

PERFORMANCE SIMULATION OF JAMMING ATTACK ON AODV AND OLSR PROTOCOLS WITH PCF USING OPNET

RAMANJEET KAUR, Er. NAVDEEP KAUR KALER

LALA LAJPAT RAI INSTITUTE OF ENGINEERING AND TECHNOLOGY MOGA
(PUNJAB)

ABSTRACT

A MANET is a group of mobile nodes which shares a wireless channel even without decentralized control or without having established communication backbone. MANET is an individual glance system of mobile devices which are connected by ad hoc wireless links. In this research work, six different scenarios were implemented. The scenarios were based on the MANET networks setup in a computer laboratory in an engineering institute. Three sets of scenarios were implemented with first for each OLSR and AODV respectively with 40 nodes, (Without attack) second OLSR and AODV respectively with 40 nodes, (With attack) OLSR and AODV respectively with 40 nodes, (PCF Recovery). As per this research, network simulator, Optimized Network Engineering Tools (OPNET) modeler 14.5 has been used as a simulation environment

Keywords: MANET, OLSR, AODV, JAMMING ATTACK, PCF, OPNET

1 INTRODUCTION

Ad hoc networks are made and used as exactly in variant environments. Routing is one of the main problems of networking to deliver data from one to the other node. Wireless ad-hoc networks are also known Mobile ad-hoc multi hop networks without predetermined topology or central control. This is because MANETs can be categorized as a dynamic, multi hop, potentially rapid changing topology. The objective of such networks is to provide communication abilities to areas with limitations or not having existing communication infrastructures. A MANET is usually built having mobile nodes using wireless communications. It adopts a peer-to-peer multi hop routing rather than static Network infrastructure for network connectivity. The nodes in MANETs are connected together using multi-hop communication paths. This means that all nodes in the hop should be willing to participate in the process of delivering a packet by forwarding it

from source to destination. It has multiple paths by which the packets travel.



Figure 1.1: Mobile Ad-hoc Network

2. PROTOCOLS

Routing is a backbone of any Network. Routing means which path Network packets will follow to reach from source to destination. Motive of Routing Protocol is to reach at destination with minimum delay. The Goal of MANET routing protocol is that performance of network should be efficient. Each routing protocol working mechanism is based on its algorithm. In MANET, it has various types of routing protocols each of them is applied according to the network circumstances.

2.1 AODV (The Ad hoc On Demand Distance Vector)

AODV is a routing protocol designed for ad hoc mobile networks. AODV build routes using a Route request & Route reply query cycle. A source node broadcasts a Route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination

with corresponding sequence number greater than or equal to that contained in the RREQ. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route. If Error accrued in RREQ & RREP then RERR Process is begin.

2.2 OLSR (Optimized Link State Routing)

It is a proactive routing protocol and is also called as table driven protocol because it permanently stores and updates its routing table. OLSR keeps track of routing table in order to provide a route if needed. Due to its nature OLSR is called as proactive routing protocol. Multipoint relay (MPR) nodes are all the nodes in the network do not broadcast the route packets. Multipoint Relay (MPR) nodes broadcast route packets. These MPR nodes can be selected in the neighbor of source node. Each node in the network keeps a list of MPR nodes. This MPR selector is obtained from hello packets sending between in neighbor nodes. These routes are built before any source node intends to send a message to a specified destination. Each and every node in the network keeps a routing table. This is the reason the routing overhead for OLSR is minimum than other reactive routing protocols and it provide a shortest route to the destination in the network. There is no need to build the new routes, as the existing in use route does not increase enough routing overhead. It reduces the route discovery delay.

3 JAMMING ATTACK

A jammer continuously emits a radio signal that represents random bits. The signal generator does not follow any MAC protocol. If the signal transmitted is strong enough to be sensed by a sender, it will always sense the medium as busy. The jammer is considered most effective when it drops the throughput to zero for a long period of time until it runs out of energy. It is also considered non-energy efficient.

4. POINT COORDINATION FUNCTION

Distributed coordination function (DCF) and Point coordination function (PCF) are the two different media access control (MAC) mechanisms which

are specified by the IEEE 802.11 standard. DCF is the basic MAC mechanism whereas PCF is built on top of DCF and provides contention-free media access. PCF can achieve higher throughput than the contention based DCF due to the nature of contention-free, and PCF provide guaranteed service which is important for real-time applications and PCF could also be used for non-real-time services which will be an attractive option for future wireless networks.

