Physical Layer Jamming Attack using Waypoint Mobility Model in WLAN

Ahmad Yusri Dak[1]*, Nurul Fazliana Samsudin[2], Noor Elaiza Abdul Khalid[3]
[1,2] Faculty of Computer and Mathematical Science, University Teknologi MARA Perlis, Malaysia
[3]Faculty of Computer and Mathematical Science, Universiti Teknologi MARA Shah Alam, Selangor, Malaysia

*Corresponding author: ***yusri@tmsk.uitm.edu.my***

Received Date: 13 August 2018
Accepted Date: 4 October 2018

ABSTRACT

Sharing nature of wireless medium provides various challenging features among various group of users. This is one of various services offered by Wireless Local Area Network (WLAN). Thus, due to popularity of WLANs, user experience suffers from various security threats especially jamming based Denial-of-Service (DoS) attack. The attacks are focused on radio channels where the transmission channel interfere with jamming attacks by sending high frequency signal to disturb the communication between the users in network. Most of attack exists at physical layer are detected randomly movable and less static attack are found. Therefore, the objective of this research is to study the pattern of randomly movable node and performance of physical layer jamming attack using Waypoint Mobility Model. To address these evaluation, a simulation model consists of physical layer jamming attack will be developed using OPNET. The performance involved physical layer attack that are evaluated using three performance metrics which is Bit Error Rate (BER), Signal-to-Noise Ratio (SNR), and throughput. Outcome concluded that these three-performance metrics show as a significant impact as detection mechanism and offer a future comprehensive research based on DoS attack.

Keywords: *DoS, Physical layer, WLAN, detect*

INTRODUCTION

Wireless Local Area Network or WLAN is a wireless dispersal technique for two or more device that often include an access point to the Internet and use a high-frequency of radio waves. In WLAN environment, while maintaining the network connection, the user can move freely around the coverage area such a home or small office. The significant of social impact are along with the playing an integral part of our life with the existence of wireless communications. Nevertheless, the industrial evolutions in wireless network have criticized the privileges made by devotees of wired networks by (Hangargi, 2016). The facts that, the standard for wireless communication is intangible. The guarantee of whenever and anyplace availability must be satisfied by wireless networks. Voice, video and other real time interactive service is the remaining challenges before the wireless local area network can effectively support by (Song, Deshpande, Kotz, Jain, & Jose, 2005).

Denial of service (DoS) attacks is a malicious node that block legitimate communication by intentional interference in the network(Subha & Selvi, 2014). Security issues and attacks management have become prime importance for communication in wireless networks. Due to the transmission environment of the wireless systems are highly exposed to attacks. Denial of Service (DoS) attacks are considered as one of the most destructive attacks by (Navid, 2017). Denial-of-Service (DoS) attack is one of the common attacks that defenseless in data network. Security system in the nowadays on guarding against DoS attacks should be taken seriously (Goyal, 2014). According to (Hangargi, 2016), virus, worm and malware are the old school of threat when it is compared to DoS attacks because DoS attacks have a potential to undermine the advantages that come with wireless data network. One of DoS attacks that occur in physical layer is jamming attacks, where DoS attack was acts to minimizes or destroys a network capacity and obstructs it to perform its expected functions. Physical layer is highly susceptible to jamming attacks as it is used for frequency selection and modulation (Jaitly, 2017).

The reputation of WLANs meets a continual increase in security attacks against WLANs, and the 2005 survey from Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) shows that WLAN manipulations (i.e., security attacks) is the only "growing" threat of computer crimes . These DoS attacks cause the WLAN or some of its wireless nodes out of services. As DoS attacks against WLANs become more and more common, this thesis is to investigate physical layer DoS attack in WLAN and simulated the DoS attack using dynamic movement model with random and constant jammer. More specifically, physical layer attacks on the Ethernet networks are covered. The focus is on wireless networks, since WLAN is the most widely used nowadays. Physical layer attacks are selected because they are the hardest to detect but easier to generate. This research is conducted for further understanding of constant and random jammer where the result in the research will be compared from performance matrices of Bit Error Rate (BER), Signal-to-Noise Ratio (SNR) and throughput.

