Journal of Computing Research and Innovation (JCRINN) Vol 2, No 2 (2017)
https://crinn.conferencehunter.com

Article 1

Physical Layer Jamming Attack Detection in MANET

Ahmad Yusri Dak, Farhah Rosidi
Faculty of Computer and Mathematical Science,
Universiti Teknologi MARA Perlis Branch, Malaysia

Noor Elaiza Abd Khalid
Faculty of Computer and Mathematical Science,
Universiti Teknologi MARA Shah Alam, Malaysia

Abstract
Mobile Ad Hoc Networks (MANETs) is gaining popularity in recent years due to being low-cost, flexible, and user-friendly. Users can easily create a spontaneous ad hoc network services for military use, emergency rescue purposes, or deploy it in rural areas, situations where mobile devices needs to communicate with each other. However, the nature of MANETs, such as open medium, dynamic mobility and lack of security, renders these networks susceptible to a range of attacks. In addition, its limitations such as hidden terminals signal interference and its open nature allows attackers to interrupt the network by denying access to users. One common technique used is jamming-based DoS(Denial-of-Service) attack, which is done by sending high frequency radio signals to disrupt communication between sender and receiver, leading to severe network damage. Most attacks exists at the physical layer, such as constant and random jammers. According to statistics recorded in 2017 by the MyCERT Response Team Malaysia, jamming attacks have increased up to 184% since 2007. To address these attacks, a study is conducted to find viable solutions to this issue. Two different scenarios were simulated and tested which involve random and constant jammers. Performance of simulated networks attacked by these jammers is evaluated using three performance metrics, Bit Error Rate (BER), Signal to Noise Ratio (SNR), and Throughput., Analyzed results concludes that these three performance metrics shows significant potential as detection mechanisms that offers insights and benchmarks for future research based on detecting jamming attacks.

Keywords: *MANET, Jamming, Physical, Constant, Random*

Introduction

In recent times, advancement of technology in wireless networking has brought fundamental changes to human life, allowing users to freely connect to the network anytime and anywhere, thus becoming part of our daily life. Wireless Network is the most popular technology available among users. For instance, MANET is a wireless ad hoc network that does not need pre-existing communication infrastructure, easy to connect and user-friendly. Mobile devices can easily enter or exit the network without disrupting other mobile devices in that network(Dak, Elaiza, & Khalid, 2012). However, the popularity of wireless networking, specifically MANETs that uses the Wi-Fi network standard poses potential security issues as attackers can exploit and cause blockage to the network.

Limitations of MANETs like hidden terminals, signal interference and its open nature gives attackers opportunity to interrupt the network by denying access to users. These attackers may use several attack techniques such as Radio Frequency (RF) jamming by injecting powerful high frequency signals to interrupt and bring down network services. Jamming attack using radio frequency technique is generated at physical layer of the protocol stack and disrupts the transmission between sender and receiver leading to severe network damage. Attacks that occur at the physical layer are usually constant and random jammers.

Statistics recorded by the Malaysian Computer Emergency Response Team [MyCERT], as shown in Figure 1, show that jamming based DoS attacks are increasing every year. Statistics compiled in 2013 indicate 19 attacks, 29 incidents in 2014 and this number increased to 66 attacks in 2016. The decreasing number of attacks from 23 in 2012 to 19 in 2013 was due to user action as they strengthened their security by implementing better security protection. However, many organizations overlook the potential impact of jamming attacks against wireless networks especially 802.11n.

