Jamming Attacks Impact on the Performance of Mobile Ad-Hoc Network and Improvement Using MANET Routing Protocols

Sabbar Insaif Jasim

Abstract*—Security in MANET has been a challenging task ever since the wireless networks came into existence. A number of works have been developed to accomplish this task. Jamming attacks can severely interfere with the normal operation of wireless networks and, consequently, mechanisms are needed that can cope with jamming attacks. This paper introduced the effect of jammer in Mobile Ad Hoc Network and presented how routing protocols can improve the performance of network in terms of some parameters. MANET Routing protocols taken in this study are OLSR (Proactive routing protocol), DSR (Reactive routing protocol), TORA and GRP (Hybrid Routing Protocol). This study was done using OPNET Modeler (v14.5) in terms of number of scenarios' parameters for HTTP application such as (Delay, Throughput, Data dropped, traffic received and sent). The results showed that Jammers would reduce the performance by increasing delay and data dropped and decreasing throughput. MANET routing protocols could improve system performance by increasing throughput and data dropped at the expense of increasing delay.

Index Terms*— MANET, OPNET, Routing Protocols, Jammers, attacks.

I. INTRODUCTION

There are two classifications of Mobile networks: infrastructure networks and Mobile Ad Hoc Networks (MANET) according to their dependence on fixed infrastructures. In a Mobile Ad Hoc Network, the network may experience rapid and unpredictable topology changes because nodes move arbitrarily. Every node in MANET has the responsibility to act as a router and routing paths in MANETs potentially contain multiple hops [1]. This nature of Mobile Ad hoc network made it vulnerable to attacks.
Jamming attacks can severely interfere with the normal operation of wireless networks , therefore, mechanisms are needed that can cope with jamming attacks [2]. this jamming attacks can affect throughput, load and delay of the network. MANET routing Protocols can improve delay, throughput, data dropped..... etc. This paper introduced four MANET Routing Protocols (DSR, OLSR, TORA and GRP) using OPNET Modeler (v14.5) in number of scenarios for each routing protocol to to investigate which of these protocols can improve the network's performance when Jamming attacks integrated into the network in terms of (delay, throughput, traffic sent and received, network load and download response time).

Manuscript received December, 2013
Sabbar Insaif Jasim, Department of Electronic, Technical Institute, Al-Dour/ Foundation of Technical Institute, City Name, Iraq.

II. RELATED WORK

Many works had been introduced on the routing protocols together with security issues in Mobile Ad-Hoc Network (MANET). Tajinderjit Kaur and Sangeeta Sharma introduced jamming attack in the networks having nodes with isotropic and directional antennas. The simulation results show that it is possible to minimize the effect of jamming attack by using different antenna Patterns [3]. Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay presented different types of attacks on integrated MANET-Internet communication [4]. Chanchal Aghi, Chander Diwaker present a review of Black hole attack in AODV routing protocol which is the most attention seeking attack in AODV routing protocol as compared to other protocols [5]. Maulik, R and Chaki, N presents a comprehensive review is done on the very recent state of the art research results on wormhole attacks and relevant mitigation measures [6].

III. MANET

MANET is a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. These nodes are equipped with wireless transmitters/receivers using antennas which may be omnidirectional (broadcast), highly- directional (point-to-point), or some combination thereof. Due to the transmission power levels, the co-channel interference levels, the movement of the nodes, and their transmitter/receiver coverage patterns, The system can be viewed as a random graph. As the nodes move or adjust their transmission and reception parameters, the network topology may change with time [7].

IV. ATTACKERS

There are different types of attacker present in MANETs as shown in Fig.1, which tries to reduce the performance of network [8].

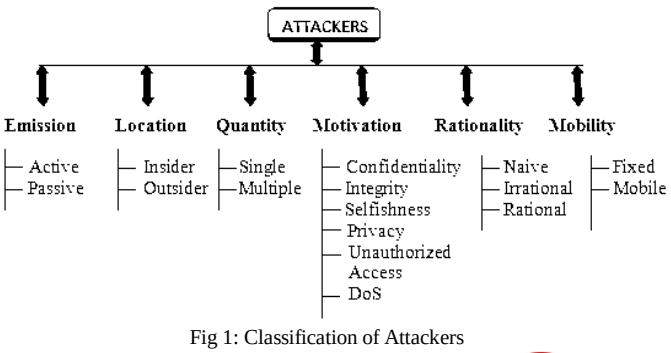

Fig 1: Classification of Attackers

Mobile Ad hoc networks are vulnerable to various attacks from outside and within the network itself. There are two different levels of attacks in Ad Hoc Networks.

1- The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing [8].
2- The second level of attacks tries to damage the security mechanisms employed in the network [8].

