2\ln 2(1 - \frac{N_c\epsilon}{N_c - 2}), \quad (66)$$

$W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) > 0$.

The conditions in (63) - (66) can be summarized and reduced to $\gamma > f^{-1}(\frac{1}{2N_c})$ and $\frac{d_{\min}^2}{\sigma_n^2} > \max(\frac{2\sqrt{\ln N_c}}{\sqrt{2}\gamma - \sqrt{\ln N_c}}, 2\ln\frac{1}{1-2\epsilon})$, where $f(x) = \frac{1}{x+2}\exp\{-\frac{x(x+1)}{x+2}\}$. Hence, Lemma 3 is proved. □

APPENDIX B
CALCULATION OF THE PROBABILITY MATRIX W_1

Let $\mathbf{x} = \boldsymbol{\alpha}s$, $\mathbf{J} = \boldsymbol{\beta}b$ with $\boldsymbol{\alpha} = v(k), \boldsymbol{\beta} = v(j)$, and $j, k \in \mathcal{I}_c$, $s, b \in \Omega$. Assume Ω is an M-PSK constellation with power P_s.

(i) When $j = k$, the received signal in the ith channel, r_i, and the corresponding Z_i defined in (5) can be calculated as

$$r_i = \begin{cases} s + b + n_k, & i = k, \\ n_i, & i \neq k, \end{cases} \quad Z_i = \begin{cases} \frac{\|b+n_k\|}{\sqrt{\|s+b\|^2+\sigma_n^2}}, & i = k, \\ \frac{\|n_i-s\|}{\sigma_n}, & i \neq k. \end{cases} \quad (67)$$

Note that $n_1, \ldots, n_{N_c}$ are i.i.d. circularly symmetric Gaussian random variables of zero mean and variance σ_n^2. For any $s, b \in \Omega$, Z_k is a Rician random variable with PDF $p_{Z_k}(z_k) = \frac{z_k}{\sigma^2}e^{-\frac{z_k^2+\nu^2}{2\sigma^2}}I_0\left(\frac{z_k\nu}{\sigma^2}\right)$ for $z_k \geq 0$, where $\nu = \frac{\sqrt{P_s}}{\sqrt{\|s+b\|^2+\sigma_n^2}}$ and $\sigma = \frac{\sigma_n}{\sqrt{2(\|s+b\|^2+\sigma_n^2)}}$; for $i \neq k$, Z_i's are i.i.d. Rician random variables with PDF $p_{Z_i}(z_i) = \frac{z_i}{\sigma^2}e^{-\frac{z_i^2+\nu^2}{2\sigma^2}}I_0\left(\frac{z_i\nu}{\sigma^2}\right)$ for $z_i \geq 0$, where $\nu = \frac{\sqrt{P_s}}{\sigma_n}$ and $\sigma = \frac{1}{\sqrt{2}}$. We have

$$\begin{aligned} W_1(k|k,k) &= \frac{1}{|\Omega|^2}\sum_{s\in\Omega}\sum_{b\in\Omega} Pr\{Z_k < Z_i, \\ &\qquad \forall i \in \mathcal{I}_c, i \neq k|\mathbf{x} = \boldsymbol{\alpha}s, \mathbf{J} = \boldsymbol{\beta}b\} \\ &= \frac{1}{|\Omega|^2}\sum_{s\in\Omega}\sum_{b\in\Omega}\int_0^\infty \left[Q_1\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_k\right)\right]^{N_c-1} \\ &\qquad \cdot\frac{2(\|s+b\|^2+\sigma_n^2)z_k}{\sigma_n^2}e^{-\frac{(\|s+b\|^2+\sigma_n^2)z_k^2+P_s}{\sigma_n^2}} \\ &\qquad \cdot I_0\left(\frac{2z_k}{\sigma_n^2}\sqrt{P_s(\|s+b\|^2+\sigma_n^2)}\right)dz_k, \quad (68) \end{aligned}$$

where Q_1 is the Marcum-Q function and I_0 is the modified Bessel function of the first kind with order zero. For M-PSK constellation with power P_s, we have $s = \sqrt{P_s}e^{j\frac{2\pi m_s}{M}}$ and

$b=\sqrt{P_s}e^{j\frac{2\pi m_J}{M}}$ where $m_s, m_J \in [0, M-1]$, then (68) can be simplified as

$$W_1(k|k,k) = \frac{1}{M}\sum_{\kappa=0}^{M-1}\int_0^\infty \left[Q_1\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_k\right)\right]^{N_c-1} \cdot \frac{2[2P_s(1+\cos\frac{2\pi\kappa}{M})+\sigma_n^2]z_k}{\sigma_n^2} \cdot e^{-\frac{[2P_s(1+\cos\frac{2\pi\kappa}{M})+\sigma_n^2]z_k^2+P_s}{\sigma_n^2}} \cdot I_0\left(\frac{2z_k}{\sigma_n^2}\sqrt{P_s[2P_s(1+\cos\frac{2\pi\kappa}{M})+\sigma_n^2]}\right)dz_k, \quad (69)$$

where $\kappa \triangleq (m_s - m_J) \mod M$ is uniformly distributed over $[0, M-1]$. Since Z_i's are i.i.d. $\forall i \in \mathcal{I}_c, i \neq k$, then

$$W_1(i|k,k) = \frac{1}{N_c-1}[1-W_1(k|k,k)], \quad \forall i \in \mathcal{I}_c, i \neq k. \quad (70)$$