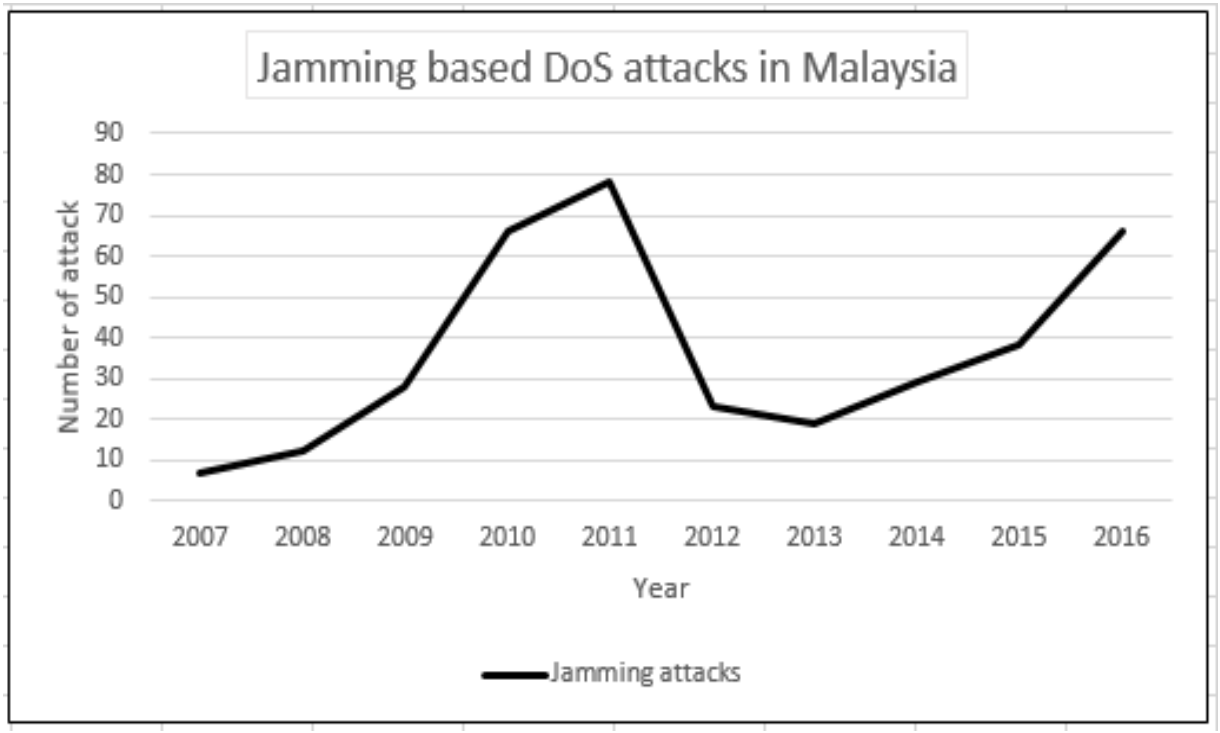

Figure 1 Statistics Jamming based DoS attack in Malaysia
(Source: MyCERT, 2017)

Due to critical issues of jamming attacks in MANETs, a study is proposed to cater to these issues and provide necessary solutions for future research. This research helped the society and other researchers for further understanding of constant and random jamming attacks.

Related Works

Xu, Trappe, Zhang and Wood, (2005)provides a complete description of the radio interference attacks and identifies the serious issue of the presence of the jamming attack. Four different jamming attack models were suggested that can be employed by an antagonist to disable a wireless

network, and formulated their efficiency in terms of how they influence the capability of a wireless node to send and obtain packets from the destination node. The authors also talked about various measurements that forms the basis for discovering a jamming attack, and explained various scenarios where every measurement is not sufficient to reliably classify the existence of a jamming attack. The author realized that carrier sensing time and signal strength are unable to conclusively determine the presence of a jammer.

Hamieh and Ben-Othman (2009) explains that military and other sensitive security procedures are still important applications for ad-hoc networks. One important challenge in planning these networks is their susceptibility to Denial-of-Service (DoS) attacks. In this paper, the author takes a specific class of DoS attacks known as Jamming. A new way to determine such an attack through formulation of error distribution was suggested.

Lu, Wang, Wang, Wang, Zhuo (2011) simulated and presented jamming attacks against time-critical traffic. The author presented a new metric, message invalidation ratio, to measure time-critical applications performance. The author indicated through real-time experiments and gambling-based simulator that there exists a phase modulation process for a time-critical application under jamming attacks.

