Cihan University-Erbil Scientific Journal (CUESJ)

Research Article

Evaluation of the Effect of Follower Jammer on the Mobile Bluetooth Network

Abdulqadir Ismail Abdullah[1]*, Adil Hussein M. Al-Dalawie[2]

[1]Department of Computer Science, College of Science, Knowledge University, Erbil, Iraq, [2]Department of Communication and Computer Engineering, College of Engineering Cihan University-Erbil, Erbil, Iraq

ABSTRACT

Bluetooth wireless communication technology has spread rapidly in the past 20 years. It has made life much easier with all the devices that use Bluetooth technology around us such as mobile phones, laptops, and watches. With all the good and useful applications of Bluetooth technology, it has been used in harmful and bad ways such as cheating in an examination. In this article, parameter design considerations have been discussed for a follower jammer to interrupt a Bluetooth network, especially when it is used in unauthorized way. The effects of the follower jammer were studied and tested. The effects were calculated for time and jamming-over-signal ratio for three different distances (1, 5, and 10 m). The testing showed that the follower jammer designed was successful in disrupting the Bluetooth signal.

Keyword: Bluetooth, follower jammer, mobile jammer

INTRODUCTION

Bluetooth wireless technology since its development by Ericsson in Sweden in 1994 has become an essential tool of everyday life. Bluetooth wireless technology (BWT) has been used by many devices such as laptops, mobile phones, and car stereo systems. It has made everyday tasks very easy and efficient.[1]

Bluetooth-enabled devices use ISM frequency band range between 2.4 GH and 2.48 GH. It uses a technique called frequency hopping (FH). This technique is useful for reducing interference. There are three classes of Bluetooth networks: Class 1 is 100-m range, Class 2 is 50-m range, and Class 3 is 10-m range.[1]

Bluetooth wireless networks are subject to interference such as jamming which could be intentional, and this disrupts the service. Not all disruptions are bad thing because some people nowadays use bluetooth networks for some purposes which are not allowed.[2]

There are deferent types of jamming techniques such as overall band noise jamming or spot jamming and swept jamming. Research into the evaluation of the effects of these three deferent methods on the mobile Bluetooth network provides good motivation to make a comparison between these techniques. The authors in a research article[3] focused on overall noise jamming techniques, spot noise with bandwidth 5 MHz and 20 Mhz, and sweep jammer. The conclusions of the research article[3] were that the block jammer signal (noise powered with different bandwidths 5 MHz and 20 MHz) does not affect the Bluetooth network, and it needs high power to overcome the processing gain and the path loss attenuator. The effect appears within 1-m distance by increasing the power density of the jamming signal; the bandwidth of the jamming signal was set to 5 MHz and uses very slow swept noise in order to affect the channels sequentially and keep the channel out of service according to Adaptive frequency hopping (AFH) and that will reduce the processing gain with time.

Due to the power problems in the previous work, a new method had to be followed in order to reach better results that, in mid, a new technology was tested and studied in the research article such as the follower jammer technique, which is effected on FH.[3]

FOLLOWER JAMMER TECHNIQUE

FH spread spectrum is particularly useful to combat jamming primarily because it is relatively easy to operate

Corresponding Author:
Abdulqadir Ismail Abdullah, Department of Computer Science, College of Science, Knowledge University, Erbil, Iraq.
E-mail: abdulqadir.abdullah@knowledge.edu.krd

Received: Mar 27, 2019
Accepted: Apr 09, 2019
Published: Aug 20, 2019

DOI: 10.24086/cuesj.v3n2y2019.pp1-4

over very large spread bands. However, FH can be efficiently jammed by follower jammers (also called "repeat back") under certain conditions. In follower jamming, the jammer intercepts the transmitted signal, tries to determine the frequency of the hop, and then generates jamming in a narrow range about this frequency. It is the purpose of this article to discuss design considerations to account for such jammers.[4] Figure 1 shows the block diagram of a simple follower jammer design.

Design Consideration of the Follower Jammer

Bluetooth wireless network uses the FH techniques which operates in the 2.4 GHz ISM band over 79 MHz bandwidth. This bandwidth is divided into 79 channels, and each channel has 1 Mbps capacity; the time for transmission is separated among 625 μs slots, where each slot uses a new hop frequency technique, as shown in Table 1.[1,3]

According to these specifications, the design of the follower jamming must cover the band of frequency between 2402 MHz and 2482 MHz with sensitivity <-70 dBm and an output between 0.5 watt and 1 watt. In order to achieve this, the antenna that must be used must be an omnidirectional antenna covering 360° in elevation and 60° in horizontal, as shown in Figure 2.[5]

The band-pass filter must be passing the frequencies between 2402 and 2482 MHz with low attenuation around 2 dB and reject rest frequencies out that range with attention −80 dB (fourth-order filter), as shown in Figure 3.

