Simulation Based Analysis of Jamming Attack in OLSR, GRP, TORA and Improvement with PCF in TORA using OPNET tool

Anupam Sharma, Deepinderjeet Kaur Dhaliwal

Desh Bhagat University Mandi Gobindgarh Punjab

---***---

Abstract : *A mobile ad hoc network (MANET) is a self-configuring network of mobile devices connected by wireless links. Backbone of any MANET is routing protocol .our research work having collaboration of three parts. In which different network model are created. First of all network of OLSR protocol is created with 20 MANET nodes taking three different server like Voice, Http, and E-mail server. Secondly same network with TORA created and same performance metrics have chosen. In third step GRP Protocol was implemented with same server and performance metrics. In these sections network was created which was not infected with Jamming attack. In second part TORA, OLSR & GRP were implemented with Jamming attack on every network and then got that performance of infected Jamming network of all three Protocols TORA, OSLR & GRP decreased and finally implemented PCF technique for improvement the network performance on TORA network and then got results which shows that infected networks performance is increased by PCF .it was not as like Network without affected Jamming attack. But with the help of PCF techniques it can improve network performance of infected network.*

Keywords: MANET, OLSR, GRP, TORA, DOS, PCF, OPNET.

1. Introduction:

A MANET is a group of mobile Nodes which shares a wireless channel even with decentralized control or without having established communication backbone.. All nodes, in the system cooperate in order to rectified route packets in multi-hop forwarding mode with effect of the unexpected mobility of Node the network topology might change constantly. Routing is one of the main problems of networking to Mobile ad-hoc multihop networks without predetermined topology or central control. This is because MANETs can be categorized as a dynamic, multihop, 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 multichip routing rather than static Network infrastructure for network connectivity and nodes in MANETs are connected together using multi-hop communication paths. Mobile nodes in the network will act as clients and servers. Figure 1.1 shows the decentralized MANET consisting of mobile nodes, Laptops working behave as routers to other mobile nodes.

Figure 1.1: Mobile Ad-hoc Wireless Network

Routing Protocols in MANET: A routing protocol uses software and routing algorithms to determine optimal network data transfer and communication paths between network nodes. On the basis of topology routing protocols categorization is as follow:

2.1 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.

2.2Optimized 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

2.3 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 improperly compromising on (control) overhead performance.

3. Denial of Service (DoS) Attack

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 in wireless networks. 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 this research, the jamming attacks are simulated on MANETs that result in collisions in the mobile wireless network.

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 802.11standard. 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.PCF provided a good functionality to improve deficiency caused by the Jammers.

5. Literature Review:

Sabbar Insaif Jasim (2014), PCF gave a good improvement to increase throughput and traffic received which were reduced by the Jammers and decrease the delay which was increased by the Jammers and good functionality to improve deficiency caused by the Jammers for TORA routing protocol using OPNET/throughput, delay, data dropped in paper" PCF Investigation To Improve The Performance Of TORA – Based MANET Against Jamming Attacks".

Kaur and Singh (2012) performance of three routing protocols namely OLSR, GRP and TORA was analyzed .OLSR performs best in terms of load and throughput.GRP performs best in terms of delay and routing overhead. TORA is the worst choice when research considers any of the four performance parameters. In summary, OLSR best as compared to GRP and TORA in all traffic volumes since it has maximum throughput.

Kumar et al. (2012) Due to dynamic infrastructure of MANETs and having no centralized administration makes such network more vulnerable to many attacks. In this paper, how different layers under protocol stack become vulnerable to various attacks is studied. These attacks can classified as an active or passive attacks. Different security mechanisms are introduced in order to prevent such network. In future study try to invent such security algorithms is needed, which will be installed along with routing protocols that helps to reduce the impact of different attacks

Neeti Yadav, Dr.Vivek Kumar, IJARCET, (June 2015) concluded that Unified mechanisms have a significant positive impact on the overall network through and it does not only mitigate the jamming attack effects, it also increases the overall performance above the normal state of the network using OPNET 16.0/Throughput, End to End Delay in paper "Securing Ad hoc Network By Mitigating Jamming Attack".

6. Simulation Results and Analysis

In this section, comparative analysis of TORA, OLSR and GRP as it described earlier. There are seven network models, which are configured according to our requirement and run.

6.1 OLSR, GRP and TORA In without Jamming Attack Scenario

In this section it created three different scenarios one for OLSR, second for TORA and third for GRP. It has taken 20 nodes for each protocol i.e. OLSR, TORA and GRP.

