Modeling And Detection Of Hostile Jamming In Spread Spectrum Systems

Qi Ling and Tongtong Li
Department of Electrical & Computer Engineering
Michigan State University, East Lansing, Michigan 48824, USA.

Abstract—Along with the rapid prevalence of wireless communications, security has become an urgent issue. Due to the lack of a protective physical boundary, wireless information transmission is subjected to hostile jamming attacks, in which the malicious users deliberately interfere the authorized users signal through various jamming techniques. It is crucial to study the essential characteristics of commonly used hostile jamming attacks, so as to distinguish malicious jamming from noise and the self-jamming effect caused by multipath propagation. This paper is focused on the modeling and detection of hostile jamming in spread spectrum systems. First, a general two-dimensional model was proposed to characterize jamming signals from both the time domain and the frequency domain. Second, the model is studied closely and refined for spread spectrum systems, including both frequency hopping and direct sequence spread spectrum systems. Third, jamming detection methods based on both the statistical hypothesis test and the measurement/calculation of power spectral density of the received signal are proposed. Finally, simulation examples are provided to illustrate the effectiveness of the proposed approaches.

I. INTRODUCTION

As people are relying more and more on wireless communications for critical information transmission, concern over the security problem has been high. Due to lack of a protective physical boundary, wireless communication, which goes through the open air, is subjected to lower layer attacks and is facing much more significant security challenges than its wired counterpart. One of the most commonly used techniques for limiting the effectiveness of an opponent’s communications is referred to as jamming. Generally, intentional jamming intends to disable the legitimate transmission by saturating the receiver with noise or false information through deliberate radiation of radio signals, and thus significantly decreases the signal-to-noise-plus-interference ratio (SNIR).

Hostile jamming can be broadly categorized into two classes: band-jamming, in which the jamming signal is modeled as a zero-mean wide sense stationary Gaussian random process with a flat power spectral density (PSD) over the bandwidth of interest; tone-jamming [1], [2], where the jamming power is concentrated around the carrier frequency. In literature, band-jamming is further classified into wideband [3], [4], partial-band [5], [6] and partial-time [7], [8].

A considerable amount of work, see [9]–[11] for example, has been dedicated to the evaluation of the performance for a particular anti-jamming algorithm, in which the jamming model is assumed to known and invariant during the signal transmission period. In practice, however, the jammer may very likely switch frequently from one pattern to another, with each jamming pattern only lasts a very short period of time, in order to deliberately malfunction the anti-jamming module. Jamming pattern detection, therefore, is particularly important in the sense that the transmitter can be dynamically adjusted to combat time-variant hostile jamming.

The paper is organized as follows: In Section II, we introduce a general two-dimensional jamming model, which contains all the existing patterns as special cases. In Sections III and IV, we refine this model for spread spectrum systems, including both frequency hopping and direct-sequence CDMA. Jamming detection methods based on statistical hypothesis test and calculation of the power spectral density of the received signal are discussed in Section V. In Section VI, simulation examples are provided to demonstrate the effectiveness of the general jamming model and jamming detection method.

II. A GENERAL JAMMING MODEL

The received signal from an AWGN channel can be represented by

\[ r(t) = s(t) + n(t) + J(t) \]  

(1)

where \( s(t) \) is the interference-free signal, \( n(t) \) is additive zero mean white Gaussian noise with one-sided power spectral density \( N_0 \), and \( J(t) \) represents the intentional jamming signal.

We model the jamming signal \( J(t) \) as the output of a time-varying jamming generating system represented by

\[ J(t) = \int_{-\infty}^{\infty} G(t,\tau)x(t-\tau)d\tau, \]  

(2)

where \( x(t) \) is the input signal and \( G(t,\tau) \) is the channel response of the jamming system at instant \( t \) to an impulse applied at time \( t-\tau \). Limited by the size and capability of the jamming generation device, the total jamming power is finite, denoted by \( P_G \).

Let \( S_G(t, f) \) be the time-varying power spectrum density of \( G(t,\tau) \). Define \( f_0 \) and \( f_1 \) as the start and ending frequencies of the available band, and let \([t_0, t_1]\) be the time duration of the message signal.

If \( S_G(t, f) = \frac{P_G}{f_1-f_0} \Delta f \), \( \forall f \in [f_0, f_1], \forall t \in [t_0, t_1] \), then \( J(t) \) with PSD \( S_G(t, f) \) is reduced to the traditional wideband jamming model as a white Gaussian process whose power spectral density is flat over the entire bandwidth.

