International Journal of Engineering & Technology, 7 (3.15) (2018) 24-30

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Integrated Combined Layer Algorithm (ICLA) for Jamming Detection in MANET

Ahmad Yusri Dak*, Noor Elaiza Abdul Khalid[2], Saadiah Yahya[3]

[1]*Faculty Science Computer and Mathematics, Universiti Teknologi MARA, Perlis Campus, Malaysia*
[2]*Faculty Science Computer and Mathematics, Universiti Teknologi MARA Shah Alam, Malaysia*
[3]*King Abdul Aziz University of Science and Technology(KAUST), Saudi Arabia*
**Corresponding author E-mail: yusri@tmsk.uitm.edu.my*

Abstract

The nature of MANETs such as open medium, dynamic mobility and lack of security makes it susceptible to a range of attacks. Jamming attacks is recorded as the highest occurring attacks that exist at physical and MAC layers in MANET. Therefore, an integrated combined layer algorithm (ICLA) is proposed using reverse engineering and anomaly detection technique. The methodology begins by collecting data through OPNET. Analysis and evaluation of the data produces three jammers detection Metrics which are used detect jammers. The performance of the outcome are then tested against other jammers' model at MAC and physical layer to evaluate the detection performance. This enables identification of jamming attack at both lower layers in MANET. It is combination of three tested metrics such as SNR, BER and throughput that able to detect jamming attack using combined layer approach. The combination of these three metrics across layers shows improvement in identification performance.

Keywords: *MANET; identify jamming; NAV; RTS/CTS; layer*

1. Introduction

Wireless networks have brought fundamental changes to human life. It is now an integral part of our everyday life, being increasingly affordable and easier to build. However, the popularity of wireless networking (802.11x) especially poses potential security issues in which an attacker can easily exploit and jammed networks. The open medium, dynamic topology, hidden terminal and energy constraint for services disruptions [2], [3] in MANET making it vulnerable to jamming attacks such as collision, misdirection, spurious RTS/CTS, Radio Frequency (RF) jamming and/or NAV attack to interrupt services [1-4]. MANET are found to be more vulnerable because communications are over a shared medium. The topology, technology and design of wireless architecture also contributes to potentially high jamming attacks [3].

Several jammer attack models have been developed by researchers to test and evaluate the performance of detection scheme. The proposed models are designed base on the specific needs of the researchers assessment of the performance model. Thus, many attack models were designed among which are military models for electronic warfare [2], model by Xu et al.[4], model by Yee et al. [5], model by Wood et al. [6] and model by Muraleedharan et al. [7]. Each of these models has been developed based on jammer characteristics or protocol layer where jammer is located. In this research, model [4] is applied as detection model due to its ability to identify jamming attack at MAC and physical layers.

In addition, the most common jamming attacks are detected at MAC and physical layer of wireless network. Analysis found that 81% of jamming attacks are initiated at both lower layer due to the nature of wireless networks [8]. It is easier to generate but harder to detect as they are often indistinguishable from normal signal propagation in wireless medium [9]–[11][12].

Present literatures are focused on individual jammer for detecting jamming attack using single metrics while developing detection algorithms. Some findings are inconsistent with other works and it is difficult to validate the findings. Due to these weaknesses, a proper study needs to be conducted to validate the reliability of the jamming attack model for detection of jammers. Studies shows a benchmark to evaluate performance of each jammer [4], [13].

Le Wang Wyglinski [13] designed a combined detection mechanism to discriminate between the numerous groups of jamming attacks based on jamming model [4] using Packets Send Ratio (PSR) and PDR as identification Metrics. However, the success of identification is hampered by low differential data.

Thus, this research proposes to design and develop a jamming detection algorithm using metrics with defined threshold value to cater jamming attacks at the physical and MAC layer in MANET.

2. Research Method

Jamming is defined as a DoS attack that interferes with the communication between nodes or corrupting packets during transmission. The objective of the adversary causing a jamming attack is to prevent a legitimate sender or receiver from transmitting or receiving packets. There are several kinds of jamming attacks that can disrupt the communication in a wireless network.

The physical jamming is found by uninterrupted transmissions and/or by assuring packet collisions at the receiver side. The jammers causing to these attacks can refuse complete access to the channel by controlling the wireless network completely. At this

layer, constant and random jammers are initiated to interrupt services by transmitting radio frequency signal.

