International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

SIMULATIVE INVESTIGATION THE PERFORMANCE ANALYSIS OF DSR AND TORA ROUTING PROTOCOL UNDER JAMMER ATTACK IN MANET

Aditi[1], Joy karan Singh[2]

[1]*M.tech Student, Dept. of CSE,CT Institute of Technology & Research , Jalandhar,India*

[2]*Assistant Professor , Dept. of ECE,CT Institute of Technology & Research , Jalandhar,India*

ABSTRACT:-***Routing is a vital matter in MANET and hence the focus of this paper along with the performance analysis of routing protocols under jamming attack. A mobile ad hoc network (MANET) is generally a kind of network that contains autonomously nodes, that can arrange themselves in different ways and operate without any network administration. In the absence of any infrastructure for security and continuously changing topology of the network makes the routing protocols vulnerable to variety of attacks. These attacks may Cause either misdirection of data traffic or denial of services. In this paper, a comparative analysis is performed on the basis of simulation for two types of routing protocols on the basis of jammer attack and a normal network over MANET. Various simulation experiments were carried out, to access and validate the feasibility of the study. The simulation experiments have taken FTP application with two scenarios (under jammer attack and under normal network).Dynamic source Routing (DSR) and Temporarily ordered Routing Protocol (TORA) has been considered for exploration in this paper based on Data Drop, delay, load, Media access delay and Retransmission attempts performance metrics using OPNET Modeler 14.5.***

Keywords DSR, TORA, JAMMER, MANET Routing Protocols

1. INTRODUCTION

In the couple of lustrum there has been a step development in the market of laptops, hand held devices and notebooks. These devices are battery operated with limited potential but have the challenge of high processing capability. With the help of these mobile devices people can easily access the internet or communicate with other devices by using wireless network. The cost of wireless networks is low and needs less effort as compared to wired networks and there is no demand of any additional devices. Security has become a key concern in order to furnish protected communication in Wireless as well as wired environment. Magnificent attention have received by mobile ad hoc networks (MANETs) in last few years, because of their self configuration and self maintenance capabilities[8]. On the other hand early research attempts assumed a friendly and collaborative environment and attentive towards the problems such as wireless channel access and multihop routing, security has become a popular concern to provide protected communication between number of nodes in a probably hostile environment. Although security has long been an dynamic research topic in wireless networks, the distinctive characteristics of MANETs present a new set of nontrivial summons to security design. These summonses include open network architecture, shared wireless medium, severe resource constraints and highly active network topology. Accordingly, the existing security solutions for wired networks do not directly register to the MANET domain. MANET provide security services, such as confidentiality, authentication, integrity and availability, to mobile users is an eventual goal of the security solutions for MANETs . Basically routing protocol are of three types Reactive protocol (On-Demand), Proactive protocol (Table driven), and Hybrid Protocol. . In this paper, we have evaluated performance of DSR and TORA routing protocols based on FTP applications[8] with normal network and under jammer attack network and analyzed by means of Data drop, delay, Network load, Throughput and Retransmission metrics by using OPNET Modeler 14.5.

2. MANET ROUTING PROTOCOLS

For the simulation environment we have chosen two protocols the first one is DSR protocol and the second one is TORA protocol. Both protocols are belongs to Reactive routing protocol category.

2.1 Dynamic source routing(DSR)

The Dynamic Source Routing protocol is basically consist of two main mechanisms to allow the discovery and maintenance of source routes in the ad hoc networks.

Route Discovery: It is the mechanism in which a Source node wants to send a packet to a destination node, acquires a source route to the destination[4]. When the source node attempts to send a packet to a destination and does not already know a route to that destination only in that case Route Discovery is used.

Route Maintenance: It is the mechanism by which a node wants to send a packet to a destination is able to recognize, while using a source route to the destination, if the network topology has switch to another topology[5]. If this is the case then it should no longer hold this route to the destination because a link along the route shattered. For this route the Route Maintenance is used only when the packets are actually delivered from source node to the destination

.