Methodology

Two scenarios simulating physical layer jamming attacks were based on configuration from (Gonzalez, 2007) and (Babar, 2015). Each scenario is configured and simulated using MANET environment set up as described in Table 1.

Table 1 MANET's configuration

Parameters	**Attributes**
Protocol	None
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	BER, SNR and Throughput,

a) Scenario 1: MANET with Constant Jammer

Scenario 1 is designed to simulate a constant jamming attack as shown in Figure 2. It consists of a transmitter, a receiver, and a constant jammer with MANET environment. The attributes of transmitter and receiver for Scenario 1 is developed based on the model proposed by (Gonzalez, 2007) and (Babar, 2015).

This attack contains a transmitter sending valid traffic receiver without any MAC protocol and a single jammer that is constantly emitting high frequency non-valid packets at a constant bit rate (1024 bps), trying to jam transmission and increase the probability of errors received.

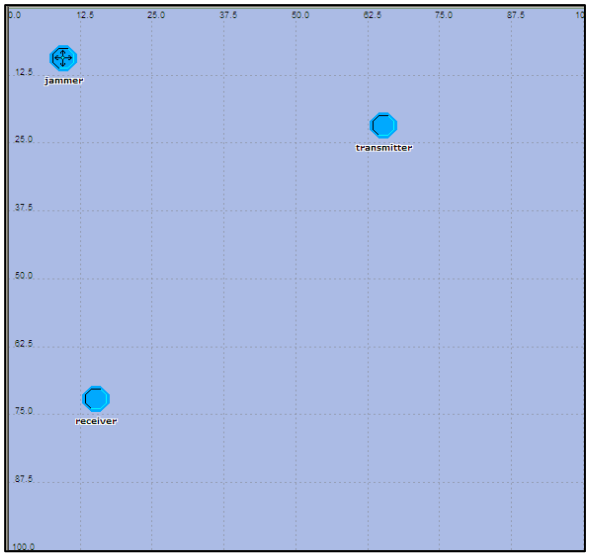

Figure 2 Network with constant jammer

b) Scenario 2: MANET with Random Jammer

Figure 3 shows the scenario for random jammer. It is a simulation with an activated random jammer. Random jammer was constructed to send data for period of time and sleep for another random period. Transmitter sends a valid data packet (1024 bps) to the receiver, turning on and off mode randomly.

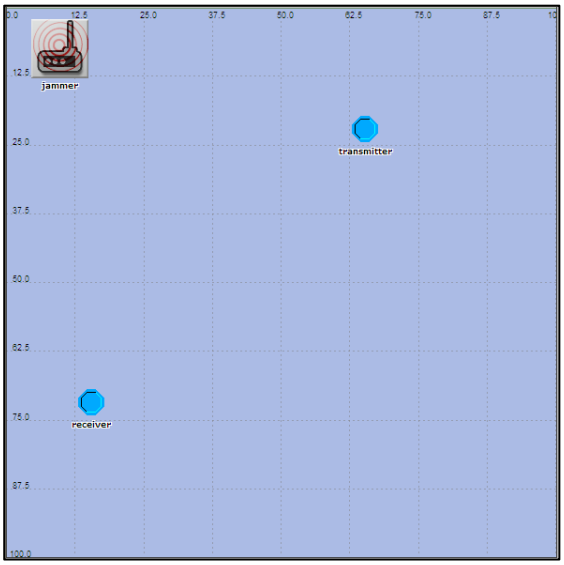

Figure 3 Network with random jammer

Results and Findings

Network performance test for scenario 1 and 2 are compared and analyzed. Network performance test that consists of BER, SNR and throughput data were chosen to identify constant jamming and random jamming. Comparative analyses for both jammers are necessary to determine effective identification metrics.