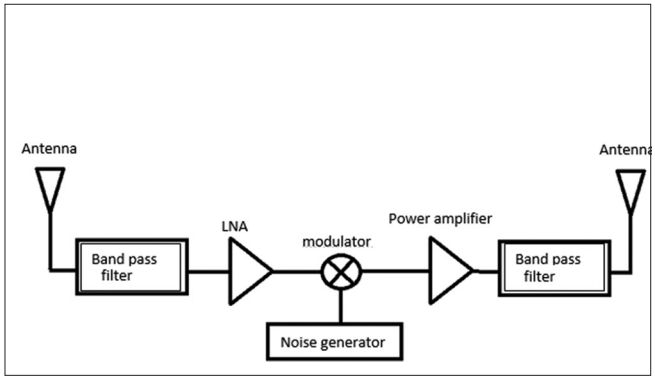

Figure 1: Follower jammer block diagram

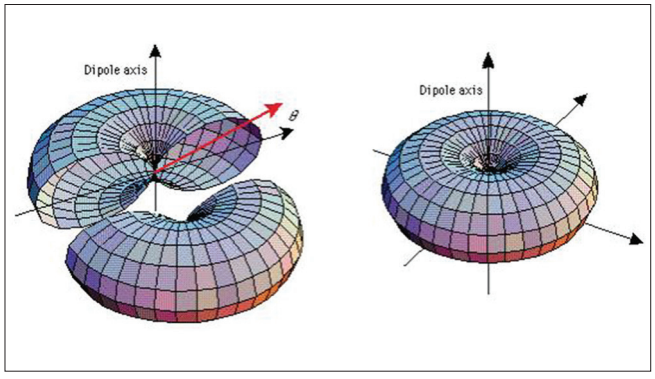

Figure 2: x-y plane omnidirectional antenna

The low-noise amplifier is designed to receive the Bluetooth frequencies and amplified for suitable level, as shown in Table 2.

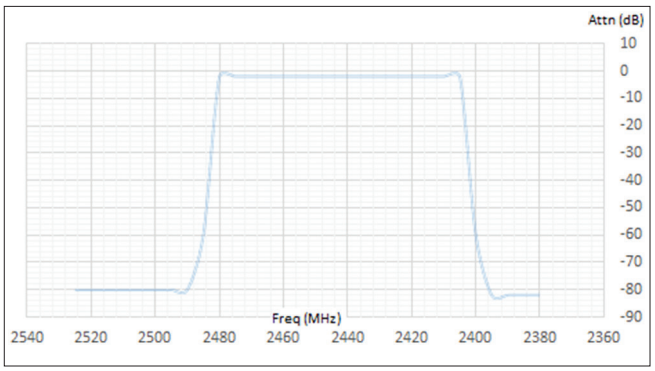

Figure 3: Band-pass filter characteristic

Table 1: Specification of Bluetooth network

Items	Specification
Power o/p	1 mw
Channel B.W.	1 MHz
Operation bandwidth	79 MHz (2402–2482) MHz
Processing gain	19 dB
Receiver sensitivity	−70 dBm
Transmitting time	625 µs
Equipment distance	(0.30–1.2) m

Table 2: Low-noise amplifiers characteristic

Parameters	Min. – typ. – max.	Units
Frequency range	2400–2480	MHz
Gain	20	dB
Noise figure	3.5	dB
RF input 1 dB compression point	18	dBm
Input third-order intercept point	23	dBm

Table 3: Modulator specification

Parameters	Min. – typ. – max.	Units
RF frequency range	2400–2480	MHz
IF input bandwidth range	0.5	MHz
Lo input frequency range	2400–2480	MHz

Table 4: The calculation of the delay and attenuation for the different distances

Distance	Delay	Attenuating
1 m	6.66 ηsec	40.19 dB
5 m	33.3 ηsec	54.17 dB
10 m	133.2 ηsec	60.17 dB

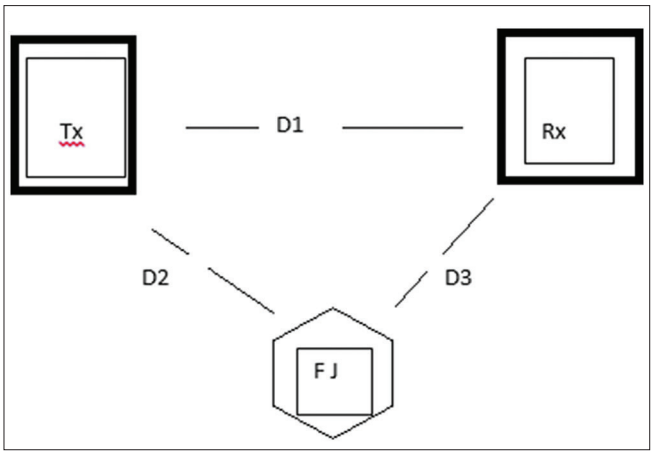

Figure 4: Bluetooth network with jammer

The modulator should consider the specification, as shown in Table 3.