Therefore, we have **(P1)**: $W_1(k|k,k) = W_1(k_0|k_0,k_0)$ and $W_1(i|k,k) = W_1(i_0|k_0,k_0)$ for any $i,k,i_0,k_0 \in \mathcal{I}_c, i \neq k, i_0 \neq k_0$.

(ii) When $j \neq k$, the received signal r_i and corresponding Z_i can be calculated as

$$r_i = \begin{cases} s+n_k, & i=k, \\ b+n_j, & i=j, \\ n_i, & i\neq j,k, \end{cases} \qquad Z_i = \begin{cases} \frac{\|n_k\|}{\sqrt{P_s+\sigma_n^2}}, & i=k, \\ \frac{\|b-s+n_j\|}{\sqrt{P_s+\sigma_n^2}}, & i=j, \\ \frac{\|n_i-s\|}{\sigma_n}, & i\neq j,k. \end{cases} \quad (71)$$

For any $s, b \in \Omega$, Z_k is a Rayleigh random variable with PDF $p_{Z_k}(z_k) = \frac{z_k}{\sigma^2}e^{-\frac{z_k^2}{2\sigma^2}}$, where $\sigma = \frac{\sigma_n}{\sqrt{2(P_s+\sigma_n^2)}}$; Z_j is a Rician random variable with PDF $p_{Z_j}(z_j) = \frac{z_j}{\sigma^2}e^{-\frac{z_j^2+\nu^2}{2\sigma^2}}I_0\left(\frac{z_j\nu}{\sigma^2}\right)$, where $\nu = \frac{\|b-s\|}{\sqrt{P_s+\sigma_n^2}}$ and $\sigma = \frac{\sigma_n}{\sqrt{2(P_s+\sigma_n^2)}}$; for $i \neq j,k$, Z_i's are i.i.d. Rician random variables with PDF $p_{Z_i}(z_i) = \frac{z_i}{\sigma^2}e^{-\frac{z_i^2+\nu^2}{2\sigma^2}}I_0\left(\frac{z_i\nu}{\sigma^2}\right)$, where $\nu = \frac{\sqrt{P_s}}{\sigma_n}$ and $\sigma = \frac{1}{\sqrt{2}}$. Then, $W_1(k|k,j)$ can be calculated as

$$W_1(k|k,j) = \frac{1}{|\Omega|^2}\sum_{s\in\Omega}\sum_{b\in\Omega} Pr\{Z_k < Z_j \text{ and } Z_k < Z_i, \forall i \in \mathcal{I}_c, i \neq k, j | \mathbf{x}, \mathbf{J}\} = \frac{1}{M}\sum_{\kappa=0}^{M-1}\int_0^\infty Q_1\left(\frac{2}{\sigma_n}\sqrt{P_s\left(1-\cos\frac{2\pi\kappa}{M}\right)}, \frac{z_k\sqrt{2(P_s+\sigma_n^2)}}{\sigma_n}\right) Q_1^{N_c-2}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_k\right) \cdot \frac{2z_k(P_s+\sigma_n^2)}{\sigma_n^2}e^{-\frac{(P_s+\sigma_n^2)z_k^2}{\sigma_n^2}}dz_k, \quad (72)$$

and

$$W_1(j|k,j) = \frac{1}{|\Omega|^2}\sum_{s\in\Omega}\sum_{b\in\Omega} Pr\{Z_j < Z_k \text{ and } Z_j < Z_i, \forall i \in \mathcal{I}_c, i \neq j, k | \mathbf{x}, \mathbf{J}\} = \frac{1}{M}\sum_{\kappa=0}^{M-1}\int_0^\infty e^{-\frac{(fP_s+\sigma_n^2)z_j^2}{\sigma_n^2}}Q_1^{N_c-2} \cdot \left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_j\right)\frac{2z_j(P_s+\sigma_n^2)}{\sigma_n^2} \cdot e^{-[\frac{P_s+\sigma_n^2}{\sigma_n^2}z_j^2+\frac{2P_s}{\sigma_n^2}(1-\cos\frac{2\pi\kappa}{M})]} \cdot I_0\left(\frac{2z_j}{\sigma_n^2}\sqrt{2P_s(1-\cos\frac{2\pi\kappa}{M})(P_s+\sigma_n^2)}\right)dz_j. \quad (73)$$

Since Z_i's are i.i.d. for any $i \in \mathcal{I}_c, i \neq j, k$, then

$$W_1(i|k,j) = \frac{1}{N_c-2}[1-W_1(k|k,j)-W_1(j|k,j)], \quad i \in \mathcal{I}_c, i \neq j, k. \quad (74)$$

Therefore, we have **(P2)**: $W_1(k|k,j) = W_1(k_0|k_0,j_0)$, $W_1(j|k,j) = W_1(j_0|k_0,j_0)$ and $W_1(i|k,j) = W_1(i_0|k_0,j_0)$ for any $i,j,k,i_0,j_0,k_0 \in \mathcal{I}_c$, $j \neq k, i \neq j,k, j_0 \neq k_0, i_0 \neq j_0, k_0$.