V. JAMMING ATTACKS

One main challenge in design of these networks is their vulnerability to Denial-of-Service (DoS) attacks. Jamming is a particular class of DoS attacks. A radio signal can be jammed or interfered, which causes the message to be corrupted or lost because the mobile hosts in mobile ad hoc networks share a wireless medium. Thus, If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications [7].

A jamming attack can impede wireless communications. It is easily delivered by emitting continuous signal injecting dummy packets into the shared medium causing interference with existing communications or in some cases abusing the MAC (Medium Access Control) layer of other nodes within a range [9]. Some possible attack strategies that a jammer can perform in order to interfere with other wireless communications are (Constant Jammer, Deceptive Jammer, Random Jammer, Reactive Jammer [7].

Jamming attacks would reduce the performance of network. MANET routing protocols could improve the performance of network in terms of some parameters. In this paper, four routing protocols (DSR, TORA, OLSR and GRP) in order to investigate which of them was suitable to improve performance of the network.

A. Dynamic source routing (DSR):

DSR is a reactive protocol used in multi-hop ad hoc networks of mobile nodes. This protocol allows the network to be self-configuring and self organizing and does not need any existing network infrastructure or administration [10].

B. Temporally ordered routing algorithm (TORA):

TORA is proposed for highly dynamic mobile, multi-hop wireless networks. TORA is a source-initiated on-demand routing protocol. It is a highly efficient, scalable, and adaptive distributed routing algorithm based on the concept of link reversal. It finds multiple routes from a source node to a destination node. [11].

C. Optimized link state routing (OLSR):

OLSR, proactive routing protocol exchanges routing information with other nodes in the network. The key concept used in OLSR is of MPRs (Multi Point Relays). It is optimized to reduce the number of control packets required for data transmission using MPRs [12].

D. Geographic Routing Protocol (GRP)

GRP offers an efficient framework that can simultaneously draw on the strengths of PRP (Proactive routing protocol) and RRP (reactive routing protocol). The goal of this protocol is to rapidly gather network information at a source node without spending a large amount of overheads which results in achieving fast (packet) transfer delay without unduly compromising on (control) overhead performance [13].

VI. SIMULATION SETUP

In this paper, the impact of jamming attackers was investigated on Mobile Ad hoc Network which can affect delay, throughput and other parameters. The study was done using OPNET Modeler Simulation program.

The OPNET Modeler environment includes tools for all phases of a study, including model design, simulation, data collection, and data analysis which supports all network types and technologies to answer the most difficult questions with confidence. OPNET Modeler based on a series of hierarchical editors that directly parallel the structure of real networks, equipment, and protocols [14].

Number of OPNET scenarios taken for the simulation setup. Each scenario consists of number of parameters as shown in the following details:

A. Scenario 1: MANET without Jamming Attackers

In this scenario, no. of client connected wirelessly to wireless server without any jammers as shown in Fig. 2.