5. SIMULATOR WORK:

OPNET Simulator is used for research work .As Mentioned before this Research work is having three parts. AODV & OLSR networks, AODV & OLSR networks effected with Jammer Attack, Finally PCF Technique is implemented on Effected Networks

5.1 AODV & OLSR NETWORKS

In this Part two different scenarios have been created one for OLSR and second for AODV. For each scenario 40 MANET nodes are taken and performance check for various performance metrics which are as follows Database query Response time, Remote-login Response Time, HTTP Page Response Time, Voice End to End Delay.



Figure: 5.1AODV NETWORK



Figure 5.2: OLSR NETWORK

5.2 AODV & OLSR NETWORKS JAMMING ATTACK

In this research work have created two different scenarios one for OLSR and second for AODV. This time both the scenarios are infected with jamming attack.

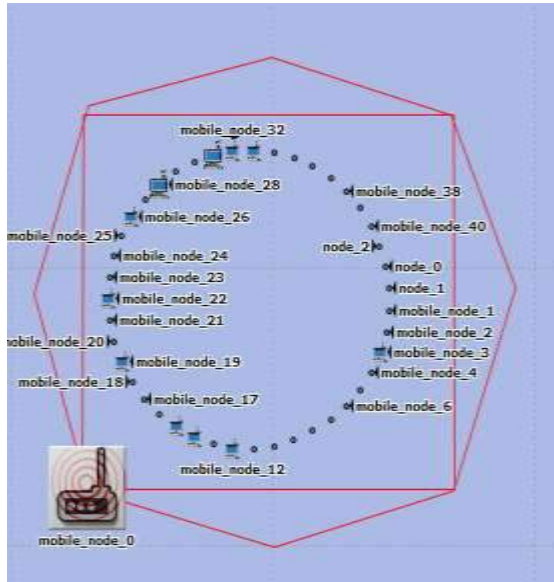


Figure 5.3: AODV JAMMING ATTACK

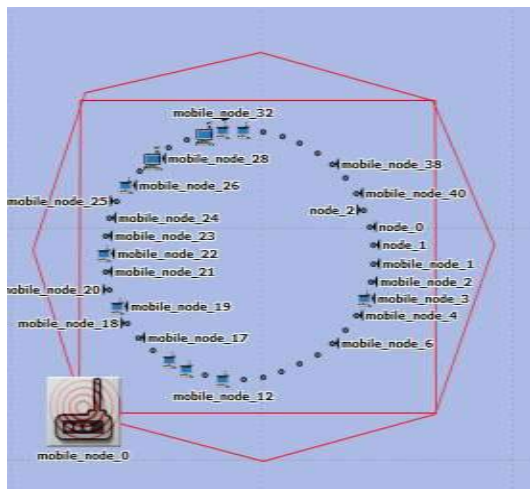


Figure 5.4: OLSR JAMMING ATTACK

5.3 AODV & OLSR NETWORKS WITH PCF

In this Part created AODV and OLSR Networks are shown with 40 nodes with performance simulation of Database query response time and Remote-login Response Time only, after that Jamming Attack is implemented on these networks. Finally PCF technique is implemented on affected networks.

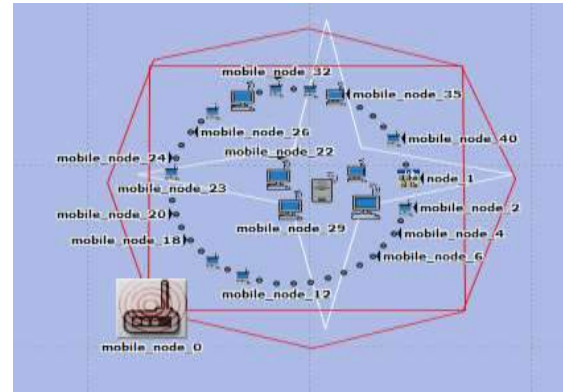


Figure 5.5: AODV WITH PCF

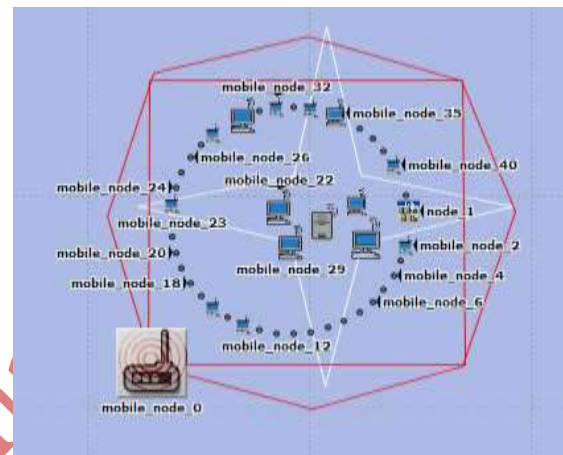


Figure 5.6: OLSR WITH PCF

5.3.1 Data Base Query Response Time (AODV)

As Figure 5:7 described AODV network shows in red line Data Base Query Response Time is 5.5 after that network is affected with jamming attack then Data Base Query Response Time reached at 17.32 finally PCF Technique is implemented and Data Base Query Response Time got improve that is 8.7

