A Band Jamming Technique with Non-coherent Detection for Wireless Network Security

Sapna Patidar and Ravi Khatri

Abstract Security in wireless networks is a serious challenge due to the access of the channel to adversaries because of the channel being unguided. Conventional encryption mechanisms cannot guarantee security in wireless networks since even the most complex encryption algorithms can be broken. Hence, deliberate jamming is one way to safeguard data from possible attacks. This paper proposes a band jamming technique using fast frequency hopping (FFH) along with non-coherent detection for evading possible attacks. The performance parameters evaluated the bit error rate (BER) and the outage probability of the proposed system. Non-coherent detection has been employed since maintaining coherence for a fast frequency hopping technique is extremely challenging under practical noisy channel conditions. The results show the various stages of the jamming and de-jamming processes.

Keywords Band jamming · Fast frequency hopping (FFH)
Non-coherent detection · Bit error rate · Outage probability

1 Introduction

Band jamming is a technique to deliberately jam the signal bandwidth so as to make the signal imperceptible to possible adversaries [1]. The principal goal of the proposed work is to create and work towards a faster version of the frequency hopping method intended for wireless networks which in turn utilizes the frequency hopping of spread spectrum. This is to ensure the effectiveness of the proposed model to prevent the attacks of adversaries. An algorithm has been suggested based on fast frequency hopping aiming to prevent the probable interception attacks by the intruders. Spread of the signal makes it unrecognizable for the attackers, but it has a con that makes the signal more vulnerable to noise that can lead to excessive bit error rate. So another priority is to also handle the BER and to keep it in lower levels

S. Patidar (✉) · R. Khatri
VITM, Indore, India
e-mail: spatidar57@yahoo.com

R. Kamal et al. (eds.), *International Conference on Advanced Computing Networking and Informatics*, Advances in Intelligent Systems and Computing 870,
https://doi.org/10.1007/978-981-13-2673-8_28

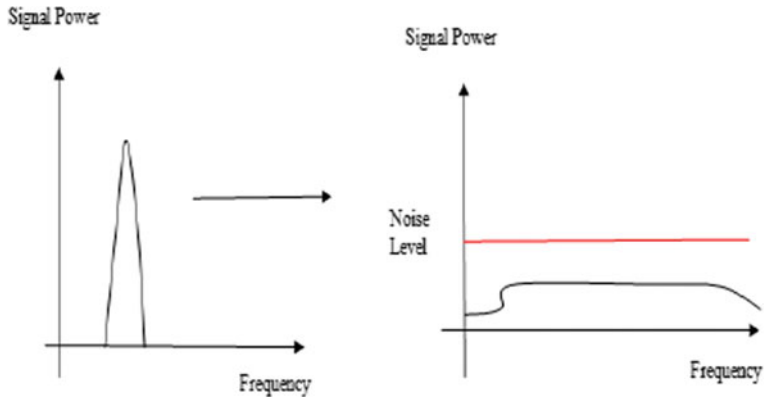

Fig. 1 Concept of spread spectrum

to maintain the quality of service norms. Spreading the signal more though helps in making it more secure, but it weakens the strength of signal. So in this context, an efficient mechanism is proposed comprising of coherent conjugate detection of the signal after de-jamming of signal. It mainly focuses on reducing effects of errors obtained in the recovered signal. The performance is measured in terms of the bit error rate (BER) of the system. The BER of the system varies in accordance with the spreading factor of the jamming process. The concept of spread spectrum can be understood using Fig. 1.

2 Fast Frequency Hopping

Fast frequency hopping is a technique wherein the bandwidth of a given signal is spread out in a larger bandwidth by changing or hopping the carrier frequency continuously [2]. Considering the bit period of a signal to be T_b and the hopping period or the chip period to be T_c

$$\text{If } T_b < T_c \tag{1}$$

Then, the case is called slow frequency hopping (SFH). On the contrary, if the following relation holds true,

$$T_b > T_c \tag{2}$$

Then, the case is called fast frequency hopping (FFH).

The ratio of the bandwidth after spreading to the bandwidth before spreading is called the spreading factor (L) defined mathematically as [3]:

$$L = B_S/B \tag{3}$$

Here,

B_S denotes the signal bandwidth after spreading, and
B denotes the signal bandwidth before spreading.

3 Proposed Methodology

(1) Generate a serial binary data stream 's_data'.
(2) Generate carriers for a hop-based modulation. Let the carriers be designated by $f_1, f_2, f_3, \ldots. f_n$.
(3) Generate the jammed signal s_jam which would be a modulated signal with a pseudo-random frequency pattern **'g'**.
(4) Then, s_jam can be given by:

$$s\_jam = \mathbf{g}(s\_data, f_1, f_2, f_3, \ldots f_n) \tag{4}$$

(5) Considering the spreaded bandwidth to be **βs** and the power of the transmitting source to be **Pi,** then the normalized interference caused to the jamming source can be given by:

$$I = (\beta s/Pi) \tag{5}$$

And the signal-to-interference ratio can be given by [4]:

$$(SIR)_1 = E_b/(\beta s/Pi) \tag{6}$$

where E_b represents the energy per bit.

