SECURING MOBILE AD-HOC NETWORKS AGAINST JAMMING ATTACKS THROUGH UNIFIED SECURITY MECHANISM

Arif Sari[1] and Dr. Beran Necat[2]

[1]Department of Management Information Systems, The American University of Cyprus, Kyrenia, Cyprus
arifsarii@gmail.com
[2]Department of Management Information Systems, The American University of Cyprus, Kyrenia, Cyprus
bnecat@gau.edu.tr

ABSTRACT

The varieties of studies in the literature have been addressed by the researchers to solve security dilemmas of Mobile Ad-Hoc Networks (MANET). Due to the wireless nature of the channel and specific characteristics of MANETs, the radio interference attacks cannot be defeated through conventional security mechanisms. An adversary can easily override its medium access control protocol (MAC) and continually transfer packages on the network channel. The authorized nodes keep sending Request-to-Send (RTS) frames to the access point node in order to access to shared medium and start data transfer. However, due to jamming attacks on the network, the access point node cannot assign authorization access to shared medium. These attacks cause a significant decrease on overall network throughput, packet transmission rates and delay on the MAC layer since other nodes back-off from the communication. The proposed method applied for preventing and mitigating jamming attacks is implemented at the MAC layer that consist of a combination of different coordination mechanisms. These are a combination of 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 process that minimizes the occurrence of collisions on the wireless network. The entire network performance and mechanism is simulated through OPNET simulation application.

KEYWORDS

MANET, OPNET Simulation, PCF, RTS/CTS, Jamming Attack, Unified Security Mechanism

1. INTRODUCTION

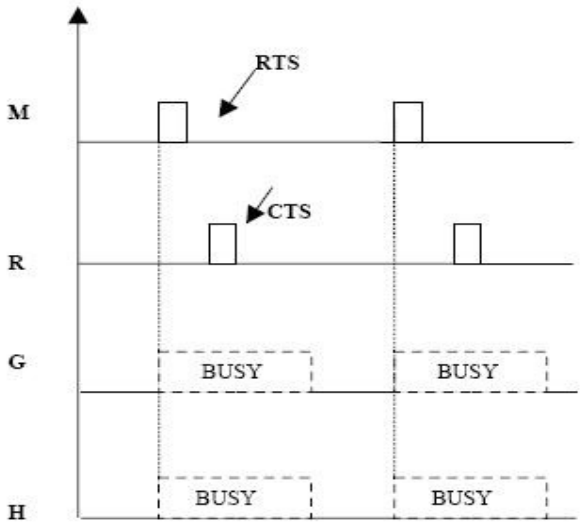
The IEEE 802.11 attacks are investigated in different studies by researchers. The most popular attack model of IEEE 802.11 is Jamming Attacks. Jamming is defined as a Denial of Service (DoS) attack that interferes with the communication between nodes. The objective of the adversary causing a jamming attack is to prevent a legitimate sender or receiver from transmitting or receiving packets on the network. Adversaries or malicious nodes can launch jamming attacks at multiple layers of the protocol suite. In the later section of this research, the jamming attacks are simulated on MANETs that result in collisions in the mobile wireless network. The jamming is divided into two categories as Physical and Virtual Jamming attacks. The physical jamming is launched by continuous transmissions and/or by causing packet collisions at the receiver. Virtual jamming occurs at the MAC layer by attacks on control frames or data frames in IEEE 802.11 protocol [1].

DOI : 10.5121/ijasuc.2012.3306

Physical or Radio jamming in a wireless medium is a simple but disruptive form of DoS attack. These attacks are launched by either a continuous emission of radio signals or by sending random bits onto the channel [2]. The jammers causing these attacks can deny complete access to the channel by monopolizing the wireless medium. The nodes trying to communicate have an unusually large carrier sensing time waiting for the channel to become idle. This has an adverse propagating effect as the nodes enter into large exponential back-off periods.

Virtual Jamming Attacks can be launched at the MAC layer through attacks on the RTS/CTS (Rate to Send/Clear to Send) frames or DATA frames [1, 3]. A significant advantage of MAC layer jamming is that the attacker node consumes less power in targeting these attacks as compared to the physical radio jamming. Here, we focus on DoS attacks at the MAC layer resulting in collision of RTS/CTS control frames or the DATA frames. In virtual jamming attack malicious node sent RTS packets continuously on the transmission with unlimited period of time. During this entire process malicious node effectively jam the transmission with a large segment of transmission on the wireless channel with small expenditure of power. This attack is much effective than physical layer jamming as this attack consume less battery power compare to the other physical layer jamming attack. For example node M is a malicious node and it starting sending a false RTS packet to node R with a large frame. When nodes G and H receive packet on wireless channel they both become blocked for a certain amount of time as apply for node M as shown on the Figure 1 below [4].

