Jamming Mitigation Techniques based on Message-Driven Frequency Hopping

Lei Zhang Jian Ren Tongtong Li
Department of Electrical & Computer Engineering
Michigan State University, East Lansing, Michigan 48824, USA.
Email: {zhangle3, renjian, 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, first, 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. It is then exploited by the receiver for effective signal detection and extraction. It is shown that AJ-MDFH is robust under strong jamming, and can effectively reduce the performance degradation caused by disguised jamming. Second, we extend AJ-MDFH to a multi-carrier scheme, named MC-AJ-MDFH, which can increase the system efficiency and jamming resistance significantly through jamming randomization and enriched frequency diversity. Moreover, by assigning different carriers to different users, MC-AJ-MDFH can readily be used as a collision-free multiple access system. Simulation examples are provided to demonstrate the performance of the proposed approaches.**

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 [2], 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 [3]. To improve the spectral efficiency, FH systems that exploit high-dimensional modulation scheme have been studied in the literature [4].

Recently, a *three-dimensional* modulation scheme, known as message-driven frequency hopping (MDFH) is proposed in [5]. 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. At the receiver, the received signal is captured by a filter bank and the carrier frequencies are determined through a carrier detection algorithm. 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 [3]. *In fact, transmission through hopping frequency control essentially adds another dimension to the signal space, thus increases the system spectral efficiency by multiple times.*

It is observed that: under single-band jamming, 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 correct detection. 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, first we propose a single-carrier 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. Second, we extend the single-carrier AJ-MDFH to multi-carrier AJ-MDFH (MC-AJ-MDFH). Based on secure group generation, MC-AJ-MDFH can increase the system efficiency and jamming resistance significantly through *jamming randomization* and enriched frequency diversity. Moreover, by assigning different carrier group to different users, MC-AJ-MDFH can also be used as a collision-free MDFH based multiple access system. Simulation examples are provided to demonstrate the effectiveness of the proposed approaches.

II. MDFH Brief Review

A. System Description

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. If N_c is a power of 2, then

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

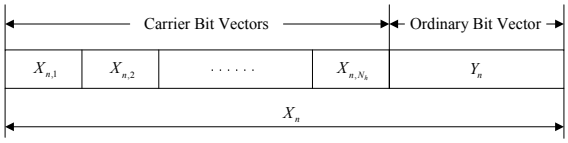
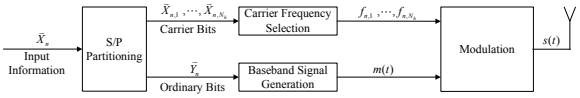


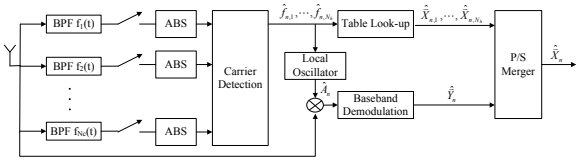
Fig. 1. The nth block of the information stream.

there exists a 1-1 map between the B_c-bit strings and the total available channels; otherwise, when N_c is not a power of 2, we will allow some B_c-bit strings to be mapped to more than one channel. Without loss of generality, here we assume that $N_c = 2^{B_c}$.

Let Ω 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 or equal to one.



(a) Transmitter structure



(b) Receiver structure

Fig. 2. Transmitter and receiver structure of MDFH. ABS means taking the absolute value.

The transmitter structure of MDFH is shown in Figure 2a. 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 Figure 1. Note that in MDFH, the whole block X_n is transmitted within one symbol period.