If \( S_G(t, f) = P_G \delta(f-f_k) \), \( \forall t \in [t_0, t_1] \), where \( f_k \in [f_0, f_1] \), then \( J(t) \) with PSD \( S_G(t, f) \) becomes an ideal single-
tone jamming with all the power accumulated on a particular frequency \( f_k \). Similar definitions can be extended to multi-tone jamming in a straightforward way.

If \( S_G(t,f) \) is a rectangular pulse along the \( f \)-axis and not varying along the \( t \)-axis from \( t_0 \) to \( t_1 \), i.e.,

\[
S_G(t,f) = \left\{ \begin{array}{ll}
0, & \text{if } f \in [f_0, f_1) \text{ or } f \in (f_j, f_1], \\
n_0, & \text{if } f \in [f_i, f_j],
\end{array} \right.
\]

where \( f_i \) and \( f_j \) with \( f_i \leq f_j \) are certain intermediate frequencies within \([f_0, f_1]\), \( \rho_f = \frac{f_i-f_f}{f_j-f_0} \) implies the fraction of the bandwidth being jammed, then \( J(t) \) is a typical partial-band jamming.

Alternatively, if \( S_G(t,f) \) is a rectangular pulse along the \( t \)-axis during \( t_0 \) and \( t_1 \) and invariant along the \( f \)-axis within \([f_0, f_1]\),

\[
S_G(t,f) = \left\{ \begin{array}{ll}
0, & \text{if } t \in [t_0, t_m) \text{ or } t \in (t_m, t_1], \\
n_0, & \text{if } t \in [t_m, t_1],
\end{array} \right.
\]

where \( t_m \) and \( t_n \) with \( t_m \leq t_n \) are certain intermediate time instances within \([t_0, t_1]\), \( \rho_t = \frac{t_1-t_m}{t_1-t_0} \) indicates the fraction of the time interval that the channel is jammed, then \( J(t) \) is a typical partial-time jamming signal.

If we use the discrete power spectrum of \( J(t) \) to characterize the jamming signal, a general jamming model is obtained:

\[
S_G(t,f) = \sum_{k=f_0}^{f_1} P_G(t,k) \delta(f-k), \quad \text{s.t.} \quad \sum_{k=f_0}^{f_1} P_G(t,k) = P_G,
\]

where \( P_G(t,k) \) stands for the jamming power allocated for the \( k \)th frequency at time instance \( t \), \( \delta \) is the Dirac delta function.

Two widely used anti-jamming systems are frequency-hopping (FH) and direct-sequence CDMA (DS-CDMA). In the following, we discuss jamming classification for these two particular communication schemes.

III. JAMMING MODEL FOR FREQUENCY HOPPING SYSTEMS

Assume that the transmitter is able to hop among \( N_c \) available channels, and each occupies a bandwidth of \( B_{ch} \). In order to retain the orthogonality among carriers, \( B_{ch} \) needs to be an integer multiple of \( \frac{1}{T} \), where \( T \) is the symbol interval in slow FH systems or the hopping duration in fast FH systems. In general, we simply set \( B_{ch} = \frac{1}{T} \), in order to save the total bandwidth.

Define a binary vector \( \alpha = [\alpha_0, \alpha_1, \ldots, \alpha_{N_c-1}] \) for the transmitter. For \( i = 0, 1, \ldots, N_c - 1 \), \( \alpha_i = 1 \) indicates the \( i \)th channel is currently used by the transmitter to convey information. Otherwise, the \( i \)th channel is idle if \( \alpha_i = 0 \). Similarly, \( \beta = [\beta_0, \beta_1, \ldots, \beta_{N_c-1}] \) is defined as the jamming index, where \( \beta_j = 1 \) implies that the \( j \)th channel is deliberately jammed, and \( \beta_j = 0 \) means that there is no intentional jamming on the \( j \)th channel, for \( j = 0, 1, \ldots, N_c - 1 \).

