IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 5, July 2014.

www.ijiset.com

ISSN 2348 – 7968

COMPARISON OF AODV, OLSR, AND TORA IN MANET UNDER JELLY FISH ATTACK

Amneet Kaur[1], Prabhneet Sandhu[2]

[1](PIET for women, Nandpur kesho, Patiala Email: amneet_libra@gmail.com)

[2](PIET for women, Nandpur kesho, Patiala Email: prabhneetsandhu@gmail.com)

ABSTRACT

This Paper focuses on the effects of jelly fish attack on MANET's routing protocols. Here three protocols AODV, OLSR and TORA are used. Performance of the network has been evaluated in terms of Data dropped (buffer overflow), Data dropped (retry threshold exceeded), Load, Media access delay, Retransmission attempts. Simulations were carried out by using OPNET 14.0 simulator.

Keywords – AODV, OLSR, TORA, Normal Flow, Jelly Fish Attack

I. INTRODUCTION

MANET is mobile ad-hoc network, which is a group of number of mobile nodes that forms ad-hoc network. Network nodes communicate with each other without the assistance of any centralized authority or management. It is a dynamic topology which forms a temporary network because nodes always move anywhere in the network. It is fast growing technology, whenever the existing technology fails in any area then mobile ad-hoc networks helps to continue the communication among the nodes in that area. Ramanathan and Jason Redi tell about PRNET (packet radio network) which were used. The goal of PRNET was to provide packet switching to mobile battlefields, hostile networks [1]. Johansson, Larsson and Hedman (1999) [2], comparison of three protocols i.e DSDV, AODV, DSR takes place. Here two sets of simulations are run: - 1) mobility varied and offered load was kept constant. 2) The offered load and mobility kept constant. The simulation shows that DSR performs better than AODV for low traffic loads. At higher traffic loads AODV performs better than DSR.

Papadimitratos and Haas (2002) [3], proposed an anomaly detection scheme using dynamic training method which is updated at regular time intervals. The rushing attack implementation on AODV protocol by malicious nodes. A scheme is proposed in which multiple black holes are seen cooperating with each other and thus discovering a solution for safe route avoiding cooperative black hole attack. SAODV (secure Ad hoc on-demand distance vector protocol) becomes the solution and prevention for black hole attack.

Aad, Hubaux and Knightly (2008) [4], discovered that mobile ad hoc network suffered from number of security issues i.e. an attack that degrades the performance of mobile ad hoc network. There are number of attacks discovered and they are categorized as active as well as passive attacks, and also categorized as layered attacks. One of them was jelly fish attack. There is a jelly fish attacker node which first needs to intrude into multicast forwarding group. V. Singla, R. Singla and A. Kumar (2009) [5], comparison the routing protocols i.e. AODV, TORA, OLSR and DSR by using metrics such as network load, throughput and delay. TORA shows good performance in terms of transmission of packets. AODV show better performance for throughput and DSR shows an average level of performance. Highest amount of traffic is sent by OLSR. Some techniques to protect MANET i.e. Flow-Based Route Access Control (FRAC), Multi-Path Routing, Source-