The receiver structure of MDFH is shown in Figure 2b, in which the transmitting frequency is captured using a filter bank as in the FSK receiver rather than using the frequency synthesizer. Recall that $\{f_1, f_2, \cdots, f_{N_c}\}$ is the set of all available carrier frequencies. To detect the active frequency band, a bank of N_c bandpass filters (BPF), each centered at f_i $(i = 1, 2, \cdots, N_c)$, and with the same channel bandwidth as the transmitter, is deployed at the receiver front end. In the case that only one frequency band is occupied at any given moment, we measure the outputs of bandpass filters at each possible carrier frequency, and the actual carrier frequency at a certain hopping period is detected by selecting the one that captures the strongest signal. As a result, the carrier frequency (hence the information embedded in frequency selection) can be blindly detected at each hop.

To further enhance the spectral efficiency, MDFH can be extended to a multi-carrier system where the subcarriers hop over non-overlapping subsets of the total available frequency bands [6]. The design of multi-carrier MDFH is not unique. Through careful hopping process design, multi-carrier MDFH can randomize jamming interference and enhance the jamming resistance of the system. This topic is further discussed in Section IV.

B. Performance of MDFH under Jamming Interference

When jamming spreads over multiple channels, we have multi-band jamming; otherwise, we have single-band jamming. In this section, we consider the performance of single-carrier MDFH under single-band jamming, as multi-band jamming is generally coped with multi-carrier diversity. For robust jamming resistance, the anti-jamming feature needs to be added to the MDFH receiver. Let P_i denote the received signal power over the ith channel. We propose to use the following threshold based carrier detection algorithm.

1) Classify each channel according to the power detection threshold η. If $P_i < \eta$, then there is only noise over channel i, we say that the channel is *inactive*; otherwise, if $P_i \geq \eta$, we say that the channel is *active*.
2) Let $A = \{i_1, i_2, \cdots, i_m\}$ be the set of the index of all the active channels, then the estimated hopping frequency index, denoted by $\hat{k}$, is determined by
$$\hat{k} = \arg\min_{i \in A} \{P_i\}. \quad (1)$$
The carrier bits can be recovered based on $\hat{k}$.
3) The ordinary bits are extracted from $r_{\hat{k}}$ following the regular demodulation process.

Let p_e denote the error probability of the hopping frequency index $\hat{k}$ detection in MDFH. As can be seen, p_e is a function of the threshold η. The optimal threshold value η_{opt} can be obtained as
$$\eta_{opt} = \arg\min_{\eta} \{p_e\}. \quad (2)$$

We compare the performance of MDFH under single-band jamming with that of the conventional FH in AWGN channels, and the result (with no channel coding) is shown in Figure 3. The jamming-to-signal ratio is defined as $JSR = \frac{N_J}{P_s}$, where N_J and P_s denote the jamming power and signal power, respectively. As can be seen, *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. Note that spectral efficiency of MDFH is $\frac{11}{3}$ times that of the conventional FH in this case.

However, we also notice that 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 unsatisfying performance. For the conventional FH, once

978-1-4244-4148-8/09/$25.00 ©2009

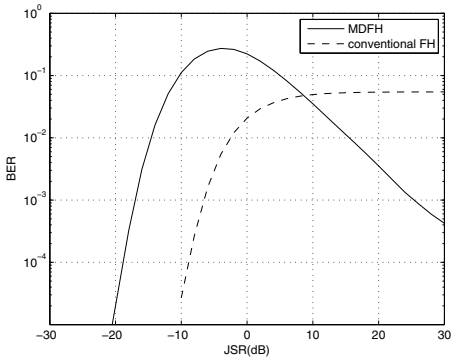


Fig. 3. Performance comparison under single-band jamming, $E_b/N_0 = 15$dB, $N_h = 3$. MDFH uses 16-QAM modulation and conventional FH uses 4-FSK modulation. In this case, the spectral efficiency of MDFH is roughly $\frac{11}{3}$ times that of the conventional FH.

the jamming power reaches a certain level, the system performance is mainly limited by the probability that signal is jammed. For MDFH, the situation is more complex. We classify the jamming into two categories: strong jamming and disguised jamming. Strong jamming denotes the case where the jamming power is much higher than the signal power. Disguised jamming denotes the case where the jamming power is close to the signal power. MDFH is robust under strong jamming, but is sensitive to disguised jamming. To enhance the jamming resistance of MDFH under disguised jamming, in this paper, we introduce the anti-jamming MDFH system, named AJ-MDFH.