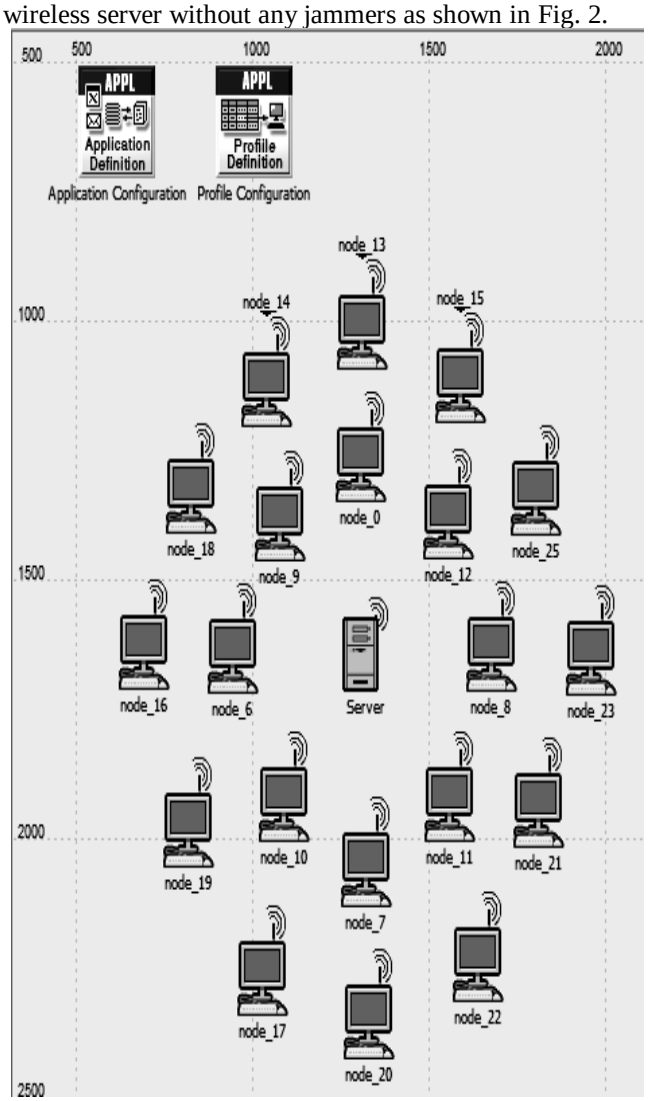

Fig. 2 MANET without Jamming Attackers

B. Scenario 2: MANET with Jamming Attackers

In this scenario, no. of client connected wirelessly to wireless server with 4 jammers. The transmit power of clients is 0.005 W and Jamming Attackers transmit at power of 0.001. this scenario shown in Fig. 3.

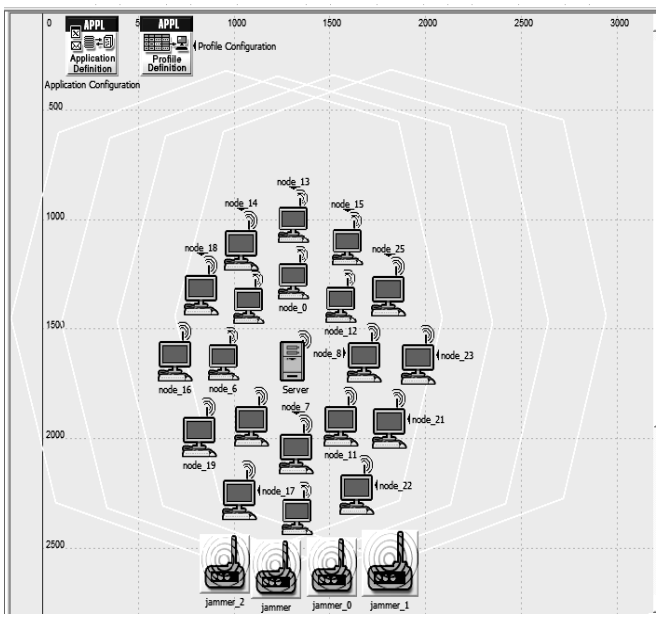

Fig.3 MANET with Jamming Attackers

Routing Protocols were configured on the network to improve delay , throughput and other parameters as in the following scenarios:

C. Scenario 3: MANET with Jamming Attackers with DSR Routing Protocol

In this scenario, no. of client connected wirelessly to wireless server with 4 jammers. The transmit power of clients is 0.005 W and Jamming Attackers transmit at power of 0.001. the routing protocol is DSR. This scenario shown in Fig. 4.

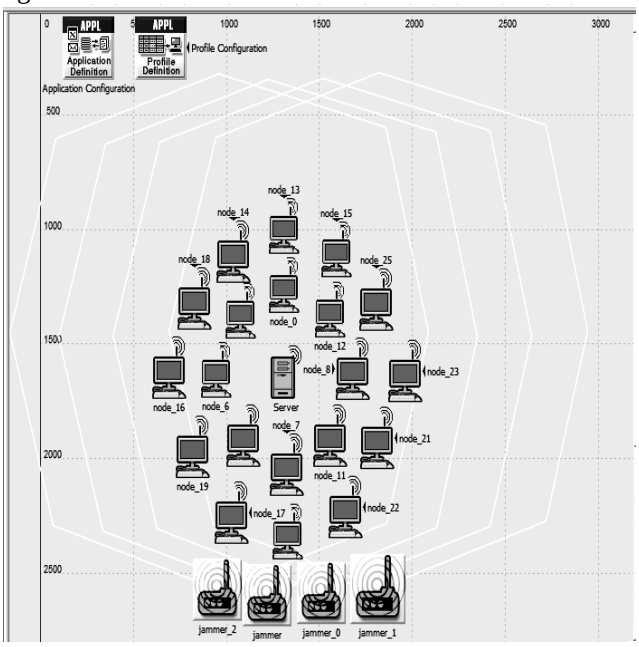

Fig.4 MANET with Jamming Attackers with DSR Routing Protocol

D. Scenario 4: MANET with Jamming Attackers with TORA Routing Protocol

In this scenario, no. of client connected wirelessly to wireless server with 4 jammers. The transmit power of clients is 0.005 W and Jamming Attackers transmit at power of 0.001. the routing protocol is TORA. This scenario shown in Fig. 5.