Virtual jamming attacks can be detected at the MAC layer by attacking 802.11 protocols such as using NAV attack or spurious RTS/CTS procedures. Deceptive and reactive jammers are attack generated from NAV attack or spurious RTS/CTS technique. A benefit of MAC layer jamming is that the attacker node takes less power in directing these attacks in comparison of physical radio jamming. In virtual jamming attack harmful node propagate Request to Send(RTS) packets without interruption on the transmission with unlimited period. During this whole process, the harmful node efficiently jam the transmission with a large amount of transmission on the wireless medium with low cost of power.

Jammers such as constant, random, deceptive and reactive are configured and setting to act out based on 802.11 environments. OPNET Modeler R13 simulation tool is used to establish four types of jammers as described in scenario 1, scenario 2, scenario 3 and scenario 4.

a. 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.

b. Scenario 2: Random Jammer:

Jammer is setting to alternate between jamming attack and sleeping mode. In brief, the jammer performs constant jammer or deceptive jammer for a random period then shut down the jammer for another random period of time.

c. Scenario 3: Deceptive Jammer:

Deceptive jammer continually injects valid packets header with a useless payload or even no payload to the channel with no gap between packets.

d. Scenario 4: Reactive Jammer:

Reactive jammer is configuring stay quiet till there is activity on the channel then devastates the reception.

Figure 1 shows a process flow for monitoring and detecting jamming attack at physical and MAC layer using metrics such as Bit Error Rate(BER), Signal to Noise Ratio(SNR) and Throughput.

BER, SNR and Throughput are proposed as detection metrics due to ability to identify jamming attacks based on reverse engineering model.

The process flow is divided into three stages and each stage consists of dedicated activities at two different layers model based on proposed combined layer technique.

The development of detection algorithm uses an anomaly-node monitoring technique where an intrusion detection system works by observing normal or abnormal traffic activities via a predefined threshold. The monitoring phase occurred when each node in MANET needs to select its state for the whole duration of the current monitoring phase according to the anomaly detection technique. Traffic activities recorded contains normal and abnormal traffic such as congested and valid traffic. Congested traffic will be detached and valid traffic that comprises of real and jammed traffics are sent to detection algorithm. It is developed to identify jammers using statistical detection analysis and combined layer method. At physical layer, detection for constant and random jammers is performed using RF jamming attack. For MAC layer, spurious RTS/CTS and NAV attack are technique developed to identify deceptive and reactive jammers. The process for identifying jamming attack are discussed in next sub-section.

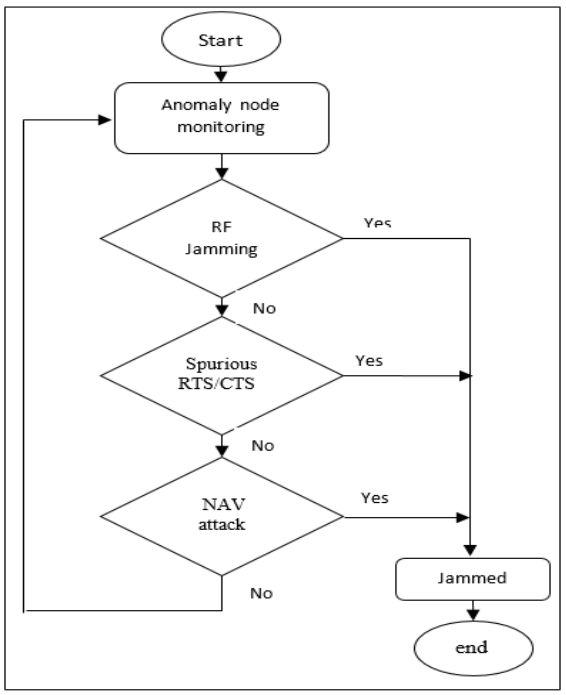

Fig 1: Process Flow for detecting jamming attack in MAC and physical layer.

Table 1 and Table 2 Table 3.5 below shows the simulation parameters used in OPNET simulation to configure four types of scenarios.

Table 1. Parameter to simulate constant and random jammers

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), Random
Performance Parameters	Throughput, BER, SNR

Table 2. Parameter to simulate deceptive and reactive jammers

Parameters	Attributes
Protocol	CSMA
Simulation Time	7200 seconds
Simulation Area	100 x 100 meters
Data Rate(bps)	11 Mbps
Packet Size(bits)	1024
Transmit Power(W)	0.005 Watt
RTS Threshold (bytes)	1024(bytes)
Modulation	dpsk
Packet Interarrival time(seconds)	Constant (1.0)
Performance Parameters	Throughput, BER, SNR