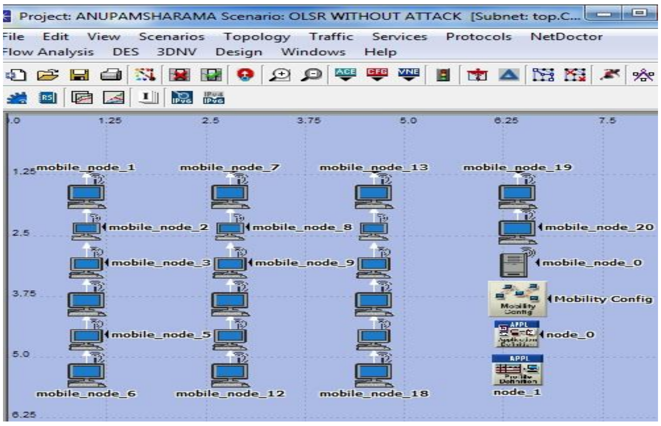

Figure 4.5: 20 Nodes Working of OLSR without Jamming Attack Scenario

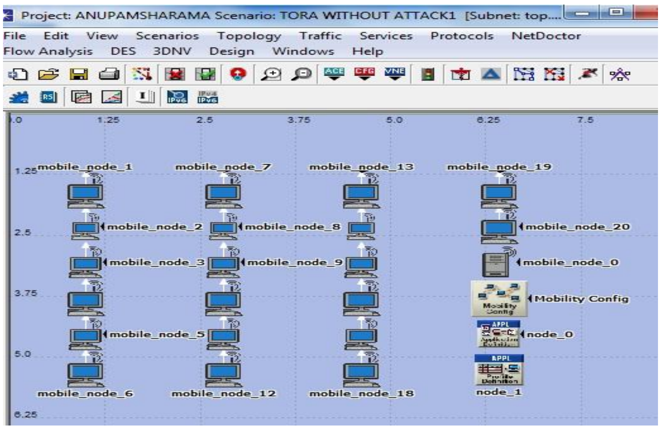

Figure 4.6: 20 Nodes Working of TORA without Jamming Attack Scenario

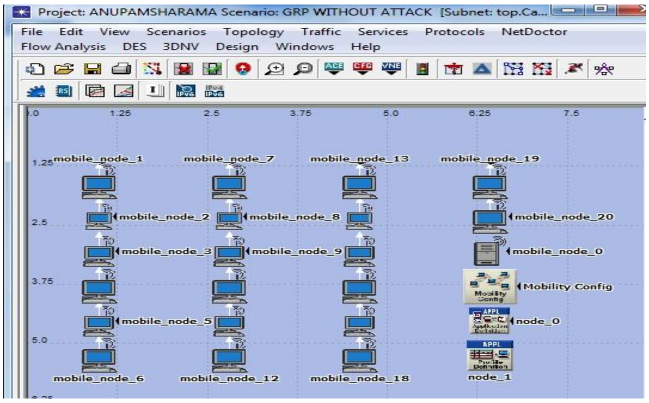

Figure 4.7: 20 Nodes Working of GRP without Jamming Attack Scenario

6.2 With Jamming Attack Scenario

In this section it created three different scenarios one for OLSR, second for TORA and third for GRP. Impact of jammer for three routing protocols with jamming attack for network of 20 nodes is analyzed.

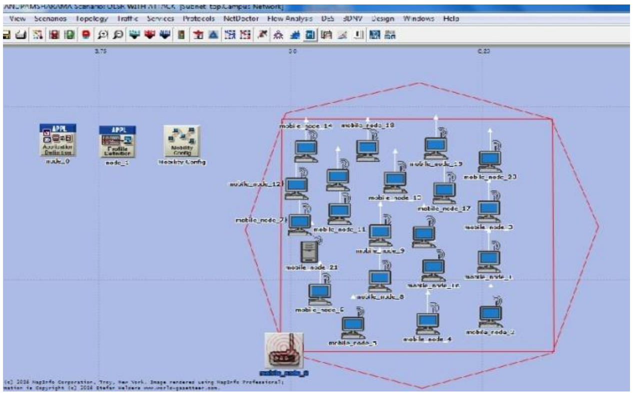
ANUPAMSHARAMA Scenario: OLSR WITH ATTACK [Subnet: top.Campus Network]