Figure 1. Jamming Attack



On the other hand, there are variety of problems occurred during provision of security in Mobile Ad Hoc Networks. A practically operating MANET must consider the trade-off between the deployment feasibility of a security patch and the system efficiency. And often, the feasibility is considered over the efficiency [5, 6]. The feasibility of a deployment (accessibility and cost) mostly depends on the deployment location. Based on this concept, the security strategies are classified as attacker-side strategies, victim-side strategies, and intermediate strategies in [7]. This taxonomy makes more practical sense to evaluate a security strategy than other taxonomies, e.g. activity level or cooperation degree [8]. My thesis will discuss the proposed solution based on this taxonomy by differentiating itself from the proposed solution

2. PROPOSED METHOD

The proposed method applied for preventing and mitigating jamming attacks is implemented at the MAC layer that consist combination of different coordination mechanisms. The network throughput may degrade due to the Request to Send (RTS) collision problem, for that reason RTS/CTS fragmentation thresholds are also involved into this mechanism. Wireless medium access control (MAC) protocols have to coordinate the transmissions of the nodes on the common transmission medium. The IEEE 802.11 working group proposed two different algorithms for contention resolution. These coordination functions of the MAC Layer are shown on the Figure 2 below. The first one is Distributed Coordination Function (DCF) which is completely distributed and the second one is Point Coordination Function (PCF) that has a centralized access protocol. The PCF requires a central decision maker such as a base station while DCF uses a carrier sense multiple access/collision avoidance protocol (CSMA/CA) for resolving channel contention among multiple wireless hosts. The malicious or selfish nodes are not forced to follow the normal operational functions of the protocols. The method implemented in this research study is PCF since in the link layer; a selfish or malicious node could interrupt either contention-based MAC protocols. A malicious jammer may also corrupt the frames easily by injecting some bits into the radio channel or launch DoS attack by exploiting the binary exponential backoff scheme.

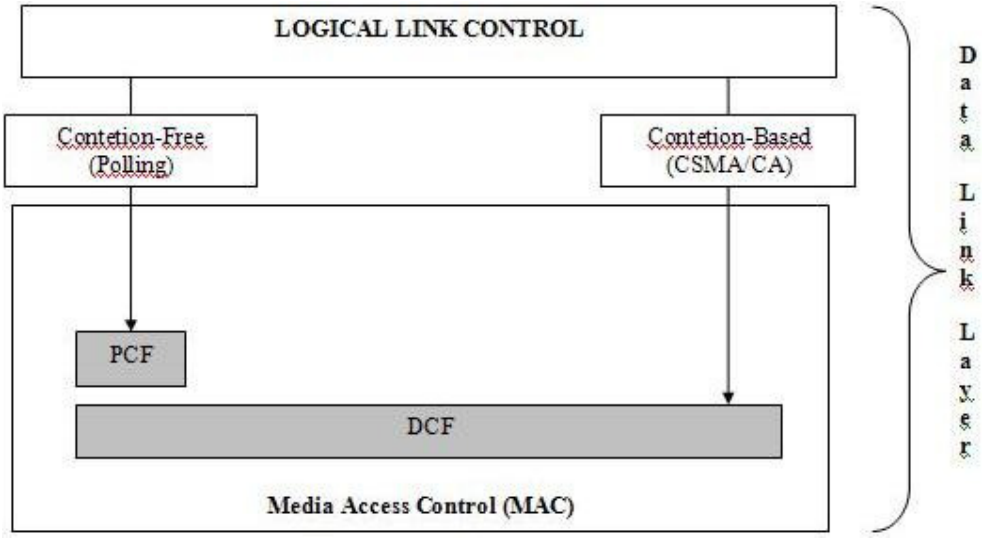


Figure 2. PCF and DCF Functionalities

In order to prevent and secure the network from hidden jammer node attacks and prevent collisions on the network, the Request to Send/Clear to Send (RTS/CTS) mechanism is also implemented. The RTS/CTS mechanism is a handshaking process that minimizes the occurrence of collisions when hidden nodes are operating on the network. The implementation of RTS/CTS mechanism will be illustrated in the next section of the research through the simulation experiment.

The working mechanism of RTS/CTS implementation is illustrated in Figure 3 below.