a. BER test

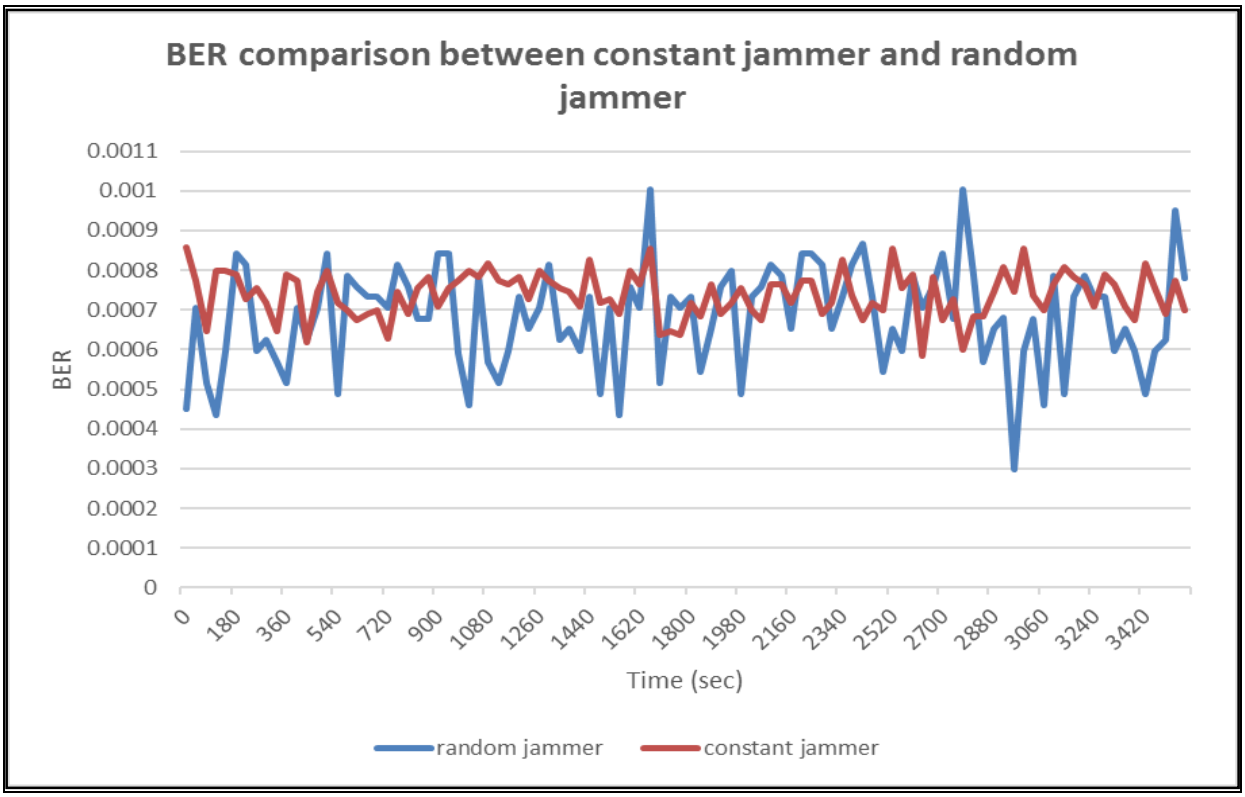

Figure 4 BER for constant jammer and random jammer

Figure 4 shows a graph for BER test that simulated constant and random jammer captured using OPNET version 13. Random jammer has the highest BER value up to 0.001% compared to constant jammer which is 0.0009%. This show that a random jammer is more effective in interrupting and corrupting bits transmission.

BER is chosen as the detection mechanism because the capability to identify physical layer jamming attack on the receiver side is based on its definition. It can define the number of bit errors received over a data stream in a communication channel that has been altered due to noise, interference, and distortion or bit synchronization errors.