3. Measuring Rf Jamming Attack.

First experiment is intended to detect RF jamming that occurs at physical layer using SNR detection metric. RF or radio frequency jamming attack is a high-power signal used to disrupt or jam valid radio signal generated by transmitter to receiver. SNR is an effective metric to identify a jamming attack such as constant and random jammer at the physical layer by measuring value in dB in between threshold value. Subsequently, data collected from the experiment are studied and analysed. Maximum and minimum threshold value for constant and random jammer are defined as (a) and (b) referred to Table 3.0 and Table 4.0 with certain series of value. If traffic detected is in defined range of SNR, the

conclusion made is that a physical layer jamming has been detected. Otherwise, no attack is assumed as referred to Figure 2. The formula to identify jammer based on SNR metric as shown in (a) calculated from average number of SNR collected at receiver side during experimentation.

$SNR_{minvalue} \ll SNR\ \{\frac{1}{n}\sum_{i=1}^{n} a_i\ \} \ll SNR_{maxvalue}$ (a)

where $a_i = a_1 + a_2 + a_3 + \ldots + a_n$, n = number of receiver node.

for constant jammer, $SNR_{minvalue}$ = 28 and $SNR_{maxvalue}$ = 44

for random jammer $SNR_{minvalue}$= -6 and $SNR_{maxvalue}$ = 4

Fig 2 : Algorithm for physical layer jamming attack

As shown in Table 3.0, traffic collected during experiment are summarized to identify types of jammer. Constant and random jammers contain a range of value that falls in within group it was defined. If traffic detected is out of the range, assumption made is that jammer is detected in network using RF jamming technique. For example, the minimum and maximum value for constant jammer is between 28dB to 44dB and if traffic detected is out of this range, the assumption is made that a constant is jammer detected. However, this condition is applied for random jammer in which value is measured between -6dB to 4dB. SNR can be used to identify constant and random jammers but requires a specific range of value to differentiate it.

3.1 Identify Spurious RTS/CTS Attack

Second experiment consists of detection for jammer attack that occur at MAC layer using Spurious RTS/CTS technique. Spurious RTS/CTS occurs because nodes receiving the RTS/CTS frame must delay its transmission, a misbehaving node may randomly send out a large number of spurious RTS or CTS frames addressed to a possibly non-existing node to block other well-behaved node in the network, thereby successfully carrying out virtual jamming. Theoretically, the transmitter sends a frame with RTS/CTS acknowledgement aspect to receive notification, but the transmission fails due to contention and keeps monitoring the number of contention attempts made to transmit for each frame. The transmitter keeps sending a frame with acknowledgement and monitors the number of failures to receive an acknowledgement. In addition, if no response of acknowledgment frame is received during a time interval, the transmitter assumes that the transmission failed due to bit error and monitors the number of bit error rate (BER) attempts made to transmit each frame and the number of BER failures to receive an acknowledgement. Thus, the wireless channel is poorly utilized as nodes delay their transmissions, even when there is no communication.

If $BER = [\frac{1}{n}\sum_{i=1}^{n} a_i = \frac{1}{n}(a_1 + a_2 + a_3 + \ldots + a_n)] \geq 10^{-3}$ (b)

Spurious RTS/CTS detected

else

no jammer detected

where BER threshold = 10^{-3} bps

Fig 3: Algorithm for Spurious RTS/CTS

According to [18], by setting the threshold for the communication failure at BER $\geq 10^{-3}$bps as in Figure 3, corresponding maximum number of bit failed to receive RTS/CTS acknowledgement are measured. When BER is higher than 10^{-3}bps, the receiver's throughput gain gradually decreases because the number of frame packets it overhears decreases, thereby decreasing the number of spoofed ACKs. From expression (b), average number of BER is calculated and measured against threshold value. If average BER value collected from receiver is greater than 10^{-3}bps, a spurious RTS/CTS attack is detected which contains deceptive and reactive jammer.

3.2 Identify NAV Attack

Third experiment is to detect jammer using NAV attack technique which is the hardest methodology. In normal condition, a node tries to gain more throughput by transmitting higher number of packets. Under NAV attack, an attacker may exploit 802.11 protocols by asserting a larger duration field in packets, thereby preventing well-behaved node from gaining access to the channel. This is more significant when large packets are transmitted such that packets began dropping drastically. This strategy could significantly reduce network throughput and diminish network's capacity to perform expected functions. Therefore, In order to identify intelligent jammer using NAV attack, throughput proposed at metric with certain threshold value defined. As shown in expression (c) in Figure 4, throughput attack is set as metric to identify intelligent jammer. It is set to a threshold value of for means of 1152bps. If average throughput detected above defined value as shown in (c), assumption is made that a NAV attack is detected which contains deceptive and reactive jammer. Otherwise, no jammer is identified.

