Anti-Jamming Message-Driven Frequency Hopping:  
Part I — System Design

Lei Zhang  Huahui Wang  Tongtong Li

Abstract—This is Part I of a two-part paper that considers anti-jamming system design in wireless networks based on message-driven frequency hopping (MDFH), a highly efficient spread spectrum technique. In this paper, we first analyze the performance of MDFH under hostile jamming. It is observed that while MDFH is robust under strong jamming, it experiences considerable performance losses under disguised jamming from sources that mimic the true signal. To overcome this limitation, we propose an anti-jamming MDFH (AJ-MDFH) system. The main idea is to transmit a secure ID sequence along with the information stream. The ID sequence is generated through a cryptographic algorithm using the shared secret between the transmitter and the receiver, it is then exploited by the receiver for effective signal extraction. It is shown that AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming, and is also robust under strong jamming. In addition, we extend AJ-MDFH to the multi-carrier case, which can increase the system efficiency and jamming resistance significantly through jamming randomization and frequency diversity, and can readily be used as a collision-free multiple access system. Part II of the paper focuses on the capacity analysis of MDFH and AJ-MDFH under disguised jamming.

I. INTRODUCTION

In wireless networks, one of the most commonly used techniques for limiting the effectiveness of an opponent’s communication is referred to as jamming, in which the authorized user’s signal is deliberately interfered by the adversary. Along with the wide spread of various wireless devices, especially with the advent of user configurable intelligent devices (such as cognitive radios), jamming attack is no longer limited to battlefield or military related events, but has become an urgent and serious threat to civilian communications as well [1]–[4].

As a widely used spread spectrum technique, frequency hopping (FH) was originally designed for secure communication under hostile environments [5]–[9]. In conventional FH, each user hops independently based on its own PN sequence, a collision occurs whenever there are two or more users transmitting over the same frequency band. Mainly limited by the collision effect, the spectral efficiency of the conventional FH is very low [10], [11]. To improve the spectral efficiency, FH systems that exploit high-dimensional modulation scheme have been studied in the literature [12]–[16]. However, the performance of these systems are still limited by the collision effect, also known as self-jamming.

Recently, a three-dimensional modulation scheme, known as message-driven frequency hopping (MDFH), was proposed in [11]. 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 controlled by the encrypted information stream rather than by a pre-selected pseudo-random sequence as in conventional FH. The most significant property of MDFH is that: by embedding a large portion of information into the hopping frequency selection process, additional information transmission is achieved with no extra cost on either bandwidth or power. In fact, transmission through hopping frequency control adds another dimension to the signal space, and the resulted coding gain can increase the system spectral efficiency by multiple times [11].

In this paper, we analyze the performance of MDFH under hostile jamming. It is observed that: MDFH is particularly powerful under strong jamming scenarios, and outperforms the conventional FH by big margins. The underlying argument is that for MDFH, even if the signal is jammed, strong jamming can enhance the power of the jammed signal and hence increases the probability of carrier detection. When the system experiences disguised jamming, where the jamming is highly correlated with the signal, and has a power level close or equal to the signal power, it is then difficult for the MDFH receiver to distinguish jamming from the true signal, resulting in performance losses. As will be shown in part II of the paper, this is essentially due to the existence of symmetry between the jamming interference and the authorized signal.

To overcome the drawback of MDFH, in this paper, we propose an anti-jamming MDFH (AJ-MDFH) scheme. The main idea is to insert some signal identification (ID) information during the transmission process. This secure ID information is generated through the Advanced Encryption Standard (AES) [17] using the shared secret between the transmitter and the receiver. The ID information can be exploited by the receiver to locate the true carrier frequency. Moreover, protected by AES, it is computationally infeasible for malicious users to recover the ID sequence.

The major difference with MDFH is that: in AJ-MDFH, we add shared randomness between the transmitter and the receiver to break the symmetry between the jamming interference and authorized signal. More specifically, in AJ-MDFH, secure ID signals are introduced to distinguish the true information channel from the disguised channels invoked by jamming interference. Our analysis indicates that: comparing with MDFH, AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming. At the same

Lei Zhang is with Marvell Semiconductor Inc., 5488 Marvell Ln, Santa Clara, CA 95054, USA. (email: lei@marvell.com).
Huahui Wang is with AT &T Shannon Laboratories, Florham Park, NJ 07932, USA. (email: huahui@research.att.com)
Tongtong Li is with the Department of ECE, Michigan State University, East Lansing, MI 48824, USA. (email:tongli@egr.msu.edu)
time, its spectral efficiency is very close to that of MDFH, which is several times higher than that of conventional FH.

Single carrier AJ-MDFH can be further extended to multi-carrier AJ-MDFH (MC-AJ-MDFH). It is observed that by exploiting secure group generation, MC-AJ-MDFH can increase the system efficiency and jamming resistance significantly through jamming randomization and enriched frequency diversity. By assigning different carrier groups to different users, MC-AJ-MDFH can also be used as a collision-free multiple access system.

We further investigate ID constellation design and its impact on the performance of AJ-MDFH under both noise jamming and disguised jamming. Noise jamming, where the jamming is modeled as Gaussian noise, has been widely adopted in literature [18]–[20]. However, disguised jamming can be much more harmful for most communication systems. For AJ-MDFH, the worst case disguised jamming is ID jamming, for which the jammer tries to mimic the ID signal, and sends symbols from the same constellation as that of the ID signal. We show that under noise jamming, the detection error probability is mainly determined by the signal to jamming and noise ratio. In this case, for a given power constraint, constant modulus constellation delivers the best results in terms of detection error probability. Under ID jamming, the situation is more complex. In the ideal case when the system is noise-free, increasing the ID constellation size can increase the ID uncertainty, hence reduce the probability of error. In this case, the ideal constellation size is $M = \infty$. However, when noise is present, we prove that the detection error probability converges as $M$ goes to infinity. In other words, there exists a threshold $M_t$, increasing the constellation size over $M_t$ will result in little improvement in error probability. This result justifies the use of practical, finite size constellations in AJ-MDFH.

This paper is organized as follows. In Section II, we introduce the concept of disguised jamming and evaluate MDFH under hostile jamming. In Section III, the proposed AJ-MDFH scheme is introduced, following by the extension to the multi-carrier case. ID constellation design is investigated in Section IV. Spectral efficiency is analyzed in Section V. Simulation examples are provided in Section VI and we conclude in Section VII. Part II of the paper [21] focuses on the capacity analysis of MDFH and AJ-MDFH under disguised jamming.