Figure 4.8: 20 Nodes Working of OLSR with Jamming Attack Scenario

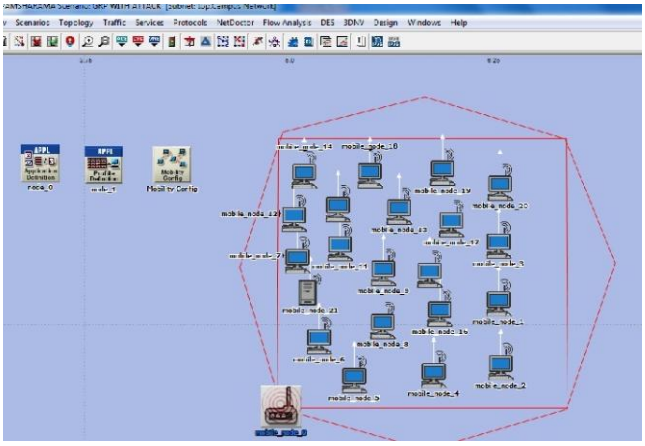
ANUPAMSHARAMA Scenario: GRP WITH ATTACK [Subnet: top.Campus Network]

Figure 4.9: Working of 20 Nodes GRP with Jamming Attack Scenario

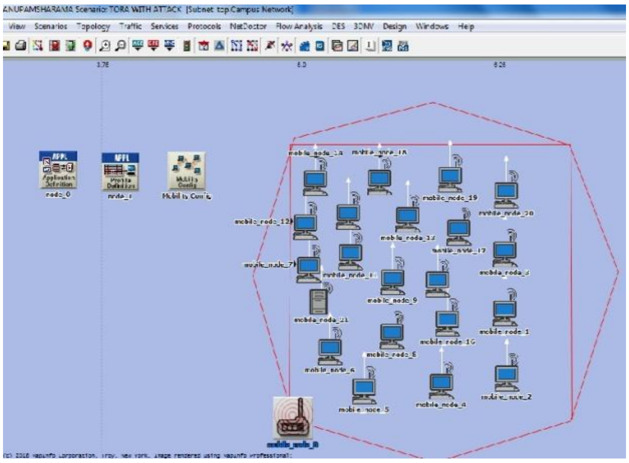
ANUPAMSHARAMA Scenario: TORA WITH ATTACK [Subnet: top.Campus Network]

Figure 4.10: 20 Nodes Working of TORA with Jamming Attack Scenario

6.3 PCF Scenario for TORA

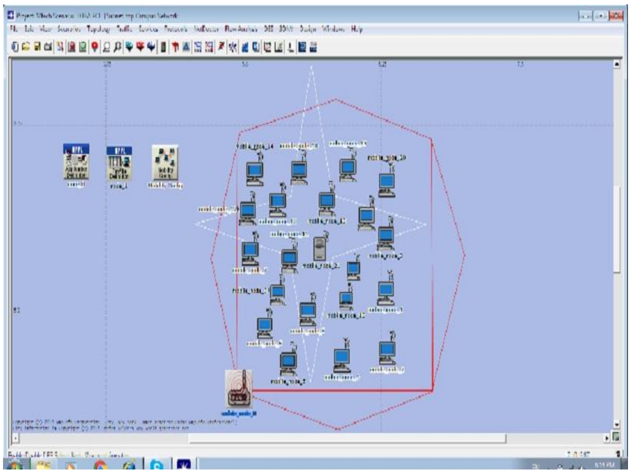

Figure 4.11: 20 Nodes Working of TORA PCF Scenario

The performance with the respective parameter of TORA, OLSR and GRP for different performance matrices is analyzed so as to see impact of jamming attack on these routing protocols.. Simulation time for all scenarios was set to 5 minute:

PCF Scenario

In this section it created three different scenarios for TORA. i.e. without attack, with attack and third with PCF for 20 nodes in network and it resulted in improving Email download Response time, Email upload Response time, HTTP page response time, Voice Packet End to End Delay as compared to with attack scenario.