For either slow frequency hopping or fast frequency hopping systems, the transmitter changes its desired traffic channels from one hop to another. In other words, \( \alpha \) is actually a time-varying vector. On the other hand, the jammer can have its own jamming strategy, by choosing arbitrary \( \beta \). Specifically, based on the particular choice of \( \beta \), the jamming model can be generalized as follows:

- If \( \beta = \varphi \), where \( \varphi \) is a vector with entries of constant binary values, then the jamming is independent of time. It is also referred to as fixed-band jamming. Two special cases are \( \varphi = 0 \) and \( \varphi = 1 \), where \( 0 \) is an all-zero vector and \( 1 \) is an all-one vector, which corresponds to no jamming and full-band jamming respectively.
- If \( \beta \) is a function of time, then random jamming happens when \( \beta \) is randomly chosen during each hopping duration. In the worst case, smart jammers can be implemented as long as the condition that \( \beta = \alpha \) is always satisfied, which means the jammer can follow the frequency hop all the time.
- If \( \beta \) is neither an all-zero nor an all-one vector at any time instance, it is generally partial-band jamming (either fixed-band or random jamming). If \( \beta \) is an all-zero vector within each dwell duration except for certain time intervals, it is referred to as partial-time jamming.

Suppose the jammer changes its jamming indices over time and spreads its available power equally over all the channels it intends to jam. We ameliorate the general white Gaussian noise model into a more sophisticated one with its time-varying power spectral density defined as follows:

\[
S_G(t,f) = P_G \sum_{j=0}^{N_c-1} \beta_j(t) \chi(f-f_0-jB_{ch}),
\]

where \( f_0 \) is the initial frequency shift,

\[
P_G = \left\{ \begin{array}{ll}
0, & \text{if } \sum_{j=0}^{N_c-1} \beta_j(t) = 0, \\
\rho_n, & \text{if } \sum_{j=0}^{N_c-1} \beta_j(t) \neq 0,
\end{array} \right.
\]

\[
\chi(t) = \left\{ \begin{array}{ll}
1, & \text{if } f \in [0, B_{ch}), \\
0, & \text{else}.
\end{array} \right.
\]

IV. JAMMING MODEL FOR DS-CDMA SYSTEMS

A. Single-user Systems

We begin with the simple case where CDMA signals are sent over an AWGN channel. At the receiver end, it yields

\[
r(t) = d(t)p(t) + n(t) + J(t), \quad 0 \leq t \leq T,
\]

where \( d(t) \) is information signal, \( p(t) \) is the signature wave, \( n(t) \) is the additive white Gaussian noise, \( J(t) \) is jamming signal and \( T \) is the symbol period.

The power spectral density of \( d(t) \) is approximately given by

\[
S_d(f) = T \left( \frac{\sin \pi f T}{\pi f T} \right)^2.
\]

Let \( s(t) = d(t)p(t) \) be the spreading signal. Since \( p(t) \) is
the chip-level waveform at a rate of $f_c$ chips/second, by substituting $\frac{1}{f_c}$ for $T$ in (10), we can easily obtain the power spectral density of $s(t)$,

$$S_s(f) = \frac{1}{f_c} \left( \frac{\sin \pi f / f_c}{\pi f / f_c} \right)^2.$$  

(11)

After despreading, we obtain

$$z(t) \triangleq r(t)p(t) = d(t) + n(t)p(t) + J(t)p(t),$$  

(12)

where $J(t)p(t)$ represents the code-modulated jamming signal. We consider two scenarios:

1) If the jamming signal expands the whole channel bandwidth, then the code-modulated jamming signal will further spread the spectrum, thus can be approximately modeled as a white noise process. On the other hand, the desired despread signal’s power is concentrated within $[-\frac{\pi}{f_p}, \frac{\pi}{f_p}]$. To extract $d(t)$, we can pass $z(t)$ through a lowpass filter of bandwidth $\frac{\pi}{f_p}$ Hz. At the output of the lowpass filter, the desired signal’s power remains largely unchanged, while the jamming power is reduced by a fraction of $f_cT$. Therefore, the jamming-to-signal ratio (JSR) is increased by $f_cT$.

2) If the jammer concentrates its energy within the bandwidth associated with the original signal, for example, $J(t) = \sqrt{E_J/T}, \forall t \in [0, T]$, where $E_J$ is the jamming energy and $T$ is the symbol duration. In this case, the PSD of $J(t)$ has the same form as that of $S_d(f)$ in (10). Due to the frequency diversity in CDMA signals, a narrow-band interference elimination filter can be used to filter out the intentional jamming completely before despreading without seriously degrading the system performance.

Beyond the AWGN channel, if the channel impulse response is modeled as

$$h(t) = \sum_{l=0}^{L-1} h_l \delta (t - d_l),$$  

(14)

where $\{h_l\}_{l=0}^{L-1}$ are complex attenuation coefficients and $\{d_l\}_{l=0}^{L-1}$ are delays for $L$ different paths, then the received signal is given by

$$r(t) = \sum_{l=0}^{L-1} h_l s(t - d_l) + n(t) + J(t)$$  

(15)

$$= h_0 s(t) + \sum_{l=1}^{L-1} h_l s(t - d_l) + n(t) + J(t),$$  

(16)

where $d_0$ is assumed to be 0, without loss of generality.