2.2Temporally-Ordered Routing Algorithm (TORA)

TORA stands for Temporally-Ordered Routing Algorithm . It is a unique approach for routing the packets to their destination in distributed routing protocol for multihop networks[1]. TORA is fully distributed, in that routers need only maintain information about adjoining routers and there is no centralized control. This is necessary for all Ad Hoc routing protocols. TORA maintains state on a per-destination basis similarly as a distance-vector routing approach. However, it does not continuously execute shortest-path computation and thus the metric used to establish the routing structure does not represent a distance. The destination-oriented nature of the routing structure in TORA supports a combination of reactive and proactive routing on a per-destination basis[3]. Sources initiates the establishment of routes to a given destination on demand during the reactive operation. The key design concepts of TORA is the near occurrence of a topological change, the control messages are localized to a very small set of nodes. To achieve this, nodes require to maintain the routing information about adjacent (one hop) nodes. Route creation, Route maintenance, Route erasure are the three functions basically performed by TORA.

3. SIMULATION ENVIRONMENT

The simulations are performed using OPNET Modeler 14.5 with the nodes spread randomly over a square area of 800 m x 800 m. The mobility model used is "Random Waypoint Model" in which a node simply chooses a objective, called waypoint and progress towards it in a straight line with a constant velocity [2]. The simulations are divided into scenarios with initially 29 nodes with normal network and with pulse jammer attack. The simulation was run for 5 simulation minute with seed value of 128 using application remote login. The pause time for the simulation is considered to be constant. The kernel mode is put to be optimized. The details are record in Table 1. Here in first scenario, used 29 mobile nodes and one fixed WLAN server under normal network. The application configuration and profile configuration was drag to workspace. The second scenario used 29 mobile nodes under pulse jammer attack. All the attributes remain the same except the jammer attack. In this scenario both protocols are tested against the similar parameters. Details for puls_jammer are in Table 2 and Table 3

Table 1. Simulation Parameters setup

.

Parameters	Values
Routing protocol	DSR,TORA
Operation mode	802.11g
Simulation time	5 minute
Attack	Pulse_jammer
Data rate(bps)	11 mpbs
Application traffic	FTP
Transmit power	0.005
Parameters of quality of services	Delay,Media access delay,Load & Retransmission attempts
No. of nodes	29
Buffer size	256000
Transmit power	0.005

Table2. Simulation Parameters for Pulse_jammer

Attributes	Values
Jammer Band base frequency	2,402
Jammer Bandwidth	100,000
Jammer Transmit power	0.001w