II. MESSAGE-DRIVEN FREQUENCY HOPPING — A BRIEF REVIEW

In this section, we briefly review the message-driven frequency hopping (MDFH) system, and evaluate its performance under different jamming scenarios.

A. System Description

The basic idea of MDFH is that a major part of the information is transmitted through carrier frequency selection in the hopping process. In other words, the hopping pattern is determined by the encrypted message information itself.

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 used to specify an individual channel here 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 $\Omega$ be the selected constellation that contains $M$ symbols, each symbol in the constellation represents $B_s = \log_2 M$ 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 $N_h = \frac{T_s}{T_h}$. We assume that $N_h$ is an integer larger than or equal to one.

![Transmitter structure of MDFH.](image)

The transmitter structure of MDFH is shown in Fig. 1. We start by dividing the encrypted information stream into blocks of 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 are used to determine the hopping frequencies, and the ordinary bits are mapped to a symbol which is transmitted through the selected channels successively. Denote the nth block by $X_n$, as illustrated in Fig. 1a. Note that in MDFH, the whole block $X_n$ is transmitted within one symbol period.

At the receiver, the transmitting frequency is captured using a filter bank as in the FSK receiver rather than using the frequency synthesizer. To detect the active frequency band, a bank of $N_c$ bandpass filters (BPF), each centered at $f_i$ ($i = 1, 2, \cdots, N_c$), is deployed at the receiver front end, followed by a demodulator equipped with matched filter and sampler. At each hopping period, the ordinary bits and the corresponding carrier frequency can be determined using the minimum distance criterion. Jamming detection algorithm can be incorporated at the receiver to improve the system performance [22].

B. Performance of MDFH under Hostile Jamming

First, we introduce the concept of disguised jamming. Disguised jamming denotes the case where the jamming is highly correlated with the signal, and has a power level close or equal to the signal power. More specifically, let $s(t)$ and $J(t)$ be the user’s signal and jamming interference, respectively. Define

$$
\rho = \frac{1}{T_0 \sqrt{P_s P_J}} \int_{t_1}^{t_2} s(t) J^*(t) dt
$$

as the normalized cross-correlation coefficient of $s(t)$ and $J(t)$ over the time period $[t_1, t_2]$, where $T_0 = t_2 - t_1$, $P_s = \frac{1}{T_0} \int_{t_1}^{t_2} |s(t)|^2 dt$ and $P_J = \frac{1}{T_0} \int_{t_1}^{t_2} |J(t)|^2 dt$. We say that $J(t)$ is a disguised jamming to signal $s(t)$ over $[t_1, t_2]$ if
1) $J(t)$ and $s(t)$ are highly correlated. More specifically, $|\rho| > \rho_0$, where $\rho_0$ is an application-oriented, predefined correlation threshold.

2) The jamming-to-signal ratio (JSR) is close to 0dB. More specifically, $|P_j - 1| < \epsilon_p$, where $\epsilon_p$ is an application-oriented, predefined jamming-to-signal ratio threshold.

In this paper, we consider disguised jamming over each hopping period, that is, $[t_1, t_2] = [mT_h, (m + 1)T_h]$ for some integer $m$. In the worst case, the constellation $\Omega$ and the pulse shaping filter of the information signal are known to the jammer, the jammer can then disguise itself by transmitting symbols from $\Omega$ over a fake channel using the same power level. That is, $J(t) = e^{i\theta}s(t)$ for some phase $\theta$.

We compare the performance of MDFH with that of conventional FH in AWGN channels, under both noise jamming and disguised jamming. The result (without channel coding) is shown in Fig. 2. The jamming-to-signal ratio is defined as $JSR = \frac{P_j}{P_s}$, where $P_j$ and $P_s$ denote the jamming power and signal power per hop, respectively. As can be seen, MDFH delivers excellent performance under strong jamming scenarios (i.e., $JSR \gg 1$), and outperforms conventional FH by big margins. Note that in this case, the spectral efficiency of MDFH is roughly 3.3 times that of conventional FH.

![Fig. 2. Performance comparison under single band jamming.](image1)

We divide the source information into blocks of size $B$ and divide the ID sequence into blocks of size $B_c$. Denote the nth source information block and ID block as $X_n$ and $Y_n$, respectively. Let $f_{X_n}$ be the carrier frequency corresponding to $X_n$, and $s_n$ the symbol corresponding to ID bit-vector $Y_n$. It should be noted that the ID symbol is refreshed at each hopping period. The transmitted signal can then be represented as

$$s(t) = \sqrt{2Re}\sum_{n=-\infty}^{\infty} s_n g(t - nT_h) e^{j2\pi f_{X_n} t}$$

$$= \sqrt{2Re}\sum_{n=-\infty}^{\infty} \sum_{j=1}^{N_c} \alpha_{i,n}s_n g(t - nT_h) e^{j2\pi f_{j} t}, \quad (2)$$

where $T_h$ is the hop duration, $g(t)$ is the pulse shaping filter,

$$\alpha_{i,n} = \begin{cases} 1 & \text{if } f_{X_n} = f_i, \\ 0 & \text{otherwise.} \end{cases}$$

In this paper, we introduce the anti-jamming MDFH (AJ-MDFH) system.

**Remark:** It is interesting to note that in the primary user emulation (PUE) attack in cognitive radio networks, the malicious user mimics the primary user’s signal in fallow bands to preempt spectrum resources that could have been used by legitimate secondary users [23]–[25]. This implies that disguised jamming can be used to interfere the authorized user’s signal directly (as discussed in this paper), and can also be used to distract other users such as in PUE attacks. Similar techniques can be used to distract/prevent eavesdropping as well.

**III. ANTI-JAMMING MDFH (AJ-MDFH)**

**A. Transmitter Design**

The main idea here is to insert some signal identification (ID) information during the transmission process. This secure ID information is generated through a cryptographic algorithm using the shared secret between the transmitter and the receiver, and can be used by the receiver to locate the true carrier frequency. Our design goal is to reinforce jamming resistance without sacrificing too much on spectral efficiency.

![AJ-MDFH transmitter structure](image2)

The transmitter structure of AJ-MDFH is illustrated in Fig. 3. Each user is assigned a secure ID sequence. We propose to replace the ordinary bits in MDFH with the ID bits. In order to prevent impersonate attack, each user’s ID sequence needs to be kept secret from the malicious jammer. The ID sequence can be generated using two steps as in [26]: (i) Generate a pseudo-random binary sequence using a linear feedback shift register(LFSR); (ii) Take the output of LFSR as the plaintext, and feed it into the Advanced Encryption Standard (AES) [17] encryptor. The AES output is then used as our ID sequence.