III. AJ-MDFH: System Description

In this section, we describe the transmitter and receiver design of the proposed AJ-MDFH scheme.

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 so that it can be used by the receiver to locate the true carrier frequency. Our design goal is to reinforce jamming resistance while maximizing the spectral efficiency of MDFH.

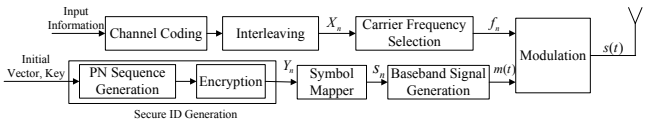


Fig. 4. AJ-MDFH transmitter structure.

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 4. As can be seen, each user is now assigned an ID sequence. Note that in MDFH, the same ordinary bits are transmitted at each hop. If we replace the ordinary bits with ID bits, the spectral efficiency is only reduced by a small factor $\frac{B_s}{N_h B_c + B_s}$. Take $N_h = 5, B_c = 8, B_s = 4$, for example, $\frac{B_s}{N_h B_c + B_s} = \frac{1}{11}$.

It should be noted that, in order to prevent impersonate attack, each user's ID sequence need 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) [7], so that it is computationally infeasible for the malicious user to recover the ID sequence. For the same reason, in AJ-MDFH, the ID bits will be varying at each hop. The ID sequence generation process is summarized as follows:

1) Generate a pseudo-random binary sequence using a 42-bit linear feedback shift register (LFSR) specified by the characteristic polynomial

$$\begin{aligned} &x^{42} + x^{35} + x^{33} + x^{31} + x^{27} + x^{26} + x^{25} \\ &+x^{22} + x^{21} + x^{19} + x^{18} + x^{17} + x^{16} \\ &+x^{10} + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1. \end{aligned} \tag{3}$$

2) Take the output of LFSR as the plaintext, group it into blocks of length K_L bits ($K_L = 128, 192$ or 256), and feed it into the AES encrypter of key size K_L. The AES output is then used 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 disguised jamming. It will also be observed 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 5. The receiver regenerates the secure ID through the shared secret (including the initial vector, the LFSR information and the key). At each hop, the received signal is first fed into

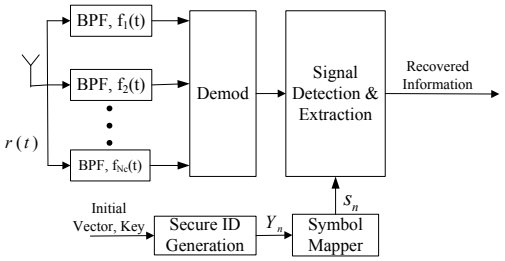


Fig. 5. AJ-MDFH receiver structure.

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

$$r(t) = s(t) + J(t) + n(t). \tag{4}$$

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

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*. Note that the true information is embedded in the index of the active carrier over which the ID signal $s(t)$ is transmitted.

For $i = 1, 2, \cdots, N_c$, the output of the ith ideal bandpass filter $\mathrm{f}_i(t)$ is

$$\begin{aligned} r_i(t) &= \mathrm{f}_i(t) * r(t) \\ &= \alpha_i(t)s(t) + J_i(t) + n_i(t). \end{aligned} \quad (5)$$

Here $\alpha_i(t) \in \{0, 1\}$ is a binary indicator for the presence of signal in channel i at time instant t. At each hopping period, $\alpha_i(t)$ is a constant: $\alpha_i(t) = 1$ if and only if $s(t)$ is transmitted over the ith channel during the mth hopping period; otherwise, $\alpha_i(t) = 0$. $J_i(t) = \mathrm{f}_i(t) * J(t)$ and $n_i(t) = \mathrm{f}_i(t) * n(t)$. When there is no jamming presented in the ith channel, $J_i(t) = 0$.