ISSN 2348 – 7968

Initiated Flow Routing, & Sequence Numbers etc. In this authors B. Jaya singh and B. Swathi (2010) [6], explain various attacks on a mobile ad hoc network corresponding to different MANET layers and they also discuss some available attack detection techniques. In they develop an algorithm that detects the Jellyfish attack at a single node and that can be effectively deployed at all other nodes. In 2010 S. Ali, K.A Omari and P. Sumari [7] reveals that, several routing algorithms are available in the literature which may be categorized as proactive, reactive, and hybrid on the basis of routing information update mechanism. Proactive or table-driven routing algorithms maintain the network topology information in the form of routing tables which are exchanged periodically to keep them update. Whenever a node requires a path to a destination it runs a path-finding algorithm as per its routing table. Few examples are DSDV, WRP, and CGSR. These algorithms use reactive approach when the destination is within the range and use proactive approach when the destination is outside the range. Few examples of such routing algorithms are CEDAR, ZRP, and ZHLS. A solution was proposed by I. Raza and S.A Hussain (2010) [8], how to counter misinterpretation packet reordering with packet loss when retransmissions are due to persistent packet reordering by malicious nodes rather than packet loss due to traditional reasons. They concluded that the performance of TCP variants differs in AODV and DSR network under packet reordering attack (persistent packet). After this G.S Bindra, A. Kapoor and A. Aggarwal (2012) [9], present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. The proposed solution can be applied to identify multiple black hole nodes and to discover secure path from source to destination. Within the IETF, the Mobile Ad Hoc Net- working (MANET) working group was born, and sought to standardize routing protocols for ad hoc networks. M. Wazid, A. Katal, and R.H Goudar (2012) [10], discusses techniques for resilience of Denial of Service attacks on a Mobile Ad Hoc Network maintaining the focus on two attacks Jelly Fish and Black Hole. In this paper the generalized technique to detect attacks like JF Delay Variance, JF Periodic Dropping and JF Reorder occurring in the MANET is proposed but the methods for prevention of these attacks has not been introduced. Researchers explain various attacks on a Mobile Ad Hoc Network corresponding to different MANET layers, some available attack detection techniques and brief idea about Jelly Fish attack. Again the prevention of JF attacks is not given. It improves the performance of proposed routing protocol in terms of packet delivery ratio (PDR) with controlled routing load and delay. In they developed an algorithm that detects the Jellyfish attack at a single node that can be effectively deployed at all other nodes. Gupta et. al [11] described in his paper that mobile ad hoc network is an infrastructure less network. They studied the on demand routing protocols such as AODV, DSR, and TORA with identical loads and environmental conditions with respect to the performance parameters such as an average end to end delay. An experimental result shows that the AODV protocol performs better among the three protocols. DSR is suitable for that network having low mobility rate and TORA is suitable for working in these network having large numbers of nodes.

II. RELATED TERMS

1. Jelly fish attack

Jelly fish attack is one of the denials of service attack and also a type of passive attack which is difficult to detect. It produces delay before the transmission and reception of data packets in the network. Applications such as HTTP, FTP and video conferencing are provided by TCP and UDP. Jelly fish attack disturbs the performance of both protocols. It is same as black hole attack but the difference is that the black hole attacker node drops all the data packets but jelly fish attacker node produces delay during forwarding packets. Jelly fish attack is categorized as Jelly fish reorder attack, JF periodic dropping attack and JF delay variance attack. Jelly fish attacks are targeted against closed loop flows [12].

2. Routing protocols

ISSN 2348 – 7968

The rules that help the data packets to route from source to destination node are called as Routing protocols. There are three types of protocols reactive, proactive and hybrid protocols.

A. Ad-hoc On-Demand Distance Vector Routing Protocol:

It is a reactive routing protocol which sends route request messages to find out the route to the destination node. When the destination node accept that message i.e. RREQ messages from the source it send RREP message to the source to inform the source node that it has accept the RREQ message and started to set up a link between the nodes. Routing tables are used to update the information about the routes and the nodes. It sends Hello message to detect their neighbors. Hello message is also used to detect the link failure between two nodes [2].

B. Temporally ordered routing protocol:

It is also a reactive protocol. It uses non-hierarchical routing algorithm that is why it attempts to achieve high level of scalability. Unlike, AODV and DSR it built directed acyclic graphs to maintain the routes and links between the nodes. Data packets flow from higher metric node to lower metric node. Route creation, maintenance and erasure are three phases which the TORA protocol follows. Links are assigned on the basis of metrics of the nodes; a node with high degree of metric assigned the link first. It adapts well with limited bandwidth [15].

C. Optimized Link State Protocol (OLSR)

It is a proactive routing protocol, so the routes are always immediately available when needed. OLSR is an optimization version of a pure link state protocol. So the topological changes cause the flooding of the topological information to all available hosts in the network. To reduce the possible overhead in the network protocol uses Multipoint Relays (MPR).[3] The idea of MPR is to reduce flooding of broadcasts by reducing the same broadcast in some regions in the network, more details about MPR can be found later in this chapter. Another reduce is to provide the shortest path. OLSR uses two kinds of the control messages: Hello and Topology Control (TC).[5] Hello messages are used for finding the information about the link status and the host's neighbors.