b. SNR test

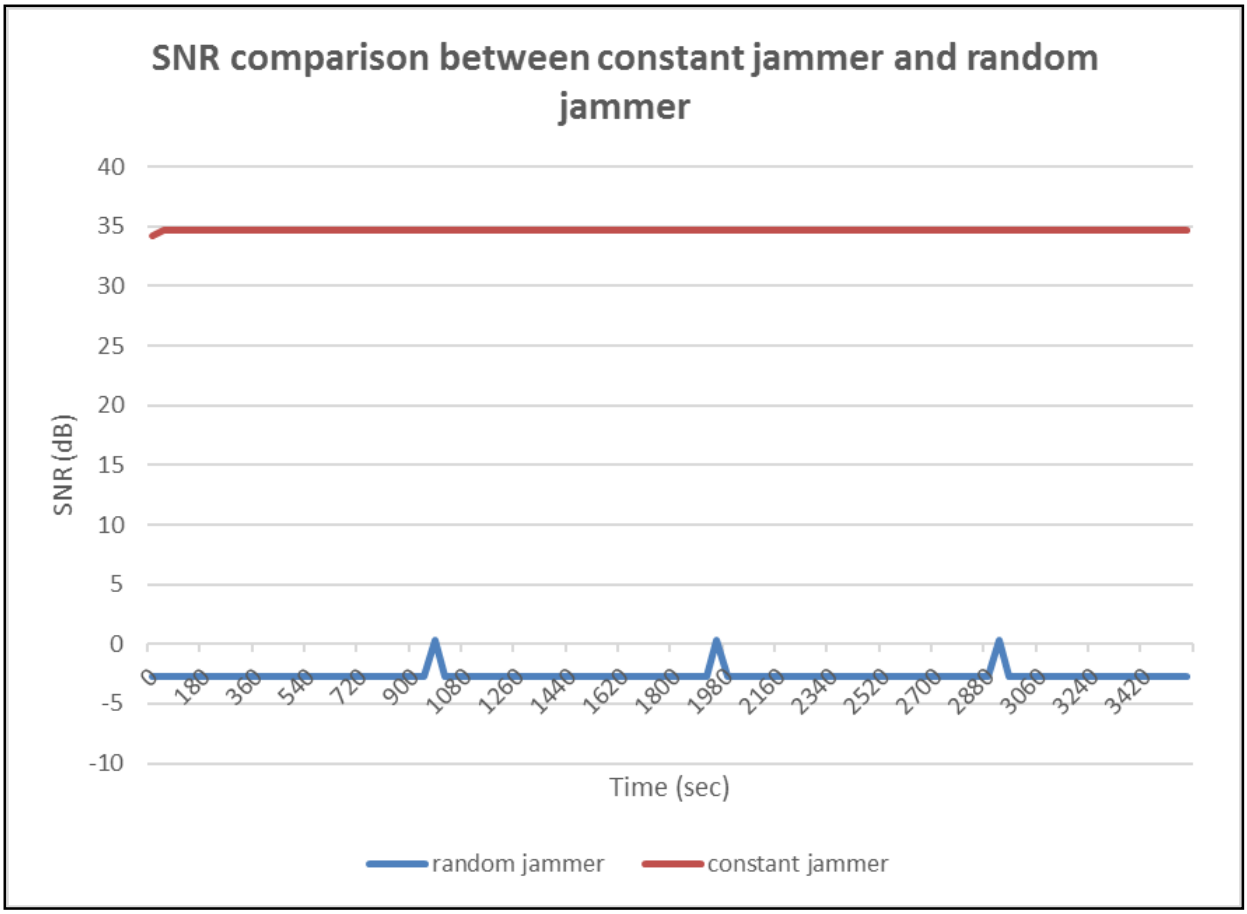

Figure 5 SNR test for constant jammer and random jammer

Figure 5 shows the graph of SNR simulation test conducted for constant jammer and random jammer. Average value captured for constant jammer is at 34.69dB, higher than random jammer which averages at -2.68118 dB for the same duration.
Constant jammer shows a constant signal capture rate over time. The higher detection rate of SNR in dB indicated a poor detection performance in RF that show more noise than signal. This result is in line with (Tan, Hu, & Portmann, 2012) that show the maximum and minimum range of result is set to distinguish between signal noise jamming and normal signal. If frequency detected is below or above the assigned limit, it is assumed to be a jammed signal; otherwise, the original signal is transmitted.