Table3. Simulation Parameters for jamming node

Attributes	Values
Pulse off time	2.0
Pulse on time	1.0

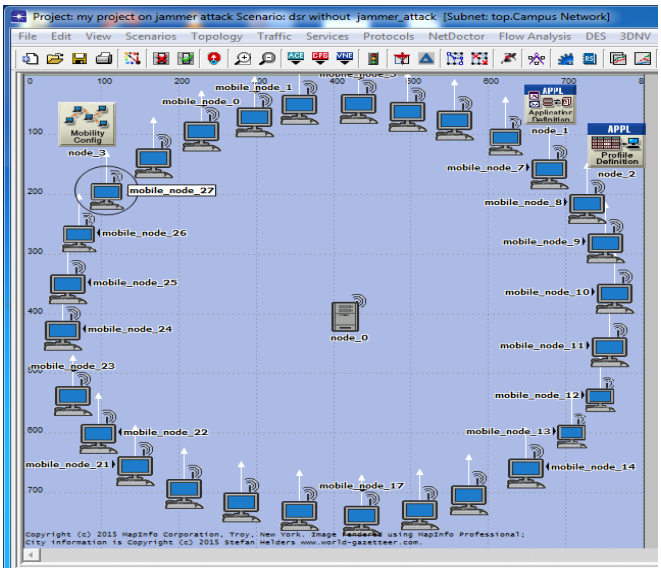

Figure 1: Scenario of 29 Nodes without attack

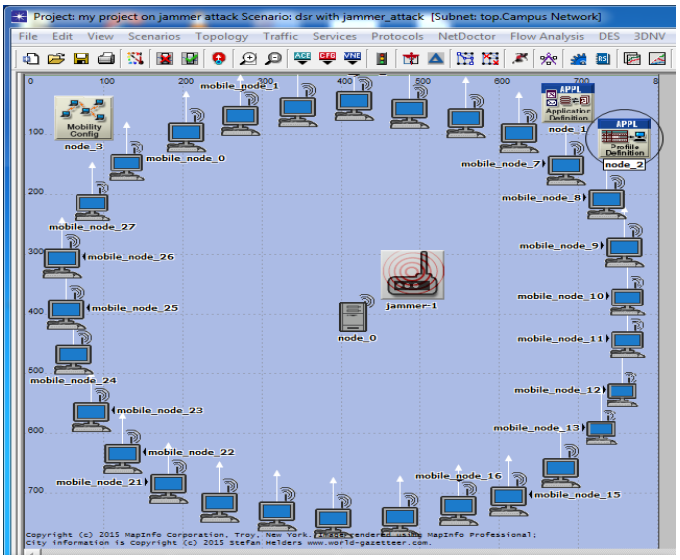

Figure 2: Scenario of 29 Nodes with jammer attack

Performances metric are important aspect to perform analysis on network and to explain the implementation of the simulation environment and a key factor to evaluate the real performance of the network. In our network simulation we decided to chose, Data drop, Retransmission attempts, delay and network load.

Delay

The packet end to end delay is the average time of the packet going through inside the network. It includes all over the delay of network like transmission time delay. It also includes the time from originating packet from sender to destination and express in seconds.

Network load

Network load is the total packet sent and received across the entire network at a particular time.

Packet Dropped

Packet dropped shows that how many packets are successfully sent and received across t he entire network. It also explains the number of packet dropped during the transmission to interference from other devices.

Retransmission Attempts

Retransmission attempts occurred in network when delivery of packet is dropped or lost without reaching to the destination nodes.

4. SIMULATION RESULTS

The main target of this paper is to evaluate the performance and behavior of each routing protocol with respect to the normal network and with pulse jammer attack for FTP application. The results are based on evaluation metrics of delay, network load, retransmission attempts and data drop. We have divided our study into two sets of experiments: the first section provide the performance status of DSR and TORA under normal network and the second one provide performance under pulse jammer attack.

4.1 Data drop

The Fig.4.1(a)& Fig.4.1(b), x-axis shows the time(minute/second) and y-axis shows the data drop(bit/sec).The value for DSR & TORA is 12.81177 &238.9274 respectively using 29 nodes under jammer attack and value under normal network for DSR & TORA is 0 & 4.71964 respectively using 29 nodes. In both cases DSR perform better than TORA protocol.