6.3.1 Email Download Response time for TORA in PCF Scenario. (20 Nodes)

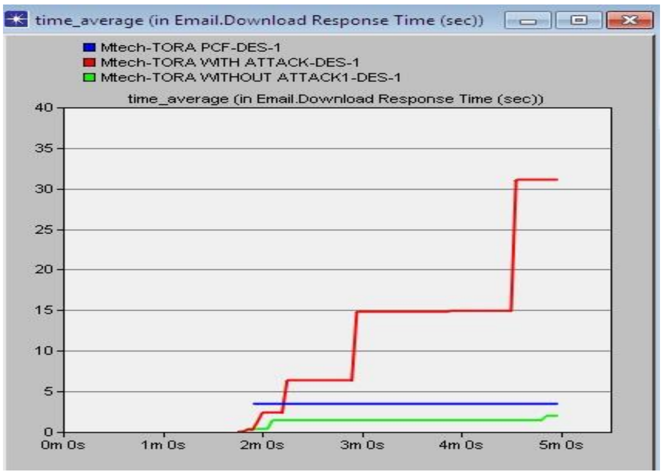

Figure 4.24: Email Download Response time for TORA in PCF Scenario (20 nodes)

In this section Performance metric Email Download Response time for TORA with three different scenarios Network without affected jamming attack, Network with affected jamming attack & PCF implementation on Network with affected jamming attack in those three different scenarios in simulation got that Email Download Response time without Jamming Attack is best which took minimum time and with Jamming Attack it increase unexpectedly and with the help of PCF techniques in simulation can reduce the some effect of affected Network.

6.3.2 Email upload Response time for TORA in PCF Scenario. (20 Nodes)

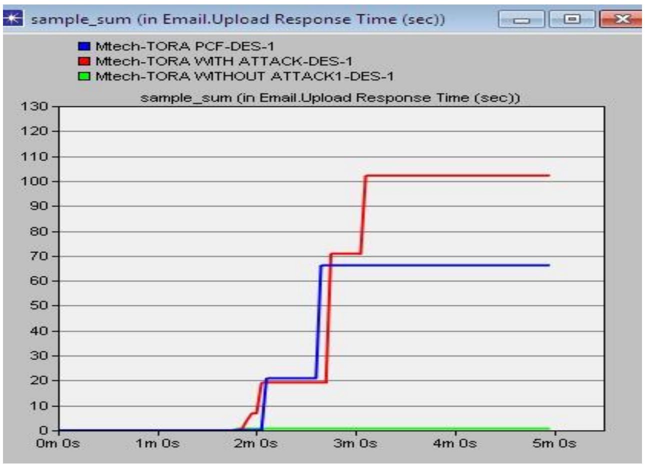

Figure 4.25 Email Upload Response time for TORA in PCF Scenario (20 nodes)

In this section Performance metric Email upload Response time for TORA with three different scenarios Network without affected jamming attack, Network with affected jamming attack & PCF implementation on Network with affected jamming attack .In those three different scenarios in simulation got that Email upload Response time without Jamming Attack is best which took minimum time and with Jamming Attack it increase unexpectedly and with the help of PCF techniques in simulation can reduce the some effect of affected Network.

6.3.3 HTTP Page Response time for TORA in PCF Scenario. (20 Nodes)

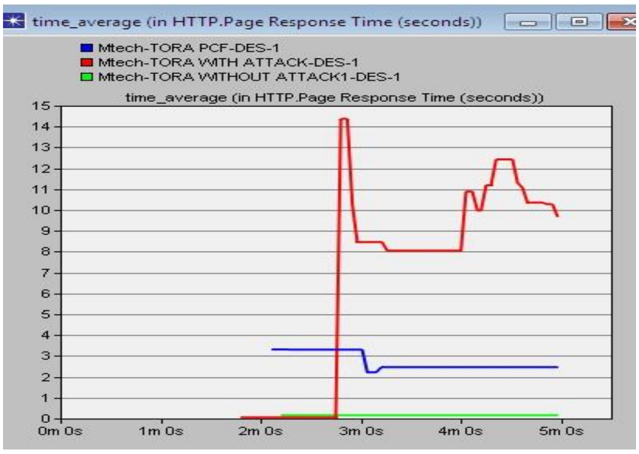

Figure 4.26: HTTP Page Response Time for TORA in PCF Scenario (20 nodes)

In this section Performance metric HTTP Page Response time for TORA with three different scenarios Network without affected jamming attack, Network with affected jamming attack & PCF implementation on Network with affected jamming attack. In those three different scenarios in simulation got that HTTP Page Response time without Jamming Attack is best which took minimum time and with Jamming Attack it increase unexpectedly .and with the help of PCF techniques in simulation can reduce the some effect of affected Network.