if Throughput $\{\frac{1}{n}\sum_{i=1}^{n} a_i\ \} > Throughput_{threshold}$ (c)

NAV attack detected

else

No jammer attack detected

where Throughput threshold = 1152 bps

Fig 4: Algorithm for NAV attack

4 Development of Integrated Combined Layer Algorithm (ICLA)

ICLA is newly proposed algorithm for intrusion detection mechanism that operated between two lower layers in protocol stack; physical and link layer and become a single functioning layer as it implemented. The development of ICLA is using reverse engineering method, anomaly-based detection technique and combined layer approach whereby different types of metrics are tested and evaluated in MANET based on scenario 1-4.

In addition, combined layer technique is a new scheme that unites physical and MAC layers into one single layer. Information from crossing layers can be loaded into statistical anomaly integrated with rule-based technique where physical layer information is passed to the MAC layers detection approach for a more accurate detection. It is designed from the concept of cross layer technique proposed due to certain limitation of cross layer technique that caters by a new proposed combined layer technique such as integration between both lower layers, and each layer has its own detection metrics.

Furthermore, the detection of jammers is started from physical layer and information sent to MAC layer. For example, detection of information related to signal strength from lower layer can be used to identify intrusion at higher layer using combined layer technique. Metrics such as Received Signal Strength Indicator (RSSI), SNR and Packet Delivery Ratio (PDR) can be used as detection metrics at physical layer before this information is sent to MAC layer. This is contrast with cross layer technique whereby intrusion can be detected by two-way approaches with different types of metrics.

A combination of tested metrics as discussed in section two integrated altogether into those workings layer to measure the performance wise. In addition, this detection algorithm is deployed in each receiver node in MANETs as a dedicated anomaly monitoring agent to observe traffics using identified

metrics for example SNR, BER and throughput in a specified time frame. Each node runs the metrics vs jammer's model independently to detect network anomalies and data will be analysed to identify the pattern of attack as shown in Table 4.0.
Figure 5 is a proposed jamming detection algorithm namely Integrated Combined Layer Algorithm(ICLA) developed using reverse engineering method, anomaly-based detection technique and combined layer approach that consists of three different metrics that enables it to detect two different layers of jamming attack. It is designed based on Table 3.0 and Table 4.0 that represents a summary of data consisting of three types of metrics, four types of jammer and maximum vs minimum value of jammer.

If $SNR_{minvalue} \ll SNR\{\frac{1}{n}\sum_{i=1}^{n} a_i\} \ll SNR_{maxvalue}$

physical jammer detected

else if $BER = [\frac{1}{n}\ a_i\ = \frac{1}{n}(a_1 + a_2 + a_3 + \ldots + a_n)] \geq 10^{-3}$

Spurious RTS/CTS detected

else if $Throughput\{\frac{1}{n}\sum_{i=1}^{n} a_i\} > Throughput_{threshold}$

NAV attack detected

else

no jammer detected

end

Fig 5: Integrated Combined Layer Algorithm

5 Experimentation Result: Scenario Model

Therefore, in order to detect four types of jamming attack as discussed in previous section, Integrated Combined Layer algorithm is proposed. Table 3.0 and Table 4.0 presented a maximum and minimum value for proposed metrics that collected during simulation environment for scenario 1-4 using jamming threat model. Each metric is analysed using minimum to maximum value to identify suitable thresholds to be used for detection algorithm.

Table 3: Physical layer jamming detection

Metric	Jammer			
	Deceptive		Reactive	
	Min	Max	Min	Max
BER	1.89×10^{-4}	6.08×10^{-4}	0	0
SNR	26	33	29	33
Throughput	1152	2620		

Table 4: MAC layer jamming detection

Metric	Jammer			
	Constant		Random	
	Min	Max	Min	Max
BER	1.07×10^{-8}	1.07×10^{-2}	0	2.11×10^{-2}
SNR	35	44	26	33
Throughput	0	1	0	1

6 Result and Finding

Data collected from OPNET simulation tool based on configuration of scenarios 1-4 are analysed and validated.