Parameters	Values
Simulator	OPNET Modeler 14.0
Area	15x15 km
Network size	30 nodes
	60 nodes
Mobility Model	Random
Topology	Random
Traffic Type	Voice
Simulation Type	10 minutes
Address Mode	IPv4
Ad Hoc Routing Parameters	AODV, TORA,OLSR
Jellyfish Attackers	Zero
	15
	25
Forwarding Rate	400000 packets/seconds for honest nodes
	5000 packets/seconds for JF attacker nodes

III. EXPERIMENTAL DESIGN OF THE NETWORK

SIMULATION SCENARIO

Table 1: Common parameters

A. Run time parameters:

Duration- 10 Minutes for all Scenarios
Speed- 128
Value per Statistics- 100
Update Interval- 500000 Events

B. Implementation of Jelly Fish Attack:

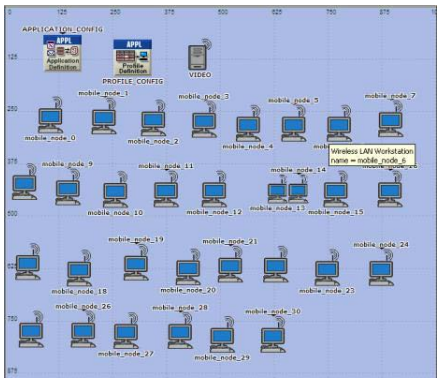
In the scenarios of jelly fish attack for all the three protocols i.e. AODV, OLSR and TORA the forwarding rate is taken as 5000 packets per second and in the normal flow scenarios of these protocols the value for forwarding rate is 400000 packets per second. In our work, OPNET 14.0 Modeler is used to analyze the effect of jelly fish attack on Mobile ad-hoc network's routing protocol. Here, we use three

ISSN 2348 – 7968

protocols AODV, OLSR and TORA. In this paper there are various simulation scenarios to analyze our results.

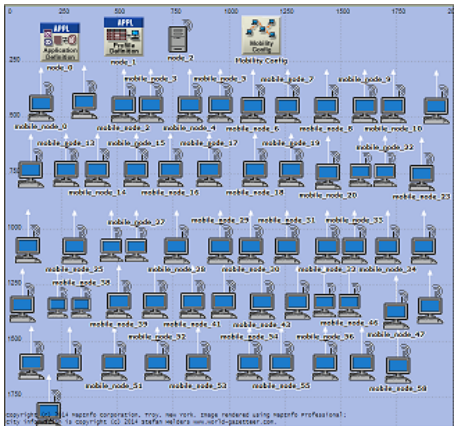
IV. SIMULATION SCENARIOS

In scenario 1, the traffic is without any JF attacker node. The traffic is running smoothly with 30 wireless mobile nodes. This scenario shows the normal flow of information between the nodes.



Scenario 1: Normal flow with 30 nodes

In scenario 2, the traffic is without any JF attacker node. The traffic is running smoothly with 60 wireless mobile nodes. This scenario shows the normal flow of information between the nodes.



Scenario 2: Normal flow with 60 nodes

V SIMULATION RESULTS:

Performance Metrics:

Following are the metrics from which calculate the performance of the network:

Data dropped (Buffer overflow) (b/sec), Data dropped (Retry threshold exceeded) (b/sec), Load (b/sec), Media Access Delay (sec), Network load (b/sec), Retransmission of packets (packets), Throughput (b/sec).

