Wireless Network Behaviour during Jamming Attacks: Simulation using OPNET

Hadeel S. Obaid
University of Information Technology and Communications, Baghdad/ Iraq.

hadeel.obaid@uoitc.edu.iq

Abstract. Jamming-style attacks can be launched easily on wireless networks because they are built upon a shared medium. These attacks can be performed by emitting radio frequency signals. These signals do not follow an underlying MAC protocol and can highly interfere with the normal operation of wireless networks. Jamming attacks represent the denial of service attack in wireless networks. In this paper, we have used OPNET Modeler to perform jamming attacks to investigate wireless network behavior. The results showed that the investigated jamming attacks can cause severe performance degradation into wireless networks and jamming attack is successfully avoided by using channel switching technique.

1. Introduction
Due to the open nature of the wireless medium, wireless networks are vulnerable to many security threats. Using a transceiver, ongoing transmissions can be eavesdropped, blocked the transmission of legitimate users or injected with bogus messages. Jamming wireless transmissions is one of the major methods to degrade the network performance [1]. In the jamming attack, the attacker distorts transmitted messages by producing electromagnetic interference in the active frequencies of the wireless network. The continuous emission of high-power interference signals for example continuous wave tones or FM modulated noise is the typical jamming approach. But, there are several disadvantages in adopting an “always-on” jamming approach. First, this form of attack is easy to detect in the continuous presence of high interference levels. Second, to jam frequency bands of interest, the attacker has to expend a significant amount of energy. Third, it is easy to mitigate these attacks either by spatial retreats, spread spectrum communications, or removal and localization of the jamming nodes.

Jamming attacks are one of the most significant attacks in denial of service attacks [2]. Jamming attacks overlap with the transmission channels by transmitting semi-valid packets to interrupt the transmission between genuine nodes because wireless networks are dependent on radio channels.

Jamming attacks that target the network infrastructure have become more prevalent because of the increase in the number of wireless networks and the importance of such networks [3]. Wireless transmissions are constantly very sensitive to interference. As an example, Microsoft's Xbox is able to interfere with 802.11n networks because they both use 2.4 GHz bands. This interference can be performed using a jammer. Outside the United States, it is legal to use frequency jammers. For
example, in France, they allow using frequency jammers to ban cell phone communications in restaurants and theatres. In Italy, jammers are used to decrease the probability of academic dishonesty in exam rooms. In Mexico, jammers are used to maintain the sacredness of religious occasions. In distributed networks, Miniature jammers are used in malicious and intentional disruptions of wireless communication. Nowadays low-power tiny, jammers can be build using Nano Electro Mechanical Systems (NEMS) and Micro Electro Mechanical Systems (MEMS) which can be spread like “dust” constructing a distributed jammer network. Such a jammer has a simple function in comparison to sensors (i.e., transmitting noise signals rather than: filtering, complex modulation, or various other type of signal processing functions). In Iraq, in the second Gulf War, the United States used these techniques.

The rest of the paper is ordered as following: Section 2 presents the related work. Section 3, jamming models. Section 4 contains OPNET Simulator. Experiments and results are found in Section 5. Finally, the conclusion in Chapter 6.

2. Related Work

The Osanaiye et al proposed a step-wise method to detect Jamming attacks using a statistical procedure control mechanism [4]. To detect peculiar changes in the intensity of a jamming attack event, they used an exponentially weighted moving average (EWMA) by using the packet inter-arrival feature of the received packets from the sensor nodes. The results acquired from a trace-driven simulation proved that the jamming attacks in WSNs can be accurately and efficiently detected using the proposed solution with no or little overhead.

Navda et al. explored the protection of 802.11 networks from jamming attacks by hiding the transmission of the legitimate transmission hop among channels from the jammer [5]. They explored the amount of throughput that can be preserved in comparison to the sustainable throughput in a jam-free environment by deploying a combination of prototype experimentation and mathematical analysis in an 802.11a environment. The results demonstrated that about 60% of the original throughput can be attained in today’s traditional 802.11a networks.

Sampath and colleagues explored the impact and feasibility of cognitive radio based jamming attacks on 802.11 networks [6]. They showed that cognitive radios’ fast channel switching capability can be used by the attacker to strengthen the jamming effect through several channels using a single radio. In addition, they examined the effect of jamming duration and hardware channel switching delays on the power of jamming.