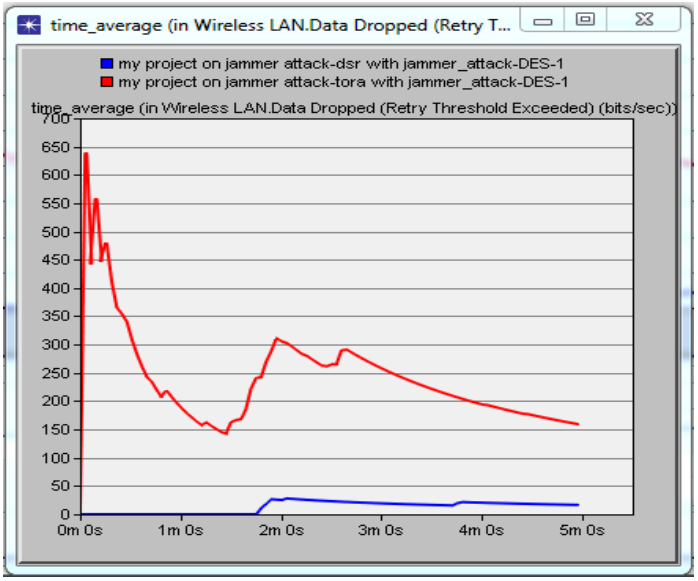

Fig 4.1(a): Comparison of DSR and TORA protocol for Data drop with attack

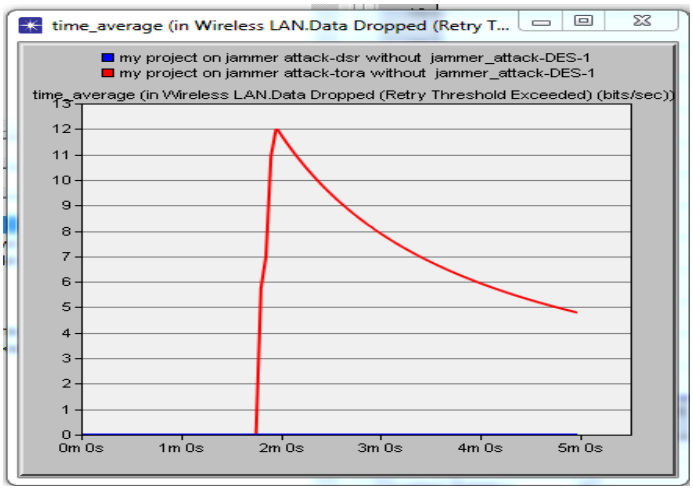

Fig 4.1(b): Comparison of DSR and TORA protocol for Data drop without attack

4.2 Delay

The Fig.4.2(a)& Fig.4.2(b), x-axis shows the time(minute/second) and y-axis shows the delay(sec).The value for DSR & TORA is 0.02166 &0.043055 respectively using 29 nodes under jammer attack and value under normal network for DSR & TORA is 0.001373 & 0.005108 respectively using 29 nodes. In both cases DSR perform better than TORA protocol.

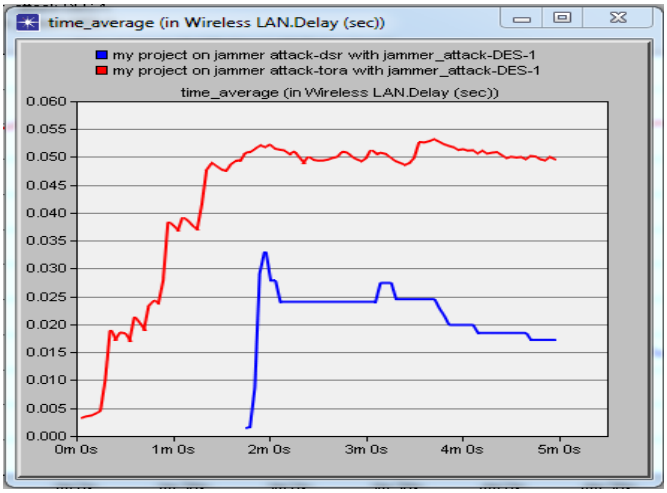

Fig 4.2(a): Comparison of DSR and TORA protocol for Delay with attack

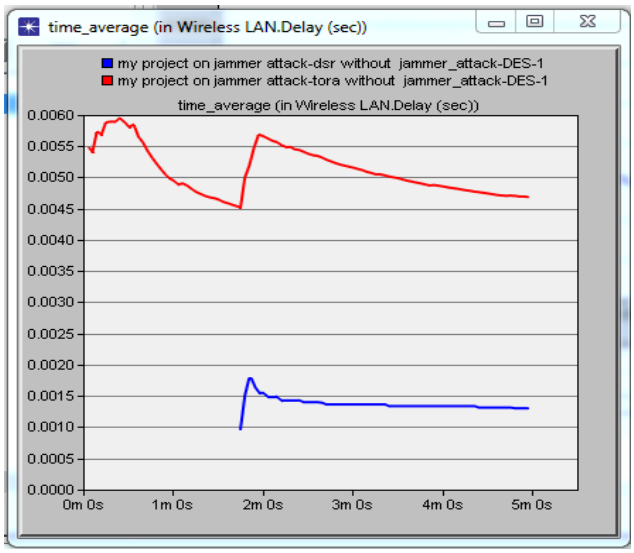

Fig 4.2(b): Comparison of DSR and TORA protocol for Delay without attack

4.3 Network load

The Fig.4.3(a)& Fig.4.3(b), x-axis shows the time(minute/second) and y-axis shows the network load (bit/sec).The value for DSR & TORA is 5750.529 &52065 respectively using 29 nodes under jammer attack and value under normal network for DSR & TORA is 5568.532 & 27236.59 Respectively using 29 nodes. In both cases DSR perform better than TORA protocol.