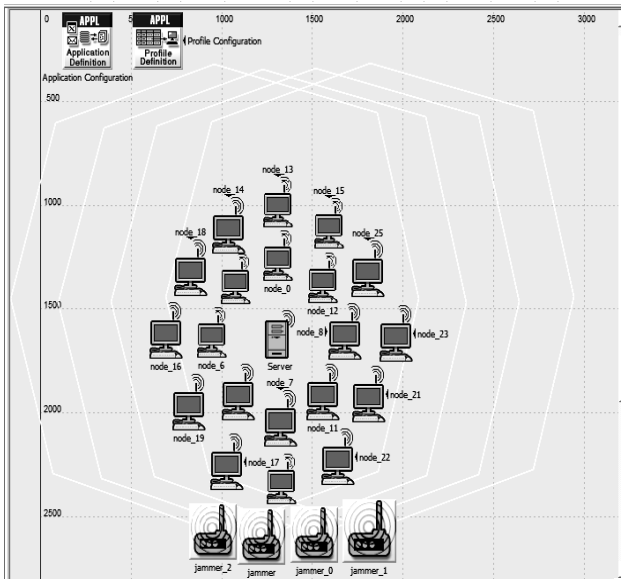

Fig. 5 MANET with Jamming Attackers with TORA Routing Protocol

E. Scenario 5: MANET with Jamming Attackers with OLSR Routing Protocol

In this scenario, no. of client connected wirelessly to wireless server with 4 jammers. The transmit power of clients is 0.005 W and Jamming Attackers transmit at power of 0.001. the routing protocol is OLSR. This scenario shown in Fig. 6.

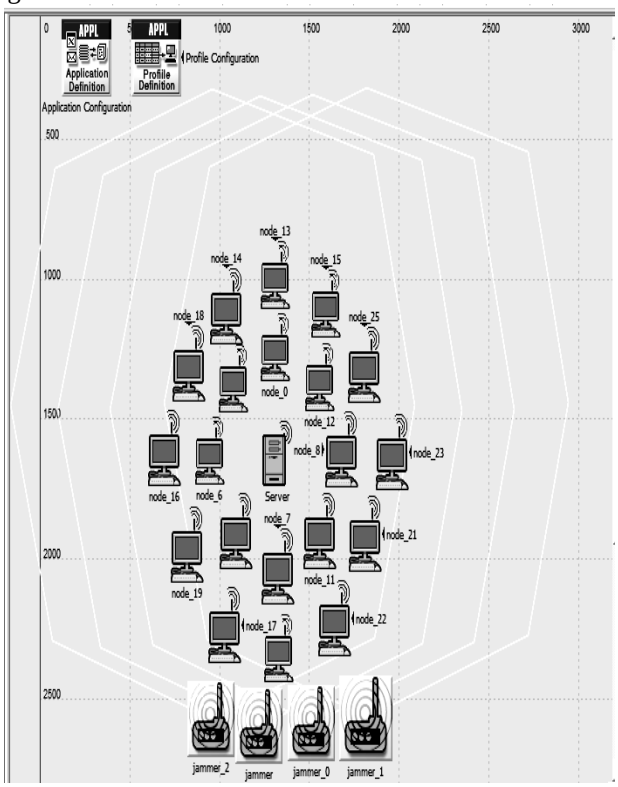

Fig. 6 MANET with Jamming Attackers with OLSR Routing Protocol

F. Scenario 6: MANET with Jamming Attackers with GRP Routing Protocol

In this scenario, no. of client connected wirelessly to wireless server with 4 jammers. The transmit power of clients is 0.005 W and Jamming Attackers transmit at power of 0.001. the routing protocol is GRP. This scenario shown in Fig. 7.

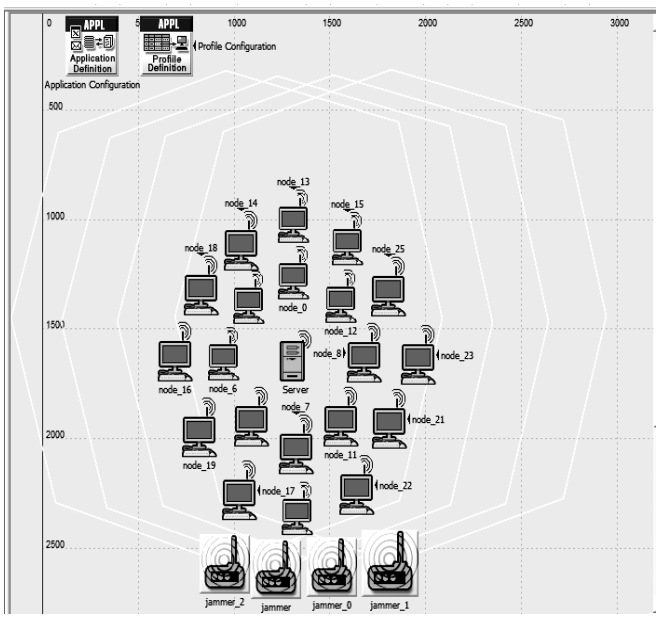

Fig. 7 MANET with Jamming Attackers with GRP Routing Protocol

Discrete Event Statistics were chosen for the proposed system in order to collect the results. The statistics are delay, throughput, network load, ……..). The simulation was run for 1 hour with seed value = 200. The results were collected as shown in the following section.