6.1 Constant Jammer

Constant jammer attack is developed based on scenario-1 as described in section two with packet sizes varying from 100 bytes to 1500 bytes injected to network. Under normal circumstances the traffic in this scenario achieves a throughput of 100% because it is an ideal scenario due to lack of obstacles, the background noise is considerably low and it is the only source of noise that OPNET takes into consideration. A constant jammer is introduced into the scenario and is designed to keep sending packets with energy levels similar to those created by the transmitter.
Figure 6 shows the outcome from scenario_1 that simulates larger packet sizes injected from transmitter and jammer has less overhead and yields higher throughput in the absence of jamming. Larger packets are more susceptible to jamming when the jamming rate is
high. This is applied to ICLA when the throughput percentage kept increasing over time that represented an efficient detection scheme by detection algorithm. On the other hand, signals received by algorithm proposed by [13] present an almost constant performance due jammer reducing the PDR thus influencing the physical rate of the throughput in the presence of jamming. The constant jammer generated strong noise that was enough to interrupt transmission from the receiver, then reducing the PDR and physical rate without being on a level. Both signals showed high fluctuation due to signals received from transmitters and jammer in different way of form, as the jammer is sending at constant bit rate.
Performance-wise, ICLA achieved up to 67.27% throughput detection rate compared to the algorithm proposed by [13] which has 31.21% throughput. The poor performance of algorithm by [13] is because the use of PDR and signal strength to measure the availability of jammer. However, the poor data from PDR can arguably be caused by many factors influencing the result such as battery failure, signal interference and nodes moving out of the range. In addition, signal strength proposed [13] is not a suitable

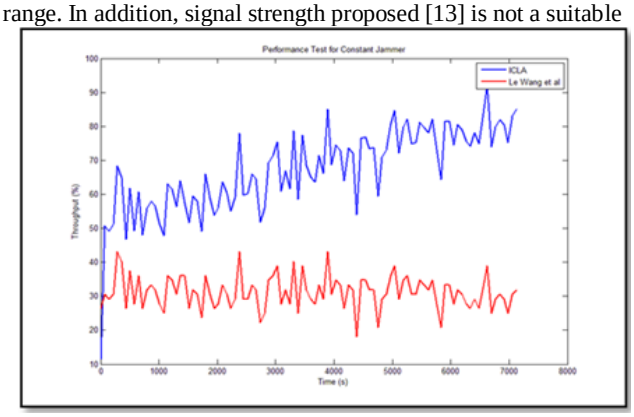

Fig 6: Performance Test for constant jammer

metric because it has a tolerable range that can be accepted between transmitter and receiver. Therefore, ICLA that contains three statistical combination metrics with combined layer approach show a better throughput performance as compared to [13].

6.2 Random Jammer

Random jammer is categorized under radio frequency jamming attacks where a more power efficient jamming strategy jams for t_j seconds and then sleeps for t_s seconds. It does not follow any MAC protocols because random jammer is located at physical layer of protocol stack. The identification of random jammer required a suitable metric that allows detecting of RF jammer with higher efficiency and accuracy. [13] proposed PDR with combination of signal strength as detection mechanism to detect random and constant jammer but it has limitations, such as

inability to determine accurately in practice and is also unstable if more than one jammer jams the network. [14], [15] and [16] propose to use RSSI with PDR to recognise constant and random jammer using RE (residual energy). Unfortunately, combinations of a metrics with PDR are not effective to identify random jammer due to energy saving caused by switching on and off. Therefore, ICLA with combination of SNR is proposed as part of detection algorithm to identify random jammer.

Figure 7 shows a graph to measure the performance of random jammer using ICLA and algorithm proposed by [13] as described in scenario_3. Algorithm proposed by [13] showed a throughput performance at average of 31.24 %, a bit lower than ICLA which is at 40.05 %. Both algorithms detected low throughput below than 50% due to misunderstanding packets received by receivers. Packets send by transmitter consist of control channel that has to be verified by receivers when the packets arrived. Unfortunately, a random jammer targeting the control channel switches on and off, that might deny access to the network altogether. Receivers are not aware of the type of packets transmitted (by means of processing the header of these packets) by transmitter that is jammed by on and off mode. Hence, receivers are assumed to jam the entire packet in order to drop it but certain packets between on sequences are still accepted and calculated.

Theoretically, algorithm by [13] such as PSR, PDR captures some packets of the traffic towards receivers due to its definitions. Adaptive threshold suggested has the drawback of continuously decreasing packets eventually random jammer blasting at channel and detector which showed the channel idle. In contrast, ICLA used metrics such as SNR, BER and Throughput that offers better performance since detection is based on signal strength and bit per bit received that is not related to control channel. The signal captured by ICLA showed a highly fluctuated gesture to express the sensitivity of the algorithm proposed. Hence a jammer fluctuates between the period of transmitting signal and the period of sleeping to minimize the energy consumption instead of transmitting signal constantly.