Recall that $B_c = \log_2 N_c$ and $B_s = \log_2 M$, where $N_c$ is the number of channels, and $M$ is the constellation size. We divide the source information into blocks of size $B_c$ and divide the ID sequence into blocks of size $B_s$. Denote the nth source information block and ID block as $X_n$ and $Y_n$, respectively. Let $f_{X_n}$ be the carrier frequency corresponding to $X_n$, and $s_n$ the symbol corresponding to ID bit-vector $Y_n$. It should be noted that the ID symbol is refreshed at each hopping period. The transmitted signal can then be represented as

$$s(t) = \sqrt{2Re}\sum_{n=-\infty}^{\infty} s_n g(t - nT_h) e^{j2\pi f_{X_n} t}$$

$$= \sqrt{2Re}\sum_{n=-\infty}^{\infty} \sum_{j=1}^{N_c} \alpha_{i,n}s_n g(t - nT_h) e^{j2\pi f_{j} t}, \quad (2)$$

where $T_h$ is the hop duration, $g(t)$ is the pulse shaping filter,

$$\alpha_{i,n} = \begin{cases} 1 & \text{if } f_{X_n} = f_i, \\ 0 & \text{otherwise.} \end{cases}$$
B. Receiver Design

The receiver structure for AJ-MDFH is shown in Fig. 4. For each hop, the received signal is first fed into the bandpass filter bank. The output of the filter bank is demodulated, and then used for carrier bits (i.e., the information bits) detection.

![AJ-MDFH receiver structure](image)

Fig. 4. AJ-MDFH receiver structure.

1) Demodulation: Let \( s(t) \) and \( J(t) \) denote the ID signal, the jamming and the noise, respectively. For AWGN channels, the received signal can be represented as

\[
r(t) = s(t) + J(t) + n(t). \tag{3}
\]

For \( i = 1, 2, \cdots, N_c \), the output of the \( i \)th ideal bandpass filter \( f_i(t) \) is \( r_i(t) = f_i(t) \cdot r(t) \). For demodulation, \( r_i(t) \) is first shifted back to the baseband, and then passed through a matched filter. At the \( i \)th hopping period, for \( i = 1, \cdots, N_c \), the sampled matched filter output corresponds to channel \( i \) can be expressed as

\[
r_{i,n} = \alpha_{i,n} s_{n} + \beta_{i,n} J_{i,n} + n_{i,n}, \tag{4}
\]

where \( s_{n}, J_{i,n} \) and \( n_{i,n} \) correspond to the ID symbol, the jamming interference and the noise, respectively; \( \alpha_{i,n}, \beta_{i,n} \in \{0, 1\} \) are binary indicators for the presence of ID signal and jamming, respectively. Note that the true information is carried in \( \alpha_{i,n} \).

2) Signal Detection and Extraction: Signal detection and extraction is performed for each hopping period. For notation simplicity, without loss of generality, we omit the subscript \( n \) in (4). That is, for a particular hopping period, (4) is reduced to:

\[
r_i = \alpha_i s + \beta_i J_i + n_i, \tag{5}
\]

Define \( r = (r_1, \cdots, r_{N_c}) \), \( \alpha = (\alpha_1, \cdots, \alpha_{N_c}) \), \( \beta = (\beta_1, \cdots, \beta_{N_c}) \), \( J = (J_1, \cdots, J_{N_c}) \) and \( n = (n_1, \cdots, n_{N_c}) \), then (5) can be rewritten in vector form as:

\[
r = s \alpha + \beta \cdot J + n. \tag{6}
\]

For single-carrier AJ-MDFH, at each hopping period, one and only one item in \( \alpha \) is nonzero. In this case, there are \( N_c \) possible information vectors: \( \alpha_1 = (1, 0, \cdots, 0), \alpha_2 = (0, 1, \cdots, 0), \cdots, \alpha_{N_c} = (0, 0, \cdots, 1) \). If \( \alpha_k \) is selected, and the binary expression of \( k \) is \( b_0 b_1 \cdots b_{B_c-1} \), with \( B_c = \lfloor \log_2 N_c \rfloor \), then the estimated information sequence is \( \hat{c} = b_0 b_1 \cdots b_{B_c-1} \).

At each hopping period, the information symbol \( \alpha_k \) or equivalently, the hopping frequency index \( k \), needs to be estimated based on the received signal and the secure ID information which can be regenerated at the receiver through the shared secret. When the input information vectors are equiprobable, that is, \( P(\alpha_i) = \frac{1}{N_c} \) for \( i = 1, 2, \cdots, N_c \), the MAP (maximum a posteriori probability) detector is reduced to the ML (maximum likelihood) detector. For the ML detector, the hopping frequency index \( \hat{k} \) can be estimated as:

\[
\hat{k} = \arg \max_{1 \leq i \leq N_c} Pr\{r|\alpha_i\}. \tag{7}
\]

When \( n_1, \cdots, n_{N_c}, J_1, \cdots, J_{N_c} \) are all statistically independent, \( r_1, \cdots, r_{N_c} \) are also independent. In this case, the joint ML detector in (7) can be decomposed as:

\[
\hat{k} = \arg \max_{1 \leq i \leq N_c} \prod_{j=1}^{N_c} Pr\{r_j|\alpha_i\} \nonumber
\]

\[
= \arg \max_{1 \leq i \leq N_c} \prod_{j=1, j \neq i}^{N_c} Pr\{r_j|\alpha_j = 0\} \cdot Pr\{r_i|\alpha_i = 1\} \nonumber
\]

\[
= \arg \max_{1 \leq i \leq N_c} \prod_{j=1}^{N_c} Pr\{r_j|\alpha_j = 0\} \cdot Pr\{r_i|\alpha_i = 1\} \tag{8}
\]

Since \( \prod_{j=1}^{N_c} Pr\{r_j|\alpha_j = 0\} \) is independent of \( i \), (8) can be further reduced to the likelihood ratio test

\[
\hat{k} = \arg \max_{1 \leq i \leq N_c} \frac{Pr\{r_i|\alpha_i = 1\}}{Pr\{r_i|\alpha_i = 0\}}, \tag{9}
\]

where

\[
Pr\{r_i|\alpha_i = 1\} = \sum_{\beta} Pr\{r_i|\alpha_i = 1, \beta\} P(\beta), \quad \text{and} \quad Pr\{r_i|\alpha_i = 0\} = \sum_{\beta} Pr\{r_i|\alpha_i = 0, \beta\} P(\beta),
\]

with \( \beta \in \{0, 1\} \). In the ideal case when \( \beta_i \) is known for \( i = 1, \cdots, N_c \), the ML detector above can be further simplified. If we assume that \( n_1, \cdots, n_{N_c} \) are i.i.d. circularly symmetric Gaussian random variables of zero-mean and variance \( \sigma_n^2 \), and \( J_1, \cdots, J_{N_c} \) are i.i.d. circularly symmetric Gaussian random variables of zero-mean and variance \( \sigma_J^2 \), then it follows from (5) and (9) that

\[
\hat{k} = \arg \max_{1 \leq i \leq N_c} \frac{||r_i||^2 - ||r_i - s||^2}{\sigma_i^2}, \tag{10}
\]

where \( \sigma_i^2 = \beta_i \sigma_J^2 + \sigma_n^2 \).