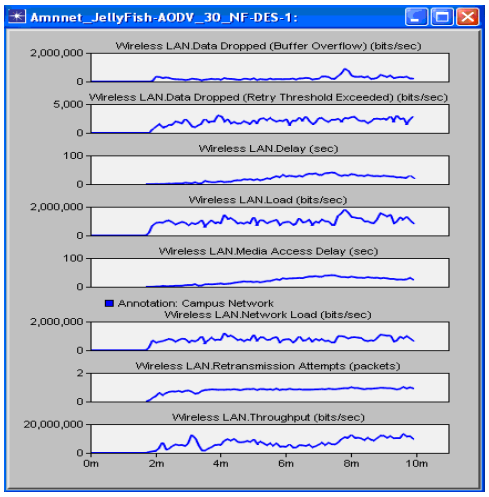


Figure1: AODV 30 Nodes NF

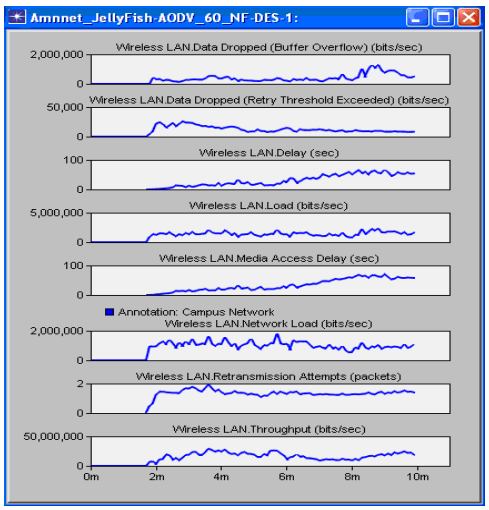


Figure2: AODV 60 Nodes NF

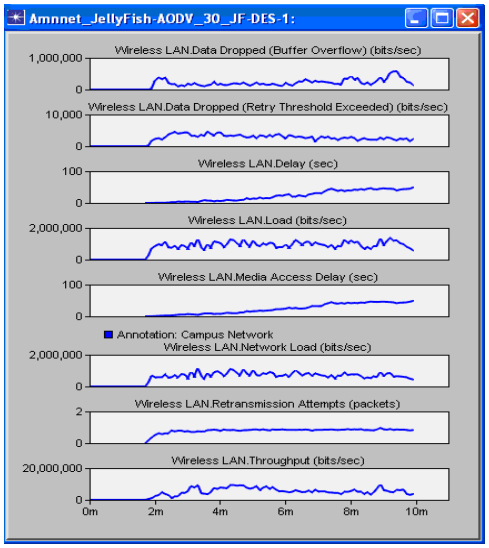


Figure3: AODV 30 Nodes JF

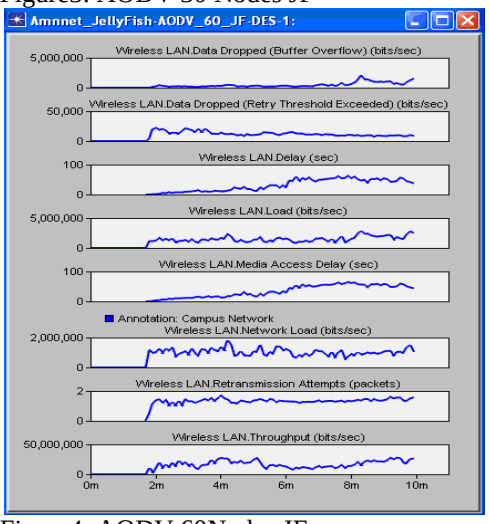


Figure4: AODV 60Nodes JF

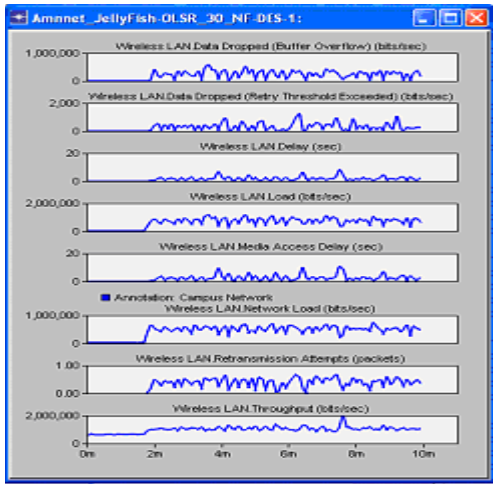


Figure5: OLSR 30Nodes NF

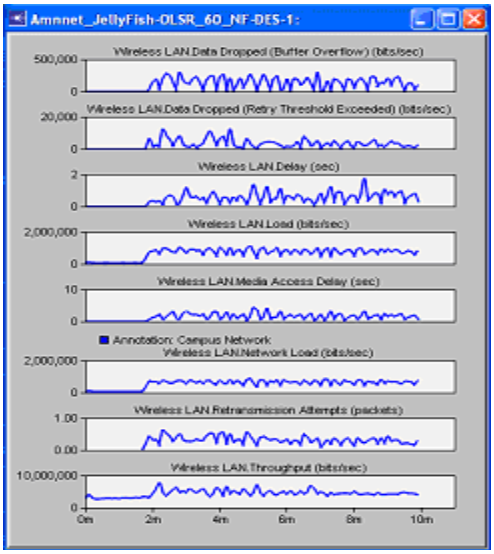


Figure6: OLSR 60Nodes NF

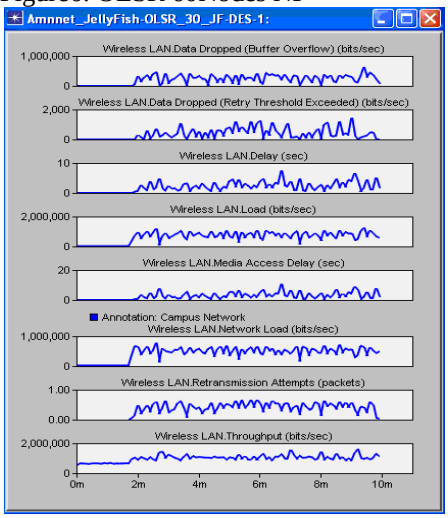


Figure7: OLSR 30Nodes JF

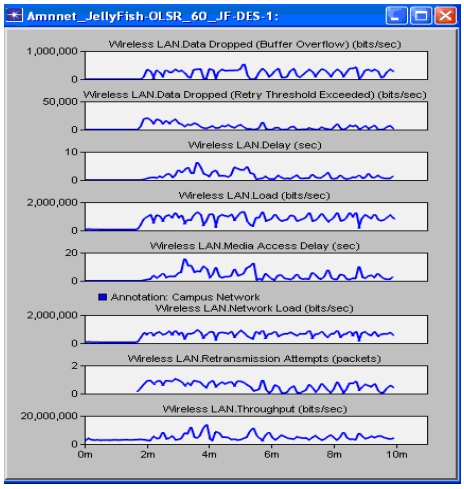


Figure8: OLSR 60Nodes JF

ISSN 2348 – 7968

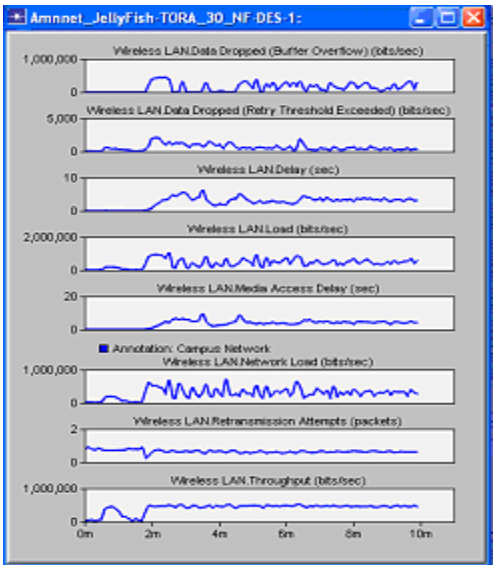


Figure9: TORA 30Nodes NF

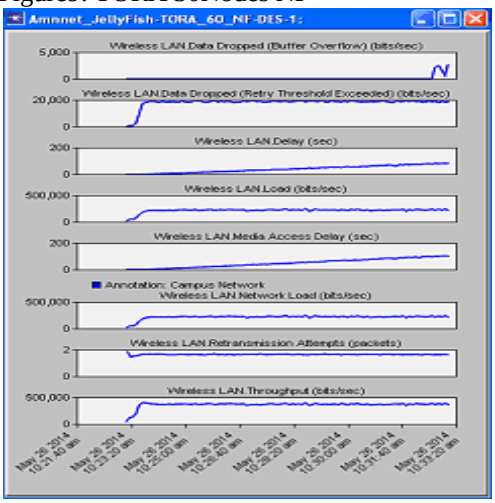