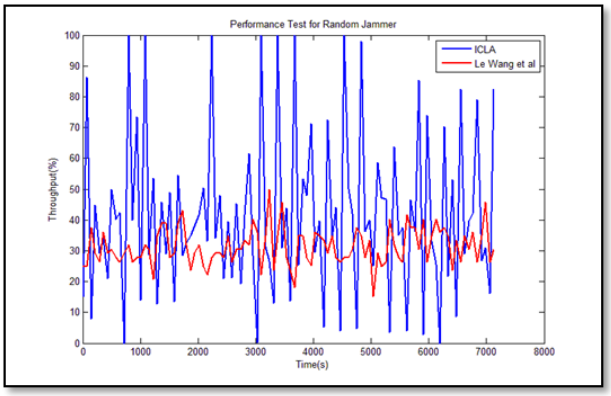

Fig 7: Performance Test for Random Jammer

6.3 Deceptive Jammer

In a deceptive jamming attack, when a node has frames to send, it has to sense the channel to see if the channel is idle. If the channel is busy, the node will stay quiet and keeps sensing the channel periodically. Once the node detects an idle channel, it will transmit frames with a probability of P (P belongs to 0-1)) as described in section 2.6.2. This is one of the weaknesses of MAC sub-layer protocol which can be used by jammer to conduct an intelligent deceptive jamming attack. If a jammer keeps transmitting a valid frame, according to the protocol, the nodes at each end of the channel will stay quiet without sending any frames. As a result, a normal communicator will be deceived into believing there is a legitimate packet and be tricked to remain in the receive state.

A scenario_2 as mentioned in section two was configured and simulated according to deceptive jamming environment. Figure 8 presented a performance test for deceptive jammer consisting of ICLA and algorithm proposed by [13]. As presented in Figure 8, the graph showed that ICLA practically has a higher throughput capability on detection performance as compared to [13]. The detection rate for [13] is at average of 95.34% as compared to ICLA which is at 98.264%. This is because the detection algorithm proposed to identify deceptive jammer to jams the idle channel with probability (P) and made the channel idle for longer time.

The operation of algorithm proposed by [13] can be described using TCP-ACKs protocol. Let's assume that the MAC layer of transmitter has n packets for transmission. Due to jamming interference, only m ($n \geq m$) of these packets can eventually be transmitted. PSR can easily compute measure which intuitively captures the effectiveness of the jammer towards a transmitter employing carrier sensing as its medium access policy. The TCP-ACKs jamming signals can render the medium busy due to carrier sensing and as a result the transmission waits in queue. Packets arriving at full queue will be dropped. The packet dropped is measured at a certain threshold value using PSR. Thus, if the packet dropped less than a pre-defined threshold, assumption is made that a deceptive jammer is detected. Moreover, depending on the semantics of the MAC protocol employed, transmissions for packets at the head of the queue can eventually expire and the packets themselves get discarded. PSR allows the monitoring of head of packet queue expiration and is able to detect dropped packet with minimum percentage.

Similarly the concept for ICLA, the effective throughput drops to 98.26% under deceptive jamming attacks. Combination of three metrics to detect deceptive jammer using statistical model are more effective than algorithm by [13]. This is due to metrics tested and evaluated provides multiple stages of detection scheme. In CSMA/CA, each pair of hosts will go through the process of Request-To-Send packet, Clear-To-Send packet, Data packet, and ACK packet (RTS/CTS/DATA/ACK) to reserve and to use the medium exclusively during early process of connection. The process of connection between node starts when transmitter send ACKs notification to receivers, some of cumulative ACKs are lost (in case of jammed). Thus, receivers select a random back-off value and sends ACK packets to the transmitter again. In addition, transmitter must use this assigned back-off value in its next transmission to the receiver and retransmit all unacknowledged data packets again, thus increasing the incurred delay while reducing the effective throughput. Reduced effective throughput performance can be detected via ICLA using BER and throughput. Furthermore, receivers interpret the loss of ACKs as congestion and throttles its packet transmission rate by reducing the size of the transmission window thus transmissions will be queued and more packet will be dropped.