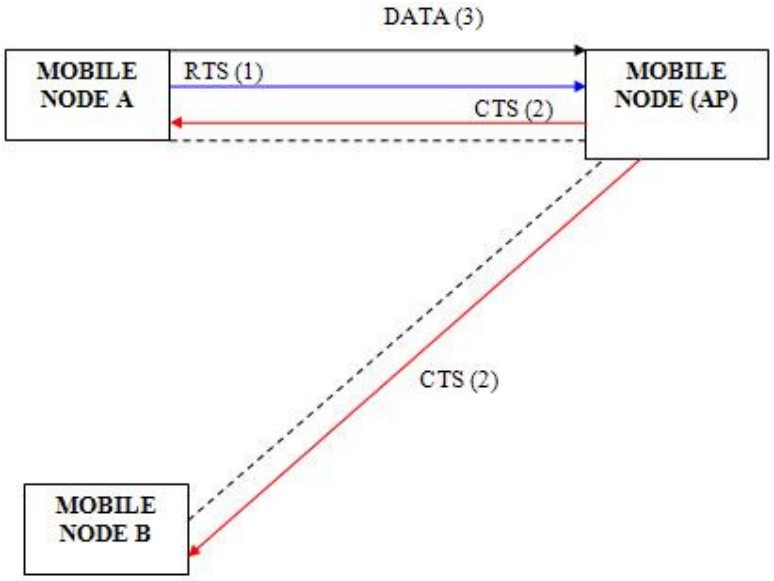


Figure 3. RTS/CTS working mechanism

As it is shown in Figure 3 above-, the AP mobile node receives RTS data from Mobile node A and replies to it with a CTS frame while authenticating it to send data. Meanwhile, the Mobile Node B receives the CTS frame since the Mobile Node A is sending data and the mechanism informs the mobile Node B that the AP is transmitting or receiving data at that time frame. This makes Mobile Node B ~~to~~ wait for a particular time. When a jamming attack is launched on the network, fake RTS frames are sent to the AP mobile node that keeps the medium busy and prevents other nodes from being able to commence with legitimate MAC operations, or introduces packet collisions causing forced and repeated back offs. Figure 4 below illustrates the unified security mechanism implemented on the mac layer that consists of both RTS/CTS and PCF mechanisms.

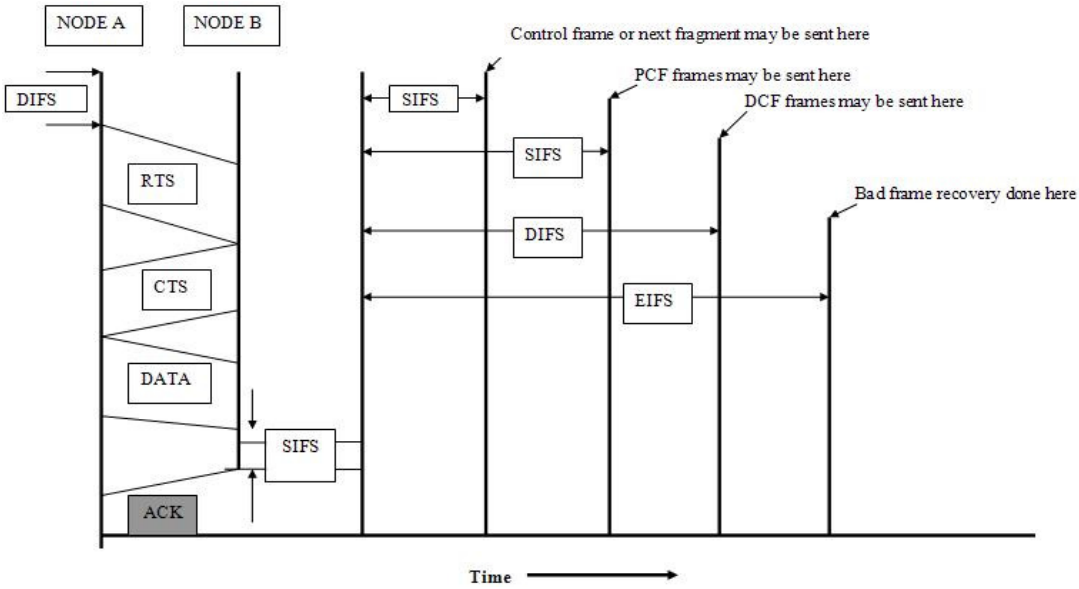


Figure 4. Structure of Proposed Unified mechanism

The proposed unified security mechanism is illustrated as a combined state in Figure 4 above. The figure shows Short InterFrame Spacing (SIFS), PCF InterFrame Spacing (PIFS), DCF InterFrame Spacing (DIFS) and Extended Inter Frame Spacing (EIFS). The interframe space (IFS) is defined to provide priority-based access to the radio channel. The shortest Interframe Space (SIFS) is used for Clear to Send (CTS) and poll response frames. DIFS is the longest IFS and is used as the minimum delay for asynchronous frames contending for access. PIFS is the middle IFS and is used for issuing polls by the centralized controller in the PCF scheme. This model illustrates the combination of RTS/CTS mechanisms with the PCF mechanism to enhance overall network throughput. In the next section, the mechanism is implemented on the node specific node models through the OPNET simulation experiment.

3. SIMULATION MODEL AND EXPERIMENT DESIGN

The tool used for the simulation study is OPNET 14.0 modeller. OPNET is a network and application based software used for network management and analysis [9-10]. OPNET models communication devices, various protocols, architecture of different networks and technologies and provides simulation of their performances in the virtual environment. OPNET provides various research and development solutions which helps in the research of analysis and improvement of wireless technologies like WIMAX, Wi-Fi, UMTS, analysis and designing of MANET protocols, improving core network technology, providing power management solutions in wireless sensor networks. In our case we used OPNET for modelling of network nodes, selecting its statistics and then running its simulation to get the result for analysis.

In this simulation experiment, 3 different scenarios are created and illustrated through the OPNET simulation package. All scenarios and nodes in these scenarios share the same global attributes during the simulation experiment. These attributes and parameters are set for creation of the simulation environment in the OPNET simulation package. Table 1 below shows the simulation parameters used in OPNET simulation in more detail.