Figure10: TORA 60Nodes NF

Node Density	30NF	60NF	30JF	60JF
Data Dropped (Buffer Overflow)	Y=35,072 X=1m	Y=11,194.6 X=1m	Y=44077.3 X=1m	Y=144,106.6 X=1m
Data Dropped (Retry Threshold Exceed)	Y=666.6 X=1m	Y=5170.6 X=1m	Y=261.3 X=1m	Y=4693.3 X=1m
Delay	Y=0.00027 X=1m	Y=0.002565 X=1m	Y=0.000314 X=1m	Y=0.002498 X=1m
Load	Y=8,258.6 X=1m	Y=36362.6 X=1m	Y=6392 X=1m	Y=35,168 X=1m
Media Access Delay	Y=0.865 X=2m	Y=0.5278 X=1m	Y=0.233 X=1m	Y=0.00324 X=1m
Network Load	Y=8,258.6 X=1m	Y=36,362.66 X=1m	Y=6392 X=1m	Y=35,168 X=1m
Retransmission Attempts	Y=0.021 X=1m	Y=0.0676 X=1m	Y=0.192 X=1m	Y=0.0776 X=1m
Throughput	Y=60,725.33 X=1m	Y=207,178.6 X=1m	Y=55,762.6 X=1m	Y=205,066.6 X=1m