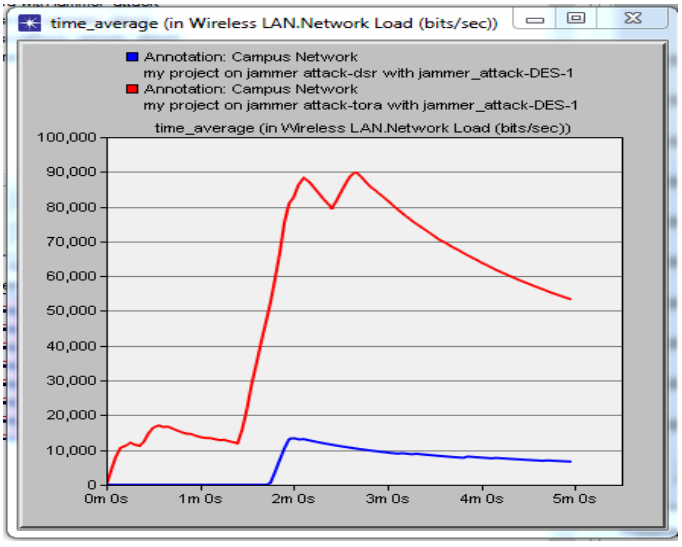

Fig 4.3(a): Comparison of DSR and TORA protocol for Network load with attack

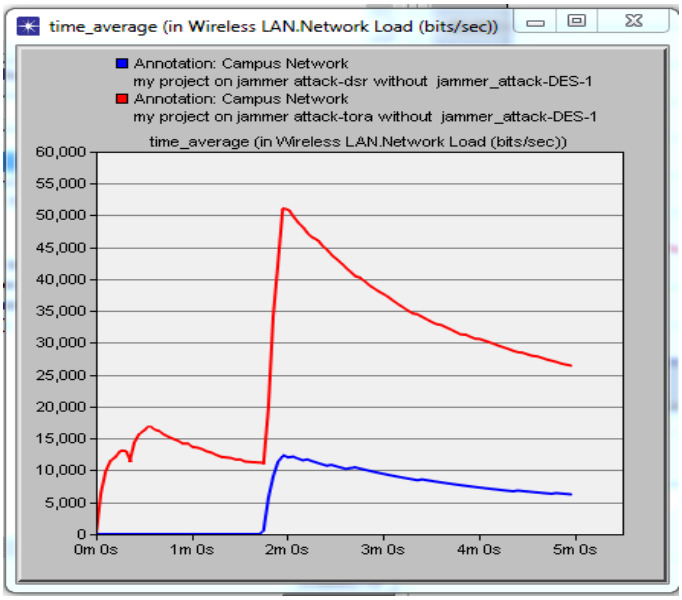

Fig 4.3(b): Comparison of DSR and TORA protocol for Network load without attack

4.4 Retransmission attempts

The Fig.4.4(a)& Fig.4.4(b), x-axis shows the time(minute/second) and y-axis shows the retransmission attempts (bit/sec).The value for DSR & TORA is 5750.529 &52065 respectively using 29 nodes under jammer attack and value under normal network for DSR & TORA is 5568.532 & 27236.59 Respectively using 29 nodes. In both cases DSR perform better than TORA protocol.

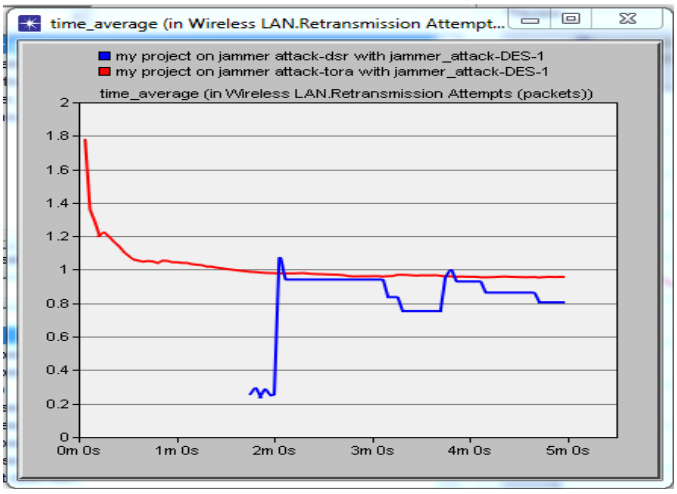

Fig 4.4(a): Comparison of DSR and TORA protocol for Retransmission attempts with attack