Table 1. Global Simulation Parameters for the Experiment

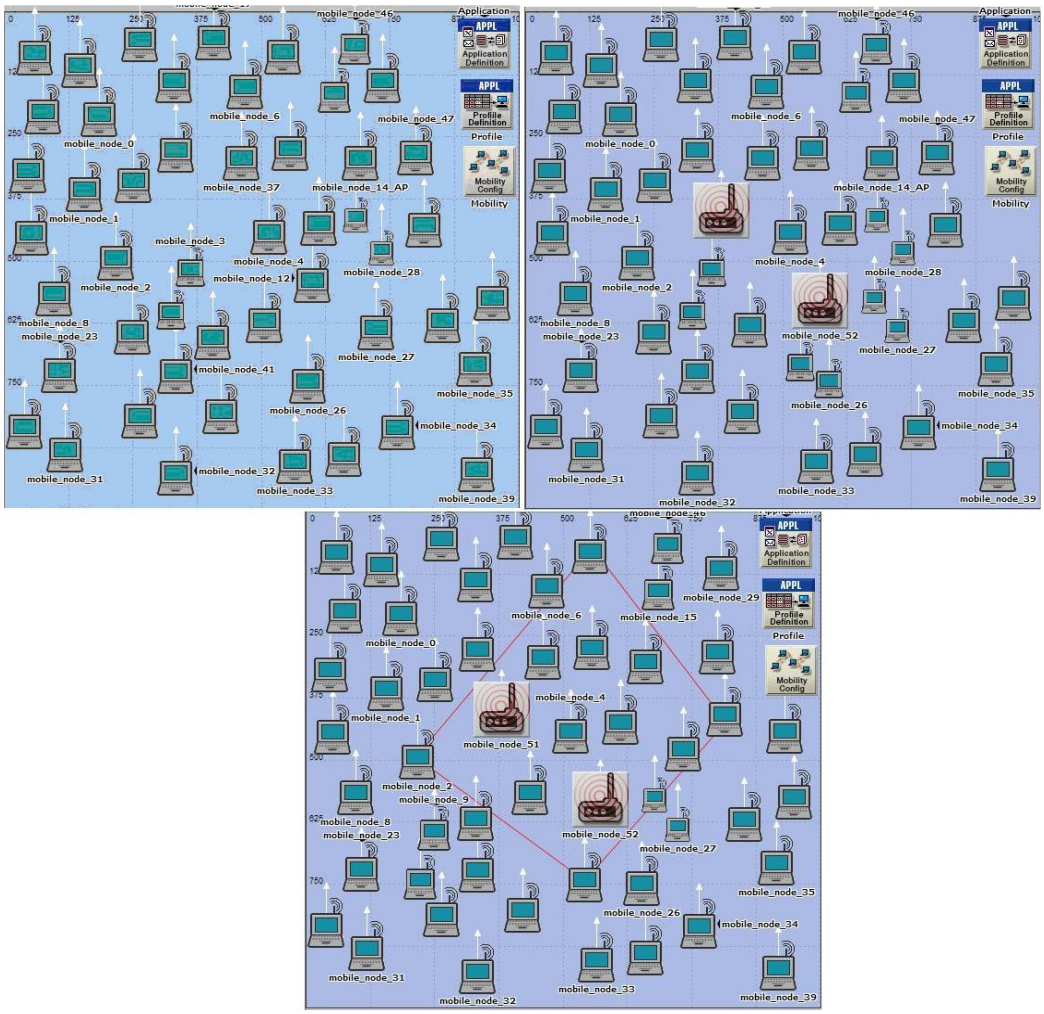
Parameters	**Attributes**
Protocol	AODV
Simulation Time	300 (seconds)
Simulation Area	1000 x 1000 (meters)
Pause Time	100 Seconds
Mobility Model	Random Waypoint
Mobility m/s	10meters/seconds
Performance Parameters	Throughput, Delay, Load, Data Drop Rate
Transmit Power(W)	0.005
RTS Threshold (bytes)	1024 (bytes)

Data Rate (Mbps)	11Mbps
Pkt. Reception power Threshold	-95
Buffer Size	1024000
Pkt. Size (bits)	2000 (exponential)
Pkt. Interarrival time (seconds)	.03 (exponential)
Trajectory	VECTOR
Start time (seconds)	10
End Time	Infinity (End of Simulation time)
No of Seeds	300

Table 3 above represents the global simulation parameters for this experiment. The protocol is selected as AODV. AODV is one of the reactive protocols. In this protocol when a node wishes to start transmission with another node in the network to which it has no route; AODV protocol provides topology information for the node. AODV use control messages to find a route to the destination node in the network. As it has been mentioned before, there are 3 different scenarios created in this research.

Figure 5 illustrates the simulation setup of three scenarios comprising of 50 mobile nodes moving at a constant speed of 10 meters per seconds. All of the scenarios are configured with mobility of 10 m/s. Number of nodes was constant to detect the impact of attacks and the simulation time took 300 seconds. The simulation area taken is 1000 x 1000 meters. Packet Inter-Arrival Time (sec) is taken exponential (0.3) and packet size (bits) is exponential (2000) as shown on ~~the~~ Table 1. The data rates of mobile nodes are 11 Mbps with the default transmitting power of 0.005 Watts. Random way point mobility is selected with constant speed of 10 meter/seconds and with pause time of constant 100 seconds. This pause time is taken after data reaches the destination only. The aim of this simulation experiment was to determine the impact of jamming attacks on mobile ad hoc networks with ADOV-based protocol and impact of our prevention mechanism. The protocol is selected as AODV which is a reactive protocol.