Note that \( \sigma_i^2 \) is generally unknown. If we replace the overall interference power \( \sigma_i^2 \) with the instantaneous power of the received signal \( ||r_i||^2 \), then it follows from (10) that:

\[
\hat{k} = \arg \min_{1 \leq i \leq N_c} \frac{||r_i - s||^2}{||r_i||^2}. \tag{11}
\]

For more tractable theoretical analysis, we can replace \( ||r_i||^2 \) with the average signal power observed in channel \( i \), \( P_i = E\{||r_i||^2\} \). Define \( Z_i = \frac{||r_i - s||^2}{\sqrt{P_i}} \), then we have

\[
\hat{k} = \arg \min_{1 \leq i \leq N_c} Z_i. \tag{12}
\]

Discussions: In the conventional FH, a frequency synthesizer is used at the receiver to capture the transmitted signal. The strict requirement on frequency synchronization turns out to be a significant challenge in FH system design, especially for fast hopping systems. In MDFH and AJ-MDFH, a bandpass filter bank is used to capture the hopping frequency. The complexity is similar to using multiple FSK receivers in parallel. It is observed that: (1) Comparing with conventional FH, MDFH based systems relax the frequency synchronization requirements.
problem. At the same time, we show that if a bandpass filter bank is used by an adversary, then the conventional FH signal as well as the PN sequence can be easily captured, making it fragile to follower jamming and resulting in total loss of the transmission. In AJ-MDFH, the encrypted information is transmitted through hopping frequency control, this is like using the one-time key pad, making it impossible for the adversary to launch follower jamming. (2) Comparing with FSK, which has zero capacity under disguised jamming, AJ-MDFH is much more efficient and robust under disguised jamming.

C. Extension to Multi-carrier AJ-MDFH

For more efficient spectrum usage and robust jamming resistance, in this section, we extend the concept of MDFH to multi-carrier AJ-MDFH (MC-AJ-MDFH). The idea is to split all the \( N_c \) channels into \( N_g \) non-overlapping groups, and each subcarrier hops within the assigned group based on the AJ-MDFH scheme. To ensure hopping randomness of all the subcarriers, the groups need to be reorganized or regenerated securely after a pre-specified period, named group period. A secure subgroup assignment algorithm can be developed as what we did in [27], to ensure that: (i) Each subcarrier hops over a new group of channels during each group period, so that it eventually hops over all the available channels in a pseudo-random manner; (ii) Only the legitimate receiver can recover the transmitted information correctly.

1) Multi-Carrier AJ-MDFH without Diversity: In this case, each subcarrier transmits an independent bit stream. The spectral efficiency of the AJ-MDFH system can be increased significantly. Let \( B_c = \log_2 N_c \) and \( B_g = \log_2 N_g \), then the number of bits transmitted by the MC-AJ-MDFH within each hopping period is \( B_{MC} = (B_c - B_g)N_g = (B_c - \log_2 N_g)N_g \). \( B_{MC} \) is maximized when \( B_g = B_c - 1 \) or \( B_g = B_c - 2 \), which results in \( B_{MC} = 2^{B_c - 1} \). Note that the number of bits transmitted by the AJ-MDFH within each hopping period is \( B_c \), it can be seen that \( B_{MC} > B_c \) as long as \( B_c > 2 \). Take \( N_c = 256 \) for example, then the transmission efficiency of AJ-MDFH can be increased by \( \frac{B_{MC}}{B_c} = 2^{\alpha_{\nu} - 1} \) times.

2) Multi-carrier AJ-MDFH with Diversity: Under multi-band jamming, diversity needs to be introduced to the AJ-MDFH system for robust jamming resistance. A natural solution to achieve frequency diversity is to transmit the same or correlated information through multiple subcarriers. The number of subcarriers needed to convey the same information varies in different jamming scenarios. Generally, the number of correlated signal subcarriers should not be less than the number of jammed bands. At the receiver, the received signals from different diversity branches can be combined for joint signal detection [28]–[30].

As will be shown in Section VI, MC-AJ-MDFH can increase the system efficiency and jamming resistance significantly through jamming randomization and frequency diversity. Moreover, by assigning different carrier groups to different users, MC-AJ-MDFH can also be used as a collision-free multiple access system.

IV. ID Constellation Design and its Impact on System Performance

For AJ-MDFH, ID signals are introduced to distinguish the true information channel from disguised channels invoked by jamming interference. In this section, we investigate ID constellation design and its impact on the performance of AJ-MDFH under various jamming scenarios.

A. Design Criterion and Jamming Classification

The general design criterion of the ID constellation is to *minimize the probability of error under a given signal power*. Under this criterion, the following questions need to be answered: (1) How does the size of the constellation impact the system performance? (2) How does the type or shape of the constellation influence the detection error? Which type should we use for optimal performance? In this section, we will try to address these questions under different jamming scenarios.

In literature, jamming has generally been modeled as Gaussian noise [18]–[20], referred as *noise jamming*. Recall that disguised jamming denotes the jamming interference which has similar power and spectral characteristics as that of the true signal. For AJ-MDFH, when the ID constellation is known to, or can be guessed by the jammer, the jammer can disguise itself by sending symbols taken from the same constellation over a different or fake channel. In this case, it could be difficult for the receiver to distinguish the true channel from the disguised channel, leading to high detection error probability. We refer to this kind of jamming as *ID jamming* or ID attack. ID jamming is the worst case disguised jamming for AJ-MDFH.