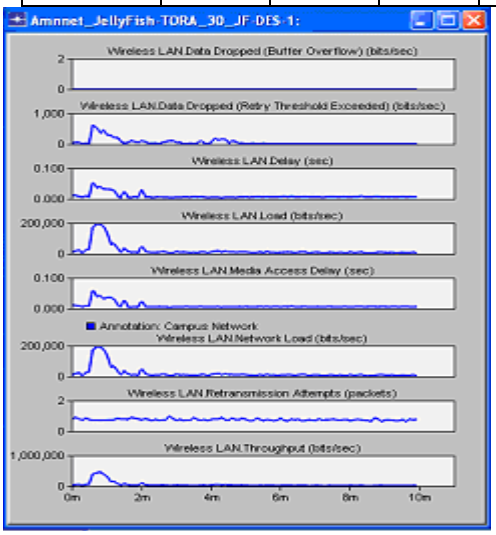
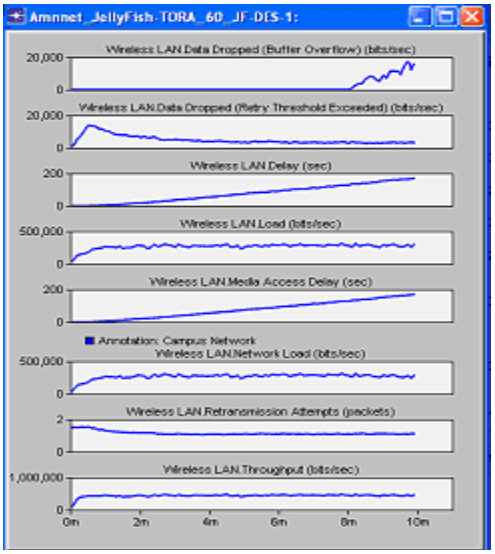


Figure11: TORA 30Nodes JF



Figur12: TORA 60Nodes JF

Starting values of AODV:

Peak Values of AODV:

Node Density	30NF	60NF	30JF	60JF
Data Dropped (Buffer Overflow)	Y=88701066 X=7m	Y=1,270,184 X=8m	Y=576432 X=9m	Y=2051213.3 X=8m
Data Dropped (Retry Threshold Exceed)	Y=3032 X=9m	Y=25,976 X=2m	Y=4602.6 X=3m	Y=21984 X=2m
Delay	Y=40.62164 X=7m	Y=67.6105 X=9m	Y=48.30149 X=9m	Y=62.5269 X=7m
Load	Y=1821410.6 X=7m	Y=2302752 X=8m	Y=1369360 X=9m	Y=2924349.3 X=8m
Media Access Delay	Y=40.28 X=7m	Y=68.2503 X=8m	Y=48.405 X=9m	Y=64.717 X=7m
Network Load	Y=1,190,234 X=4m	Y=1,791,517.3 X=5m	Y=1,132,624 X=3m	Y=1,844,344 X=4m
Retransmission Attempts	Y=1.014 X=9m	Y=1.9393 X=3m	Y=0.9567 X=8m	Y=1.701 X=4m
Throughput	Y=13,216,328 X=9m	Y=29,242,154.6 X=3m	Y=9,804,413.3 X=8m	Y=27,685,661.3 X=9m

Starting Values of OLSR

Node Density	30NF	60NF	30JF	60JF
Data Dropped (Buffer Overflow)	Y=47066.6 X=1m	Y=28,672 X=1m	Y=57501.3 X=1m	Y=97898.6 X=1m
Data Dropped (Retry Threshold Exceed)	Y=66.66 X=1m	Y=400 X=1m	Y=333.3 X=2m	Y=160 X=1m
Delay	Y=0.013626 X=1m	Y=0.004392 X=1m	Y=0.03002 X=1m	Y=0.189363 X=1m
Load	Y=22394.6 X=1m	Y=97738.6 X=0m	Y=370832 X=1m	Y=71530.6 X=0m
Media Access Delay	Y=0.5767 X=1m	Y=0.6606 X=1m	Y=0.5240 X=1m	Y=0.4326 X=1m
Network Load	Y=25,120 X=0m	Y=63,584 X=0m	Y=19,589.33 X=0m	Y=54,261.33 X=0m
Retransmission Attempts	Y=0.044 X=1m	Y=2020 X=1m	Y=0.055 X=1m	Y=0.1782 X=1m
Throughput	Y=692,602.66 X=0m	Y=2628,122.66 X=0m	Y=650,864 X=0m	Y=2,205,685,33 X=0m