Figure 5. Simulation Scenarios for 50 Mobile Nodes

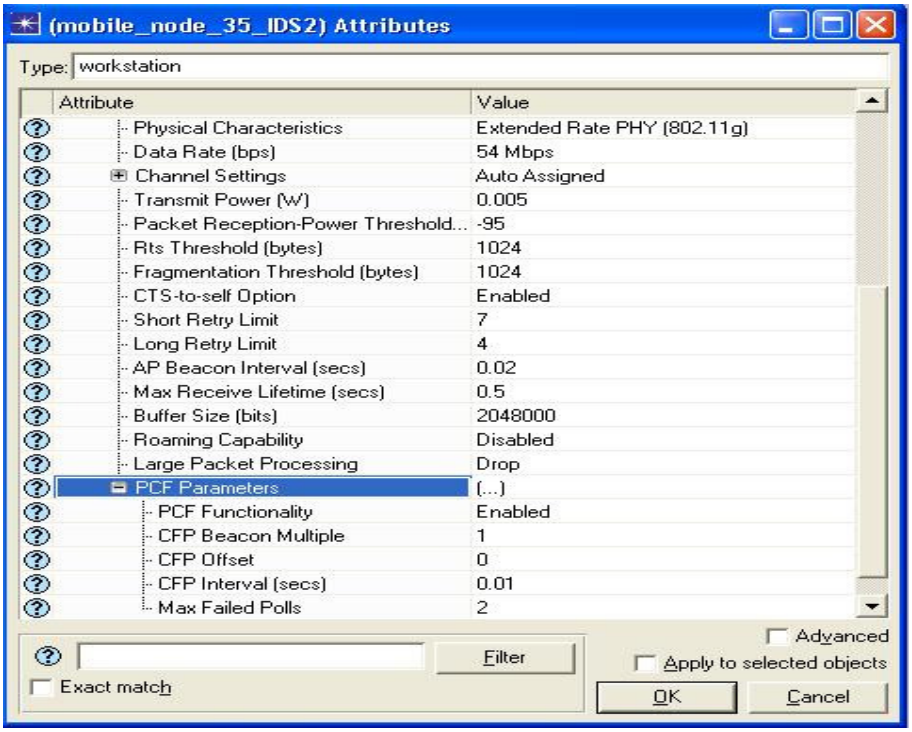


As shown in Figure 5 there are three different scenarios for a mobile network that is formed with a 50 MANET node on the area of 1000x1000, mobile network with 50 MANET nodes and 2 mobile jammers within the same area and 50 MANET nodes, 2 mobile jammers with configured security nodes according to unified security mechanism. The simulation run time is set as 300 seconds which is equal to 20 minutes. Seed value is set as 300. Simulation Kernel is set as optimization. Application profile, Profile configuration, and Mobility are configured to work the network according to our requirements specified in Table 1. The network model consists of three scenarios. The first scenario is a standard scenario without any misbehaving node or attack on the network. In this scenario, one of the participating mobile nodes acting as an access point that represented as "mobile_node_14_AP". The basic service set identifier value for the access point is "1" which is global for all other mobile nodes. The basic service set identifier represents that ~~the~~ all other mobile nodes participate under the same cluster. The Independent basic service set is used in this research that has no backbone infrastructure and consists of at least two wireless stations. This type of network is very suitable for the MANET environment since it can be constructed quickly without much planning. The second scenario illustrates the Jammer attack with routing implementation AODV. The third scenario illustrates

the implementation of the proposed security mechanism to prevent jamming attacks on AODV-based mobile ad-hoc networks.

The modified nodes with PCF and RTS/CTS mechanisms are shown in Figure 6 below. The modification implemented on the selected guard nodes, including AP node are in order to detect the communication on the network. The guard nodes deployed on the network are to coordinate the network functionalities each with assigned same basic service set functions.

Figure 6. Guard Node Implementation modification



As it is shown in Figure 6 ~~above~~, the PCF functionality of the guard nodes and AP node are enabled. The data packages that are routed among nodes are transmitted through guard nodes. The 2 mobile jammers deployed on the network inject malicious traffic through 802.11 radio channel and cause collision. The mobile guard nodes deployed on the network detect the malicious traffic and drop the traffic from the corresponding node. The hidden jammer node problem rises on MANETs when the PCF mechanism is implemented on the network. The hidden node is a mobile node that communicates with only the AP node and does not communicate with other mobile nodes within the range. For that reason, the RTS/CTS mechanism is also enabled and modified with a specific value set.

3.1 MANET TRAFFIC MODEL

The specific MANET traffic parameters are set for this simulation experiment. The traffic model is used to generate traffic on the network and has a set of applications that generates the packet in both exponential and constant form when the simulation time starts, with random destinations or defined destination packet delivery. Furthermore, it is essential to specify a trajectory for mobile nodes to provide mobility where nodes in the network are constantly

moving. Table 2 illustrates the parameters defined for the MANET traffic model of this simulation experiment.