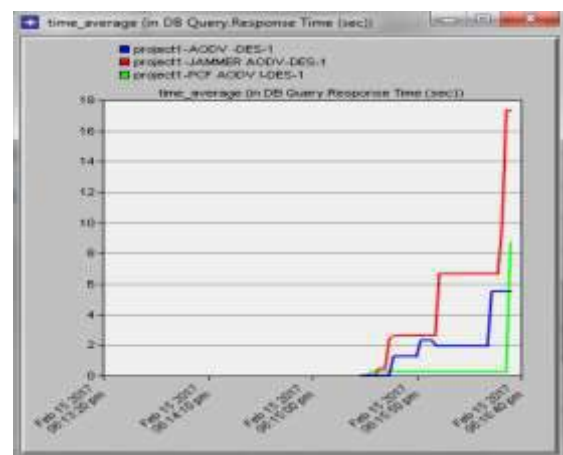


Figure 5.7: Data Base Query Response Time (AODV)

5.3.2 Data Base Query Response Time (OLSR)

As Figure 5:8 described OLSR Network Shows in Red line Data Base Query Response Time is 2.6 after that network is affected with jamming attack then Data Base Query Response Time reached at 10.66 finally PCF technique is implemented and Data Base Query Response Time got improve that is 6.12

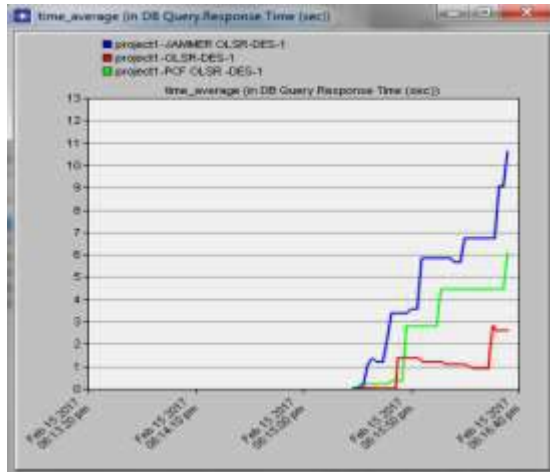


Figure 5.8: Data Base Query Response Time (OLSR)

5.3.3 Remote Login Response Time (AODV)

As Figure 5:9 described AODV Network Shows Remote login Response Time is 0.13 after that Network is affected with jamming attack then Remote login Response Time Reached at 6.30 finally PCF Technique is implemented and Remote login Response Time got improve that is 1.51

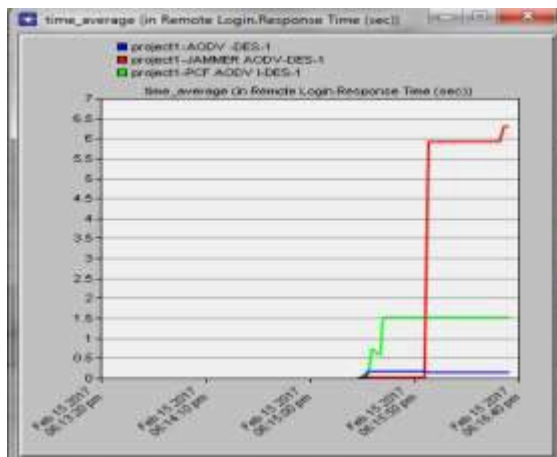


Figure 5.9: Remote Login Response Time (AODV)

5.3.4 Remote Login Response Time (OLSR)

As Figure 5:10 described OLSR network Shows in Remote login Response Time is 0.009 after that Network is affected with jamming attack then Remote login Response Time Reached at 4.4 finally PCF Technique is implemented and Remote login Response Time got improve that is 3.9

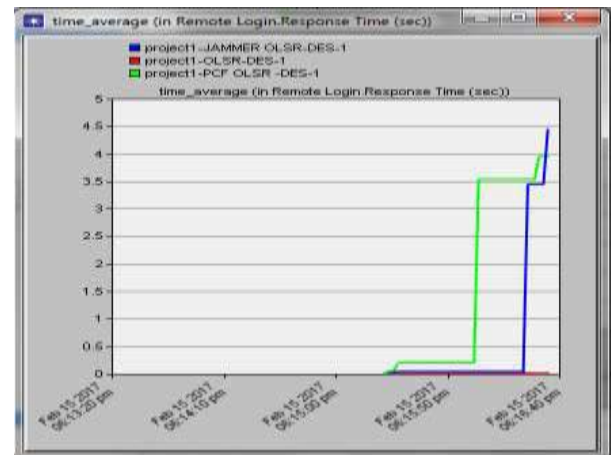


Figure 5.10: Remote Login Response Time (OLSR)