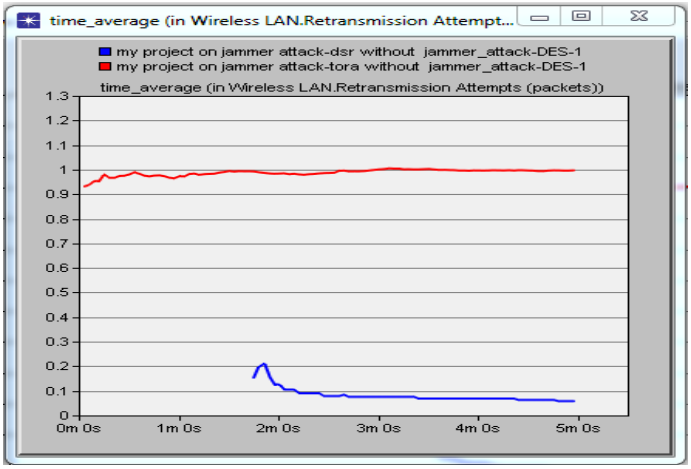

Fig 4.4(b): Comparison of DSR and TORA protocol for Retransmission attempts without attack

4.5 Throughput

The Fig.4.5(a)& Fig.4.5(b), x-axis shows the time(minute/second) and y-axis shows the throughput (bit/sec).The value for DSR & TORA is 6320.963 & 48315.04respectively using 29 nodes under jammer attack and value under normal network for DSR & TORA is 6520.579 & 99624.19 Respectively using 29 nodes. In both cases TORA perform better than DSR protocol.