Table 2. MANET Traffic Model Parameters

Attribute	**Value**
Trajectory	VECTOR
AD-HOC Routing Parameters	
Ad Hoc Routing Protocol	AODV
MANET Traffic Generation Parameters	
Start Time	10 seconds
Packet Interarrival time	.03 seconds (exponential)
Packet Size (bits)	2000 (exponential)
Destination IP Address	Random
Stop Time	End of Simulation
WLAN Parameters	
Data Rate (bps)	11 Mbps
Channel Settings	Auto Assigned
Transmit Power	0.005 Watt
RTS Threshold	1024 bytes
Buffer size	1024000 bits

3.2 SCENARIO CREATION

This section describes the different scenarios, ~~and~~ attributes and parameters used in these scenarios. In the 1st scenario, the mobile ad hoc network is simulated without any jammers or misbehaving – malicious traffic. This scenario is created in order to compare the other scenarios and situations and understand the impact of attack and effectiveness of the detection mechanism on the network. The 2nd scenario contains 2 jammers that inject unauthorized traffic into the network and affect the mobile network that has no specific detection or prevention mechanism against jamming attacks. The 3rd scenario which is specifically designed to prevent jamming attacks on the network has the same characteristics with the proposed prevention mechanism.

Table 3 below shows the detailed information about scenario parameters. The table shows different parameters for each scenario.

Table 3 Simulation Parameters for Specific Scenarios

	Parameters	*Values*
Scenario 1	Protocol	AODV
	Simulation Duration	300sec.
	Number of Seeds	300
	Number of Nodes	50
	Transmit Power (W)	0.005
	Data Rate	11Mbps
	Packet Size	2000
	Number of Jammers	0
Scenario 2	*Parameters*	*Values*
	Protocol	AODV
	Simulation Duration	300sec.
	Number of Seeds	300
	Number of Nodes	50
	Transmit Power (W)	0.005
	Data Rate	11Mbps
	Packet Size	2000
	Number of Jammers	2

	Parameters	*Values*
Scenario 3	Protocol	AODV
	Simulation Duration	300sec.
	Number of Seeds	300
	Number of Nodes	50
	Transmit Power (W)	0.005
	Data Rate	11Mbps
	Packet Size	2000
	Number of Jammers	2
	Number IDS Node	5

The main reason for simulating ~~the~~ scenario 1 where no malicious node or jammer were used, is to identify the state of the network under normal conditions and this will help us to compare and differentiate the impact of a jamming attack on the network in later stages. In the 2nd scenario, the jamming attack is simulated on MANET. This scenario is created with 50 mobile nodes like the 1st scenario, but 2 jammers are used in this scenario. Each of the jammers are modified according to the specifications and requirements of the project. The jammer specifications are illustrated in Table 4 below. The jammers used in this scenario are mobile jammers that are used to continuously emit a radio signal in order to inject a specific amount of packages to the network. These jammers are considered to be the most effective type of jammer since they drop the throughput of the network to zero and when launched they attack for a long period of time until it runs out of energy. Figure 7 below illustrates the jammer's source and transmitters that are used to inject data packets into the network.

Figure 7. Jammer Node Inner Module

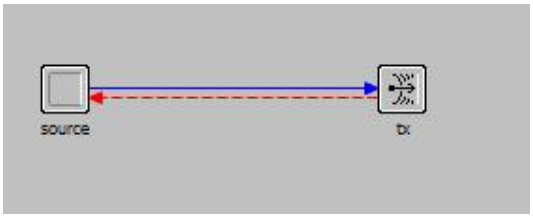


Table 4. Jammer Configurations

Parameters	**Attributes**

Transmit Power(W)	0.005
Trajectory	VECTOR
Jammer Bandwidth	100,000
Jammer Band-base Frequency	2,402
Pulse Width	2.0
Start time (seconds)	10
End Time	Infinity (End of Simulation time)

Since the prevention mechanism aims to prevent "jamming attacks", the jammer designed here shares the common characteristics of some of the jammer types mentioned in the previous chapter. However, due to the scope of this work, jamming is any attack to deny service to legitimate users by generating high Radio Frequency (RF) noise or fake /legitimate protocol packets with spurious timing effect on the network.

3.3 PERFORMANCE METRICS

The performance metrics chosen for the evaluation and prevention of jamming attacks on MANETs are network throughput, network load and packet end-to-end delay. Table 5 illustrates the selected performance metrics for the simulation experiment.

Table 5. Simulation Performance Metrics

Performance Metrics
Network Throughput
WLAN Delay
Network Load
WLAN Data Dropped

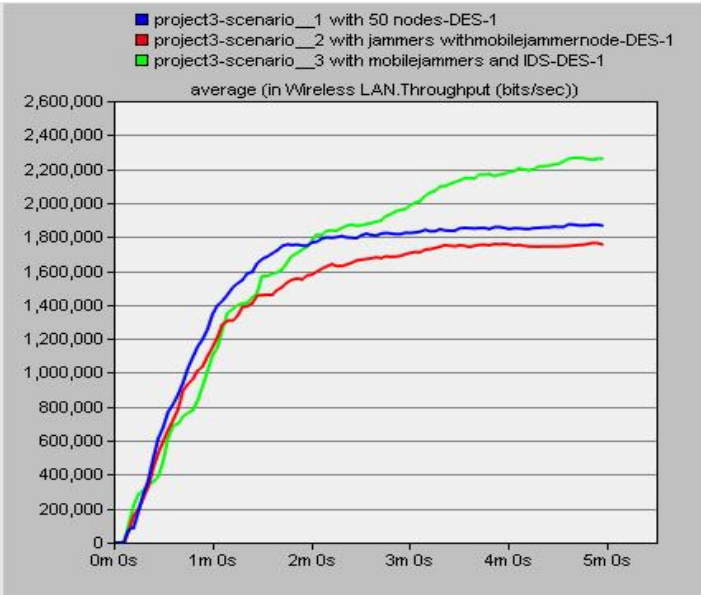
The network throughput is the overall performance of the network. It represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network. The WLAN Delay represents the end to end delay of all the packets