B. Constellation Design under Noise Jamming

Without loss of generality, we consider the case where the ID symbol is transmitted through channel 1, i.e.,

\[
\alpha = (\alpha_1, \ldots, \alpha_{N_c}) = (1, 0, \ldots, 0). \tag{13}
\]

Recall that for \( i = 1, \ldots, N_c \), \( r_i = \alpha_i s + \beta_i I_i + n_i \). Let \( \bar{n}_i = \beta_i I_i + n_i \), and denote its variance as \( \sigma_i^2 = \beta_i^2 \sigma_I^2 + \sigma_n^2 \), which may vary from channel to channel. Following the definition in (12), we have \( Z_1 = \frac{\|\bar{n}_i\|}{\sqrt{\|s\|^2 + \sigma_I^2}} \), and \( Z_i = \frac{\|\bar{n}_i - s\|}{\sigma_i} \) for \( 2 \leq i \leq N_c \). It can be seen that \( Z_1 \) is a Rayleigh random variable with probability density function (PDF)

\[
p_{Z_1}(z_1) = \frac{z_1}{\sigma^2} e^{-\frac{z_1^2}{2\sigma^2}}, \quad z_1 > 0, \tag{14}
\]

where \( \sigma^2 = \frac{\sigma_I^2}{2(\|s\|^2 + \sigma_I^2)} \). For \( 2 \leq i \leq N_c \), \( Z_i \) is a Rician random variable with PDF

\[
p_{Z_i}(z_i) = \frac{z_i}{\sigma^2} e^{-\frac{z_i^2 + \nu^2}{2\sigma^2}} I_0 \left( \frac{z_i \nu}{\sigma^2} \right), \quad z_i > 0, \tag{15}
\]

where \( \nu = \frac{\|s\|}{\sigma_I} \), \( \sigma = \frac{1}{\sqrt{2}} \), and \( I_0(x) \) is the modified Bessel function of the first kind with order zero.

According to (12), the carrier can be correctly detected if and only if \( Z_1 < Z_i \) for all \( 2 \leq i \leq N_c \). Assuming that
the symbols in constellation $\Omega$ are equally probable, then the carrier detection error probability is given by

$$P_e = 1 - \sum_{s \in \Omega} Pr\{Z_1 < Z_2, \ldots, Z_1 < Z_{N_c}\} p_S(s)$$

$$= 1 - \frac{1}{|\Omega|} \sum_{s \in \Omega} \int_0^\infty P_r(s, z_1) dz_1,$$

Note that $Z_2, \ldots, Z_{N_c}$ are i.i.d. Rician random variables, then it follows from (14) and (15) that

$$P_e = 1 - \frac{1}{|\Omega|} \sum_{s \in \Omega} \int_0^\infty Q_1 \left( \frac{\sqrt{2}}{\sigma_c} \right) \left( \frac{z_1}{\frac{1}{2} \sigma_c^2} \right) dz_1,$$

where $Q_1$ is the Marcum Q-function [31]. We have the following result:

**Proposition 1:** Assuming the true channel index is $k$. Under noise jamming, an upper bound of the carrier detection error probability $P_e$ can be obtained as:

$$P_{e}^{U} = \frac{1}{|\Omega|} \sum_{s \in \Omega} \left[ 1 - \left( 1 - \frac{\sigma_c^2}{|s|^2 + 2\sigma_c^2} \right) \sum_{k \neq s} e^{-\frac{|s|^2}{2\sigma_c^2}} \right]^{N_c - 1},$$

where $m = \arg \max\{ \sigma_c^2 \}$ for $1 \leq l \leq N_c, l \neq k$.

**Proof:** See Appendix A.

Assuming the true channel index is $k$, let $x = \frac{|s|^2}{\sigma_c^2}$ and

$$a(x) = 1 - \left( 1 - \frac{1}{2\pi} e^{-\frac{1}{2\pi} x^2} \right) e^{-\frac{1}{4\pi} x^2} N_c.$$

Then $P_{e}^{U}$ can be written as $P_{e}^{U} = a(x)$ with $\zeta = \frac{\sigma_c^2}{\sigma_m^2}$. Note that when $x \gg 1$, $a(x) \approx \frac{1}{x} e^{-\frac{1}{2} x}$ which is approximately $a(x)$. It can be shown that when $x \gg 1$, $a(x)$ is a convex function. By Jensen’s inequality [32], we have

$$P_{e}^{U} \approx \frac{1}{|\Omega|} \sum_{s \in \Omega} a\left( \frac{|s|^2}{\sigma_c^2} \right) \geq \frac{1}{|\Omega|} \frac{\sigma_c^2}{\sigma_m^2} \sum_{s \in \Omega} |s|^2$$

$$= a\left( \frac{\sigma_c^2}{\sigma_m^2} \right).$$

The equality is achieved if and only if $|s| = \sigma_c$ for all $s \in \Omega$. This implies that: under the condition that the signal to jamming and noise ratio over channel $k$ satisfies $|s|^2 \gg 1$, $P_{e}$ is approximately minimized when the constellation is constant modulus, that is, $|s|^2 = \sigma_c$ for all $s \in \Omega$.

An intuitive explanation for this result is that the signal power in constant modulus constellations always equals to the maximal signal power available. Moreover, it can be seen that $P_{e}^{U}$ is independent of the constellation size $|\Omega|$, but is only a function of $\sigma_c^2/\sigma_m^2$. Next, we will investigate how the constellation size affects the system performance under ID attacks.

**C. Constellation Design under ID Jamming**

Clearly, under ID attacks, the uncertainty of the ID symbol needs to be maximized. Under the assumption that all the symbols in a constellation $\Omega$ of size $M$ are all equally probable, then the average symbol entropy

$$H(s) = -\log_2 \frac{1}{|\Omega|} = \log_2 M \text{ bits}. \hspace{1cm} (19)$$

In the ideal case when the channel is noise-free, the optimal constellation size would be $M = \infty$. However, when noise is present, a larger $M$ also implies there is a larger probability for an ID symbol to be mistaken for its neighboring symbols. More specifically, we have the following result:

**Theorem 1:** For a given SNR and assuming PSK constellation is utilized, under ID jamming, the carrier detection error probability $P_e$ is a function of constellation size $M$ and

$$\lim_{M \to \infty} P_e(M) = \tilde{P}_e.$$

In other words, for any given $\epsilon > 0$, there always exists an $M_\epsilon$ such that for all $M > M_\epsilon$, $|P_e(M) - \tilde{P}_e| < \epsilon$.

The expression of $\tilde{P}_e$ and the proof of the theorem can be found in Appendix B. This theorem essentially says that: for a given SNR, due to the noise effect, increasing the constellation size over a threshold $M_\epsilon$ will result in little improvement in detection error probability. This result justifies the use of finite constellation in AJ-MDFH.

**V. Spectral Efficiency Analysis**

The spectral efficiency $\nu$ is defined as the ratio of the information bit rate $R_b$ to the transmission bandwidth $W_t$, i.e., $\nu = \frac{R_b}{W_t}$. In this section, we will analyze and compare the spectral efficiency of the existing and proposed frequency hopping schemes, including conventional FH, MDFH and (MC-)AJ-MDFH.