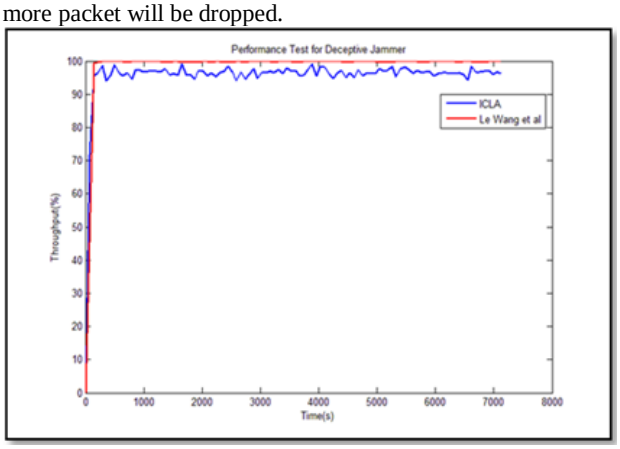

Fig 8: Performance test for Deceptive Jammer

6.4 Reactive Jammer

Figure 9 shows the throughput's performance for reactive jammer which consists of a graph from [13] and ICLA. The graph was simulated based on scenario_4 as described in section two. Reactive jammer sends data only if it detects energy on the channel and this is the most effective jammer since it saves energy it uses. It can corrupt data with high probability and is harder to detect. As showed in Figure 9, algorithm proposed by [13] displays the throughput's performance at an average of 96.28%. This indicates that the algorithm presented by [13] allows the identification of reactive jammer using combination of PDR and PSR with appropriate threshold value set in the detection algorithm. In addition, PSR with correct threshold value can be easily measured by a wireless device by keeping track of the number of packets it intends to send and the number of packets that is successfully sent out at transmitter side. In contrast, analysis from [4], [17] [12] found that the detection of jammer using PSR is 100% accurate. This result achieves maximum percentage due to its definition of PSR which is measuring of packets sent and received at transmitter instead of at receiver side during jamming attack. It is in line with algorithm proposed by [13]. Therefore, from study and definition it is found that PSR is not suitable to be used as detection scheme for reactive jammer as implemented. [13] and verified by [4][17].

On the other hand, ICLA that used combination of three metrics (SNR, BER and throughput) displayed only 69.15% throughput percentage of the reactive jammer detected at receiver with the same scenario conducted. This comparison result gives the conclusion that ICLA is less effective to detect reactive jammer due to low throughput percentage received by receiver. However, if these three metrics were studied from the perspective of reactive jammer it is found that reactive signal injected and detected from a legitimate node on any channel interferes with all the receivers in its range. Thus, the result is drastically decreased in the SNR and a drop in the communication throughput of the network. A reactive jammer tries not to waste resources by only jamming when it senses that something is transmitting. Its target is not the sender but the receiver, trying to input as much noise as possible in the packet to modify it, and consequentially corrupt as many bits as possible over packets at the receiver. This packet with corrupted bit will be classified as not valid and therefore discarded. The discarded packet can be identified by BER and throughput but decreasing in SNR to show the availability of reactive jammer. Thus, combination of these metrics showed up to 69.15% throughput percentage detected.

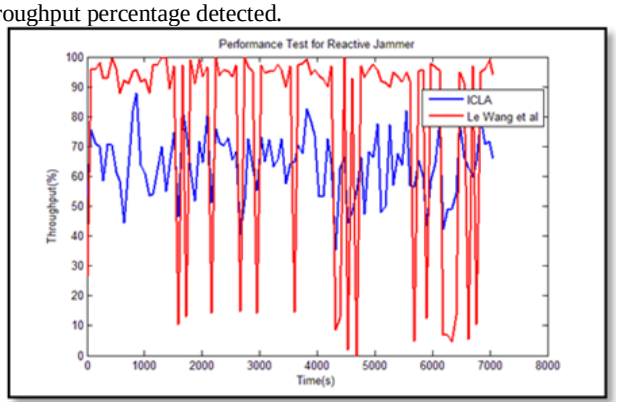

Fig 9: Performance Test for Reactive Jammer

7 Conclusion

There are several issues related to jamming detection at physical and MAC layer that are required to develop a new detection algorithm. Concerns such as higher jamming attack at physical and MAC layers, migration from wired to wireless network that causes network instability and detection using single or dual metrics which has less detection performance needs to be resolved with development of new detection algorithm.

To achieve the defined objective, a methodology was constructed using reverse engineering approach. Throughout the early stage, a simulation model that consists of four scenarios were set up, configured and simulated. Data collected from OPNET simulation tool comprises of six types of metrics vs jammer model which were captured and analysed using statistical approaches. From the analysis, only three metrics were selected as detection keys that will be used as part of detection algorithm.

The performance analysis of jamming attacks shows that intelligent jammers are more difficult to detect than other attack because of its manipulation of 802.11 protocols. OPNET simulation tool is used as instrument to measure the performance. For physical layer jamming attack, result for constant and random jammer showed a better throughput performance with an average of 67.27% and 40.15%. A similar result is captured for deceptive and reactive jammer where throughput's performance is achieved at 95.34% and 69.15%. This outcome showed that ICLA generated better throughput performance as compared to algorithm proposed by [13].