REFERENCES

[1] Q. Ling and T. Li, "Message-driven frequency hopping: Design and analysis," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1773–1782, April 2009.

[2] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping: Part I – system design," *IEEE Trans. Wireless Commun.*, 2012, to appear.

[3] D. Blackwell, L. Breiman, and A. Thomasian, "The capacities of certain channel classes under random coding," *The Annals of Mathematical Statistics*, pp. 558–567, 1960.

[4] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Academic press, 1981, vol. 244.

[5] I. Csiszár and P. Narayan, "Arbitrarily varying channels with constrained inputs and states," *IEEE Trans. Inf. Theory*, vol. 34, no. 1, pp. 27–34, 1988.

[6] I. Csiszar and P. Narayan, "The capacity of the arbitrarily varying channel revisited: Positivity, constraints," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, 1988.

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

[8] A. Sarwate, "Robust and adaptive communication under uncertain interference," Technical Report No. UCB/EECS-2008-86, University of California at Berkeley, Tech. Rep., 2008.

[9] T. Ericson, "Exponential error bounds for random codes in the arbitrarily varying channel," *IEEE Trans. Inf. Theory*, vol. 31, no. 1, pp. 42 – 48, Jan. 1985.

[10] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Probability Theory and Related Fields*, vol. 44, no. 2, pp. 159–175, 1978.

[11] *Advanced Encryption Standard*, FIPS-197, National Institute of Standards and Technology Std., Nov. 2001.

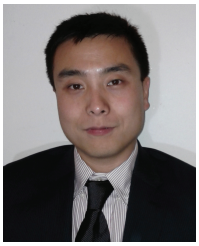
[12] J. Daemen and V. Rijmen, *The Design of Rijndael: AES–the Advanced Encryption Standard*. Springer, 2002.

[13] S. Stein, "Unified analysis of certain coherent and noncoherent binary communications systems," *IEEE Trans. Inf. Theory*, vol. 10, no. 1, pp. 43–51, Jan 1964.

[14] J. Borden, D. Mason, and R. McEliece, "Some information theoretic saddlepoints," *SIAM journal on control and optimization*, vol. 23, p. 129, 1985.

[15] T. Basar and Y. W. Wu, "Solutions to a class of minimax decision problems arising in communications systems," *J. Optim. Theory Appl.*, vol. 51, pp. 375–404, Decr 1986.

[16] T. Başar, "The gaussian test channel with an intelligent jammer," *IEEE Trans. Inf. Theory*, vol. 29, no. 1, pp. 152–157, 1983.
[17] T. Başar and G. Olsder, *Dynamic noncooperative game theory*. Society for Industrial Mathematics, 1999, vol. 23.
[18] I. Stiglitz, "Coding for a class of unknown channels," *IEEE Trans. Inf. Theory*, vol. 12, no. 2, pp. 189 – 195, apr 1966.
[19] A. Viterbi, "A processing satellite transponder for multlple access by low rate mobile users," in *Proc. Digital Satellite Commun. Conf.*, Montreal, Canada, Oct 1978.
[20] J. Goh and S. Maric, "The capacities of frequency-hopped code-division multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 1204–1211, 1998.
[21] M. Simon and M. Alouini, "Exponential-type bounds on the generalized marcum q-function with application to error probability analysis over fading channels," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 359 –366, mar 2000.



Lei Zhang received the B.S. and M.S. degrees in communication engineering in 2005 and 2007, respectively, both from Xidian University, Xi'an China. He received the Ph.D. degree in electrical and computer engineering in 2011, from Michigan State University, East Lansing MI. Dr. Zhang joined Marvell Semiconductor in 2011, and is currently working in the area of mobile SOC design and verification.

Tongtong Li received her Ph.D. degree in Electrical Engineering in 2000 from Auburn University. From 2000 to 2002, she was with Bell Labs, and had been working on the design and implementation of 3G and 4G systems. Since 2002, she has been with Michigan State University, where she is now an Associate Professor. Dr. Li's research interests fall into the areas of wireless and wired communications, wireless security, information theory and statistical signal processing. She is a recipient of the National Science Foundation (NSF) CAREER Award (2008) for her research on efficient and reliable wireless communications. She served as an Associate Editor for IEEE Signal Processing Letters from 2007-2009, and an Editorial Board Member for EURASIP Journal Wireless Communications and Networking from 2004-2011. She is currently serving as the Associate Editor for IEEE Transactions on Signal processing.