VII. RESULTS

Number of results were collected in terms of many parameters:

1- 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. Jammers would affect the performance of system by increasing the delay as shown in the Fig.8.

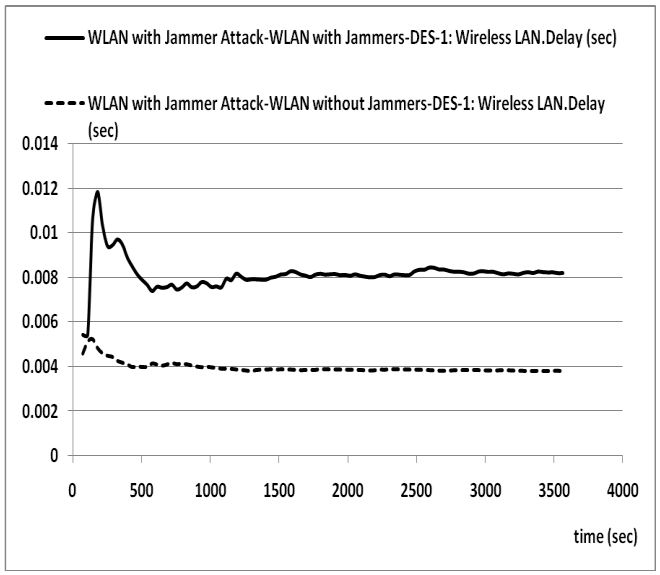

Fig. 8 Delay

2- Throughput: Represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network. Jammers would affect the performance of system by decreasing the throughput as shown in the Fig.9.

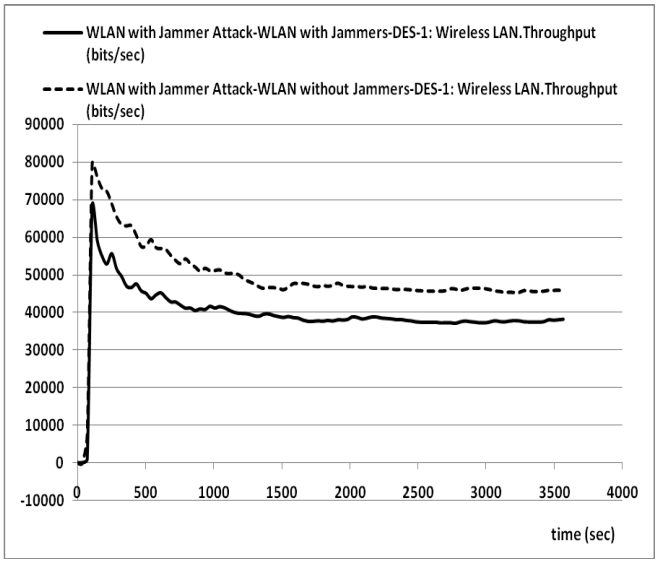

Fig.9 Throughput

3- Data dropped: Total higher layer data traffic (in bits/sec) dropped by the all the WLAN MACs in the network as a result of consistently failing retransmissions. Jammers could affect the network by increasing Data dropped of network as shown in Fig.10.

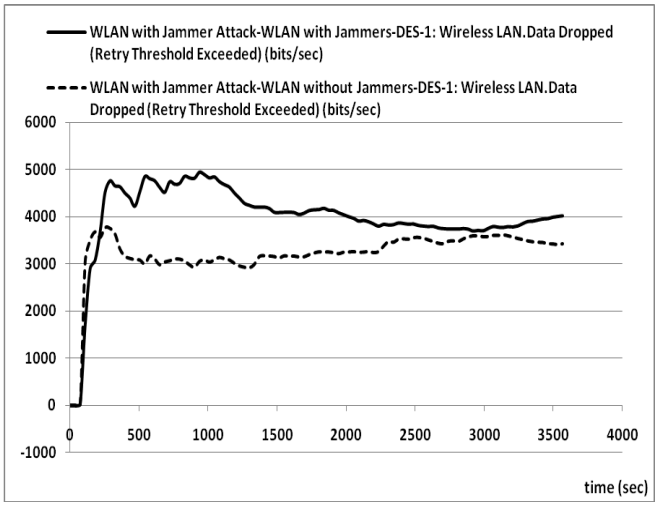

Fig. 10 Data Dropped

4- Traffic received and sent: jammers increase traffic received and sent for HTTP (web browsing application) which as an application example as shown in Fig.11 and Fig.12 respectively.