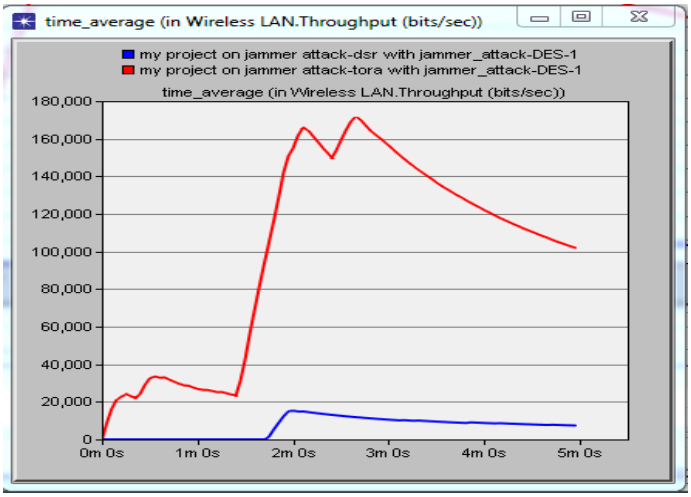

Fig 4.5(a): Comparison of DSR and TORA protocol for throughput with attack

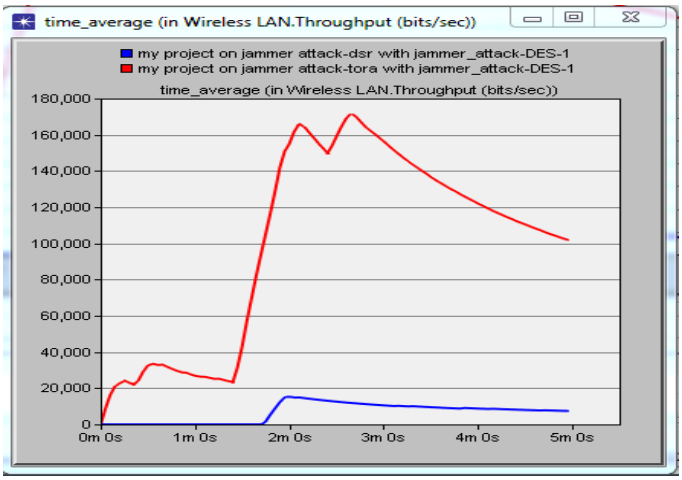

Fig 4.5(b): Comparison of DSR and TORA protocol for Throughput without attack

5. RESULT ANALYSIS

The result analysis of DSR and TORA protocols is shown in this section with the help of the simulation outputs with four performance metrics. The aim of this comparative study of DSR and TORA routing protocols is to analyze the presentation of protocols. DSR in our simulation experiments present the overall best performance. The execution of increase in the number of nodes is also clearly display in the result tables shown below.

Performance Metric	DSR with jammer attack	TORA with jammer attack
Data drop	12.81177	238.9274
Delay	0.02166	0.043055
N/W Load	5750.529	52065
Retransmission attempts	0.0823982	1.010218
Throughput	6320.963	48315.04

Table 5.1. Results with jammer attack

Performance Metric	DSR with jammer attack	TORA with jammer attack
Data drop	0	4.71964
Delay	0.001373	0.005108
N/W Load	5568.532	27236.59
Retransmission attempts	0.081652	0.98792
Throughput	6520.579	99624.19

Table 5.2. Results without jammer attack

6. CONCLUSION

In project, the simulation consisted of two routing protocol TORA and DSR set up over MANET using medium FTP analyzing their actions with respect to performance parameters, Data drop, network load, Retransmission attempts, Throughput and delay. The aim was to captured the performance under intelligent pulse jammer attack and under normal network. Simulation traffic is compared with different routing protocols i.e with pulse jammer attack and normal network in terms of performance i.e. Network load, Delay, Data drop, retransmission attempts and throughput. It shows several security breaches under pulse jammer attack and normal network models using OPNET. Intelligent pulse jammer model showed the network decreasing performance by generating noise on the radio frequency hence the jammer spotlight the security aspect and made more complicated for nodes to communicate on wireless radio frequency.

REFERENCES

[1] Vincent D. Park and M. Scott Corson. "Temporally-OrderedRouting Algorithm (TORA) version 4: Functional specification". Internet-Draft, draft-ietfmanet-TORA-spec-04.txt, July 2001.

[2] Rakesh Kumar Jha and Dr Upena Dalal "Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN)" International Conference on Recent Trends in Information, Telecommunication and Computing, IEEE Xplore,kerela,March 2010.

[3] Chee V., and Yau W., "Security analysis of TORA routing protocol," Computational Science and Its Applications–ICCSA. Springer Berlin Heidelberg, pp. 975-986 , 2007.

[4] Dempsey T., Sahin G., and Morton Y., "Passive and Active Analysis in DSR-Based Ad Hoc Networks," Ad Hoc Networks. Springer Berlin Heidelberg , pp. 623-638 , 2010.

[5] Rana S., and Kapil A., "Security-Aware Efficient Route Discovery for DSR in MANET," Information and Communication Technologies. Springer Berlin Heidelberg, pp.186-194, 2010.

[6] Sharma N., and Sharma A., "The Black-hole node attack in MANET,"Advanced Computing & Communication Technologies (ACCT), Second International Conference on. IEEE, pp. 546-550, 2012.

[7] Rajakumar P., Prasanna T., and Pitchaikkannu A. "Security attacks and detection schemes in MANET," Electronics and Communication Systems (ICECS), 2014 International Conference on. IEEE, 2014.

[8] Kampitaki D., Economides A., "ISimulation study of MANET routing protocols under FTP traffic." Procedia Technology, pp.231-238, 2014.

[9] Kapur R., and Khatri S., "Analysis of attacks on routing protocols in MANETs," Computer Engineering and Applications (ICACEA),

2015 International Conference on Advances in. IEEE, pp. 791-798, 2015.

[10] Khan M., Jadoon Q., and Khan M., "A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks," Mobile and Wireless Technology 2015. Springer Berlin Heidelberg, pp .137-145, 2015.