Bommalapati Malleswari, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 12, Issue 7, (Series-I) July 2022, pp. 64-66

RESEARCH ARTICLE OPEN ACCESS

White Paper on Jamming Margin in Wi-Fi Systems

Bommalapati Malleswari, T.S Swamy, Bhaskara Rao S
Centre for Development of Telematics, Electronic City, Phase-1
Hosur Road, Bengaluru India, 560100, Telephone: +91-80-25119181

Abstract
In this paper, we proposed a test method to measure Jamming Margin in Wi-Fi systems (for Direct Sequence Spread Spectrum (DSSS) modulation schemes). In this method, jamming margin will be detected using Packet Error Rate (PER) and Signal to Noise Ratio (SNR) both taken as reference. To evaluate the jamming margin, Signal generator is used to generate jammer signals to block the signals between Wi-Fi AP and Client. Results shows that the proposed test method can detect jamming margin. Index Terms—Packet error rate, Bit Error Rate, Jamming Margin, RSSI, Jammer to Signal Ratio, Signal to Noise Ratio.

Date of Submission: 01-07-2022 Date of Acceptance: 12-07-2022

I. INTRODUCTION

Jammers that aim to block the legitimate transmissions by injecting jamming signals into wireless media can severely degrade network performance. Multiple types of jammers, such as constant jammers, random jammers, reactive jammers and smart jammers, have been found to attack wireless networks and have received extensive research attention [1]–[5]. Most existing anti-jamming techniques assume accurate jamming detection [6]–[8]. For example, a code tree system based on the unique properties of code sequences to detect jamming attacks in spread spectrum communication systems was proposed in [6]. In [7], a new jamming detection approach was presented using the measure of correlation among the error and the correct reception times. Jamming detection has become an important issue to improve security in wireless networks [10]. Signal-to-Noise ratio and Packet Error Rate has been used to detect jamming in direct sequence spread spectrum systems.

Most existing work on jamming detection focus on sensor networks and traditional Wi-Fi systems. In this paper, we investigate the jamming margin in Wi-Fi systems based on the Received Signal Strength Indicator (RSSI), SNR and PER for IEEE 802.11b systems as the type of modulation used is DSSS. Signal generator is used to generate jammer signals, which are performed to evaluate the impact of jamming attacks on the transmission between wireless systems. Results show that it can detects jamming margin accurately. We present a Jamming Margin measurement for Wi-Fi systems in Section II. Results are provided in Section III. Finally, we conclude our work in Section IV.

II. JAMMING MARGIN MEASUREMENT

In this paper, we consider the transmission between Wi-Fi systems. A Wi-Fi system consists of Wi-Fi Access Point and Wi-Fi client. Jammer signal is combined with desired signal output from Access Point and then fed to Client Wi-Fi system to detect the jamming margin. More specifically, a high packet loss rate can result from jamming or a large channel fading between the Client and AP. Here, we present a jamming detection method for Wi-Fi systems based on the packet error rate and the throughput received at the Client using Jperf tool. Generally this measurement will be carried out at RSSI l levels of at around-45dBm to -60dBm.A high signal strength corresponds to low packet error rate. A low RSSI results in high packet loss. This occurs due to large propagation loss. In the proposed jamming detection criteria is based on observation that the absence of jamming corresponds to a low packet error rate. The test measurement setup is shown in figure1.

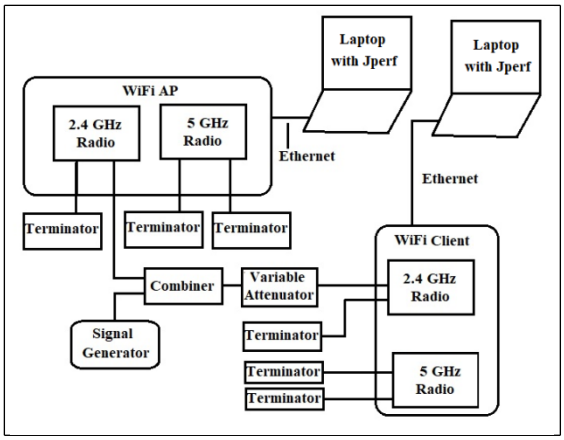

Figure 1: Test Setup for Jamming Margin Measurement

Proposed procedure for measuring Jamming Margin:

This measurement can be performed in two steps. In first step, we have to measure band power (EIRP) using a Spectrum Analyser with channel power option [1] with connecting fixed attenuator 6dB by setting channel 2&lowestlevel at 2.4GHz Radio port 0/1. In the second step ensure the RSSI at client side should be -45dBm to -60dBm by adjusting variable attenuator value now from signal generator, apply the jammer signal of configured channel frequency (for channel no. 2, it is 2.417GHz) with level at -25dBm and then run Jperf in Laptops which are connected to AP to Wi-Fi Client and check for 0% Packet Error Rate. Then slowly increase the signal level in steps of 1/0.5dBand check PER% for every step and note down the signal generator signal level till the allowed maximum PER ≤7.31%. Using Jperf tool in both Laptops, check the throughput. Repeat the above procedure for any selected channels from1 to 11.