We start with the *single-user case*. Recall that $T_s$ and $T_h$ denotes the symbol period and the hopping duration, respectively; $N_h = T_s/T_h$ is the number of hops per symbol period. For fair comparison, we assume that all systems have: (i) The same number of available channels $N_c$; (ii) The same hopping period $T_h$ to ensure the hopping channels have the same total bandwidth $W_c = 2/T_h$; (iii) The same frequency spacing $\Delta f$ between two adjacent subcarriers, where $\Delta f \geq 1/T_h$. The bit rate of conventional FH can be calculated as $R_b = \frac{\log_2 M}{T_s}$, and the corresponding spectral efficiency can be obtained as $\nu = \frac{R_b}{W_t} = \frac{\log_2 M}{T_s N_h}$. The bit rate and spectral efficiency of other frequency hopping schemes can be obtained similarly. The results are listed in Table I.

**TABLE I**

<table>
<thead>
<tr>
<th>$R_b$ (b/s)</th>
<th>$\nu$ (b/s/Hz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>conventional FH</td>
<td>$\log_2 M/T_s N_h$</td>
</tr>
<tr>
<td>MDFH</td>
<td>$\frac{N_c R_b}{T_s N_h}$</td>
</tr>
<tr>
<td>AJ-MDFH</td>
<td>$R_b/T_s$</td>
</tr>
<tr>
<td>MC-AJ-MDFH</td>
<td>$\frac{M \log_2 M}{T_s N_h W_s}$</td>
</tr>
</tbody>
</table>

Next, we consider the more general *multiuser case*. The multiple access scheme for conventional FH, namely FHMA, was proposed in [6]. The multiple access extension of MDFH, denoted as E-MDFH, has been analyzed in [11]. Due to the variability in multiple access system design, a closed-form expression of the spectral efficiency is hard to obtain. Here we
compare the total information bits allowed to be transmitted by each system under the same BER and bandwidth requirements, and illustrate the spectral efficiency comparison through the following example.

Let \( N_u \) denote the number of users and we chose the number of channels be \( N_c = 64 \) (i.e., \( B_c = 6 \)). For MC-AJ-MDFH, we choose \( N_b = N_u = 4 \); For E-MDFH, we choose 8-PSK to modulate \( B_c = 3 \) ordinary bits and \( N_g = N_u = 4, N_h = 3 \). For FHMA, we choose 64-FSK modulation, \( N_h = 3 \), and consider \( N_u = 2, 3, 4 \), respectively. The required BER is \( 10^{-4} \). Fig. 5 depicts the performance of these multiuser systems. From Fig. 5a, it can be seen that both MC-AJ-MDFH and E-MDFH achieve the desired BER at \( \frac{E_b}{N_0} \approx 6.5\text{dB} \). From Fig. 5b, it can be observed that: due to severe collision effect among different users, FHMA can only accommodate up to 2 users at \( \frac{E_b}{N_0} \approx 6.5\text{dB} \) for the desired BER. In this particular example, the spectral efficiency of both MC-AJ-MDFH and E-MDFH are 4 times and 5 times that of FHMA.

Based on our analysis above, as well as the performance analysis of AJ-MDFH under various jamming attacks in Section VI, it can be shown that: while AJ-MDFH is much more robust than MDFH under various jamming attacks, its spectral efficiency is very close to that of MDFH, which is several times higher than that of conventional FH. A comprehensive capacity analysis for MDFH and AJ-MDFH under disguised jamming is provided in Part II of the paper [21].

VI. SIMULATION RESULTS

In this section, simulation examples are provided to illustrate the performances of the proposed AJ-MDFH and MC-AJ-MDFH schemes under various jamming scenarios. For all the systems considered in the following examples, we assume the total number of available channels is \( N_c = 64 \), that is, \( B_c = 6 \).

Example 1: Impact of the ID constellation size In this example, we consider the impact of the ID constellation size on the BER performance of AJ-MDFH under single-band ID jamming. From Fig. 6, it can be seen that in the ideal case where the system is noise-free, the BER performance of AJ-MDFH improves continuously as the constellation size increases. However, when noise is present, the BER converges once the constellation size reaches a certain threshold \( M_t \).

For example, for \( E_b/N_0 = 15\text{dB} \), we can choose \( M_t = 32 \). This example demonstrates the theoretical result in Theorem 1. Based on the result of Example 1, in the following examples, we choose to use 32-PSK to modulate the ID signal of AJ-MDFH and MC-AJ-MDFH.

Example 2: Performance comparison under single band jamming In this example, we consider both noise jamming and disguised jamming. SNR is taken as \( E_b/N_0 = 10\text{dB} \) and Jamming-to-Signal Ratio (JSR) is defined as the ratio of the jamming power to signal powers during one hopping period. For conventional FH, 4-FSK modulation scheme is used and we assume that the adjacent frequency tones in 4-FSK correspond to the center frequencies of the adjacent MDFH channels. For MDFH, QPSK is used to modulate ordinary bits and the number of hops per symbol period is \( N_h = 3 \). From Fig. 7, it can be observed that AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming, while remaining robust under noise jamming. Note that JSR=0dB under disguised jamming corresponds to the ID jamming for AJ-MDFH. It can also be seen that the performance of AJ-MDFH improves significantly when the jamming power differs from the signal power. This implies that uncertainty in the signal power is another dimension in combating ID jamming.

Example 3: Performance comparison under multi-band noise jamming and disguised jamming In this example,
For disguised jamming, the jammer takes symbols randomly from the same constellation as the ID signal. The jammed bands are selected independently and randomly. For MC-AJ-MDFH without diversity, the channels are divided into 32 groups to maximize the spectral efficiency; for MC-AJ-MDFH with diversity, each symbol is transmitted simultaneously over 4 subcarriers to achieve frequency diversity. The equal gain combination scheme is adopted for the joint detection metric at the receiver. From Fig. 8 and Fig. 9, it can be seen that MC-AJ-MDFH delivers much better performance than single carrier AJ-MDFH under multi-band jamming.

When noise is present, the detection error probability converges as the constellation size goes to infinity. Moreover, AJ-MDFH can be extended to MC-AJ-MDFH by allowing simultaneous multi-carrier transmission. With jamming randomization and enriched frequency diversity, MC-AJ-MDFH can increase the system efficiency and jamming resistance significantly, and can readily be used as a collision-free multiple access scheme.