RELATED WORKS

Kumar et al. (2017) proposed a study to analyze the performance of DoS attack in an office environment. Global Wireless LAN Delay, Global DB Query Traffic Sent, Global DB Query Traffic Received, Node IP Traffic Dropped, Point-to-Point Queuing Delay, Point-to-Point, throughput and Point-to-Point Utilization are measured to detect the presence of a jammers which utilizes frequency sweeping. A comparison of performance under the normal conditions and DoS scenario were analyzed. As a result, the defense mechanism is not achieved the maximum reliability on what DoS claims and improvement the Quality of Service (QoS) of WLANs has the effects of DoS attack. In addition, (Yubo & Xi, 2009) investigated by analyzing the third version of WAI in WAPI standard using finite-state verification tool named Mur Modeling in WLAN environment. The result or weaknesses of WAI is insecure against DoS attack both in certificate authentication and key agreement. Researcher also conducted an experiment to mitigate and detect DoS attack by using Software Defined Networking concept (SDN) that combine OpenFlow architecture for SDN with Monitoring API to study this case. The outcome of this research is a defence applications should be there configured to completely secure the customer network and time security related to communication between control and data plane should be secure.

Kim et al. (2006) propose a DoS detection method via reflecting resource constraints of sensors in Hierarchical Sensor Networks. And the result of this study, the researcher state that the method is calculated with only multiplication operation instead of algorithm. (Pawani & Raj, 2007) study about mitigation of jamming attack in mobile ad hoc networks. The research was held because of conventional security mechanism cannot eliminated the radio disturbance. This study is in Medium Access Control (MAC) protocol which involve jamming attack. The researcher proposed several techniques such as there have Point Controller Functions (PCF) that are used to coordinate entire network activities at the MAC layer and RTS/CTS (Clear-To-Send) mechanisms which is a handshaking procedure that decreases the collisions on the wireless network used for mitigating and preventing jamming attack.

Table 1 below show the comparison of research conducted in WLAN environment mostly by comparing what are their technique or methodology and weaknesses.

Table 1 Summary of DoS attack in Wireless Network

Author	Technique/ Methodology	Types of wireless network.	Weakneasses
(Kumar, Abdelfattah, Holbrooks, & Perez, 2017)	Analysed : Global Wireless LAN Delay, Global DB Query Traffic Sent, Global DB Query Traffic Received, Node IP Traffic Dropped, Point-to-Point Queuing Delay, Point-to-Point Throughput, Point-to-Point Utilization	WLAN	Defense mechanism is not achieve the maximum reliability on what DoS claims and improve the Quality of Service (QoS) of WLANs as the research is to exolired the effects of DoS attacks on WLAN (campus) .
(Yubo & Xi, 2009)	Analyse the third version of WAI in WAPI standard, using finite-state verification tool named MUR? MODELING	WLAN	The third version of WAI is insecure against Denial of Service attack both in certificate authentication and key agreement.
(Navid, 2017)	Using Software Defined Networking concept (SDN) combine OpenFlow architecture for SDN with Monitoring API is used to detect and mitigate DoS attack.	Wireless network.	What kind of API and applications should be there to completely secure the customer network. time security related to SDN is also a concern e.g. as controller is the central point so it central point of failure is introduced in the system. communication between control and data plane should be secure.
(M. Kim, Doh, & Chae, 2006)	Practical Entropy Estimation	Hierarchical Sensor Networks	calculated with only multiplication operation instead of logarithm,
(Pawani & Raj, 2007)	The researcher proposed several technique such as there have Point Controller Functions (PCF) that are used to coordinate entire network activities at the MAC layer and RTS/CTS (Clear-To-Send) mechanisms which is a handshaking procedure that decreases the collisions on the wireless network used for mitigating and preventing jamming attack	Mobile Ad Hoc Networks	The jamming attack yields packet drop rate and low throughput effect on the network, the rate of delay appears acceptable on the network.

