JAMMING RESISTANCE REINFORCEMENT OF MESSAGE-DRIVEN FREQUENCY HOPPING

Lei Zhang  Huahui Wang  Tongtong Li
Department of Electrical & Computer Engineering, Michigan State University, East Lansing, MI 48824, USA.
Email: {zangle3, wanghuah, tongli}@egr.msu.edu

Abstract—This paper considers spectrally efficient anti-jamming system design based on message-driven frequency hopping (MDFH). As a highly efficient frequency hopping scheme, MDFH is particularly robust under strong jamming. However, disguised jamming from sources of similar power strength can cause performance losses. To overcome this drawback, in this paper, we propose an anti-jamming MDFH (AJ-MDFH) system. The main idea is to transmit an 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. Therefore, it can be used by the receiver to locate the true carrier frequency or the desired channel. At the same time, it is computationally infeasible to be recovered by malicious users. Comparing with MDFH, AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming. Moreover, AJ-MDFH can be extended to a multi-carrier scheme for higher spectral efficiency and/or more robust jamming resistance. Simulation examples are provided to demonstrate the effectiveness of the proposed approaches.

Index Terms—Anti-jamming, physical layer security, message-driven frequency hopping.

I. INTRODUCTION

As a widely used spread spectrum technique, frequency hopping (FH) was originally designed for secure communication under hostile environments [1]. In conventional FH, each user hops independently based on its own PN sequence, a collision occurs whenever there are two users transmitting over a same frequency band. Mainly limited by the collision effect, the spectral efficiency of the conventional FH is very low [2].

Recently, an alternative approach, known as message-driven frequency hopping (MDFH) is proposed in [2], [3]. 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 the conventional FH. At the MDFH receiver, the carrier frequencies are captured using a filter bank which selects the strongest signals from all the frequency bands. The most significant property of MDFH is that, by embedding a large portion of information into the hopping selection process, additional information transmission is achieved with no extra cost on either bandwidth or power [2]. In fact, transmission through hopping frequency control essentially adds another dimension to the signal space, and the resulting coding gain can increase the system spectral efficiency by multiple times.

It is observed that when combined with jamming detection method, MDFH delivers excellent performance under strong jamming scenarios, and outperforms the conventional FH by big margins. The underlying argument is that: strong jamming can enhance the power of the jammed signal and hence increases the correct detection probability. When the system experiences disguised jamming, that is, when the jamming power is close to the signal power, it is difficult for the MDFH receiver to distinguish jamming from true signal, resulting in performance losses.

To improve the performance of MDFH under disguised jamming, 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 ID information is generated through a cryptographic algorithm using the shared secret between the transmitter and the receiver. Therefore, it can be used by the receiver to locate the true carrier frequency or the desired channel. At the same time, it is computationally infeasible to be recovered by malicious users. Comparing with MDFH, AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming and deliver significantly better results when the jamming power is close to that of the signal power. At the same time, it is robust under strong jamming just as MDFH. Moreover, AJ-MDFH can be extended to a multi-carrier scheme for higher spectral efficiency and/or more robust jamming resistance. Simulation examples are provided to demonstrate the effectiveness of the proposed approaches.

II. ANTI-JAMMING MDFH (AJ-MDFH) SYSTEM

To enhance the jamming resistance of MDFH under disguised jamming, in this section, we will introduce the anti-jamming MDFH system, named AJ-MDFH.

A. Transmitter Design

The main idea here is to insert some signal identification (ID) information during the transmission process. This ID information is shared between the transmitter and the receiver, therefore, it 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.

Without loss of generality, here we assume that $N_c$ be the total number of available channels, with $\{f_1, f_2, \cdots, f_{N_c}\}$ being the set of all available carrier frequencies. Without loss of generality, here we assume that $N_c = 2^{B_c}$ for an integer $B_c$. Let $\Omega$ be the selected constellation that consists of $M$ symbols, each symbol in the constellation represents $B_s = \log_2 M$ bits. Let $N_h$ be the number of hops in one ordinary symbol period. At each symbol period, MDFH transmits a block of length $L \triangleq N_h B_c + B_s$ bits. Each block contains $N_h B_c$ 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.