(6) Considering additive white Gaussian noise (AWGN) conditions, generate noise and add to the jammed signal to emulate a practical channel [5]. Considering the noise to be given by n(t), the signal after the addition of noise can be given by:

$$s\_jam\_noise = s\_jam + n(t) \tag{7}$$

(7) De-jam the signal at the receiving end by using non-coherent conjugate detection described as:

If the transmitted carrier is given by [6]:

$$E_T(z, t) = E_{0.} \exp(-\alpha z) \cdot \exp(\omega t - \beta z) \tag{8}$$

And the receiving carrier is given by

$$E_R(z, t) = E_{0.} \exp(-\alpha z) \cdot \exp(\omega t - \beta z + \varphi) \tag{9}$$

Here, φ represents the phase difference between the transmitting and the receiving carriers. The design of a band-pass filter stops the carrier components out of band and recovers the signal 's_data'.

(8) Compute the BER and outage probability of the system.

4 Experimental Results

The results of the proposed system are evaluated in terms of:

(1) Bit error rate or probability of error given by: [2]

$$P_{re} = \frac{1}{\sqrt{2\,\pi\,\varphi_N^2}} \int_{\frac{b-b_2}{2\sigma_\varphi}}^{\infty} e^{(-x^2/2)} \varphi_N dx \tag{10}$$

Here, N represents the double-sided power spectral density of the noise.
Using the Q function, the BER of the system can be given by:

$$P_{re} = Q[(b_1 - b_2)/2\varphi_N) \tag{11}$$

Here,

b_1 and b_2 represent the bits 0 and 1,
φ_N represents the noise power spectral density (psd),
x is the random variable assuming two values for bits 0 and 1, and
Q represents the Q function.

The outage probability can be computed using the signal-to-noise-plus-interference ratio given by [7]:

$$\text{Prob}(S_{Rec} < S_T)$$

where

S_{Rec} represents the received signal power, and
S_T represents the threshold of signal power above which the quality of service is satisfactory.

Explanation of Results:
Figure 2a–d is combined and shown as a single figure for the sake of brevity and to augment the sequential flow of steps in the jamming and the de-jamming processes.

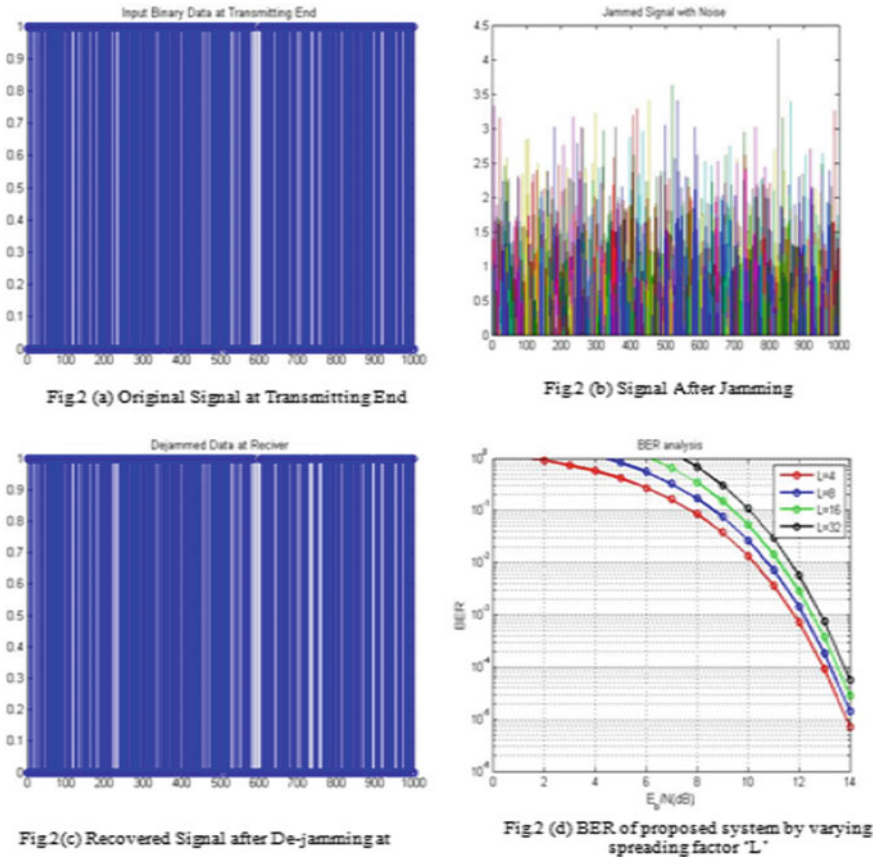

Fig. 2 **a–d** Represents the original binary message, binary message after jamming, de-jammed signal at receiving end and BER performance by varying spreading factor (L), respectively

Figure 2a depicts the discrete counterpart of the binary serial data which acts as the secret message. The discrete plot of 0 s and 1 s has been used to depict the binary message.