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

$$r_{i,m} = \alpha_{i,m}s_m + \beta_{i,m}J_{i,m} + n_{i,m}, \quad (6)$$

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

2) Signal Detection and Extraction: Signal detection and extraction is performed at each hopping period. *For notation simplicity, without loss of generality, we omit the subscript m in (6).* That is, for a particular hopping period, (6) is reduced to:

$$r_i = \alpha_i s + \beta_i J_i + n_i, \quad \text{for } i = 1, \cdots, N_c. \quad (7)$$

Define $\mathbf{r} = (r_1, \ldots, r_{N_c})$, $\vec{\alpha} = (\alpha_1, \ldots, \alpha_{N_c})$, $\vec{\beta} = (\beta_1, \ldots, \beta_{N_c})$, $\mathbf{J} = (J_1, \ldots, J_{N_c})$ and $\mathbf{n} = (n_1, \ldots, n_{N_c})$, then (7) can be rewritten in vector form as:

$$\mathbf{r} = s\vec{\alpha} + \vec{\beta} \cdot \mathbf{J} + \mathbf{n}, \quad (8)$$

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:

$$\begin{aligned} \vec{\alpha}_1 &= (1, 0, \ldots, 0); \\ \vec{\alpha}_2 &= (0, 1, \ldots, 0); \\ \vdots &= \quad \vdots \\ \vec{\alpha}_{N_c} &= (0, 0, \ldots, 1). \end{aligned}$$

If $\vec{\alpha}_k$ is selected, and the binary expression of k is $b_0 b_1 \cdots b_{B_c}$, with $B_c = \lfloor \log_2 N_c \rfloor$, then the estimated information sequence is $b_0 b_1 \cdots b_{B_c}$.

So at each hopping period, the information symbol $\vec{\alpha}$, 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. Here we use the *maximum likelihood* (ML) detector. If the input information is equiprobable, that is, $p(\alpha_\mathbf{i}) = \frac{1}{N_c}$ 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

$$\hat{k} = \arg \max_{1 \le i \le N_c} p\{\mathbf{r}|\vec{\alpha}_i\}. \quad (9)$$

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 (9) can be decomposed as:

$$\begin{aligned} \hat{k} &= \arg \max_{1 \le i \le N_c} \prod_{j=1}^{N_c} p\{r_j|\vec{\alpha}_i\} \\ &= \arg \max_{1 \le i \le N_c} \prod_{j=1, j \ne i}^{N_c} p\{r_j|\alpha_j = 0\} \cdot p\{r_i|\alpha_i = 1\} \\ &= \arg \max_{1 \le i \le N_c} \prod_{j=1}^{N_c} p\{r_j|\alpha_j = 0\} \cdot \frac{p\{r_i|\alpha_i = 1\}}{p\{r_i|\alpha_i = 0\}}. \end{aligned} \quad (10)$$

Since $\prod_{j=1}^{N_c} p\{r_j|\alpha_j = 0\}$ is independent of i, (10) can be further simplified as

$$\hat{k} = \arg \max_{1 \le i \le N_c} \frac{p\{r_i|\alpha_i = 1\}}{p\{r_i|\alpha_i = 0\}}, \quad (11)$$

where $p\{r_i|\alpha_i = 1\} = \sum_{\beta_i} p(r_i|\alpha_i = 1, \beta_i)p(\beta_i)$ and $p\{r_i|\alpha_i = 0\} = \sum_{\beta_i} p(r_i|\alpha_i = 0, \beta_i)p(\beta_i)$, 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 (11) can be rewritten as:

$$\hat{k} = \arg \max_{1 \le i \le N_c} \Lambda_i. \quad (12)$$

If we further assume that $n_1, \ldots, n_{N_c}$ are i.i.d. Gaussian random variables of zero mean and variance $\sigma_n^2 = \frac{N_0}{2}$, and $J_1, \ldots, J_{N_c}$ are i.i.d. Gaussian random variables of zero mean and variance $\sigma_J^2 = \frac{N_J}{2}$, then it follows from (7) and (11) that:

$$\hat{k} = \arg \max_{1 \le i \le N_c} \frac{\frac{p\{\beta_i=0\}}{\pi N_0} e^{-\frac{\|r_i - s\|^2}{N_0}} + \frac{p\{\beta_i=1\}}{\pi(N_0+N_J)} e^{-\frac{\|r_i - s\|^2}{N_0+N_J}}}{\frac{p\{\beta_i=0\}}{\pi N_0} e^{-\frac{\|r_i\|^2}{N_0}} + \frac{p\{\beta_i=1\}}{\pi(N_0+N_J)} e^{-\frac{\|r_i\|^2}{N_0+N_J}}}. \quad (13)$$

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.

In the case of successive *multi-band jamming*, as in partial-band jamming, $J_1, \ldots, J_{N_c}$ are no longer statistically independent, and hence the joint detector in (9) can no longer be decomposed as in (11). To resolve this problem, in the following section, we propose the multi-carrier AJ-MDFH scheme by exploiting rich frequency diversity. The multicarrier AJ-MDFH can ensure much better jamming resistance and spectral efficiency through successful jamming randomization.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

IV. MULTI-CARRIER AJ-MDFH

The multi-carrier AJ-MDFH (MC-AJ-MDFH) transmitter is illustrated in Fig.6. The basic idea is to split all the N_c channels into N_g non-overlapping groups, denoted by $G_l, l = 1, 2, \ldots, N_g$. The lth subcarrier hops over group G_l based on the AJ-MDFH scheme. To maximize hopping randomness of all the subcarriers, the channel 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 [5] 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. Secure G_l generation is synchronized at the transmitter and the receiver. At the receiver, the received signal is fed to N_g single-carrier AJ-MDFH receiver for signal extraction and recovery.

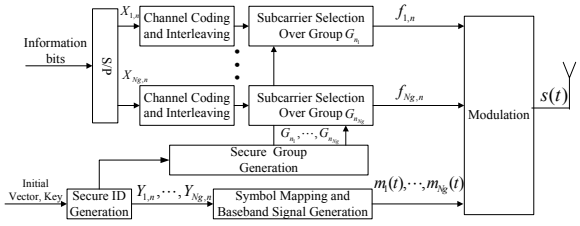


Fig. 6. Transmitter structure of MC-AJ-MDFH.

A. Increased Spectral Efficiency

With simultaneous transmission from multiple carriers, 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 each group has $N_{gc} = 2^{B_c - B_g}$ carriers. The number of bits transmitted by the MC-AJ-MDFH within each hopping period is $B_{MC} = N_g(B_c - B_g)$. 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 up to $\frac{B_{MC}}{B_c} = \frac{2^{B_c-1}}{B_c} = 16$ times.

B. Enhanced Jamming Resistance

MC-AJ-MDFH can reinforce the jamming resistance of AJ-MDFH significantly through jamming randomization and increased frequency diversity. As we mentioned earlier, multi-band jamming is a serious challenge for single-carrier AJ-MDFH. However, with secure group generation, MC-AJ-MDFH can successfully randomize multi-band jamming, just in the way that burst errors are randomized by interleavers. If all together q bands are jammed, then on average, only $\frac{q}{N_g}$ bands are jammed within each group.

To further increase the jamming resistance of MC-AJ-MDFH under multi-band jamming, the frequency diversity of the system can be increased by transmitting the same or correlated information over more than one subcarriers. At the receiver, the received signal corresponding to each subcarrier can be combined for joint signal detection. Note that different subcarrier may transmit different ID symbols, the conventional diversity combination methods can not be applied directly [8]. So instead of combining the received signal, we will combine the likelihood ratio Λ (see (12) in Section III-B2) of the channels corresponding to each subcarrier.