Graph for random jammer showed a high peak (0.28675 dB) and a lower peak signal (-2.68118 dB) indicating that the signal is affected by a random jammer during sleep and active time frame. Random jammer capture value below than 0 db is due to a tradeoff that occurs between jamming and sleeping mode. The ratio between sleeping and jamming time can be manipulated to adjust this trade-off between efficiency and effectiveness. The detection rate is average -2bB, showing a jamming attack can be considered effective if the SNR is less than one(Pintea & Pop, 2014).

c. Throughput Test

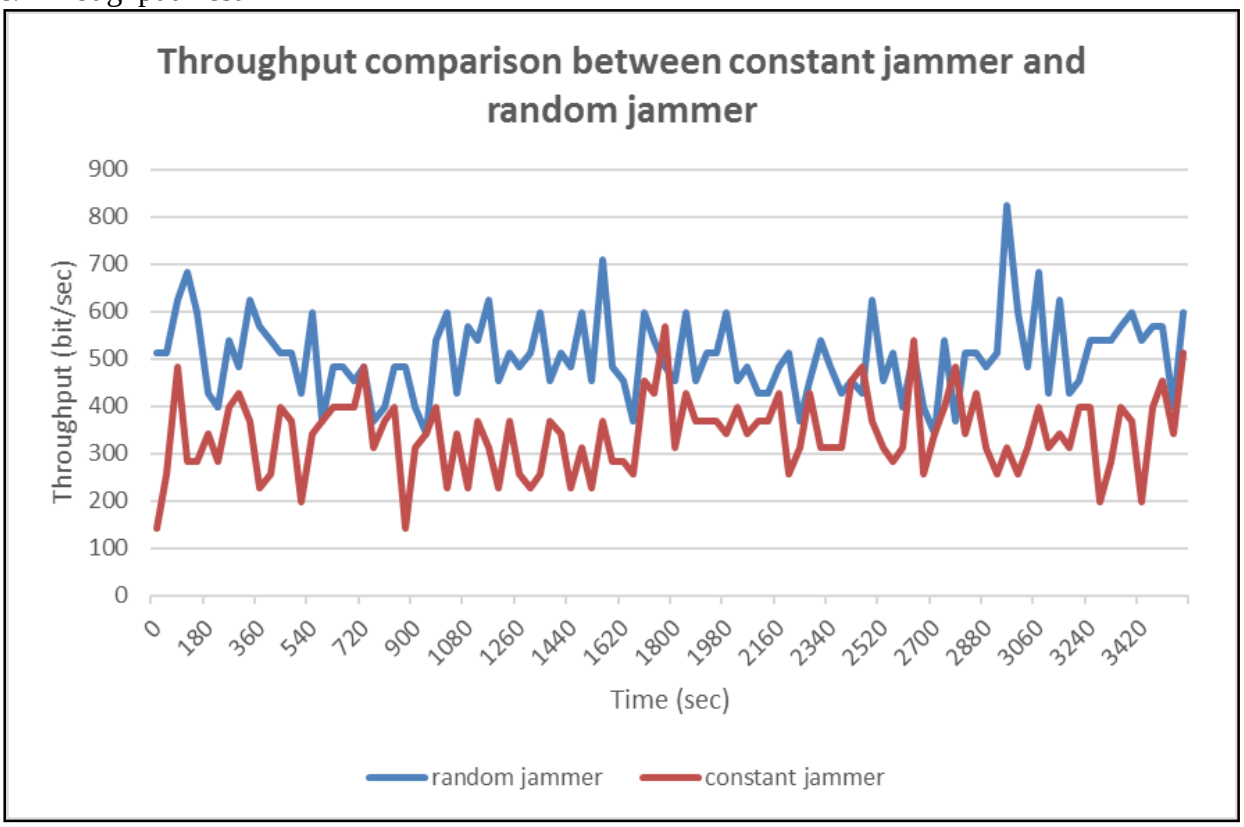

Figure 6 Throughput test for constant jammer and random jammer

Throughput is defined as the ratio of 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 overhead. Figure 6 showed the graph of throughput tested for constant jammer and random jammer. Random jammer has the highest throughput value at 80.6%, compared to constant jammer at 52.8%. This showed that random jammer allowed more bits to arrive at the receiver compared to constant jammer. Under random jammer attack, a node tries to gain more throughput by transmitting more packets. This becomes higher when large packets are transmitted. Node gains more throughput in comparison to other nodes, causing some packets to be dropped there. Therefore, throughput rate is more effective to detect random jammer compared to constant jammer. Thus, the result showed that random jammer allowed more throughput than constant jammer.