References

[1] A. Sharma and J. K. Singh,(2017) "Detection of Jamming Attack in MANET Using Watchdog Technique," *Int. J. Futur. Gener. Commun. Netw.*, vol. 10, no. 3, pp. 11–20.

[2] D. C. Schleher(1999) "Electronic Warfare in the Information Age," in *Artech House Radar Library*, 1999, pp. 240–246.

[3] J. Deng, Z. Zhang, S. Pagadala, P. K. Varshney, N. Orleans, and C. Science, (2008)"Protecting MANETs from Spurious CTS Attacks with Randomized Carrier Sensing," in *Proceedings of IEEE Sarnoff Symposium '08 Princeton, NJ, USA April 28-30, 2008*, 2008, pp. 1–5.

[4] W. Xu, W. Trappe, Y. Zhang, and T. Wood,(2005) "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in *Proceedings of the 6th ACM International Symposium on Mobile ad hoc Networking and Computing {(MobiHoc 05)*, 2005, p. 46.

[5] Y. W. Law, M. Palaniswami, L. Van Hoesel, J. Doumen, P. Hartel, and P. Havinga, (2009) "Energy-Efficient Link-Layer Jamming Attacks Against Wireless Sensor Network MAC Protocols," *ACM Trans. Sens. Networks*, vol. 5, no. 1, pp. 1–38, 2009.

[6] G. Z. Anthony D. Wood, John A. Stankovic,(2007) "DEEJAM : Defeating Energy-Efficient Jamming inIEEE 802.15.4-based Wireless Networks," in *The 4th Annual IEEE Communication Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON 2007), San Diego, CA, USA, June 2007.*, 2007, pp. 60–69.

[7] R. Muraleedharan and L. a. Osadciw,(2006) "Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System," in *Proc. Wireless Sensing and Processing, 2006*, 2006, p. 62480G–62480G–12.

[8] H. Jadidoleslamy, (2011) "A Comparison of Physical Attacks on Wireless Sensor Networks," *Int. J. Peer to Peer Networks Vol.2, No.2, April 2011 A*, vol. 2, no. 2, pp. 24–42, 2011.

[9] G. Thamilarasu, S. Mishra, and R. Sridhar,(2006) "A Cross-layer Approach to Detect Jamming in Wireless Ad hoc Networks," in *IEEE Military Communications Conference 2006, Washington, D.C., October 2006*, 2006.

[10] G. Thamilarasu and R. Sridhar,(2007) "Exploring Cross-Layer Techniques for Security : Challenges and Opportunities in Wireless Networks," in *Military Communications Conference, MILCOM 2007*, 2007.

[11] G. Thamilarasu, S. Mishra, and R. Sridhar,(2011) "Improving Reliability of Jamming Attack Detection in Ad hoc Networks," *Int. J. Commun. Networks Inf. Secur. 2011*, no. April 2011, pp. 57–66, 2011.

[12] M.-A. El Houssaini, A. Aaroud, A. El Hore, and J. Ben-Othman,(2016) "Detection of Jamming Attacks in Mobile Ad Hoc Networks Using Statistical Process Control," in *The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)*, 2016, vol. 83, no. 83, pp. 26–33.

[13] 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*, 2011.

[14] M. V. . and S. Kumar, (2012)"Detection of Jamming Style DoS attack in Wireless Sensor Network," in *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, 2012, pp. 563–567.

[15] R. Singh and J. Singh,(2012) "A Performance Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network," *Glob. J. Comput. Sci. Technol. Network, Web Secur. V*, vol. 12, no. 12, pp. 1–10, 2012.

[16] N. Sufyan, N. A. Saqib, and M. Zia, "Detection of Jamming Attacks in 802 . 11b Wireless Networks," *J. Wirel. Commun. Netw.*, vol. 1, no. 208, pp. 1–18, 2013.

[17] M. Zuba, Z. Shi, Z. Peng, and J. Cui,(2011) "Short Paper : Launching Denial-of-Service Jamming Attacks in Underwater Sensor Networks," in *Proceedings of the Sixth ACM International Workshop on Underwater Networks*, 2011, pp. 10–14.

[18] Sarkar, N. I. (2011). A Cross Layer Framework for WLANs : Joint Radio Propagation and MAC Protocol. *13th International Conference on Computer and Information Technology 2010 (ICCIT 2010) 23-25 December 2010*.