METHODOLOGY

OPNET R13 simulation tool is used to establish two proposed scenarios. Jammers such as constant and random are configured and setting to act out based on 802.11 environments. Scenarios 1 and 2 were established for generating jamming attack at physical layer.

Both simulation model is configured with Random Waypoint Model where node selects a random destination in the simulation area at random speed between 0 (excluded) and some maximum speed. The node moves to this destination and again pauses for a fixed period before another random location and speed. This behaviour is repeated for the length of the simulation.

Scenario 1: Constant Jammer:

Jammer is configured to continuously send high frequency with constant packet and meaningless signal to the channel disregarding the MAC protocols. Table 2 presented a simulation configuration for constant jammer.

Table 2. Parameter to simulate constant jammer

Parameters	Attributes
Protocol	Random Waypoint Model
Simulation Time	7200 seconds
Simulation Area	100 x 100 meters
Data Rate(bps)	11 Mbps
Packet Size(bits)	1024
Transmit Power(W)	0.05 Watt
RTS Threshold (bytes)	1024(bytes)
Modulation	BPSK
Packet Interarrival time(seconds)	Constant(1.0),
Performance Parameters	Throughput, BER, SNR

Scenario 2: Random Jammer:

Random jammer is setting to alternate between jamming attack and sleeping mode. In brief, the jammer performs a random period then shut down the jammer for another random period of time. Table 3 shows a parameter to configured random jammer.

Table 3: Parameter to simulate random jammer

Protocol	Random Waypoint Model
Simulation Time	7200 seconds
Simulation Area	100 x 100 meters
Data Rate(bps)	11 Mbps
Packet Size(bits)	1024
Transmit Power(W)	0.05 Watt
RTS Threshold (bytes)	1024(bytes)
Modulation	BPSK
Packet Interarrival time(seconds)	Random
Performance Parameters	Throughput, BER, SNR

Metrics Used to Measure Performance

(Bit Error Rate) BER

BER is proposed as a metric to detect reactive jammer that occurr at MAC layer of protocol stack. Strasser et al. (2010) and Xu et al. (2006) described in their research that metrics such as BER is a very effective metric for detecting protocol jamming attack for instance NAV attack and are also proven to identify reactive jamming attack.

BER can be calculated as the number of bit errors (corrupted bits) divided received at receiver side to the total number bits received by a node during a transmission session. BER is a unitless performance measure, often measured in percentage.

$$BER = \frac{number\ of\ corrupted\ bits}{Total\ number\ of\ bits\ received}\ x\ 100\%.$$

Signal to Noise Ratio (SNR)

Misra et al. (2010) calculated SNR as the percentage of received signal power at a receiver side to the received noise power (or jammer power).

a. $SNR = \frac{Signal\ Power}{Noise\ Power}$ x 100%

It is an effective metric to identify a jamming attack at the physical layer as tested by Schleher et al. (1999), Misra et al. (2010) and Kim (2010). Fragkiadakis et al. (2010) proposed anomaly intrusion detection algorithm for detecting physical layer jamming attacks using statistical characteristics of the Signal to Noise Ratio (SNR). In addition, SNR is recommended to detect traffic activities at physical layer by Misra et al. (2010) such as constant and random jammer generated from RF jamming using high frequency approaches. Therefore, SNR is an effective metric to detect physical layer attack such as constant and random jammer.

Throughput

Throughput is defined as the number of transactions per second an application can handle, or in other words the amount of transactions produced over time during a test. To evaluate it, in a first step, the aggregate throughput of one simulation run r, Th_r, is calculated as

$$Th_r = \frac{\sum_{k=1}^{n} N_{k,r} N_p}{T_{sim}}$$

where k is the number of nodes in the network, $N_{k,r}$ is the number of successfully transmitted packets of node k in run r with a packet size of N_p bits, and T_{sim} is the simulation time per run. The result of Th_r depends strongly on the placement of the nodes in the scenario. Thus, N_r runs are performed while every time the nodes are newly randomly placed. We approximate the expected value IE{}of the aggregate throughput by the mean value $\overline{Th}$ of the N_r runs:

On the other hand, throughput is used with BER to identify deceptive and reactive jammers that manipulates reservation based MAC protocols such as 802.11 DCF allowing it to bring down the network throughput essentially to zero by using limited energy Acharya et al. (2005). A few studies from Acharya et al. (2006), Zhang et al. (2008) and Goyal et al. (2014) show that network throughput dropped significantly when intelligent jammers such as deceptive and reactive is detected. In order to compare these results with Le Wang Wyglinski et al. (2011), the threshold

$$\overline{Th} = IE\{Th\} = \lim_{N_{R\to\infty}} \frac{1}{N_R} \Sigma_{r=1}^{Nr} Th_r$$

The 95% confidence interval is analysed to check if the number of runs NR is sufficient to approximate IE$\{Th\}$(Korger, 2011). Throughput (TPUT) also used as detection metrics to monitor abnormal activities like Spurious RTS/CTS at MAC layer as discussed in section 4.5.3.

FINDINGS AND DISCUSSION

This chapter presents achieved results which are based on two scenarios as discussed in previous section. Network performance test for scenario 1 and scenario 2 were compared. Network performance resulting from constant jamming and random jamming was varied from each other. Comparative analysis for both jammers was necessary to determine which jammer is more effective in causing disruption to the data transmission.

Performance test for BER

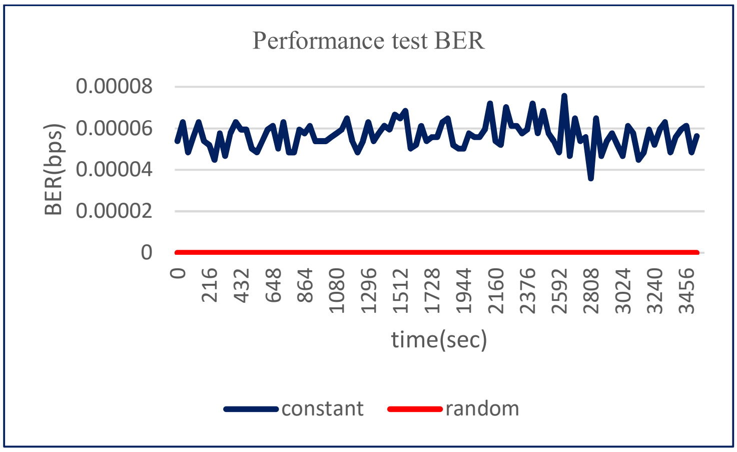

Figure 1: BER comparison for constant jammer and random jammer

Figure 1 shows the performance test for BER that is tested for constant and random jammers using Waypoint mobility model. Nodes are configured to randomly move around 100m x 100m network area. Constant and random signal are injected for each of simulation scenario and data were collected for analysis.

As presented in Figure 1, constant shows a fluctuated graph while fluctuating result displayed of constant jammer. Constant jammer has the highest BER value, which is 0.0078% compared to random jammer which is 0%. This shows that constant jammer is more effective attack in interrupting the bit transmission using constant high frequency signal. In addition, BER enable to identify constant jammer as compare to random jamming attack where transmitted bits were corrupted more often when constant jammer activated. According to Stresser et al. (2009) and Misra et al. (2010), BER is an effective metrics but calculation and updating of BER is not feasible because it involves collection of voluminous data regarding every bit of a valid and invalid packet from the leading nodes. Therefore, BER is proposed as detection metric to identify constant jammers due to impressive result collected during simulation scenario.