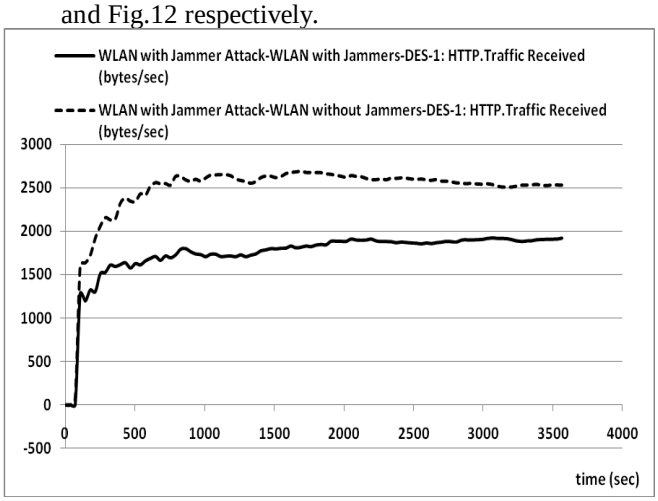

Fig.11 Traffic received

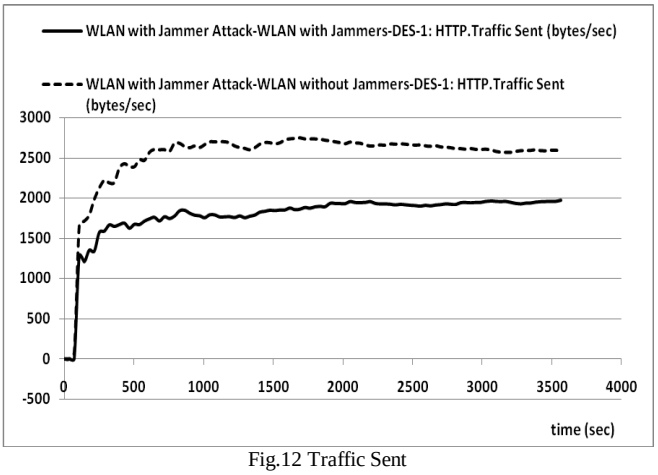

Fig.12 Traffic Sent

5- Four routing protocols (DSR, TORA, OLSR and GRP) increase the delay and traffic received and sent of MANET with attackers at the expense of improving the throughput and data dropped as will be observed as shown in Fig.13 , Fig.14 and Fig.15 respectively.