Conclusion

Constant and random jamming attacks at the physical layer disrupt and corrupt data transmission, which happens due to the nature of MANET. Results obtained from experiments done in this study show that these jamming attacks affects the transmission's BER, SNR and throughput. The evaluation of the three metrics mentioned also shows that random jammer causes more disruption compared to constant jammer.

Future Works

Further continuation of this study in the future would include researching two other jamming attacks: reactive and deceptive jammers. These jammers are more complex as they can manipulate the wireless protocols in the network. Thus, more work is needed to understand the characteristics of these jammers.

References

Dak, A. Y., Elaiza, N., & Khalid, A. (2012). A Novel Framework for Jamming Detection and Classification in Wireless Networks. In *8th International Conference on Computing and Networking Technology (INC, ICCIS and ICMIC)* (pp. 240–246).

Hamieh, a., & Ben-Othman, J. (2009). Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution. *2009 IEEE International Conference on Communications*, 1–6. http://doi.org/10.1109/ICC.2009.5198912

Tan, W. L., Hu, P., & Portmann, M. (2012). SNR-based Link Quality Estimation. In *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th*.

Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing MobiHoc 05*, 46. Retrieved from http://portal.acm.org/citation.cfm?doid=1062689.1062697

Lu, Z., Wang, W., Wang, C., & Wang, Zhuo Lu Wenye, C. (2011, April). From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic. http://doi.org/10.1109/INFCOM.2011.5934989

Babar, S. D. (2015). *Security Framework and Jamming Detection for Internet of Things*. Aalborg University, Denmark.

Dak, A. Y., Elaiza, N., & Khalid, A. (2012). A Novel Framework for Jamming Detection and Classification in Wireless Networks. In *8th International Conference on Computing and Networking Technology (INC, ICCIS and ICMIC)* (pp. 240–246).

Ekpenyong, M., & Joseph Isabona. (2010). Modeling Throughput Performance in 802 . 11 WLAN. *IJCSI International Journal of Computer Science Issues*, *7*(3).

Gonzalez, J. M. (2007). *Exploring Jamming Attack using OPNET 12.0*. University of Pittsburgh.

Hamieh, a., & Ben-Othman, J. (2009). Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution. *2009 IEEE International Conference on Communications*, 1–6. http://doi.org/10.1109/ICC.2009.5198912

Lu, Z., Wang, W., Wang, C., & Wang, Zhuo Lu Wenye, C. (2011, April). From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic. http://doi.org/10.1109/INFCOM.2011.5934989

Pintea, C., & Pop, P. C. (2014). Sensitive Ants for Denial Jamming Attack. *Advanced Intelligent Soft Computing Journal*, *239*, 1–4.

Tan, W. L., Hu, P., & Portmann, M. (2012). SNR-based Link Quality Estimation. In *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th*.

Team(MyCert), M. E. R. (2017). MyCERT Incident Statistics. Retrieved March 30, 2016, from https://www.mycert.org.my/statistics/2012.php

Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing MobiHoc 05*, 46. Retrieved from http://portal.acm.org/citation.cfm?doid=1062689.1062697

Gonzalez, J. M. (2007). *Exploring Jamming Attack using OPNET 12.0*. University of Pittsburgh.

Babar, S. D. (2015). *Security Framework and Jamming Detection for Internet of Things*. Aalborg University, Denmark.

Team(MyCert), M. E. R. (2017). MyCERT Incident Statistics. Retrieved March 30, 2016, from https://www.mycert.org.my/statistics/2017.php