As can be seen, in addition to the noise $n(t)$ and the jamming signal $J(t)$, multipath propagation results in self-jamming.

Considering the well-known fact that the original data is spread by pseudo-random sequences making $s(t)$ a wideband signal, any delayed or scaled version of $s(t)$ does not change the signal’s bandwidth, eventually resulting in the wideband characteristic of the self-jamming term.

If $J(t)$ only occupies a narrow frequency band with strong power within that band, the hostile jamming can be easily detected, since the other terms except $J(t)$ on the right side of (16) are all wideband signals with low power spectral density. That is, we are able to distinguish partial-band jamming from self-jamming, by simply taking samples over the entire bandwidth of the power spectral density of the received signal.

B. Multi-user Systems

For multiple access DS-CDMA systems, in addition to inter-symbol interference within each user’s signal caused by frequency selective fading, self-jamming among authorized users occurs when the orthogonality of spreading codes among users is not maintained due to multipath propagation or asynchronous transmission.

Take downlink CDMA as an example. In this case, all users are synchronous. The transmitted signal can be written as

$$s(t) = \sum_{k=0}^{K-1} d_k(t)p_k(t),$$  

(17)

where $d_k(t)$ is the $k$th user’s signal wave, $p_k(t)$ is the combined spreading and scrambling code for the $k$th user. The received signal through the channel in (14) is given by

$$r(t) = s(t) + h(t) + n(t) + J(t),$$  

(18)

where $*$ denotes linear convolution.

Even if $p_i(t)$ and $p_j(t)$ are orthogonal with each other for $i \neq j$, self-jamming due to multiuser interference cannot be completely cancelled, if multipath propagation is taken into consideration. In the multi-user case, distinction of hostile jamming from noise and self-jamming is much more complex and is currently under investigation.

V. JAMMING DETECTION

An important application of jamming detection is to avoid transmission over the intentionally jammed channels, because it is most likely that the detected and decoded information is erroneous due to the low SNIR even if jamming suppression approaches are applied at the receiver.

The intuitive measurement for jamming is either the signal strength (if jammer emits a constant amplitude signal), or the energy level (if jammer emits a noise-like signal such as white Gaussian signals). Generally, clear, unjammed data record is needed at the receiver end to establish a statistical model describing the normal energy level prior to jamming.

A. Jamming detection for frequency hopping systems

We follow the idea of the hypothesis test and apply it to jamming detection. Here, the jamming signal is simply modeled as a zero-mean white Gaussian process with single-sided PSD $N_f$. The hypothesis test is generalized as follows,

Here, we consider two cases:
\[ H_0 : \text{the channel is not jammed,} \]
\[ H_1 : \text{the channel is jammed.} \]

1) Training available: First, the receiver subtracts the training symbols from \( r(t) \). Under null hypothesis \( H_0 \), \( r(t) \) is white Gaussian with single-sided PSD \( N_0 \); under the alternative hypothesis \( H_1 \), \( r(t) \) is white Gaussian with single-sided PSD \( N_0 + N_J \).

- If \( N_J \) is unknown (but definitely positive), during training phase, we measure the samples’ energy, and build a threshold presenting the normal energy level, e.g., \( E[|r(t)|^2] = \lambda \). During test phase, compare the average energy level obtained from samples \( r_k \) to the threshold,

\[
\frac{|r_k|^2}{H_0} \gtrless \lambda.
\]

(19)

- If \( N_J \) is fixed and known (or estimated from previous samples), the likelihood ratio test (LRT) becomes

\[
\Lambda(r_k) = \frac{N_J}{N_0 + N_J} \frac{|r_k|^2}{H_1} \gtrless \eta.
\]

(20)

2) Training unavailable: Since no pilot symbols are available, the receiver utilizes blind detection. The two hypotheses turn out to be

\[ H_0 : r(t) = s(t) + n(t), \]
\[ H_1 : r(t) = s(t) + n(t) + J(t). \]

First examine the mean of \( r(t) \) under two hypotheses, since both \( n(t) \) and \( J(t) \) are of zero mean,

\[
E[H_0] = E[s(t)] = m,
\]
\[
E[H_1] = E[s(t)] = m.
\]

Without loss of generality, \( m = 0 \) is assumed. The simplest solution under this circumstance is to calculate the covariance of \( r(t) \) through time-averaging.