For AJ-MDFH, we propose to replace the ordinary bits in MDFH with the ID bits. The transmitter structure of AJ-MDFH is illustrated in Figure 1. As can be seen, each user is now assigned an ID sequence. Note that in MDFH, most information is transmitted as carrier bits through hopping frequency selection, and the same ordinary bits (represented using bit vector $Y_n$ in Figure 1) are...
transmitted at each hop. If we replace the ordinary bits with ID bits, the spectral efficiency is only reduced by a factor $\frac{\beta_s}{N_0+\beta_s}$.

It should be noted that, in order to prevent impersonation attack, each user's ID sequence needs to be kept secret from the malicious jammer. Therefore we generate the ID sequence through a reliable cryptographic algorithm, such as the Advanced Encryption Standard (AES) [4], so that it is computationally infeasible for the malicious user to recover the ID sequence. That is, we first generate a pseudorandom sequence using a linear shift feedback register, encrypt it using AES, and then take the AES output as our ID sequence.

As will be demonstrated in Section V, AJ-MDFH is robust under strong jamming, and can effectively reduce the performance degradation caused by disputed jamming. Note that jamming resistance of AJ-MDFH can be further improved through channel coding, which corrects the residue errors using controlled redundancy.

### B. Receiver Design

The receiver structure for AJ-MDFH is shown in Figure 2. The receiver regenerates the secure ID through the shared secret (including the initial vector, the LFSR information and the key).

![AJ-MDFH receiver structure](image)

**Fig. 2.** AJ-MDFH receiver structure.

For each hop, the received signal is first fed into the bandpass filter bank. The output of the filter bank is first demodulated, and then used for carrier bits (i.e., the information bits) detection.

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

$$r(t) = s(t) + J(t) + n(t).$$

We assume that $s(t)$, $J(t)$ and $n(t)$ are independent of each other. If the spectrum of $J(t)$ overlaps with the frequency band of $s(t)$, then the signal is jammed; otherwise, the signal is jamming-free. If $J(t)$ spreads over multiple channels, we have multi-band jamming; otherwise, we have single band jamming. Note that the true information is embedded in the index of the active carrier over which the ID signal $s(t)$ is transmitted.

For $i = 1, 2, \ldots, N_c$, the output of the $i$th ideal bandpass filter $f_i(t)$ is

$$r_i(t) = f_i(t) * r(t).$$

For demodulation, $r_i(t)$ is first shifted back to the baseband, and then passed through a matched filter. At the $n$th hopping period, for $i = 1, \ldots, N_c$, the sampled matched filter output corresponds to channel $i$ can be expressed as

$$r_{i,n} = \alpha_{i,n}s_n + \beta_{i,n}J_{i,n} + n_{i,n},$$

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 (3). That is, for a particular hopping period, (3) is reduced to:

$$r_i = \alpha_i s + \beta_i J_i + n_i, \quad \text{for } i = 1, \ldots, N_c. \quad (4)$$

Define $r = (r_1, \ldots, r_{N_c})$, $\vec{\alpha} = (\alpha_1, \ldots, \alpha_{N_c})$, $\vec{\beta} = (\beta_1, \ldots, \beta_{N_c})$, $J = (J_1, \ldots, J_{N_c})$ and $n = (n_1, \ldots, n_{N_c})$, then (4) can be rewritten in vector form as:

$$r = s\vec{\alpha} + \vec{\beta} \cdot J + n. \quad (5)$$

For single-carrier AJ-MDFH, at each hopping period, one and only one item in $\vec{\alpha}$ is nonzero. That is, there are $N_c$ possible information vectors: $\vec{\alpha}_1 = (1, 0, \ldots, 0)$, $\vec{\alpha}_2 = (0, 1, \ldots, 0)$, $\ldots$, $\vec{\alpha}_{N_c} = (0, 0, \ldots, 1)$. If $\vec{\alpha}_k$ is selected, and the binary expression of $k$ is $b_{k1} \cdots b_{k_{N_c}}$, with $B_c = \lfloor \log_2 N_c \rfloor$, then the estimated information sequence is $b_{k1} \cdots b_{k_{N_c}}$.

