Adaptive Band Jamming in Wireless Networks using Fast Frequency Hopping and Non-Coherent Detection

Sapna Patidar¹, Ravi Khatri²  
¹,² Department of CSE, VITM, Indore

Abstract—Wireless Networks suffer from a serious challenge of ensuring security due to the absence of guided media. Data is prone to attacks from adversaries since there always exists a possibility of the attacker tuning in to the frequency of transmission by brute force or otherwise. This paper presents an adaptive technique comprising of band jamming using fast frequency hopping and non-coherent conjugate detection. The algorithm developed is adaptive in the sense that the user can change the spreading factor for transmission. The performance is measured in terms of Bit Error Rate (BER) of the system. It has been found that the proposed algorithm performs better than previous work employing jamming.

Keywords—Spread Spectrum, Fast Frequency Hopping (FFH), Signal to Noise Ratio (SNR), Bit Error Rate (BER), Spreading Factor (L).

I. INTRODUCTION

Wireless technology has become on the forefront with wireless transmission becoming more common with increased bandwidth availability and better modulation techniques. This has also increased more amounts of data being transferred wirelessly. Conventionally encryption algorithms have been employed to secure data from adversaries, but off late due to higher processing capability from computational platforms, the chances of encryption mechanisms been broken have also increased. Complex encryption mechanisms now stand a greater threat of intercept or eavesdropping from adversaries.

Generally signals are band-limited in nature and occupy a bandwidth ‘B’ within which most of its power is concentrated and out of which the signal fades drastically. Figure.1 depicts a typical signal spectrum. It can be seen that the signal occupies a narrow bandwidth. Hence spread spectrum has caught the attention of researches to make the data being transmitted after modulation imperceptible to adversaries by making their amplitude level lesser than noise level thereby making it undetectable.
for attackers to detect and attack the signal. Spreading the signal would mean spreading the signal’s spectrum and reducing the power below noise level. This is depicted in Figure.2.

![Figure.2 Spreading the Signal Spectrum](image_url)

II. TYPES OF SPREADING AND UTILITY OF FAST FREQUENCY HOPPING

There are fundamentally two ways in which spread spectrum can be implemented namely direct sequence spread spectrum (DSSS) and Fast Frequency Hopping (FFH). In direct sequence spread spectrum, the bit stream is multiplied by a narrow width sequence called the spreading sequence which narrows down the bit sequence in time domain and hence spreads it in the frequency domain. Mathematically, it can be expressed as:

\[
y(t) = x(t).s(t) \quad (1)
\]

\[
Y(f) \rightarrow X(f)*S(f) \quad (2)
\]

Here,
x(t) represents the time domain signal,
s(t) is the spreading sequence
y(t) is the spreaded sequence
Also * represents the convolution operation between signals

The technique of Direct Sequence Spread Spectrum (DSSS) is more prone to attacks since the adversary just needs to get hold of the spreading sequence s(t). The better alternative is frequency hopping spread spectrum in which the carrier frequency hops randomly with respect to the adversary but is actually governed by a pseudo-random code that is available with the transmitter and receiver. The mathematical formulation is given below:

Let the message be represented by x(t).
The carrier be represented by c(t)=A_c \cos(2\pi f_i t + \phi)
Let the pseudo-random sequence be represented by: s(t)
Then the carrier hops between ( f_1 to f_n ) i.e. f_i \in (f_1 to f_n)
As a result, the transmitted signal through the channel hops between S(f_i) to S(f_n)

Thus the signal that was band-limited to ‘B’ is now spread across N.B where N is called the spreading factor. Spreading factor is defined as:

N=B'/B \quad (3)

Here B’ stands for the spreaded bandwidth while B stands for the original bandwidth of the signal before spreading.

Frequency Hopping can be categorized into two categories:
1) Slow Frequency Hopping
2) Fast Frequency Hopping
Slow Frequency Hopping occurs when the hopping duration T_HOP is larger than bit duration T_B
Mathematically,

T_{HOP}> T_B \quad (4)

Fast Frequency Hopping occurs when the hopping duration T_{HOP} is smaller than bit duration T_B
Mathematically,

\[ T_{\text{HOP}} < T_B \]  \hspace{1cm} (5)

Fast frequency hopping (FFH) is less susceptible to attacks by adversaries because of the fact that its not just the pseudo-random code that needs to be broken but rather the signal needs to be intercepted first of all from multiple hopping noise level amplitudes that makes the detection even more complex. Hence the approach chosen in this paper is Fast Frequency Hopping.