Considering the independence among the data symbol, the additive noise and jamming signal, under \( H_0 \), \( E[|r(t)|^2] = E[|s(t)|^2] + E[|n(t)|^2] = \sigma_s^2 + N_0 \), while under \( H_1 \),

\[
E[|r(t)|^2] = E[|s(t)|^2] + E[|n(t)|^2] + E[|J(t)|^2] = \sigma_s^2 + N_0 + N_J.
\]

Therefore, we have a simple decision rule:

\[
\frac{|r_k|^2}{H_1} \gtrless \lambda .
\]

(23)

Taking channel fading effects into consideration, we stack \( N \) samples of the received signal into a column vector \( r \),

\[
r = Hs + n, \quad \text{if } H_0, \]
\[
r = Hs + n + J, \quad \text{if } H_1,
\]

(24)

where \( s, n \) and \( J \) are \( N \)-sample column vectors corresponding to data, noise and jamming, respectively, and \( H \) is channel convolution matrix. The autocorrelation matrices of \( r \) under \( H_0 \) and \( H_1 \) are given as follows:

\[
E[rr^H] = \sigma_s^2 HH^H + N_0 I, \quad \text{if } H_0, \]
\[
E[rr^H] = \sigma_s^2 HH^H + N_0 I + N_J I, \quad \text{if } H_1,
\]

(25)

where \( H \) denotes Hermitian transpose, \( I \) represents an identity matrix.

Note that the discriminant between \( H_0 \) and \( H_1 \) only exists on the main diagonal of \( E[rr^H] \). Consequently, we first calculate the autocorrelation matrix of the received signal, then take the average of all the entries on the main diagonal. If the averaged value is greater than a threshold, then \( H_0 \) is rejected, and vice versa.

B. Jamming detection for DS-CDMA systems

Since signals in CDMA systems are characterized by low power spectrum density, jamming detection in frequency domain is more suitable for DS-CDMA systems.

The amplitude of the normal energy of all the frequency components of \( r(t) \) under \( H_0 \) where \( J(t) = 0 \) is first derived, where no significant difference in strength among all the frequency components should be detected. Then for the received signal \( r(t) \), the power spectrum can be estimated via the magnitude squared of the FFT of the windowed signal [12]. If there is only one frequency component with an unusually high amplitude in the estimate of power spectral density, it is most likely that this frequency is jammed and should be excised or interpolated.

VI. SIMULATION EXAMPLES

In the simulation, a CDMA system with spreading factor 16 is considered. The binary spreading codes are randomly generated, BPSK signals are transmitted over the AWGN channel. JSR is defined as the ratio of the total jamming power to signal power, while SNR is defined as the ratio of the averaged signal power to noise power. The jammer uniformly distributes its available power over the randomly chosen band. At the receiver end, hostile jamming is informed if the unusually high amplitudes of frequency components are discovered beyond a certain threshold. There are basically two types of detection errors: probability of miss and probability of false alarm. If no jamming is detected when jammer is actually working, then miss detection happens. On the contrary, if the receiver think frequency band is being occupied by the hostile jamming signal when jammer is actually off, the false alarm arises.

Fig. (1) shows the performance of jamming detection with respect to different levels of JSR. According to the definition, probability of false alarm is not related to JSR, but dependent upon SNR. Thresholds with regard to different SNRs are determined in a way that the probability of false alarm is approximately 0.04. As can be seen, it is more likely that jamming can be exhaustively detected as the total jamming power is increased. Moreover, the noise strength on the channel will affect the performance of jamming detection. Given a fixed jamming power, if the noise power is large enough to make a significant contribution on the receiver’s power spectral.
density, then the threshold must be enough high to achieve a small probability of false alarm, which consequently leads to a big chance that the receiver will fail to detect the existence of jamming, that is, a miss is likely to occur.

Effective detection of hostile jamming makes it possible for the transmitter to implement a dynamic anti-jamming transmission scheme, and hence plays a key role in jamming prevention.

VII. CONCLUSIONS

This paper considered modeling and detection of hostile jamming in wireless systems, particularly, for spread spectrum systems. First, a general two-dimensional model was proposed to characterize jamming signals from both the time domain and the frequency domain. It contains all the existing models as special cases. Second, focused on spread spectrum systems, jamming classification was discussed in detail for both DS-CDMA systems and frequency hopping systems. Finally, both training based and blind jamming detection methods were presented, together with illustrative simulation examples.

REFERENCES