So at each hopping period, the information symbol $s\vec{\alpha}$, or equivalently, the hopping frequency index $k$, needs to be estimated based on the received signal and the ID information which is shared between the transmitter and the receiver. We start with the maximum likelihood (ML) detector. If the input information is equiprobable, that is, $p(\alpha_i) = \frac{1}{2}$ for $i = 1, 2, \ldots, N_c$, then the MAP detector is reduced to the ML detector. For the ML detector, the estimated hopping frequency index $\hat{k}$ is given by

$$\hat{k} = \arg \max_{1 \leq i \leq N_c} p(r|\vec{\alpha}_i). \quad (6)$$

Recall that the information signal, the ID signal, the jamming interference and the noise are independent to each other. Assume both the noise and the jamming interference are totally random, that is, $n_1, \ldots, n_{N_c}$, $J_1, \ldots, J_{N_c}$ are all statistically independent, then $r_1, \ldots, r_{N_c}$ are also independent. In this case, the joint ML detector in (6) can be decomposed as:

$$\hat{k} = \arg \max_{1 \leq i \leq N_c} \prod_{j=1}^{N_c} p(r_j|\alpha_j) = \arg \max_{1 \leq i \leq N_c} \prod_{j=1}^{N_c} p(r_j|\alpha_j = 0) \cdot p(r_j|\alpha_j = 1) \cdot p(r_j|\alpha_j = 0) \cdot p(r_j|\alpha_j = 1). \quad (7)$$

Since $\prod_{j=1}^{N_c} p(r_j|\alpha_j = 0)$ is independent of $i$, (7) can be further simplified as

$$\hat{k} = \arg \max_{1 \leq i \leq N_c} p(r_i|\alpha_i = 1) \cdot p(r_i|\alpha_i = 0), \quad (8)$$

where $p(r_i|\alpha_i = 1) = \sum_{\beta_j} p(r_i|\alpha_i = 1, \beta_i)p(\beta_i)$ and $p(r_i|\alpha_i = 0) = \sum_{\beta_j} p(r_i|\alpha_i = 0, \beta_i)p(\beta_i)$, with $\beta_i \in \{0, 1\}$. Define $\Lambda_i \triangleq \frac{p(r_i|\alpha_i = 1)}{p(r_i|\alpha_i = 0)}$, be likelihood ratio for channel $i$, then (8) can be rewritten as:

$$\hat{k} = \arg \max_{1 \leq i \leq N_c} \Lambda_i. \quad (9)$$

If we further assume that $n_1, \ldots, n_{N_c}$ are i.i.d. circularly symmetric complex Gaussian random variables of zero mean and variance $\sigma_n^2 = N_0$, and $J_1, \ldots, J_{N_c}$ are i.i.d. circularly symmetric complex Gaussian random variables of zero mean and variance $\sigma_J^2 = N_J$, then it follows from (4) and (8) that:

$$\hat{k} = \arg \max_{1 \leq i \leq N_c} \frac{p(\beta_i = 1)}{p(\beta_i = 0)} e^{\frac{|x_i - \bar{\alpha}_i|}{N_0}} + \frac{p(\beta_i = 1)}{p(\beta_i = 0)} e^{\frac{|x_i - \bar{\beta}_i|}{N_0+N_J}}.$$
If \( q = \sum_{i=1}^{N_c} \beta_i \) bands are jammed, then \( p(\beta_i = 1) = \frac{q}{N_c} \) and \( p(\beta_i = 0) = \frac{N_c-q}{N_c} \); and \( s \) is the ID symbol shared between the transmitter and the receiver.

When the jammed channel indexes are known, or equivalently, \( \beta_i \) is known for \( i = 1, \cdots, N_c \), then the ML detector above can be further simplified. Define \( N_i = \beta_i N_j + \tilde{N}_i \), then it follows from (9) that

\[
\hat{k} = \arg \max_{1 \leq i \leq N_c} \frac{\|r_i\|^2 - \|r_i - s\|^2}{N_i} \quad (11)
\]

However, in reality, jamming side information is generally unknown. Here we develop the following two suboptimal detectors. If we replace the overall interference power \( N_i \) in (11) with the instantaneous received signal power \( |r_i|^2 \), then it can be obtained that:

\[
\hat{k} = \arg \min_{1 \leq i \leq N_c} \|r_i - s\|^2 \quad (12)
\]

III. ID Constellation Design and Its Impact on System Performance

A. Design Criterion and Jamming Classification

For AJ-MDFH, ID signals are introduced to distinguish the true information channel from disguised channels invoked by jamming interference. The general design criterion of the ID constellation is to minimize the probability of error under a given signal power. Under this criterion, there are two 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 and which type should we use for optimal performance?