Fang et al. proposed an anti-jamming communication [7]. The proposed system allows communication in a high power reactive jammer environment. To use the system in scenarios where conventional methods fail, the system does not assume a reactive jammer with limited transmit power and spectrum coverage. Using GNURadio, they developed a prototype of the proposed system. The evaluation of the experiment showed that the prototype still keeps communication in the presence of a powerful reactive jammer while schemes such as 802.11 DSSS failed entirely.

Zuba et al. studied the impacts of denial-of-service jamming attacks on underwater acoustic networks (UANs) using real-world field tests [8]. In order to examine the characteristics of different models of jamming attack on a network, they developed their own jammer hardware and signals. The experiments are applied on an orthogonal frequency division multiplexing modem prototype and several commercial brand acoustic modems and. The results showed that using carefully timed attacks, UANs can be easily jammed.

Bhattarai investigated the effect of jamming attacks on the performance of LTE networks [9]. To explore different jamming threats, they developed a three dimensional theoretical space. Using the dimensions of this space, they built a set of attack scenarios. They used ns-3 to implement the scenarios to evaluate the attacks based on standard network metrics and to observe the impact on the performance LTE network. The results showed that the performance of LTE networks can be easily degraded when the investigated jamming attacks are present.
3. Jamming Models

There are four main jamming models. Jamming models capture strategy, which follow the malicious attacker [10]. These models are characterized by effectiveness and simplicity:

Constant jammer: this jammer transmits radio signals continually to the wireless medium. Signals contain a totally random bits’ sequence; the rules of any MAC protocol apply electromagnetic energy transmissions. The aim of the jammer is twofold: (a) to form interference on transmitting nodes to mess their packets at the receiver and (b) to make legal transmitter sensing the channel busy, as a result prohibiting legitimate transmitter from accessing the medium.

Deceptive jammer: this jammer is identical to the constant jammer in that it continually transmits frequencies. However, the variation is that in the deceptive jammer the emitted frequencies are non-random. This jammer repeatedly transmits bits at regular intervals using a channel with no breaks between communications. This makes the user sensing the medium believe that the transmission is legal. Therefore, any machine would stay in sensing mode even if it should send data. Another significant variation is that this jammer is harder to detect by monitoring tools of the network because these tools sense legal broadcast on the channel. The disadvantage for both of the mentioned jamming techniques is power effectiveness. Transmitting signals continuously to a wireless channel reduces the jammers' capability of being independent on an external source of power.

Random Jamming: this jammer is more power effective. Attacks that use random jamming, tj seconds jams and applying ts seconds of sleep. Where tj and ts are variable, different aggressiveness and power savings levels are achieved; different jamming cycles create different tj and ts. Deceptive and constant jamming attempt to interfere with the packets reception and try to prevent transmission when CSMA is used, where this decreases the power and effectiveness of the jammer.

Reactive jammer: this jammer is power effective because it aims at the reception of a packet. There is permanent sensing of the medium, and when sensing a transmission of a packet, it directly emits a radio signal causing a collision at the receiver. Recent standards for wireless data communications are now working in favour of the jammer. For instance, IEEE 802.11 for a PHY layer does not assist in error correction. The jammer may send enough power to distort a single bit to make a received packet fail the cyclic redundancy check (CRC). For this protocol, wireless systems have been designed to be resilient to non-malicious, including noise, interference. The jammer can take advantage of this and effectively employ low power that deactivates the entire communication network.

4. OPNET Simulator

OPNET is a simulator tool that simulates any network and shows its performance and behaviour [11]. OPNET is different from other simulators in its versatility and power. This tool works with the OSI model from the Application layer to the Physical layer. Moreover, OPNET software has some characteristics over other simulation tools. For instance, OPNET provides a graphical environment to design a network topology and simulate a network authentically that users can then start gathering information about the network and monitor them. One more advantage of OPNET is widely used for its reliability in creating simulated results.

Below, we have used the OPNET Modeler 14.5, which is a high-level tool for network simulation [12]. It allows the design and analysis of communication networks, types of devices, applied protocols, and user application. Technology and government organizations such as Pentagon, UIC and MIT use this modeler to speed up the R&D process. It enables one to develop models from real world networks and protocols.