Performance Test for SNR

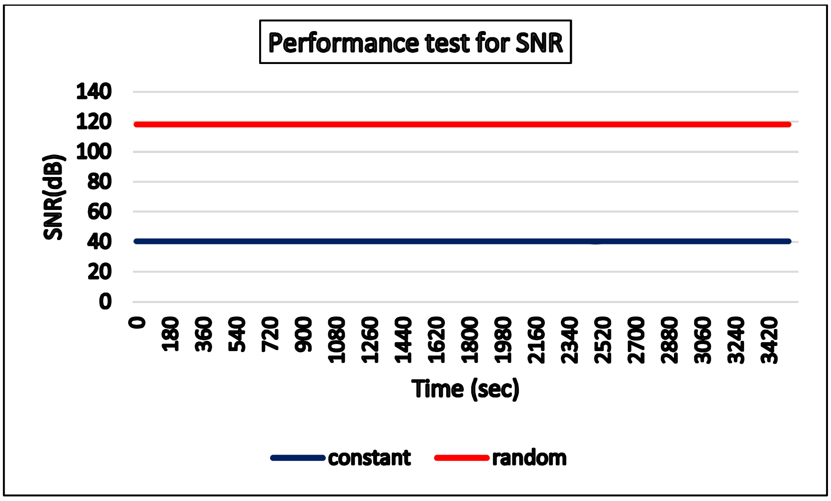

Figure 2: SNR comparison for constant jammer and random jammer

Figure 2 shows the performance result for SNR. SNR is calculated as the ratio of the received signal power to the received noise power (or jammer power) at the receiver node. The operations started when transmitter is configured to transmit signal at random time frame in order to increase the background noise in the channel and thereby causing many errors in the packet. When packet reaches the receivers it cannot be corrected the errors in the packet, therefore discarding it. From Figure 2, random jammer is most affected during sleep and active time frame. Both graph captured value between 40db and 120db due to a trade-off occurring between jamming effectiveness and energy saving. The ratios between sleeping and jamming time can be manipulated to adjust trade-off between efficiency and effectiveness. The highest SNR value that represents more noise than constant jammer. Therefore, random jammer can be assumed as more effective jammer compare to constant jammer. Therefore, SNR is an effective metric to identify a jamming attack at the physical layer as there can be no jamming without the SNR dropping low Misra et al.(2010).

Performance Test for Throughput

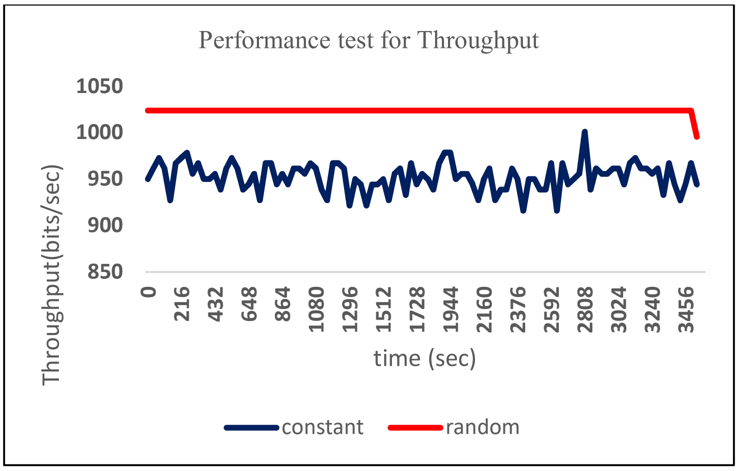

Figure 3: Throughput comparison between constant jammer and random jammer

Figure 3 shows throughput comparison between constant jammer and random jammer. Throughput is defined as the ratio of the expected delivered data payload to the expected transmission time (Ekpenyong & Joseph Isabona, 2010). It is the percentage of undistorted data packets received without errors and what the user sees after network overhead. In this section, throughput is tested to detect constant and random jammers in WLAN. Under constant attack, a node tries to gain more throughput by transmitting higher number of packets. There is more overhead required when large packets are transmitted. Therefore, less throughput detected by SNR for constant jammer as compared random jammer. It shows that SNR an effective metric to detect random jammer due to sleep and active time occur allowed more bits to arrive at the receiver.

CONCLUSION

The simulation experiment is conducted to measure the effect of movement node in WLAN when the network was flooding by packets or was under jamming attack. This research was focusing on two types of jammer which is constant and random jammer and performance analyzed based on DoS attack with dynamic movement point. As well this project is to detect the movement of DoS attack within the three performance metrics such as BER, SNR and throughput. Hence, there was two simulation that has been carried out.

Based on data collected, the conclusion for this research is the random jammer allowed more bits to arrive at the receiver compared to constant jammer. As compared to the two-performance metrics, random jammer can be concluded as the effective jammer, it is because it seems the random jammer allowed more throughput than constant jammer.