In this section, we will try to address these questions under different jamming scenarios.

Recall that for AJ-MDFH, the message signal is embedded in the index of the hopping frequency or channel. In the worst case if the ID is known to the jammers, or can be easily guessed by the jammers, then the jammers can disguise itself by sending the same ID symbol over a different or fake channel. In this case, it would be difficult for the receiver to distinguish the true channel from the disguised channel, leading to high detection error probability. We define this kind of jamming as **ID jamming** or ID attack. In literature, jamming has generally been modeled as Gaussian noise. We refer this kind of jamming as **noise jamming**.

B. Constellation Design Under Noise Jamming

Without loss of generality, we assume that during one hop the ID symbol is transmitted through channel \( i \), i.e., \( \alpha_1 = 1, \alpha_2 = \cdots = \alpha_{N_c} = 0 \). Recall that for \( i = 1, \cdots, N_c \), \( \eta_i = \alpha_i s + \beta_i \tilde{N}_i + \tilde{n}_i \). Define \( \bar{n}_i = \tilde{N}_i + \tilde{n}_i \), and denote the variance of \( \bar{n}_i \) as \( \bar{\sigma}_i^2 \). Under random noise jamming, \( \bar{\sigma}_i^2 \) varies from channel to channel.

Applying the metric defined in (12), we get \( Z_1 = \frac{|r_1|^2 - |s|^2}{\bar{\sigma}_1^2} \), and \( Z_i = \frac{|r_i|^2 - |s|^2}{\bar{\sigma}_i^2} \) for \( 2 \leq i \leq N_c \). It can be seen that \( Z_1 \) is a Rayleigh random variable with probability density function (pdf) \( p_{Z_1}(z_1) = \frac{z_1 e^{-z_1^2/2}}{\sqrt{2\pi} \bar{\sigma}_1^2} \), where \( \sigma_i^2 = \frac{\bar{\sigma}_i^2}{2|s|^2 + \bar{\sigma}_i^2} \). For \( 2 \leq i \leq N_c \), \( Z_i \) is a Rician random variable with pdf \( p_{Z_i}(z_i) = \frac{z_i e^{-z_i^2/2}}{\sigma_i^2} I_0 \left( \frac{\rho s^2}{\sigma_i^2} \right) \), where \( \nu = \frac{|s|^2}{\sigma_i^2} \), \( \sigma = \frac{1}{\sigma_i^2} \) and \( I_0(x) \) is the modified Bessel function of the first kind with order zero.

The carrier will 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

\[
p_e = 1 - \sum_{i \in \Omega} P(Z_1 < Z_i) = 1 - \sum_{i \in \Omega} \left( 1 - \frac{1}{|\Omega|^{|S|^2 + \sigma_i^2}} e^{-\rho s^2/2 \sigma_i^2} \right) N_c - 1,
\]

where \( \sigma_{max} = \max \{ \sigma_i^2 \} \) for \( 2 \leq i \leq N_c \). Let \( \rho = \sigma_i^2/\sigma_{max} \) and \( a(x) = 1 - (1 - \frac{x}{\sigma_i^2} e^{-x^2/2}) N_c - 1 \). It can be shown that: when \( x \gg 1 \), \( a(x) \) is a convex function of \( x \). Therefore, if \( \frac{|s|^2}{\sigma_i^2} \gg 1 \), we can apply the Jensen’s inequality to obtain

\[
p_e = 1 - \sum_{i \in \Omega} \left( 1 - \frac{1}{|\Omega|^{|S|^2 + \sigma_i^2}} \left( \frac{1}{|\Omega|^{|S|^2 + \sigma_i^2}} \right) a \right) = \left( \frac{P_e}{\sigma_i^2} \right),
\]

The equality is achieved if and only if \( |s|^2 = P_s \) for all \( s \in \Omega \), where \( P_s = \frac{1}{|\Omega|^{|S|^2 + \sigma_i^2}} \sum_{i \in \Omega} |s|^2 \).