Assume that the same information is transmitted through the hopping frequency index of N_d subcarriers over N_d groups $\{G_{n_1}, G_{n_2}, \ldots, G_{n_{N_d}}\}$. As before, each group has N_{gc} channels. That is, the information is transmitted over the same hopping frequency index in each group. Note that for randomization purpose, the channel index in each group is random, and does not necessarily come in ascending or descending order.

Let Λ_i^l denote the likelihood ratio of channel i in group n_l, then the active hopping frequency index can be estimated by

$$\hat{k} = \arg \max_{1 \le i \le N_{gc}} \prod_{l=1}^{N_d} \Lambda_i^l, \tag{14}$$

The diversity order N_d can be dynamic in different jamming scenarios to achieve tradeoff between performance and efficiency.

C. Multi-carrier AJ-MDFH based multiple access scheme

MC-AJ-MDFH can readily be extended to a collision-free anti-jamming MDFH scheme to accommodate more users in the multiple access environment. To ensure collision-free multiple access among all users, different users will be assigned to different subcarriers. The number of subcarriers assigned to each user can be different based on the data rate and QoS requirement of the user. The secure group generation algorithm ensures the randomness of the subcarrier frequencies occupied by each user.

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 hostile jamming. The number of available channels is $N_c = 64$ ($B_c = 6$). For AJ-MDFH and MC-AJ-MDFH, we choose to use a two-level 16-QAM which has a circular star constellation, where each level has 8 symbols. For conventional FH, we use the 4-FSK modulation scheme.

Example 1 We first look at the performance of AJ-MDFH versus different JSR levels under single-band jamming. The SNR is chosen to be $\frac{E_b}{N_0} = 15$dB. From Figure 7, it can be observed that, in comparing with MDFH, AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming. At the same time, it is robust under strong jamming just as MDFH. When channel coding is applied (here we adopt the rate-$2/3$ turbo code [9]), the performance can be improved significantly. In this example, the spectral efficiency

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

of the single-band AJ-MDFH is three times higher than that of the conventional FH.

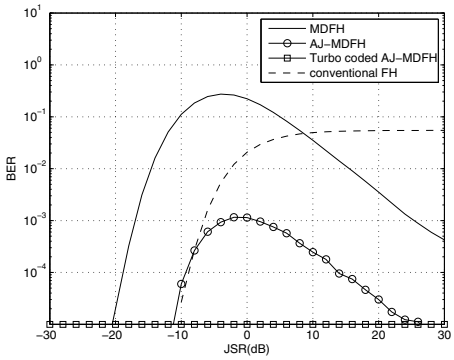
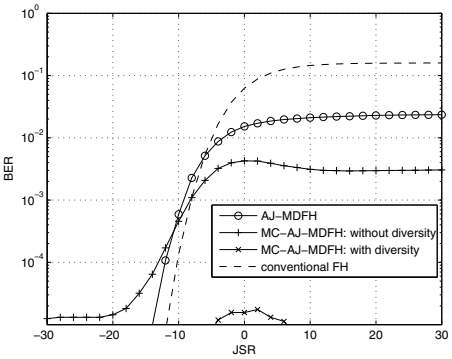


Fig. 7. Performance comparison under single-band jamming, $N_C = 64, E_b/N_0 = 15$dB. In this case, the spectral efficiency of AJ-MDFH is three times that of the conventional FH.