Follow below settings to run the Jperf tool:AP (Access Point) Jperf mode: Client, Server address & Port: Server IP address & Port number, Protocol: UDP, Transmit time: 60sec, UDP Bandwidth: Set as shown in the below table, UDP packet size: 1000 octets.

Client

Jperf mode: Server, Protocol: UDP, UDP packet size: 1000 octets.

After configuration, click on start button and check the average receiving packets in the client side for 60 sec. Send the packets from AP to client and check that client is able to receive packets with ≤ 7.31% error rate (average for 60 sec). If packet loss is more than 7.31%, then reduce 'UDP Bandwidth' at AP side and repeat the above procedure.

III. RESULTS

From the measurement results, we will find out Jamming Margin and further we will calculate the processing gain. Standards specifies that the processing gain of a direct sequence systems shall be minimum10dB.

Formula for Calculation of Processing Gain (PG):

Processing Gain = $S/N + M_j + L_{sys}$

Where S/N = Signal to Noise Ratio required at the receiver output for 10^{-5}bit error rate of an ideal receiver for the demodulation schemes

M_j = Jamming Margin or Jammer to Signal (J/S) Ratio

L_{sys} = System losses (2dB max)

Packet Size of 1000octets in which Payload as 950 octets,

Bit Error Rate (BER) 10^{-5} taken as reference.

S/N= 13.0 dB (taken from Wireless Information Networks by Pahalvan & Levesque)

Then Packet Error Rate (PER) is obtained as:

$PER=1-(1-BER)^{\text{Payload in Bits}}$

$\%\ PER=1-(1-10^{-5})^{(950*8)} x100=7.31\%.$

Table: PER Results for Channel no. 2

Tx Data Set in AP	TX power set (dB) Wlan0 Port0	Measured Band Power (dB)	Jammer signal level	Set rate Kbps in **Jperf tool**	Received Throughput in Kbps **Jperf tool**	Packet Loss (%) in **Jperf tool**
1 Mbps	0	-5.02	-10	750	700	0
				850	750	2.3
				900	800	7.3
2 Mbps	0	-5.67	-10	1000	900	0
				1200	1000	0
				1350	1200	0.3
				1500	1350	1.7
				1600	1400	2.9
				1700	1500	7.23

M_j (Jamming Margin) calculation:

M_j (Jammer to signal Ratio in dB (J/S)) =

-10-(-5.02) = -4.98 (for set data 1Mbps)

-10-(-5.67) = -4.33 (for set data 2Mbps)

Processing Gain = $S/N + M_j + L_{sys}$

13-4.98 +2 = 10.02dB (for set data 1Mbps)

13-4.33 +2 = 10.67dB (for set data 2Mbps)

IV. CONCLUSIONS

In this paper, Jamming Margin in Wi-Fi systems is detected based on the PER, derived from the BER at good RSSI levels. Signal to Noise Ratio taken as reference, the Results demonstrate that this method can easily detect Jamming Margin for the allowed packet error rate ≤7.31%.

REFERENCES

[1]. Bommalapati Malleswari, Mohan Kumar S, Bhaskara Rao S "Fast Band Power Measurement technique in Wi-Fi systems using Spectrum Analyzer" International Journal of Applied Power Engineering (IJAPE) Vol.11, No. 1 March 2022, pp. 1~6 ISSN: 2252-8792

[2]. L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast using uncoordinated frequency hopping," IEEE Trans. Information Forensics and Security, vol. 7, no. 1, pp. 297–309, 2011.

[3]. L. Xiao, H. Dai, and P. Ning, "Mac design of uncoordinated fh-based collaborative broadcast," IEEE Wireless Commun. Letters, vol. 1, no. 3, pp. 261–264, 2012.

[4]. C. Li, H. Dai, L. Xiao, and P. Ning, "Analysis and optimization on jamming-resistant collaborative broadcast in large-scale networks," in Proc. Asilomar Conf. Signals, Systems and Computers, pp. 1859–1863, 2010.

[5]. Y. Li, L. Xiao, J. Liu, and Y. Tang, "Power control stackelberg game in cooperative anti-jamming communications," in Proc. Int'l Conf. Game Theory for Networks, pp. 93–98, 2014.

[6]. J. Chiang and Y. Hu, "Cross-layer jamming detection and mitigation in wireless broadcast networks," IEEE/ACM Trans. Networking (TON), vol. 19, no. 1, pp. 286–298, 2011.

[7]. A. Hamieh and J. Ben-Othman, "Detection of jamming attacks in wireless ad hoc networks using error distribution," in Proc. IEEE Int'l Conf. Commun. (ICC), pp. 1–6, 2009.

[8]. Y. Lin and M. Li, "Distributed detection of jamming and defense in wireless sensor networks," in Proc. IEEE Annual Conf. Information Sciences and Systems, pp. 829–834, 2009.

[9]. N. Sufyan, N. Saqib, and M. Zia, "Detection of jamming attacks in 802.11 b wireless networks," EURASIP Journal on Wireless Communications and Networking, vol. 2013, no. 1, pp. 1–18, 2013.

[10]. A. Fragkiadakis, V. Siris, N. Petroulakis, and A. Traganitis, "Anomalybased intrusion detection of jamming attacks, local versus collaborative detection," Wireless Commun. And Mobile Computing, vol. 15, no. 2, p. 276C294, 2013.