REFERENCES

Acharya, M., Sharma, T., Thuente, D., & Sizemore, D. (2006). Intelligent Jamming in 802 . 11b Wireless Networks. *Proceedings of the 2006 IEEE Conference on Military Communications MILCOM'06*, 1–10.

Acharya, M., & Thuente, D. (2005). Intelligent Jamming Attacks, Counterattacks and (Counter) Attacks in 802.11b Wireless Networks. In *Proceedings of the OPNETWORK-2005 Conference, Washington DC, USA*.

Fragkiadakis, A. G., Siris, V. A., & Petroulakis, N. (2010). Anomaly-Based Intrusion Detection Algorithms for Wireless Networks. In *Springer-Verlag Berlin Heidelberg 2010* (pp. 192–203).

Goyal, U., Gupta, M., & Kaur, K. (2014). Meliorated Detection Mechanism for the Detection of Physical Jamming Attacks under AODV and DSR protocols in MANETs. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, *3*(10), 134–144.

Kim, M., Doh, I., & Chae, K. (2006). Denial-of-Service (DoS) Detection through Practical Entropy Estimation on Hierarchical Sensor Networks. In *Proceedings of IEEE-ICACT 2006 International Conference* (pp. 1562–1566).

Kim, Y., & Lee, H. (2010). On Classifying and Evaluating the Effect of Jamming Attacks. In *The 24th edition of the International Conference on Information Networking (ICOIN) 2010, Jan. 27-29, 2010.*

Korger, U. B. (2011). *Joint PHY-MAC Cross-Layer Design in Wireless Ad Hoc Networks*. Unpublished doctoral dissertation, Technical University of Munchen, Germany.

Kumar, G., Abdelfattah, E., Holbrooks, J., & Perez, A. (2017). *Analyzing the Effect of DoS Attacks on Network Performance*.

Le Wang Wyglinski. (2011). A Combined Approach for Distinguishing Different Types of Jamming Attacks Against Wireless Networks. In *Proceedings of the 2011 IEEE Pacific Rim Conference on Communications, Computers, and Signal Processing (Victoria, BC, Canada), August 2011*.

Misra, S., Singh, R., & Rohith Mohan, S. V. (2010). Information Warfare-Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks using a Fuzzy Inference System. *Sensors 10 (Basel, Switzerland)*, *10*(4), 3444–3479.

Navid, W. (2017). *Detection and Mitigation of Denial of Service (DoS) Attacks Using Performance Aware Software Defined Networking (SDN)*. Islamabad, Pakistan.

Pawani, & & Raj. (2007). Mitigation of Jamming Attack in Mobile Ad Hoc Networks. *International Journal of Innovative Research in Computer and Communication Engineering (An ISO Certified Organization)*, *3297*(6). https://doi.org/10.15680/IJIRCCE.2016

Schleher., C. (1999). *Electronic Warfare in Information Age*. M. Artech House.

Strasser, M., Danev, B., & Čapkun, S. (2010). Detection of Reactive Jamming in Sensor Networks. *ACM Transactions on Sensor Networks 2010*, *7*(2), 1–29.

Subha, V., & Selvi, P. (2014). Detecting of Jamming Attacks in Wireless Sensor Networks. In *International Conference on Information and Image Processing (ICIIP-2014)* (pp. 155–157).

Xu, W., Ma, K., Trappe, W., & Zhang, Y. (2006). Jamming Sensor Networks: Attack and Defense Strategies. *IEEE Explore*, *20*(3), 41–47.

Yubo, S., & Xi, C. (2009). The Denial of Service Attack Analysis of WLAN Authentication Infrastructure. In *International Conference on Multimedia Information Networking and Security* (pp. 407–411). https://doi.org/10.1109/MINES.2009.209

Zhang, Z., Wu, J., Deng, J., & Qiu, M. (2008). Jamming ACK Attack to Wireless Networks and a Mitigation Approach. In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '08), New Orleans, LA, USA* (pp. 4966–4970). IEEE.