6.3.4 Voice Packet End to End Delay for TORA in PCF Scenario.(20 Nodes)

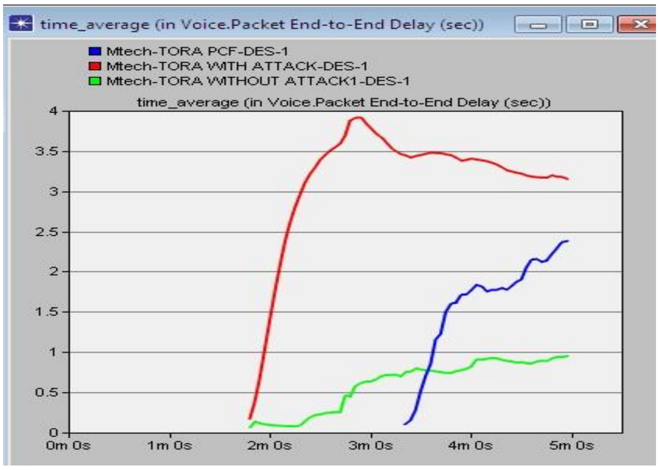

Figure 4.27: Voice Packet End to End Delay time for TORA in PCF Scenario (20 nodes)

In this section Performance metric voice end to end delay for TORA with three different scenarios Network without affected jamming attack, Network with affected jamming attack & PCF implementation on Network with affected jamming attack In those three different scenarios in simulation got that voice end to end delay without Jamming Attack is best which took minimum time and with Jamming Attack it increase unexpectedly and with the help of PCF techniques in simulation can reduce the some effect of affected Network.

7. Conclusion & Future Scope: As per Resultant, it has taken different type of result and analysis on the behalf of reactive and proactive routing protocol between OLSR, TORA and GRP. Results are taken from different seven scenarios two for each OLSR, TORA and GRP respectively with and without jamming attack on which in proposed model checked the behavior of various metrics as follows. Email Download Response time; Email Upload Response time HTTP Page Response Time and Voice End to End Delay. And seventh scenario created on TORA network infected with attack was implemented with PCF In the entire without and with infected Jamming network and different performance metric in this proposed model got mix results in which some performance metrics GRP giving us best results and in some others OLSR and TORA. In third part PCF technique is used for TORA and in this PCF implementation scenario performance is improved. As in this proposed model reactive and proactive routing protocols are used. Three protocols OLSR, TORA and GRP are taken for references. It concluded that for future references hybrid protocols can be used. In proposed model implementation with three different performance metrics is carried out while in future other performance matrices can be used like Video, Data base for better result and in this research used PCF technique is used on TORA here. PCF can be implemented on OSLR and GRP in future.

8. REFERENCES:

[1] Vahide Babaiyan, Manijeh Keshtgary "Performance Evaluation of Reactive ,Proactive and Hybrid routing protocols in Manets" in International Journal of Computer Science and Engineering.

[2]Xu, W. Trappe, W. Zhang, Y. And Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. International Symposium on Mobile Ad Hoc Networking & Computing.

[3] Arif Sari,And Dr. Beran Necat,"Securing Mobile Ad-Hoc Networks Against Jamming Attacks Through Unified Security Mechanism" International Journal Of Ad Hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3, June 2012.

[4] Neeti Yadav, Dr. Vivek Kumar," Securing Ad hoc Network By Mitigating Jamming Attack"International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 6, June 2015 2502 ISSN: 2278 – 1323 .

[5] Chaitanya, K. C., & Ghosh, A. (2010). Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation.Middlesex University, 1-13

[6] Ali Hamieh, Jalel Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using
Error Distribution", 978-1-4244-3435-0/09 IEEE, 2009.

[7] Sabbar Insaif Jasim ,"Jamming Attacks Impact on the Performance of Mobile Ad-Hoc Network and Improvement Using MANET Routing Protocols"International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-3, Issue-2, December 2013
ISSN: 2249 – 8958, Volume-3, Issue-2, December 2013

[8] 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.

[9] Faraz Ahsan, Ali Zahir, Sajjad Mohsi, Khalid Hussain, "Survey on survival approaches in wireless network against jamming attack", Journal of Theoretical and Applied Information Technology, 15th.

[10] Kuldeep Vats, Monika Sachdeva, Dr. Krishan Saluja , "Simulation and Performance Analysis of OLSR,GRP and DSR routing protocols" in International Journal of Emerging trends in Engineering and Development, Issue 2, Vol.2 (March-2012).