That is, when the SNR is high enough, the upper bound of the detection error probability \( p_e \) is minimized when the constellation is constant modulus.

C. Constellation Design under ID Jamming

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

\[
H(s) = -\log_2 \frac{1}{|\Omega|} = \log_2 |\Omega| = \log M.
\]

In the ideal cases when the channel is noise-free, then we have that the optimal constellation size would be \( M = \infty \). However, when noise is present, larger \( M \) also implies there is a larger probability for an ID symbol to be mistaken for its neighboring symbols. More specifically, it can be shown that: for a given SNR and assuming PSK constellation is utilized, the carrier detection error probability \( p_e \) will converge to a limit \( \tilde{p}_e \) as constellation size \( M \) increases. That is, for any \( \varepsilon > 0 \), there always exists an \( M \) such that for all \( M > M_1 \), \( |p_e - \tilde{p}_e| < \varepsilon \).

IV. MULTI-CARRIER AJ-MDFH

For more efficient spectrum usage, we can extend the concept of MDFH to multi-carrier AJ-MDFH (MC-AJ-MDFH). The idea is to split all the \( N_c \) channels into \( N_c \) 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 after a pre-specified period, named group period. A secure group generation algorithm
can be developed as in [6], so that each subcarrier will hop over a new set of channels at the beginning of each group period.

1) Multi-carrier AJ-MDFH without diversity — each subcarrier transmits independent bit stream: In this case, 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 $B_{MC} = (B_c - 2)N_g + (B_g - \log_2 N_g)N_g$. $B_{MC}$ is maximized when $B_g = B_c - 1$ or $B_g = B_c - 2$, which results in $B_{MC} = 2B_c - 1$. 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 $\frac{B_{MC}}{B_c} = 2^{B_c - 1} = 16$ times.

We assume that jamming is random and equally distributed among all the groups. Then the overall carrier detection error probability $p_e$ of MC-AJ-MDFH is equal to that corresponding to each subcarrier $f_k$ for $k = 1, \ldots, N_g$. Let $p_{e,k}$ denote the carrier detection error probability corresponding to the $k$th subcarrier or the $k$th group, then we have $p_e = p_{e,k}$ and

$$p_{e,k} = p_{0,k} \cdot p_{\text{carrier detection}} \text{signal not jammed} + p_{1,k} \cdot p_{\text{incorrect carrier detection}} \text{signal jammed}, \quad (17)$$

where $p_{0,k}, p_{1,k}$ denote the probability that the $k$th carrier is jamming-free or jammed, respectively.

2) Multi-carrier AJ-MDFH with diversity — multiple subcarriers transmit the same or correlated information: In the multi-band jamming case, diversity needs to be introduced to the AJ-MDFH system for robust jamming resistance. A natural solution is to achieve frequency diversity by transmitting the same or correlated information through multiple subcarriers. The number of subcarriers needed to convey the same information differs in different jamming scenarios. Ideally, the number of correlated signal carriers should not be less than the number of jammed bands. Furthermore, for MC-AJ-MDFH with diversity, joint signal detection is generally applied for optimal performance.

V. SIMULATION RESULTS

In this section, we illustrate the performance of the proposed AJ-MDFH and MC-AJ-MDFH through simulation examples. We assume that the signal is transmitted through AWGN channels and experiences random jamming. The number of available channels is $N_c = 64$ ($B_c = 6$). The PSK modulation scheme is used for MDFH, AJ-MDFH and MC-AJ-MDFH while the BFSK modulation scheme is used for conventional FH.

Figure 3 illustrates the performance of the AJ-MDFH versus constellation size under single-band ID jamming. In this case, the spectral efficiency of AJ-MDFH is six times that of the conventional FH.

VI. CONCLUSION

In this paper, we proposed a highly efficient anti-jamming scheme AJ-MDFH based on message-driven frequency hopping. It was shown that AJ-MDFH is robust under strong jamming and can effectively reduce the performance degradation caused by disguised jamming. Moreover, AJ-MDFH can be extended to a multi-carrier scheme for higher spectral efficiency and/or more robust jamming resistance. The proposed approaches can be applied to both civilian and military applications for reliable communication under jamming interference.

REFERENCES