### III. PROPOSED SYSTEM

The system design utilizes fast frequency hopping and non-coherent detection whose validation is put forth subsequently. The proposed system can be took further form simulations by using a frequency synthesizer which hops frequencies according to a randomly changing bit pattern. The process is explained below: The fast frequency hopping is governed by a hopping sequence that hops or changes the carrier frequency pseudo randomly. The mathematical modeling can be explained as follows:

Let the original signal be band-limited to \( B_m \)

Let the spreaded signal be band-limited to \( B'_h \)

After spreading, the signal can be expressed as:

\[ X(t) = \cos(B_m + B'_h)t + \Theta \]

Where \( \Theta \) represents some added phase.

Let the bit or symbol period be represented by \( T_S \)

Let the hopping chip period be represented by \( T_C \)

Chip period represents the time for which the signal hopping output remains unaltered.

Let the Signaling Rate be \( 1/T_S \)

Let Chip Rate be \( 1/T_C \)

Let a signal be band-limited to \( B_s \).

Let the power produced by the jamming source be \( P_j \).

The Power Spectral Density (psd) encountered by the jamming source is \( (B_s/P_j) \)

Then the signal to interference ratio can be expressed by \( (\text{SIR})_1 = Eb/(B_s/P_j) \)

In case the signal is spreaded to a bandwidth of \( B_c \) where

\( B_c = L.B_s \)

Here \( L \) represents the spreading factor.

Then the signal to interference ration inclusive of jamming can be presented by:

\[ (\text{SIR})_2 = Eb/(B_c/P_j) \]

If \( B_c >> B_c \)

Then \( (\text{SIR})_1 >> (\text{SIR})_2 \)

This causes the adversary much larger interference and hence the probability that the signal will get intercepted becomes less.

In case the complete jamming power is completely dedicated to a bandwidth of \( B_c \), then among the \( N \) sub-bands, one experiences a strong interference whose probability can be given by:

\[ P_b = ((L-1)/L).0.5\exp(-Eb/2N)+1/2L \]  \hspace{1cm} (6)

The de-jamming at the receiver can be obtained by a de-jamming process that generates the carrier at the receiving end. The carrier generated at the receiving end can be done in two ways:

1) Coherently

2) Non-Coherently
Coherent detection refers to the technique in which the receiver carrier is completely in phase with the transmitter carrier. It is simpler to implement on hardware but is more prone to errors in case of fast frequency hopping since maintain complete synchronization among two far off sources is extremely difficult keeping in maid the rate at which the frequencies change. Non-coherent on the other hand is less simpler to implement on hardware by does not suffer from the problem of errors arising out of non-synchronization between transmitting and receiving ends.

The mathematical formulation for non-coherent detection can be modelled as:

Let the carrier signal be given by:

\[ C(t) = \text{Real}(Ae^{jwt}) \]  

(7)

The carrier utilized for de-jamming can be given by:

\[ C'(t) = \text{Real}(Ae^{jwt+\phi}) \]  

(8)

The de-spreaded signal is obtained by utilizing the condition that the final signal is band-limited by:

\[ S(f^2) = 2S(f) \]  

(9)

Using low band separation, the signal in the spectrum of ‘2f’ can be separated from that of ‘f’

IV. RESULTS

The results obtained can be depicted in the form of graphs which sequentially depict the process that takes place in the jamming and de-jamming process finally culminating in the BER curve of the proposed systems by varying the spreading factor. It can be seen from the graphs that as the spreading factor (L) increases, the BER of the system increases, and a degradation in BER performance of the system can be seen. Also the Quality of Service of the system can be evaluated based on the Outage Probability of the system which is a measure of the non-acceptability of the system performance. It can be seen from the outage probability curve that as the signal to noise ratio increases, the outage probability decreases. This is a validation check that depicts the fact that higher SNR reduces the BER o the system which in turn reduced the outage probability of the system. The obtained results are illustrated in the following section.

![Figure 4 Message Signal prior to transmission](image-url)
**Figure 5** Signal after employing FFH

**Figure 6** Noise in Channel
Figure 7. Noise addition in signal at Channel

Figure 8. De-jammed Signal at receiving end
V. CONCLUSION

It can be concluded from the previous discussions and mathematical deductions that band-limited signals can be safeguarded from attacks from adversaries using jamming employing FFH spread spectrum. The paper proposes a non-coherent detection approach for the de-jamming and signal detection process at the receiving end. It can be seen that the approach uses an adaptive jamming approach in which the spreading factor can be increased depending upon system requirements. The
BER curve depicts the fact that the BER gets degraded with increasing factor since the signal strength plummets and makes it difficult to de-jam at the receiving end. Finally the outage probability is shown to have an inverse relationship with the signal to noise ratio indicating the amount of power to be transmitted from the transmitting end.

REFERENCES