received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer. This delay includes medium access delay at the source MAC, reception of all the fragments individually, and transfers of the frames via AP, if access point functionality is enabled. The network load represents the statistic that is dimensioned in order to measure the network load separately for each BSS. Hence, each dimension is a global statistic covering one WLAN BSS of the network. The statistic represents the total data traffic (in bits/sec) received by the entire WLAN BSS from the higher layers of the MACs that is accepted and queued for transmission. This statistic doesn't include any higher layer data traffic that is rejected without queuing due to full queue or the large size of the data packet. Any data traffic that is relayed by the AP from its source to its destination within the BSS is counted twice for this statistic (once at the source node and once at the AP), since such data packets are double-loads for the BSS because both the source node and the AP have to contend for their transmissions via the shared medium. The WLAN Data Dropped rate is the total size of the higher layer data packets (in bits/sec) dropped by all the WLAN MACs in the network due to, full higher layer data buffer, or the size of the higher layer packet, which is greater than the maximum allowed data size defined in the IEEE 802.11 standard.

4. SIMULATION RESULTS AND DISCUSSION

After compilation of 3 scenarios with 50 mobile nodes and different parameters for each scenario, the simulation results are gathered and analyzed in this section. The 3 scenarios are compiled within a Discrete Event Simulation (DES) environment, and collected information is analyzed based on the performance metrics mentioned in ~~the~~ section 3.3. According to the simulation experiment outcomes, the following figures are generated. Figure 8 shows the throughput performance evaluation of the 3 scenarios.

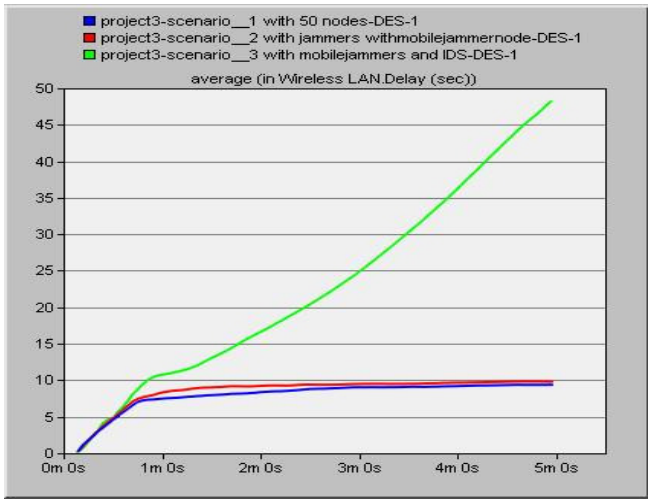
Figure 8. Average WLAN Throughput Statistics



As it is clearly shown in the Figure above, the WLAN Throughput of the entire network is analyzed with DES. Scenario 1, represents the scenario with no malicious event and normal network state, scenario 2 represents the network that is under the jamming attack and scenario 3 represents the mobile jammers and implementation of the proposed method. It can be clearly seen, that the jamming attack decreases the overall network throughput in comparison to the

normal network state. However, the entire network throughput is increased once the proposed unified mechanism is implemented. In addition to this, the state of the throughput has increased more than the no attack scenario after implementing the unified security mechanism. Figure 9 below illustrates the WLAN Delay among scenarios.

Figure 9. Average WLAN Delay Statistics



As it is shown in Figure 9, there is a significant increase observed on MANET delay for scenario 3 where the proposed mechanism is implemented. However, due to jamming attack on the network, the increase in MANET delay differs slightly from the normal state of the network which means that, implementation of such a mechanism leads to an increase in WLAN Delay. Figure 10 below illustrates the Network Load, which was computed from WLAN.