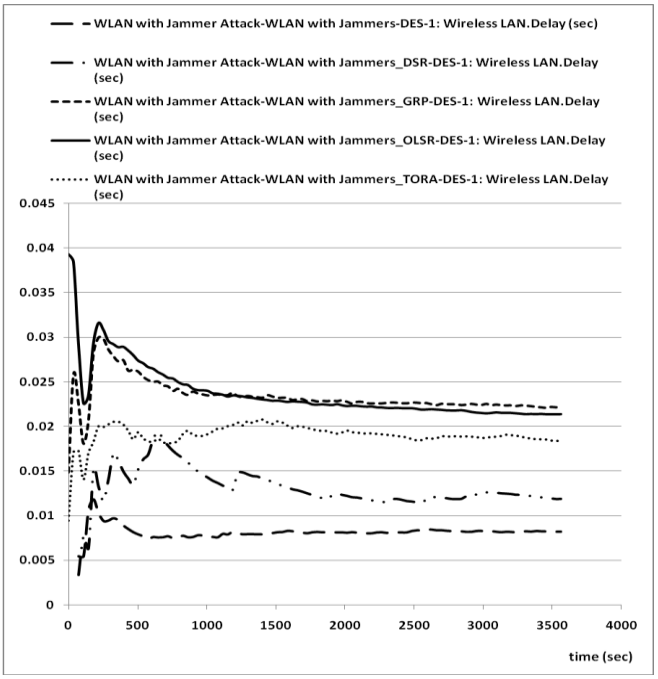

Fig. 13 Delay

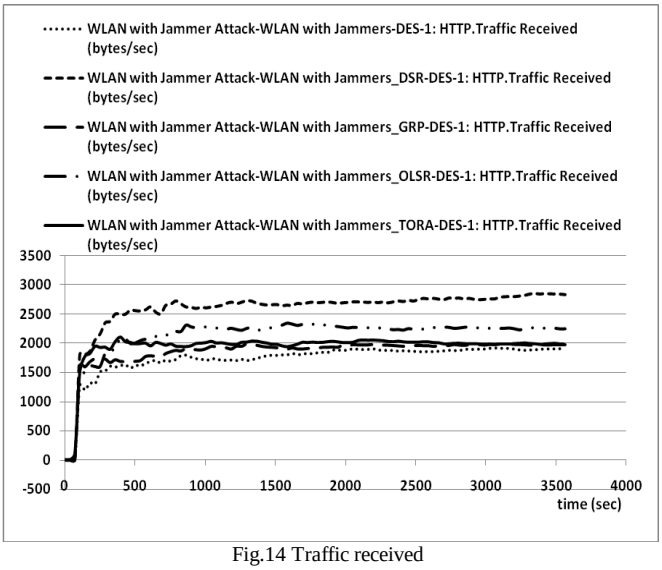

Fig.14 Traffic received

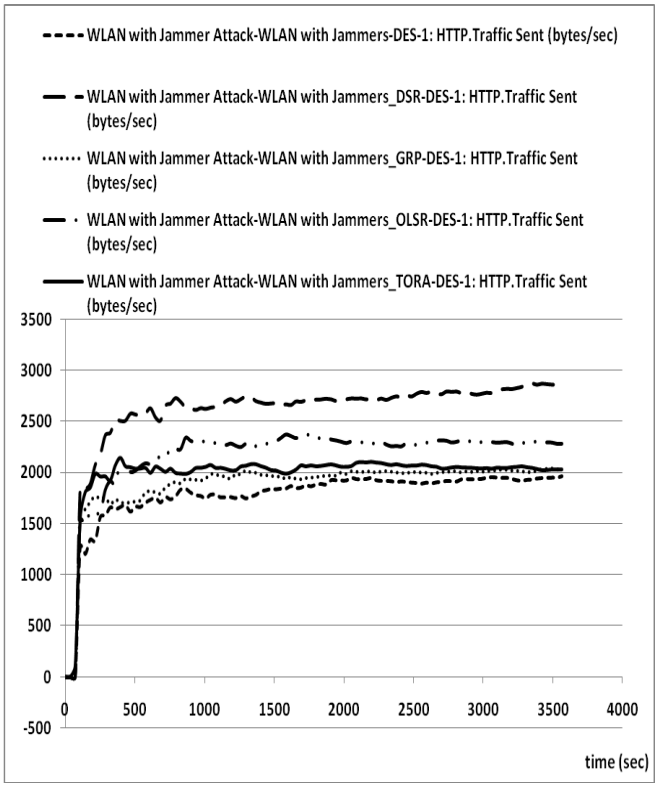

Fig.15 Traffic sent

6- Four routing protocols (DSR, TORA, OLSR and GRP) improve the throughput of MANET with attackers by increasing it as shown in Fig. 16.

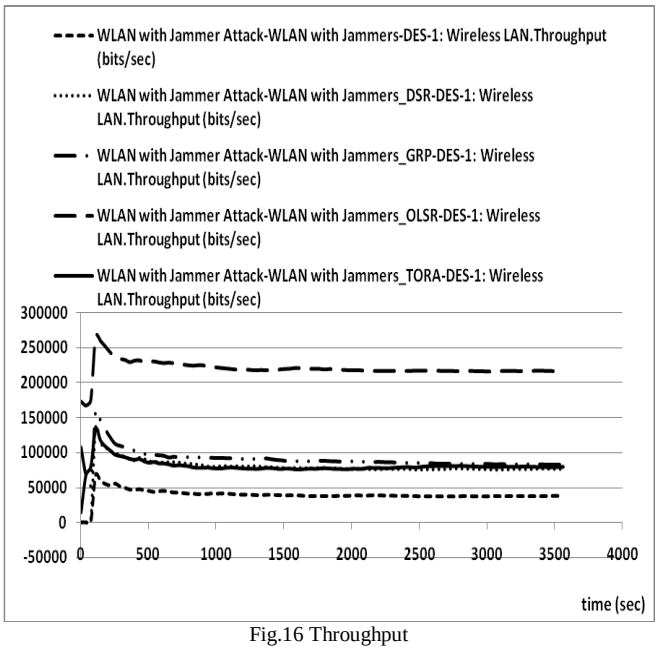

Fig.16 Throughput

Jammers would decrease throughput of Mobile Ad-Hoc Network and the four routing protocols (DSR, TORA, OLSR and GRP) improve the performance of the network and the OLSR routing protocol would had larger throughput than (DSR, TORA, GRP).

7- Four routing protocols (DSR, TORA, OLSR and GRP) improve the performance of the network by decreasing data dropped as shown in Fig.17.