**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 PROPOSITION 1**

It follows from (16) that

\[
P_e = 1 - \frac{1}{|\Omega|} \sum_{s \in \Omega} \frac{N_c}{2} \prod_{l=2}^{N_c} Q_1 \left( \frac{\sqrt{2}}{\sigma_l} \| s \|, \sqrt{2} z_1 \right) p_{Z_1}(z_1) dz_1
\]

where \( m = \arg \max_{2 \leq l \leq N_c} \{ \sigma_l^2 \} \). The inequality follows from the fact that for fixed \( \| s \| \) and \( z_1, Q_1 \left( \frac{\sqrt{2}}{\sigma_l} \| s \|, \sqrt{2} z_1 \right) \) is a monotonically decreasing function with respect to \( \sigma_l \). The equality can be achieved when \( \sigma_2 = \cdots = \sigma_{N_c} \).

Assume \( N_c \geq 2 \). For \( N_c = 2 \), it is easy to show that \( P_e = P^U_e \) with \( \sigma_m = \sigma_2 \). Note that for fixed \( s \) and \( \sigma_m, Q_1 \left( \frac{\sqrt{2}}{\sigma_2} \| s \|, \sqrt{2} z_1 \right) = Pr\{ Z_m > z_1 | s, z_1 = Z_1 \} \) is a function of \( z_1 \). For \( N_c > 2 \), \( f(x) = x^{N_c-1} \) is convex when \( x > 0 \). By Jensen’s inequality, we obtain

\[
\int_0^{\infty} Q_1^{N_c-1} \left( \frac{\sqrt{2}}{\sigma_m} \| s \|, \sqrt{2} z_1 \right) p_{Z_1}(z_1) dz_1
\]

which follows from (21). By Jensen’s inequality, we obtain

\[
\int_0^{\infty} Q_1^{N_c-1} \left( \frac{\sqrt{2}}{\sigma_m} \| s \|, \sqrt{2} z_1 \right) p_{Z_1}(z_1) dz_1
\]

According to (33), \( Pr\{ Z_1 < Z_m | s \} \) can be calculated as

\[
Pr\{ Z_1 < Z_m | s \} = 1 - \frac{\sigma^2}{\| s \|^2 + 2\sigma^2} e^{-\frac{\| s \|^2(\| s \|^2 + 2\sigma^2)}{\sigma^2(\| s \|^2 + 2\sigma^2)}} \]

Following (21)-(24),

\[
P_e \leq \frac{1}{|\Omega|} \sum_{s \in \Omega} \left[ 1 - \left( 1 - \frac{\sigma^2}{\| s \|^2 + 2\sigma^2} e^{-\frac{\| s \|^2(\| s \|^2 + 2\sigma^2)}{\sigma^2(\| s \|^2 + 2\sigma^2)}} \right)^{N_c-1} \right]
\]

where \( P^U_e \) for \( N_c > 2 \).

Overall, \( P_e \leq P^U_e \) for \( N_c \geq 2 \).
APPENDIX B
PROOF OF THEOREM 1

Note that the system is under ID attack. If the power of the M-ary PSK constellation is $P_s$, then the signal and jamming symbol can be written as $s = \sqrt{P_s}e^\frac{2\pi im}{M}$, $j = \sqrt{P_j}e^\frac{2\pi jm}{M}$ respectively, where $M = |\Omega|$ and $0 \leq m_s, m_j \leq M - 1$. Without loss of generality, we assume that: (i) Both the ID and jamming take the symbols in $\Omega$ with equal probability $1/M$; (ii) The signal is transmitted in channel 1 ($\alpha_1 = 1$) and channel $j$ is jammed ($\beta_j = 1$).

- When $j = 1$, jamming collides with the ID signal. In this case, $r_1 = s + J_1 + n_1$ and $r_l = n_l$ for $l = 2, \ldots, N_c$. We have $Z_1 = \frac{|s + J_1 + n_1|^2}{\sigma_v^2}$ and $Z_l = \frac{|n_l|^2}{\sigma_n^2}$, where $\sigma_v^2$ is the noise variance. The detection error probability in this case can be calculated as

$$P_{e1} = 1 - \frac{1}{M^2} \sum_{s \in \Omega} \sum_{J_1 \in \Omega} \int_0^\infty \left[ Pr\{z_1 < Z_2|s, J_1, z_1\}\right]^N_{-2} p_{Z_1}(z_1)dz_1. \quad (26)$$

Note that $Z_1$ is a Rician random variable with PDF $p_{Z_1}(z_1) = \frac{z_1}{\sigma_v^2}e^{-\frac{z_1^2}{2\sigma_v^2}}I_0 \left( \frac{2z_1}{\sigma_v} \right)$, where $\nu = \frac{\sqrt{M}}{\sigma_v}$, $\sigma^2 = \frac{\sigma_v^2}{2(\sigma_v^2 + \sigma_n^2)}$ and $Z_l$'s are i.i.d. Rician random variables with $\nu = \frac{\sqrt{M}}{\sigma_v}$, $\sigma^2 = \frac{1}{2}$. Then (26) can be written as in (27), where $\kappa \triangleq \mod (m_s - m_j, M)$ is uniformly distributed over $[0, M - 1]$.

- When $j = 2, \ldots, N_c$, jamming does not collide with ID signal. In this case, $r_1 = s + n_1$, $r_j = J_j + n_j$, and $r_l = n_l$ for $l = 2, \ldots, N_c, l \neq j$. We have $Z_1 = \frac{|s + n_1|^2}{\sigma_v^2}$, $Z_j = \frac{|J_j + n_j|^2}{\sigma_v^2}$ and $Z_l = \frac{|n_l|^2}{\sigma_n^2}$. The detection error probability in this case can be calculated as

$$P_{e2} = 1 - \frac{1}{M^2} \sum_{s \in \Omega} \sum_{J_1 \in \Omega} \int_0^\infty \left[ Pr\{Z_1 > z_1|s, J_1, z_1\}\right]^N_{-2} p_{Z_1}(z_1)dz_1. \quad (28)$$

Note that $Z_1$ is a Rayleigh random variable with PDF $p_{Z_1}(z_1) = \frac{z_1}{\sigma_v^2}e^{-\frac{z_1^2}{2\sigma_v^2}}$, where $\sigma^2 = \frac{\sigma_v^2}{2(\sigma_v^2 + \sigma_n^2)}$, $Z_j$ is a Rician random variable with $\nu = \frac{|J_j|^2}{\sigma_v^2}$, $\sigma^2 = \frac{\sigma_v^2}{2(\sigma_v^2 + \sigma_n^2)}$ and $Z_l$'s are i.i.d. Rician random variables with $\nu = \frac{\sqrt{M}}{\sigma_v}$, $\sigma^2 = \frac{1}{2}$. Then (28) can be written as in (29).