Parameters such as throughput, load, data dropped and delay are used in our experiments. Below is the definition of each one of them:

1. Throughput: relates to the overall amount of data traffic where it is received and dispatched by the Media Access Control layer (MAC) to a higher layer and it is measured in bits/sec.
2. Delay: defines the delay of the packets that are received by the MAC layer and sent to the upper layer which is measured in sec.
3. Load: the data amount that are transmitted in the wireless network and measured in bits/sec.
5. Experiments and Results

In our experiment, we simulate DoS jamming attacks. The objective of this experiment is to simulate DoS jamming attacks and study their effects, analyse and compare them in cases of normal traffic and assess them in situations of DoS jamming attacks. We have three WLANs scenarios to test the effect of DoS jamming attacks. In OPNET, there are several types of jammers. We have chosen the fixed node Pulsed jammer to jam the WLAN. A pulsed jammer emits noise with power spreads over the entire bandwidth of the system [13]. The idea of the pulsed jammer intensifies the jamming power through the “on” time to badly disrupt the communication system [14]. Our experiment consists of three scenarios. Scenario1 (normal traffic), Scenario2 (DoS jamming traffic) and Scenario3 (Channel switching prevention).

5.1. Scenario1

Scenario1 represents normal traffic where there is no DoS jamming attack and the network should work smoothly without any disruption are shown in Figure 1. The topology of this includes:

- One access point (wlan_ethernet_slip4_adv).
- One server (ethernet_server).
- One switch (ethernet32_switch).
- Eight fixed workstations (wlan_wkstn_adv).
- One Profile configuration.
- One Application configuration.
- 100BaseT to connect the access point to the switch and connect the switch to the server.

In the application configuration, we can specify the application is running in the network. In order to have a normal traffic, we have chosen a videoconference application to be run in the network with a low-resolution video application at ten frames/second and 128x120 pixels. We have kept the configuration for the other devices as default. The Switch, the Server and the Access Point are connected via a 100 Base T duplex link. The eight workstations all have the same characteristics and are modelled by wlan_wkstn_adv.

![Figure 1: scenario 1 normal traffic topology](image-url)
5.2. Scenario 2

In Scenario 2, Scenario 1 is duplicated, and the same configurations and attributes for all the network nodes are kept [15]. However, the Pulsed jammer to the network is added to display the effects of the DoS jamming attack on the network. The pulsed jammer is designed to cyclically interfere which is a result from a periodic pulse train and a band pass white noise. The base frequency of the pulse jammer is set to 2401MHz with 22MHz bandwidth. This frequency can only affect channels 1 and 5. The pulsed jammer attributes are shown Figure 2. The process model of the pulse jammer is indicated in Figure 3. Also, the jammer consists of a radio transmitter and a source as shown in Figure 4.

![Figure 2: pulsed jammer attributes](image1)

![Figure 3: pulse jammer process model](image2)
Figure 4: pulse jammer components

Three different states control the signal that is generated in the source. The first state is “wait for the first pulse” if packets are allowable to send. The second state “TX_ON” controls packets being sent from source to the radio transmitter. The third state is “TX_OFF” generate and schedule pulses. We add the codes for the pulse generator in the process model of the pulsed jammer in the “TX_ON” state as shown Figure 5. Also, the “TX_OFF” state is added as shown Figure 6. The network topology when it is under DoS jamming attacks Figure 7.

Figure 5: codes in the “TX_ON” state
Figure 6: codes in the “TX_OFF” state

Figure 7: jamming topology
5.3. Scenario 3

In this scenario, prevention of a DoS jamming attack on the network using channel switching is applied. Channel switching or hoping from a channel to another is the most common prevention of jamming [18]. Based on IEEE 802.11 standards, devices in the wireless networks use channels to communicate with each other. The wireless channels are determined by frequencies. Each channel is defined by a range of frequencies (e.g., Channel 1 frequencies) that range from 2.401 GHz to 2.423 GHz and the frequency centre is 2.412 GHz. Figure shows the ranges of frequencies for each channel. 5MHz is the interval of each channel. Because of this interval, only 3 channels are independent, which are channels 1, 6 and 11 as shown in Figure 8:

![IEEE WLAN 2.4GHz channels](image)

**Figure 8: IEEE WLAN 2.4GHz channels**

In OPNET, all devices include access points that are automatically allocated to Channel 1. Jammers in OPNET are assigned to Channel 1, which has a 2,401 MHz frequency. In scenario 3, the transmission of the wireless network is switched from Channel 1 to Channel 6. All nodes including the Access Point, are switched to Channel 6. When the channel setting is switched to Channel 6, the frequency of the channel is also changed to 2426 MHz and 22 MHz bandwidth. The jammer will continue the transmission on Channel 1 with the DoS jamming prevented. The channel in all the workstations in the wireless network have been switched to Channel 6. Also, the attributes of the Access Point show that the transmission channel is switched to Channel 6 as shown in Figure 9:

![access point attributes](image)

**Figure 9: access point attributes**
5.4. Scenario 1 and Scenario 2 Results Comparison

Figures 10 & 11 show that the delay in scenario 2 has increased because of the DoS jamming in all the devices of the network. For example, the delay in node 7 has increased from 0.65 sec to 0.9 sec. Figures 12 & 13 show the increase in delay after the jammer is introduced in the network. Regarding scenario 1, node 3 average delay is 0.697 sec. After jamming the network in scenario 2, node 3 average delay is 0.875 sec. The Access Point average delay in scenario 1 is 0.269 sec but in scenario 2 it is increased to 0.362. Therefore, the jammer causes a delay in all devices of the network. Figure shows a comparison of the overall delay results in the network.

Figure 14 shows a comparison of the overall delay results in the network. The blue line represents the delay in the network with DoS Jamming. The red line is the delay in the network with no DoS Jamming. The delay in the network was 0.40 seconds without jamming. It is then increased to 0.54 seconds when the jamming is present in the network.

Figure 15 & 16 shows the throughput in Ave, Min, Max and STDev. The Average throughput of the Access Point in scenario 1 is 1,153,892 bits/sec and then becomes 870,963 bits/sec in scenario 2 due to the DoS jamming attack. If we look at other nodes, we can see a drop in the throughput. For example, node 5 Average throughput was 112,966 bits/sec in scenario 1 and decreases to 76,804 bits/sec in scenario 2; this is an indication of the degradation in performance of the network. While Figure 17 illustrates the overall throughput in the network. The red line is the throughput in the normal traffic network and the blue line is the throughput in the Jamming network. The throughput in the network dropped from about 1,780,000 bits/sec to nearly 1,380,000 bits/sec.

![Figure 10: Scenario 1 Delay Results](image1)

![Figure 11: Scenario 2 Delay Results](image2)
Figure 12: delay in scenario 1

Figure 13: delay in scenario 2

Figure 14: jamming measurements
5.5. Scenario 2 and 3 Results Comparison

To see the effect of channel switching on the network while the pulsed jammer is presented in the network, a comparison between scenarios’ 2 and 3 results is applied. We see that the delay in the network has dropped when the channel is switched as shown in Figures 18 &19. For example, the delay in the Access Point was 0.35 seconds then it decreased to 0.22 seconds. The delay in node 7
dropped from 0.9 seconds to 0.55 seconds. The performance of the wireless network improved when the communication channel is switched to channel 6.

Figures 20 & 21 display more detail about the delay. The average delay in the access point in the DoS jamming network was 0.362 seconds and became 0.225 seconds when the jamming is prevented by channel switching. This is also true for the other nodes in the network.

Regarding the throughput, Figure 22 & 23 display the throughput results in the wireless network devices. In Figure 22, the jamming is prevented using the channel switching technique. For example, the throughput is increased in the Access Point from around 900,000 bits/sec to around 1,490,000 bits/sec. Also, in node 1, the throughput is improved from about 180,000 bits/sec to 250,000 bits/sec. While, Figure 24 illustrates a comparison between the delay in the access point in scenarios 2 and 3. The delay is dropped in the channel switching from 0.35 sec to 0.23 sec.