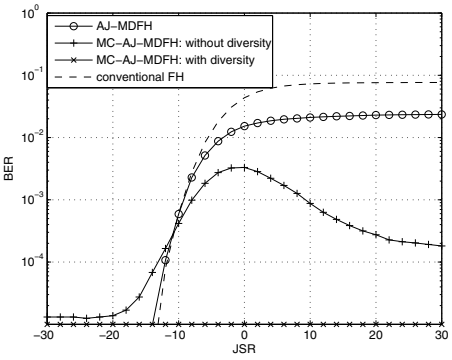
Example 2 This example examines the performance of AJ-MDFH, MC-AJ-MDFH and conventional FH under random and successive four-band jamming, respectively. The SNR is also chosen to be $\frac{E_b}{N_0} = 15$dB. To maximize the spectral efficiency of MC-AJ-MDFH, the group number is chosen to be $N_g = 32$. By "MC-AJ-MDFH without diversity", we mean that each subcarrier transmits independent information. In this example, the spectral efficiency of MC-AJ-MDFH (without diversity) is $16/3$ times that of the single-carrier AJ-MDFH, and 16 times that of the conventional FH, as each symbol in the single-carrier AJ-MDFH stands for 6 bits, and each symbol in MC-AJ-MDFH is only one bit, but the information is transmitted through 32 subcarriers simultaneously. By "MC-AJ-MDFH with diversity", we mean that the same information is transmitted over two subcarriers. As a result, in this particular case, the spectral efficiency MC-AJ-MDFH with $N_d = 2$ is $8/3$ times that of the single-carrier AJ-MDFH and 8 time that of the conventional FH. Figure 8a and 8b illustrate the performance of the these systems under random and successive four-band jamming, respectively. It can be seen that MC-AJ-MDFH can successfully randomize successive multi-band jamming, resulting in significantly better performance. And as expected, increased frequency diversity effectively enhances the jamming resistance of the system.

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 MC-AJ-MDFH by allowing simultaneous multi-carrier transmission. MC-AJ-MDFH can increase the system efficiency and jamming resistance significantly through jamming randomization and enriched frequency diversity. Moreover, by assigning different carriers to different users, MC-AJ-MDFH can readily be used as a collision-free multiple access system.



(a) Random band jamming



(b) Successive band jamming

Fig. 8. Performance comparison of AJ-MDFH, MC-AJ-MDFH and conventional FH under four-band jamming. $N_C = 64, N_g = 32, E_b/N_0 = 15$dB. In this case, the spectral efficiency of MC-AJ-MDFH without and with diversity are 16 and 8 times that of the conventional FH, respectively.

References

[1] M. Simon and A. Polydoros, "Coherent detection of frequency-hopped quadrature modulations in the presence of jamming–part I: QPSK and QASK modulations," *IEEE Trans. Commun.*, vol. 29, pp. 1644–1660, Nov 1981.

[2] A. Viterbi, "A processing-satellite transponder for multple access by low rate mobile users," *IEEE J. Sel. Areas Commun.*, Oct 1978.

[3] Q. Ling, J. Ren, and T. Li, "Spectrally efficient spread spectrum system design: message-driven frequency hopping," *Proc. IEEE Intl. Conf. Commun.*, pp. 4775–4779, May 2008.

[4] S. Glisic, Z. Nikolic, N. Milosevic, and A. Pouttu, "Advanced frequency hopping modulation for spread spectrum WLAN," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 1, pp. 16–29, Jan 2000.

[5] T. Li, Q. Ling, and J. Ren, "A spectrally efficient frequency hopping system," *Proc. IEEE Global Telecommun. Conf.*, pp. 2997–3001, Nov. 2007.

[6] Q. Ling and T. Li, "Message-driven frequency hopping‖ design and analysis," *IEEE Trans. Wireless Commun.*, accepted.

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

[8] J. Lee, R. French, and L. Miller, "Probability of error analyses of a BFSK frequency-hopping system with diversity under partial-band jamming interference–part I: Performance of square-law linear combining soft decision receiver," *IEEE Trans. Commun.*, vol. 32, no. 6, pp. 645–653, Jun 1984.

[9] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: turbo-codes," *IEEE Trans. Commun.*, vol. 44, pp. 1261–1271, Oct. 1996.

978-1-4244-4148-8/09/$25.00 ©2009