The overall detection error probability in noisy environment is given as

$$P_e = Pr\{j = 1\}P_{e1} + Pr\{2 \leq j \leq N_c\}P_{e2} = \frac{1}{N_c}P_{e1} + \frac{N_c - 1}{N_c}P_{e2}. \quad (30)$$

When $\frac{M}{\sigma_v^2}$ is fixed, it follows from (27) and (29) that $P_e$ is a function of $M$ given as

$$P_e = \frac{1}{M} \sum_{\kappa = 0}^{M-1} b \left( \frac{2\pi\kappa}{M} \right), \quad (31)$$

where $b(x)$ is given in (32). As $M$ approaches infinity, $P_e$ converges. In fact, we have,

$$\bar{P}_e = \lim_{M \to \infty} P_e = \lim_{M \to \infty} \sum_{\kappa = 0}^{M-1} b \left( \frac{2\pi\kappa}{M} \right) \cdot \frac{2\pi}{M} = \frac{1}{2\pi} \int_0^{2\pi} b(x)dx. \quad (33)$$

Note that $b(x)$ is the detection error probability when the angle between the signal symbol and the jamming symbol is $x$, hence $0 \leq b(x) \leq 1$ and we have

$$0 \leq \bar{P}_e = \frac{1}{2\pi} \int_0^{2\pi} b(x)dx \leq 1. \quad (34)$$

That is: $\forall \epsilon > 0$, there always exists an integer $M_\epsilon$ such that $\forall M > M_\epsilon$, $|P_e - \bar{P}_e| < \epsilon$. ■

REFERENCES


\[
P_{c1} = 1 - \frac{1}{[Ω]^2} \sum_{s \in Ω} \sum_{j \in J} \int_0^∞ Q_1^{N_c-1} \left( \frac{2T_p s}{\sigma_n}, \sqrt{2z_1} \right) 2z_1 \left\| s + J_j \right\|^2 + \sigma_n^2 \nabla^\top \frac{2z_1}{\sigma_n} \int_0^∞ \frac{\sigma_n^2}{(z_1^2 + P_s)} I_0 \left( \frac{2z_1}{\sigma_n^2} \sqrt{P_s \left( \left\| s + J_j \right\|^2 + \sigma_n^2 \right)} \right) dz_1 \\
= 1 - \frac{1}{M} \sum_{k=0}^{M-1} \int_0^∞ Q_1^{N_c-1} \left( \frac{2T_p s}{\sigma_n}, \sqrt{2z_1} \right) 2z_1 \left\| 2P_s \frac{1 + \cos \pi \kappa}{M} + P_s \frac{\sigma_n^2}{\sigma_n^2} \right) \frac{z_1^2}{P_s} I_0 \left( \frac{2z_1}{\sigma_n^2} \sqrt{2P_s \left( 1 + \cos \pi \kappa \right)} + P_s \frac{\sigma_n^2}{\sigma_n^2} \right) dz_1.
\]

\[
P_{c2} = 1 - \frac{1}{[Ω]^2} \sum_{s \in Ω} \sum_{j \in J} \int_0^∞ Q_1 \left( \frac{P_s + \sigma_n^2}{\sigma_n^2} \right) 2z_1 \left\| J_j - s \right\|, \frac{\sigma_n^2}{\sigma_n^2} \nabla^\top \frac{2z_1}{\sigma_n} \int_0^∞ \frac{\sigma_n^2}{(z_1^2 + P_s)} I_0 \left( \frac{2z_1}{\sigma_n^2} \sqrt{P_s \left( 1 - \cos \pi \kappa \right)} + P_s \frac{\sigma_n^2}{\sigma_n^2} \right) dz_1 \\
= 1 - \frac{1}{M} \sum_{k=0}^{M-1} \int_0^∞ Q_1 \left( \frac{P_s + \sigma_n^2}{\sigma_n^2} \right) 2z_1 \left\| 2P_s \frac{1 - \cos \pi \kappa}{M} + P_s \frac{\sigma_n^2}{\sigma_n^2} \right) \frac{z_1^2}{P_s} I_0 \left( \frac{2z_1}{\sigma_n^2} \sqrt{2P_s \left( 1 - \cos \pi \kappa \right)} + P_s \frac{\sigma_n^2}{\sigma_n^2} \right) dz_1.
\]

\[
b(x) = 1 - \frac{1}{N_c} \int_0^∞ Q_1^{N_c-1} \left( \frac{2T_p s}{\sigma_n}, \sqrt{2z_1} \right) 2z_1 \left\| 2P_s \frac{1 + \cos x}{\sigma_n^2} \right\|, \frac{\sigma_n^2}{\sigma_n^2} \nabla^\top \frac{2z_1}{\sigma_n} \int_0^∞ \frac{\sigma_n^2}{(z_1^2 + P_s)} I_0 \left( \frac{2z_1}{\sigma_n^2} \sqrt{2P_s \left( 1 + \cos x \right)} + P_s \frac{\sigma_n^2}{\sigma_n^2} \right) dz_1 \\
= \frac{N_c - 1}{N_c} \int_0^∞ Q_1 \left( \frac{P_s + \sigma_n^2}{\sigma_n^2} \right) 2z_1 \left\| P_s \left( 1 - \cos x \right) + \sigma_n^2 \right\|, \frac{\sigma_n^2}{\sigma_n^2} \nabla^\top \frac{2z_1}{\sigma_n} \int_0^∞ \frac{\sigma_n^2}{(z_1^2 + P_s)} I_0 \left( \frac{2z_1}{\sigma_n^2} \sqrt{2P_s \left( 1 - \cos x \right)} + P_s \frac{\sigma_n^2}{\sigma_n^2} \right) dz_1.
\]

[33] S. Stein, “Unified analysis of certain coherent and noncoherent binary
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.

Huahui Wang received his B.S. degree in Electronics from Peking University, China in 2001, and the M.Eng and Ph.D degrees in Electrical Engineering from National University of Singapore and Michigan State University in 2003 and 2006, respectively. Dr. Wang’s research interests involved various design aspects of wireless communication and networking, including PHY layer system design and MAC/higher lay protocol analysis. From 2007 to 2008, he worked as a research engineer in LG/Zenith Electronics and contributed to the standardization of the new mobile DTV systems for the United States. From 2009 to 2010, he worked as a Research Associate at Michigan State University working on cognitive radios and anti-jamming systems. In 2010, he joined AT&T Labs at Florham Park, NJ, where he is currently a Senior Member of Technical Staff. His main research activities are in the area of network planning and optimization for both UMTS and LTE systems.

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.