6. CONCLUSION AND FUTURE SCOPE

In this research work has produced different types of results and analysis on the behalf of reactive and proactive routing protocols between OLSR and AODV. Three sets of scenarios were implemented with first for each OLSR and AODV respectively with 40 nodes,(Without attack)second OLSR and AODV respectively with 40 nodes,(With attack) OLSR and AODV respectively with 40 nodes,(PCF Recovery). In this research work, the behavior of OLSR and AODV MANET networks has been checked based on various performance metrics. These are Database Query Response Time, Remote Login Response Time. Upon analysis of derived results, it can be concluded that OLSR gives better response than AODV, For Second part a jamming attack is deployed on each network in which some malicious node is generated. It can be determined that network having malicious node shows worst results than a simple network. For third part the PCF Technique is implemented so that it can overcome the effect of jamming attack. Finally it can be concluded that when the PCF Technique has been implemented, it recovered most of the degraded performance of the two networks after jamming attack. So from the derived results in the research work, PCF technique is found to be a successful approach for eliminating the aftermaths of jamming attack on MANET networks employing AODV or OLSR routing protocol. It can also be concluded that of these two protocols,

for future references a hybrid protocol can be designed. Security analysis for both OLSR and AODV can be done.

7. REFERENCES

- [1] Anjali. & Singh,M. (2012), "Simulation and Performance Analysis of AODV, OLSR, GRP Routing Protocol", International Journal of Future Computer and Communication, 2 (6).
- [2] Chander, Diwaker & Gill.A. (2012), "Comparative Analysis of Routing in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, pp. 309-314.
- [3] Devi,R., Sumathi,B., Gandhimathi,T. & Alaiyarasi,G. (2012), "Performance Metrics of MANET in Multi-Hop Wireless Ad-Hoc Network Routing Protocols", International Journal of Computational Engineering Research.
- [4] Dhawan,S. & Saroha,V. (2013), "Optimize the routing protocol (GRP, OLSR, DSR) using OPNET & its performance evaluation", International Journal of Advances in Engineering & Technology, pp. 13-99.
- [5] Gagandeep, Aashima & Kumar,P. (2012), "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), 1 (5), pp. 269-275.
- [6] Gupta,S., Arora,S. & Banga,G. (2012), "Simulation Based Performance Comparison of AODV and DSR Routing Protocols in MANETS", International Journal of Applied Engineering Research, 7 (11).
- [7] Helen,D. & Arivazhagan,D. (2014), "Applications, Advantages and Challenges of Ad Hoc Networks", Journal of Academia and Industrial Research , 2 (8), pp. 453-457.
- [8] Hinds,A., Ngulube,M., Zhu,S. & Al-Aqrabi,H. (2013), "A Review of Routing Protocol for Mobile Ad-Hoc Network (MANET)", International Journal of Information and Education Technology, 3 (1), pp. 1-5.
- [9] Jasvinder & Sachdeva,M. (2013), "Effects of Black Hole Attack on an AODV Routing Protocol through the Using Opnet Simulator", International Journal of Advanced Research in Computer Science and Software Engineering, 3 (8), pp.657-664.
- [10] Ray,P., Mondal,R. & Sarddar,D. (2016), "Design of Power Aware AODV Routing Protocol" International Research Journal of Engineering and Technology, 3 (5), pp. 2100-2110.
- [11] Sarmal,I., Singh,S. & Singh,A. (2016), "Introducing Restricted Access Protocol to Enhance the Security and Eliminate Ddos Attack",

International Research Journal of Engineering and Technology, 3 (2), pp. 440-442.

- [12] Sharma,A. & Dhaliwal,K. (2016), "Simulation Based Analysis of Jamming Attack in OLSR, GRP,TORA and Improvement with PCF in TORA using OPNET tool", International Research Journal of Engineering and Technology, 3 (3).

[13] Singh,M. & Kaur,G. (2013), "A Surveys of Attacks in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, 3 (6), pp. 1631-1636.

- [14] Sonia, Lakeshwar & Vats,K. (2014), "Different Qos based OLSR Proactive Routing using 802.11" International Journal of Computer Science and Mobile Computing", 3 (6), pp. 898-906.