Peak Values of OLSR

Node Density	30NF	60NF	30JF	60JF
Data Dropped (Buffer Overflow)	Y=612288 X=3m	Y=296437.3 X=6m	Y=622394.6 X=9m	Y=559845.3 X=5m
Data Dropped (Retry Threshold Exceed)	Y=1266.6 X=6m	Y=12880 X=4m	Y=1466.6 X=9m	Y=20,240 X=2m
Delay	Y=8.596097 X=7m	Y=1.78515 X=8m	Y=7.566484 X=6m	Y=6.377083 X=3m
Load	Y=1209410.6 X=4m	Y=1154512 X=4m	Y=1261616 X=9m	Y=1318101.3 X=5m
Media Access Delay	Y=8.5744 X=7m	Y=3.661 X=5m	Y=10.6098 X=6m	Y=15.900 X=5m
Network Load	Y=744,970,66 X=8m	Y=881,498.66 X=4m	Y=784,744 X=2m	Y=939,781.33 X=3m
Retransmission Attempts	Y=0.6964 X=7m	Y=0.643 X=2m	Y=0.67 X=5m	Y=1.0386 X=2m
Throughput	Y=1,969,272 X=7m	Y=7,943,178.66 X=2m	Y=1,607,341.33 X=9m	Y=13,822,586.66 X=3m

Starting Values of TORA

Node Density	30NF	60NF	30JF	60JF

ISSN 2348 – 7968

Data Dropped (Buffer Overflow)	Y=206 466.6 X=7m	Y=0 X=0m	Y=0 X=0m	Y=1013 X=8m
Data Dropped (Retry Threshold Exceed)	Y=53.3 3 X=0m	Y=186. 6 X=0m	Y=26.6 6 X=0m	Y=1893. 3 X=0m
Delay	Y=0.00 497 X=1m	Y=0.01 7933 X=1m	Y=0.01 187 X=0m	Y=0.050 281 X=0m
Load	Y=233 33.3 X=0m	Y=22.6 6 X=0m	Y=941 3.33 X=0m	Y=3106 6.6 X=0m
Media Access Delay	Y=0.46 166 X=1m	Y=3.80 7 X=1m	Y=0.01 23 X=0m	Y=4.091 6 X=1m
Network Load	Y=19,1 20 X=0m	Y=22,6 66.6 X=0m	Y=191 20.00 X=0m	Y=31,06 6.6 X=0m
Retransmission Attempts	Y=795 2 X=0m	Y=1.85 50 X=0m	Y=1.00 52 X=2m	Y=1.453 9 X=0m
Throughput	Y=42,9 60 X=0m	Y=50,9 06.6 X=0m	Y=185 86.66 X=0m	Y=69,04 0 X=0m

Peak Values of TORA

Node Density	30NF	60NF	30JF	60JF
Data Dropped (Buffer Overflow)	Y=442946. 6 X=2m	Y=266 6.6 X=7m	Y=0 X=9m	Y=1770 6.6 X=9m
Data Dropped (Retry Threshold Exceed)	Y=2066.6 X=2m	Y=195 46.6 X=2m	Y=613. 33 X=0	Y=1378 6.6 X=0m
Delay	Y=6.36882 6 X=3m	Y=81.7 45834 X=7m	Y=0.05 398 X=0m	Y=170.3 05115 X=9m
Load	Y=1065613 .3 X=2m	Y=231 093.3 X=3m	Y=193 546.6 X=0m	Y=3077 60 X=6m
Media Access Delay	Y=9.9699 X=3m	Y=101. 76 X=7m	Y=0.06 083 X=0m	Y=169.5 91 X=9m
Network Load	Y=721,680 X=4m	Y=250, 960 X=4m	Y=193 546.66 X=7m	Y=315,5 73.33 X=7m
Retransmissi on Attempts	Y=0.911 X=0m	Y=1.85 50 X=0m	Y=0.91 12 X=0m	Y=1.539 6 X=0m
Throughput	Y=520,640 X=6m	Y=399, 893.33 X=5m	Y=454 533.33 X=0m	Y=480,2 13.33 X=7m

VI. OBSERVATIONS

Some of the observations for this paper are as follows:

☐ If we increase the node density then data dropped due to buffer overflow is low in TORA and at node density 30, OLSR has lower data dropped in Normal flow as well as jelly fish flow scenario. This drop of data is due to number of higher layer packets that are dropped because the MAC layer could not receive any acknowledgement for the retransmission of those packets that are dropped.

☐ Data dropped (retry threshold excceed) is due to the reason that the size of the higher layer packets is greater than the maximum allowed data size defined in IEEE 802.11 standard. At node density 30 and 60 TORA has lowest data dropped due to retry threshold only in normal flow but in jelly fish scenario with node density 30, AODV has lower data drop.