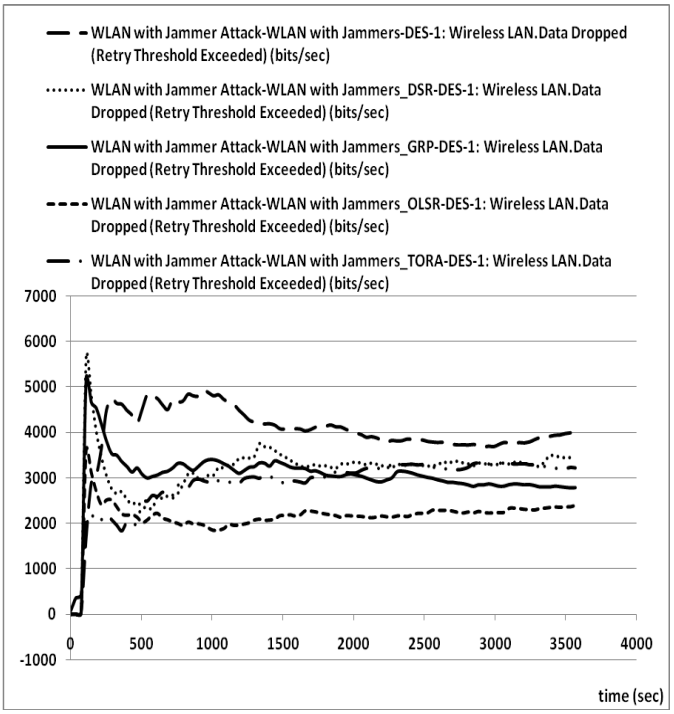

Fig.17 Data Dropped

As shown previously, OLSR routing protocol was better than three routing protocols (DSR, TORA, GRP) by decreasing data dropped in the network.

VIII. CONCLUSION

Jammers attacks can affect network's performance because the jammers interfere with the normal operation of the network. The effect of attackers studied in this paper was by increasing delay, data dropped traffic received and sent and decreasing throughput of the network. There are three categories for Mobile Ad-Hoc Network routing protocols, Proactive, Reactive and Hybrid routing protocols. Four protocols were taken in this paper DSR , OLSR, TORA and GRP in order to show which of them can improve the performance of the network in terms of the parameters affected by the attackers. The network was simulated using OPNET Modeler (v14.5) which was suitable tool for this simulation study. Routing protocols were increased delay, HTTP traffic received and sent at the expense of increasing throughput and decreasing data dropped. OLSR protocol was more successful in increasing throughput and decreasing data dropped but it caused larger delay. This study was about the effect of attackers on the network's performance. Other parameters could be taken for this study for other application such as (FTP, data access, Email) applications. Some security works can be done to reduce the effect of attackers.

REFERENCES

[1] Harminder S. Bindra1, Sunil K. Maakar and A. L. Sangal, "Performance Evaluation of Two Reactive Routing Protocols of MANET using Group Mobility Model", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 10, May 2010, pp38-44.

[2] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", MobiHoc'05, , UrbanaChampaign, Illinois, USA., ACM 1595930043/ 05/0005 , May 25–27, 2005.

[3] Tajinderjit Kaur, Sangeeta Sharma, "Mitigating the Impact of Jamming Attack by Using Antenna Patterns in MANET", VSRD International Journal of CS & IT Vol. 2 (6), 2012, pp. 437-445.

[4] Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), 2010, pp.265-274.

[5] Chanchal Aghi1, Chander Diwaker, "Black hole attack in AODV routing protocol: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013, pp.820-823.

[6] Kannhavong, B. , Nakayama H., Nemoto Y., Kato N, Jamalipour A., "A survey of routing attacks in mobile ad hoc networks",IEEE Wireless Communications, **Volume**: 14, **Issue**: 5, 2007, pp.85-91.

[7] Ali Hamieh, Jalel Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution", IEEE International Conference on Communications, 2009, pp.1-9.

[8] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012, pp.269-275.

[9] Kwangsung Ju and Kwangsue Chung, "Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks", International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012, pp.149-154.

[10] Rajeshwar Singh, Dharmendra K Singh, Lalan Kumar, "Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks", International Journal of Advanced Networking and Applications Vol. 02, Issue: 04, 2011, pp. 732-737.

[11] Anuj K., Dr. Harsh S., Dr. Anil K., "Performance analysis of AODV, DSR & TORA Routing Protocols", IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010, pp. 226-231.

[12] Kirti Aniruddha Adoni and Radhika D. Joshi, "Optimization of Energy Consumption for OLSR Routing Protocol in MANET", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 1, February 2012, pp. 251-262.

[13] Chang Wook Ahn, "Gathering-based routing protocol in mobile ad hoc networks", Computer Communications 30 (2006) 202–206.

[14] OPNET official website www.opnet.com

Sabbar Insaif Jasim have M.Sc. degree in Computer Control Engineering from Baghdad university. He received B.Sc. degree from Baghdad University, collage of engineering in Electrical Engineering. He is a lecturer in Department of Electronics, Al-Dour Technical Institute, He presents many papers in national journals and participate in number of conferences.