The noise generator can use Pin diode (PN) noise generator with clock 500 KHz or PIN diode or a Zener diode with amplifier and low-pass filter 500 KHz.

The power amplifier is going to amplify the modulated Bluetooth frequencies by the noise. The output power was around 1 watt or 30 dBm to satisfy the jamming-over-signal ratio (J/S) >3 dB. The filter and antenna are considered the same as mentioned before.

THE CRITICAL POINT IN THE FOLLOWER JAMMER

The time response of the jammer and time wave traveling from Bluetooth sender to the jammer and from the jammer to Bluetooth receiver must reduce the delay as much as possible to follow transmitting time of the Bluetooth network.

If we consider the wave speed at 3×10^8 m/sec, meaning the wave traveling 1 m during 3.33 ηsec and this time is very short comparing with the time of the transmission time which is 625 μsec and that gives the confidence in the method.

OPERATION CONSIDERATION

An important consideration is the distance of the jammer from the Bluetooth network. For the design parameters in this research work we considered the distances where the Jammer is located at 1, 5, and 10 m from the Bluetooth network, as shown in Figure 4. For this purpose, the distances D2 and D3 which represents the distances of the jammer from the Bluetooth units as D2 and D3 are equalt to (1, 5, or 10 m).

The delay and the attenuation based on the different distances D2 and D3 were calculated. The calculations are shown in the Table 4.

The estimation of the timing coverage on the frequency slot according to the distance can be seen in Table 5 which shows the percentage time coverage on frequency hop, as we notice that the effect of delay from the distance is almost negligible.

Table 5: Percentage time coverage on frequency hop

Distance	Delay	Percentage ratio
1 m	6.66 ηsec	99.999
5 m	33.3 ηsec	99.994
10 m	133.2 ηsec	99.978

Table 6: Bluetooth network link budget

Item	Value	Units
Output power	0	dBm
path attenuation @1 m	40.19	dB
Sensitivity	−70	dBm
Processing gain	19	
Gain margin	46.81	dB

Table 7: Calculations of the J/S with respect to distance

Distance	J dBm	J/S dB
1 m	−9.81	57.38
5 m	−24.17	43.02
10 m	−30.17	37.02

J/S: Jamming-over-signal ratio

In order to do a scientific comparison with Bluetooth wireless network specification and the follower jammer, we must calculate the link budget for all cases to find the effect from the power view and J/S ratio (Table 6).

With the follower jammer technique, the gain processing will be neglected because it uses the same frequencies at the same time, so that the gain margin against this technique will change from 19 dB and will become 23.81 dB. Then, the Bluetooth power at 1 m will be=−114+46.81=−67.19 dBm. Table 7 shows the calculation of the J/S with respect to distance. From the results shown here, it is clear that this technique will affect the Bluetooth wireless network and blocks it.

CONCLUSION

Many jamming techniques have been used to disrupt Bluetooth wireless networks for many purposes. One useful way of jamming BW networks is when it is used by unauthorized persons. In this article, an approach was studied using the follower jammer in order to evaluate its effects on the network. The design considerations were followed in order to come up with the best results. From the test results, we can determine that the jammer follower can disrupt successfully a Bluetooth network when it can receive the Bluetooth signal. It was noticed that in order to avoid the circulation path from transmitter of the jammer to the jammer receiver, the antenna of the jammer must be isolated between them with using RF switch Single Pole Single Throw (SPST) controlled by signal output of the power amplifier.

REFERENCES

1. D. S. Kushwaha. “Application of blutooth wireless technology”. *International Journal of Mathematics and Computer Research,* vol. 1, no. 3, pp. 79-82, 2013.
2. P. Patel, A. Merchant, N. Tailor and C. Trivedi. “Bluetooth security issues”. *International Journal of Computer Science and Information Technologies,* vol. 6, no. 6, pp. 5295-5299, 2015.
3. A. H. M. Al-Dalowi and G. QasMarrogy. “Performance evaluation of noise power jammer on the Bluetooth network”. *International Journal of Computer Networks and Communications,* vol. 6, no. 5, pp. 167-174, 2014.
4. E. B. Felstead. “Follower Jammer Considerations for Frequence Hopped Spread Spectrum”. IEEE Military Communications
5. P. D. Vita. “Antenna Selection Guidelines”. ST Microelectronics, Switzerland, 2012.