☐ Delay is low in OLSR if we increase the node density. It is the delay produced during transmission and reception of data packets. Load is less in case of AODV and TORA.

☐ For lower density of nodes i.e. 30, OLSR performs better for Media Access Delay and Retransmission Attempts and when we increase the density up to 60 nodes, AODV performance is good.

VII. CONCLUSIONS AND FUTURE SCOPE

If good time services and no loss of information needs then we have to choose TORA and if we want low delay produced during transmission and reception of information and data then we go for AODV. OLSR is used as optional at the place of AODV. If we increase node density, forwarding rate of packets, use diferent protocol and introduced JF periodic dropping attack the performance may vary. This work can be further extended to calculate the performance of Mobile ad-hoc networks.

VIII. ACKNOWLEDGEMENTS

We are thanking to our management for their continuing support and encouragement for completing this work and we are thanking our head of the department for his valuable suggestion.

REFERENCES

[1] Ram Ramanathan and Jason Redi, “A brief overview of Ad-hoc networks: Challenges and direction”, IEEE Communications magazine 50 Anniversary commemorative Issue/May 2002.

[2] Per Johnson, Tony Larsson, and Nicklas Hedman, "Scenario based performance analysis of routing protocols for Mobile ad-hoc network", Mobicom '99 Scattle Washington USA, copyright ACM 1999 1-58113-142-9/99/08.

[3] Sanjay Ramaswami, Huirong Fu, Manohar sreekantaradhya John Dixon and Kendall Nygard, "Prevention of cooperative Black hole attack in wireless ad-hoc networks", 2003.

[4] Panagiotis papadimitratos and Zygmunt Haas, "Security routing for Mobile ad-hoc networks". In proceedings of CNDS 2002, San Antonio, TX, January 27-31, 2002.

[5] Imran Raza, S.A.Hussian, Amjad Ali, Muhammad Hassan Raza"Persistant packet reordering attack in TCP based Ad-hoc wireless network", IEEE, 978-1-4244-8003-6/10-2010.

[6] Ahmed.M.Abdel Mo'men, Haitham.S .Hamzas and Iman.A.Saroit, "A survey on security enhanced multicast routing protocol in mobile ad-hoc network", IEEE, 978-1-4244-8003-6/10-10-2010.

[7] Nidhi Purohit, Richa Sinha and Khushbu Maurya, "Simulation study of black hole and jelly fish attack on MANET using NS-3", Institute of technology, Nirma University, Ahmedabad-382481 08-10 December, 2011.

[8] Songbai Lu Longxuan Li Lingyan Jia, "SAODV: A MANET Routing protocols that can withstand black hole attack", International Conference on computational Intelligence and Security, 2009.

[9] Pramod Kumar Singh, Govind Sharma, "An efficient prevention of black hole problem in AODV routing protocol in MANET", IEEE11th Conference on Trust, Security and Privacy in Computing Communication, 2012.

[10] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, "Detection and Removal of co-operative black hole attack and gray hole attacks in MANET", International Conference on System Engineering and Technology, Bandung, Indonesia, September 11-1-2012.

[11] Shinni Mittal,Harish Taluja, "Analysis of co-operative black hole attack using Dynamic source protocol", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8,August 2012.

[12] Mohammad Wazid, Vipin Kumar, RH Goudar, "Comparative performance analysis of routing protocols in mobile ad-hoc network under Jelly fish attack", 2nd IEEE International Conference on parallel, distributed and grid computing, 2012.

[13] Mohammad Wazid, Avita Katal, RH Goudar,"Cluster and Super cluster based Intrution Detection and Prevention Techniques for Jelly fish reorder attack", 2nd IEEE International Conference on parallel, distributed and grid computing, 2012.

[14] Md.Anisur Rahman, Md.Shohidul Islam, Alex Talevski, "Performance Measurement of various routing protocols in Ad-hoc network", In the proceedings of International Multi Conference of Engineers and Computer Scienstists, Hong Kong, Volume 1, IM ECS 2009, March 18-20-2009.

[15] Saleh Ali, K.AL-Omari and Putra Sumari, "An overview of mobile ad-hoc network's for the existing protocols and applications", Journal on Application of Graph Theory in Wireless Ad-hoc Networks and sensor network's (J GRAPH-HOC) Vol.2, No. 1, March 2010.