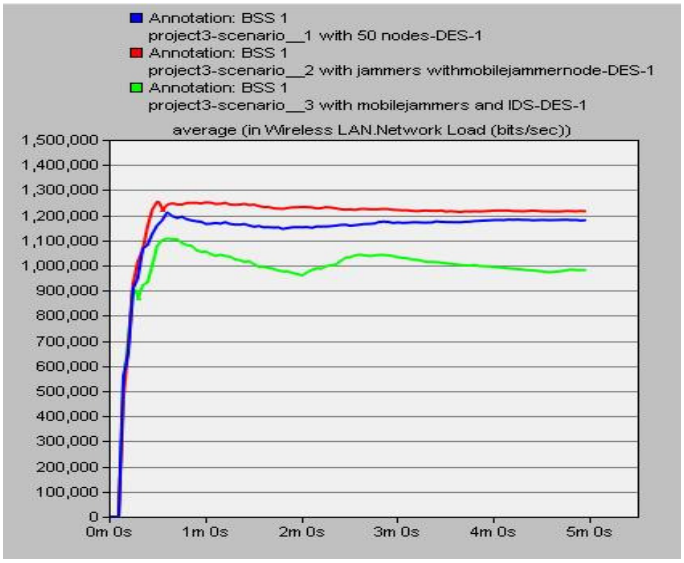


Figure 10. Average WLAN Network Load

As it can be seen from the above figure, the WLAN Load level is increased when the jamming attack is launched. On the other hand, the load is decreased when the mechanism is implemented on the specific nodes in the network. The normal state of the network illustrated that the network load is around 1,100,000 bits/sec.–Figure 11 illustrates the average data dropped on the WLAN.

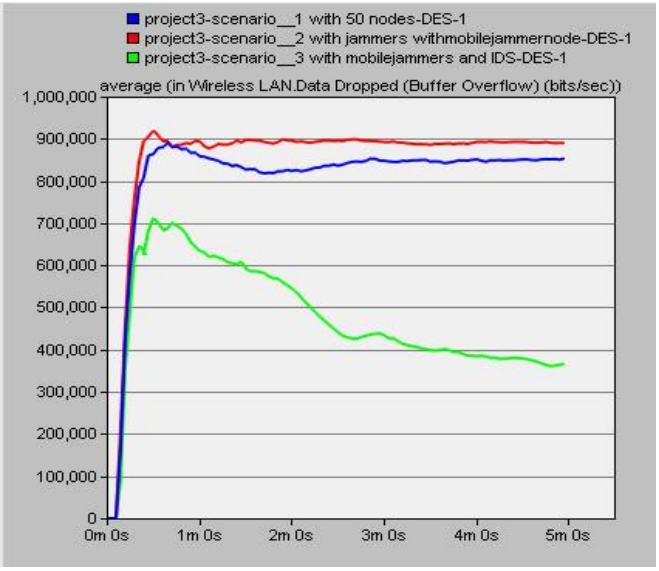


Figure 11. Average WLAN Data Dropped Rate

This is the total size of higher layer data packets dropped by all the WLAN MACs in the network due to full higher layer data buffer or a greater size of the higher layer packet which is not allowed defined 802.11 standards. As it is shown, there is a significant decrease in buffer overflow and data drop due to this problem when implementing PCF –RTS/CTS mechanism together on the MANET. It also decreases the overall data drop rate in comparison to the normal state of the network.

5. CONCLUSION

The goal of this simulation research study was to observe the impact of a combination of security mechanisms against jamming attacks. The unified mechanism is implemented on the selected nodes on the network and deployed in the specific area. The findings of the resarch clearly states that, the implementation of such unified mechanisms have a significant impact on the overall network through positively. On the other hand, the implementation of such mechanisms does not only mitigate the jamming attack effects, it also increases the overall performance above the normal state of the network. The unified mechanism that contains a combination of RTS/CTS and PCF shows adequeate performance in MANET. Since 2 mobile jammers used in this simulation experiment, the proposed security mechansim satisfactorly mitigated the effects of the jamming attack on the network and increased the overall performance of the network while improving data drop rate. The data dropped rate decreased succsseffully. Since the jamming attack leads packet drop rate and low throughput impact on the network, the rate of delay seems acceptable on the network. Future studies can be carried out to modify the current model to decrease an overall delay on the network

REFERENCES

[1] D. Chen, J. Deng, and P. K. Varshney, "Protecting wireless networks against a denial of service attack based on virtual jamming," in MOBICOM -Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking, ACM, 2003.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in MobiHoc '05:Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 46–57, 2005.

[3] D. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in Proceedings of the 25th IEEE Communications Society Military Communications Conference (MILCOM), October 2006.

[4] Ashikur Rahman, Pawel Gburzynski, 2006. Hidden Problems with the Hidden Node Problem. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.61.365&rep=rep1&type=pdf. [Accessed Feb – 2012]

[5] S. Convery, D. Miller and S. Sundaralingam, Cisco SAFE: Wireless LAN Security in Depth 2003, CISCO Whitepaper.

[6] Barbara Guttman, Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers and Computer Security Officials. 1992, NIST Special Publication 800-4.

[7] H. W. Fletcher, K. Richardson, M. C. Carlisle and J.A. Hamilton. "Jr. Simulation Experimentation with Secure Overlay Services". In Summer Computer Simulation Conference. 2005. Philadelphia, Pa.

[8] A. Habib, M. Hefeeda and B. Bhargava. "Detecting Service Violations and DoS Attacks". In The 10th Annual Network and Distributed System Security Symposium 2003. San Diego, California. pp. 177-189.

[9] Cavin, D., Y. Sasson and A. Schiper, 2002. On the accuracy of MANET simulators. Proceedings of the 2nd ACM International Workshop on Principles of Mobile Computing, Oct. 30-31, ACM Press, Toulouse, France, pp: 38-43.

[10] Opnet Technologies, Inc. "Opnet Simulator," Internet: www.opnet.com, [Accessed May - 2012]