Figure 2b depicts the composite noisy jammed signal where noise is added in the channel.

Figure 2c depicts the de-jammed signal at the receiving end. The noise added is AWGN in nature, and it can be seen that after noise is added, the composite signal resembles noise to deceive potent adversaries.

Figure 2d depicts the variation of the BER of the system with increasing spreading factor. It can be seen that the BER reduces below 10^{-4} for spreading lengths up to 32. It can be seen that the BER degrades with increasing spreading factor which exhibits coherence with theoretical concepts, given by Eq. (11)

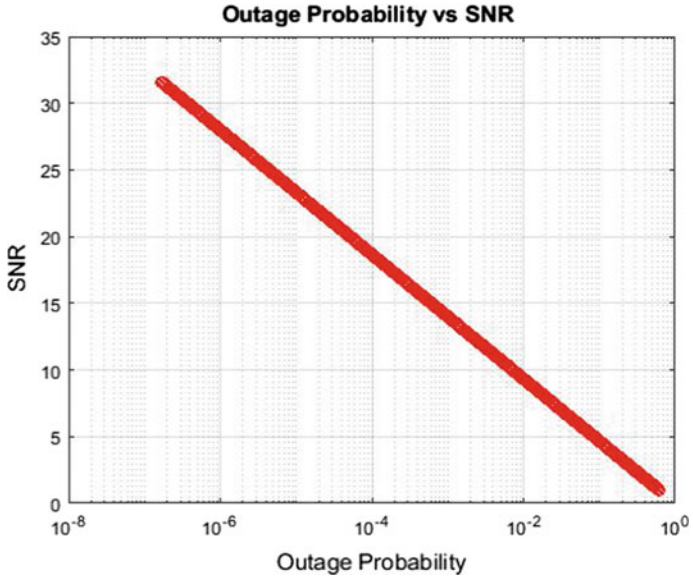

Fig. 3 Depicts the outage probability of the system as a function of signal-to-noise ratio

The outage probability of the system shows the relation among the quality of data communication as a function of signal-to-noise ratio. Thus, attaining relatively high SNR for high spreading factors would mean acceptable communication quality (Fig. 3).

5 Conclusion

This paper presents a band jamming technique in conjugation with non-coherent conjugate detection which is an effective technique for recovering the original signal at the receiving end in case the frequency hops frequently within a bit period and maintaining coherence between the transmitted and received carriers becomes difficult. Moreover, it can be seen that the proposed approach attains a BER of almost 10^{-5} at a relatively less SNR of 14 decibel. Thus, the technique is thought to mitigate the challenge of attack by adversaries and noisy nature of the wireless channel. It can also be seen that the proposed system's outage reduces with increase in signal-to-noise ratio (SNR).

References

1. W. Stallings, *Network Security and Cryptography*. 4th edn (Pearson Publication)
2. A.F. Molisch, *Wireless Communication* (Wiley India Publications)
3. J. Zhang, K. Teh, K. Li, Performance study of fast frequency hopped/ M-ary frequency-shift keying systems with timing and frequency offsets over Rician-fading channels with both multitone jamming and partial-band noise jamming. IET Commun. **4**(10), 1153–1163 (2010)
4. J. Zhang, K. Teh, K.H. Li, Maximum-likelihood FFH/MFSK receiver over Rayleigh-fading channels with composite effects of MTJ and PBNJ. IEEE Trans. Commun. **59**(3), 675–679 (2011)
5. L.-M.-D. Le, K.C. Teh, K.H. Li, Jamming rejection using FFH/MFSK ML receiver over fading channels with the presence of timing and frequency offsets. IEEE Trans. Inf. Forensics Security. **8**(7), 1195–1200 (2013)
6. L.-M.-D. Le, K. Teh, K. Li, Performance analysis of a suboptimum fast frequency hopped/M-ary frequency-shift-keying maximum likelihood receiver over Rician-fading channels with composite effects of partialband noise jamming and multitone jamming. IET Commun. **6**(13), 1903–1911 (2012)
7. F. Yang, L.-L. Yang, A single-user non coherent combining scheme achieving multiuser interference mitigation for FFH/MFSK systems. IEEE Trans. Wireless Commun. **12**(9), 4306–4314 (2013)