Figures 25 & 26 show the throughput in the channel switch scenario and DoS jamming scenario. The throughput is enhanced in the network when applying the channel switching prevention. In the access point, the average throughput is elevated from 870,963 bits/sec to 1,321,038 bits/sec; the same occurs in the other devices in the network.
Figure 21: delay measurements in scenario 3

Figure 22: wireless LAN throughput scenario 2

Figure 23: wireless LAN throughput scenario 3

Figure 24: delay in the access points in scenario 2 and scenario 3
6. Conclusion
The jamming attack was launched using the pulsed jammer. The pulsed jammer sends pulsed signals to interfere with proper signals coming from legitimate nodes and occupies the transmission channel. Scenario 1 is the normal network where no jammer is present in the network and Scenario 2 is the attack network where a pulsed jammer attacks the network. The results show that the delay in the network is increased because of the pulsed frequencies that come from the jammer (i.e. the packets take more time to be received by the MAC layer and sent to the upper layer). Moreover, the overall throughput in the network is decreased significantly (i.e. some of the packets have failed to be received and dispatched by the Media Access Control layer (MAC) to a higher layer). This proves that the pulsed jammer degrades the performance of the network and many packets fail to be received by the MAC layer and are dropped causing a denial of service. In Scenario 3, the channel switching approach is used to avoid the jamming attack. The result shows that channel switching is a successful defence against the pulsed jammer, where the jammer continues to transmit using channel 1 and the network devices have been switched to channel 6.

References
[1] Proano, A., and Lazos, L.: ‘Selective jamming attacks in wireless networks’, (IEEE, 2010), pp. 1-6
[2] Bandaru, S.: ‘Investigating the Effect of Jamming Attacks on Wireless LANS’, International Journal of Computer Applications, 2014, 99, (14), pp. 5-9

Figure 25: delay in the access points in scenario 2

Figure 26: delay in the access points in scenario 3
[3] Akhter, S., Myers, J., Bowen, C., Ferzetti, S., Belko, P., and Hnatyshin, V.: ‘Modeling DDoS Attacks with IP Spoofing and Hop-Count Defense Measure Using OPNET Modeler’, (2013), pp.

[4] Osanaiye, O., Alfa, A., and Hancke, G.: ‘A statistical approach to detect jamming attacks in wireless sensor networks’, Sensors, 2018, 18, (6), pp. 1691.

[5] Navda, V., Bohra, A., Ganguly, S., and Rubenstein, D.: ‘Using channel hopping to increase 802.11 resilience to jamming attacks’, (IEEE, 2007), pp. 2526-2530.

[6] Sampath, A., Dai, H., Zheng, H., and Zhao, B.Y.: ‘Multi-channel jamming attacks using cognitive radios’ (IEEE, 2007), pp. 352-35.

[7] Fang, S., Liu, Y., and Ning, P.: ‘Wireless communications under broadband reactive jamming attacks’, IEEE Transactions on Dependable and Secure Computing, 2015, 13, (3), pp. 394-408.

[8] Zuba, M., Shi, Z., Peng, Z., Cui, J.H., and Zhou, S.: ‘Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks’, Security and Communication Networks, 2015, 8, (16), pp. 2635-2645.

[9] Bhattarai, S., Wei, S., Rook, S., Yu, W., Erbacher, R.F., and Cam, H.: ‘On simulation studies of jamming threats against LTE networks’, (IEEE, 2015), pp. 99-103.

[10] Pelechrinis, K., Iliofotou, M., and Krishnamurthy, S.V.: ‘Denial of service attacks in wireless networks: The case of jammers’, IEEE Communications surveys & tutorials, 2010, 13, (2), pp. 245-257.

[11] Seyed Hasan Mortazavi Zarch, S.H.M.Z.a.M.Y.: ‘Attacks Simulation On Computer Networks By Simulator’, Journal of Engineering Computers & Applied Sciences, 2014, 3.

[12] Fazeli, M., and Vaziri, H.: ‘Assessment of throughput performance under opnet modeler simulation tools in mobile ad hoc networks (manets)’, (IEEE, 2011,), pp. 328-331.

[13] Coelho, B.B.: ‘Time-Frequency Jammer excision for Multi-carrier spread spectrum using adaptive filtering’, University of Pittsburgh, 2006.

[14] Tse, C., and Lau, F.: ‘Chaos-based digital communication systems’, Operating Principles, Analysis Methods and Performance Evaluation, 2003.