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

Behavior of Jamming Attack in OLSR, GRP, TORA and improvement with PCF in TORA using OPNET tool

Anupam Sharma, Deepinderjeet Kaur
Desh Bhagat University Mandi Gobindgarh Punjab

Abstract- MANETs have distinguishing characteristics like dynamic topology, wireless radio medium, limited resources and lack of centralization; as a result, they are vulnerable to different types of malicious attacks in different layers of protocol stack. Each node in a MANET is capable of acting as a router. The necessity for a secure MANET networks is powerfully tied to the security and privacy features. This Jamming attacks are one of them. These occur by transmitting continuous radio ways to inhibit the transmission among sender and receiver. These attacks affect the network by decreasing the network performance. For our proposed work we will take the OLSR, TORA and GRP protocols. The proposed work includes a network with high mobility. Implementation of jamming attack and impact of jamming attack, and finally we will use the PCF technique so that we will reduce the jamming effect.

***Key Words*: MANET, DOS Attack, Jamming Attack, Routing Protocols**

1. Introduction: A mobile ad hoc network (MANET) is generally defined as a network that has many free or independent nodes, often composed of mobile devices or other mobile pieces that can arrange themselves in various ways and operate without firm top-down network administration. It uses decentralized approach. Ad-hoc network has opened a new dimension in wireless networks. It allows wireless nodes to communicate with each other in the absence of centralized support. It does not follow any fixed infrastructure because of the mobility of nodes and multi-path propagations. Link instability and node mobility make routing a core issue in MANETs. A suitable and effective routing mechanism helps to extend the successful deployment of MANETs. In this paper, we have studied details of TORA, OLSR and GRP routing protocols we have found that among the three protocols, no single protocol can successfully provide optimum efficiency in different MANET scenarios.

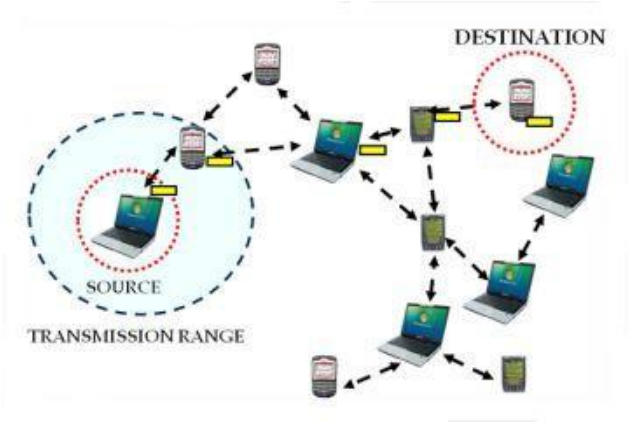

Figure: 1.1 working of MANET network

2 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

Routing Property	Proactive	Reactive	Hybrid
Routing Structure	Both Flat and Hierarchal	Flat except CBRP	Hierarchal
Route Availability	Always available, if nodes are reachable	Determined when needed	Depends on location of destination
Traffic Control volume	Usually High	Low	Mostly lower than Proactive and Reactive
Mobility Handling Effect	Usually updates occur based on mobility at fixed interval	ABR introduced LBQ,AODV uses local route discovery	Usually more than one path availability
Storage requirements	low	Usually Lower than Proactive	Usually depend on size of each cluster
Delay level	Small routes are predetermined	Higher than Proactive	Small For local destinations . inter zone may be as large as reactive protocols
Scalability Level	Usually up to 100 nodes	Source routing protocols up to few 100 nodes point-to-point may scale higher	Designed for up to 1000 or more nodes

3. DOS Denial of Service attack

Denial of Service attacks is the most common style of attacks which attempting to make the network crash by flooding it with useless traffic, which then uses all the resources in the network so the legitimate users cannot connect to the system. It is constantly used by hackers to attack network systems, because it is easy to launch and hard to avoid. DoS attacks can be launched in various protocol layers and DoS attacks in different layers can vary.

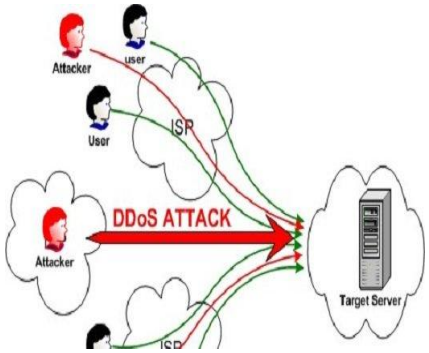

Figure 3.1 Dos attack on netowok

DOS attack in different protocol layers

Protocol Layer	Attacks	Defenses
Physical	Jamming	Sleep
	Node destruction	Hide nodes or tamper proof packaging
MAC	Denial of sleep	Sleep, authentication and anti-replay
Network	Spoofing, replaying	Authentication, anti-replay
	Hello floods	Geographic routing
	Homing	Header encryption
Transport	SYN flood	SYN cookies
	De synchronization attack	Packet authentication
Application	Path based DoS	Authentication and anti-replay protection
	Reprogramming attacks	

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 goal 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. The jamming is divided into two categories as Physical and Virtual Jamming attacks.[2] The physical jamming is launched by continuous transmissions and/or by causing packet collisions at the receiver. Virtual jamming occurs at the MAC layer by attacks on control frames or data frames in IEEE 802.11 protocol. Physical or Radio jamming in a wireless medium is a simple but disruptive form of DoS attack. These attacks are launched by either a continuous emission of radio signals or by sending random bits onto the channel. Handling of Jamming attacks much harder than other attacks. The attacker disrespects the medium access control (MAC) protocol and transmits on the shared channel; either periodically or continuously to target all or some communication, respectively [12]. In fact, a wireless medium is shared in the mobile hosts in mobile ad hoc networks. A radio signal can be interfered or jammed, which causes the message to be corrupted or lost. The attacker with a powerful transmitter causes that the generated signal will be strong enough to crush the targeted signals and damage communications. Jamming is caused by continuously sending the radio signals in between the transmission which injects the dummy packets thus causing interferences. Since the radio frequency is an open medium, therefore jamming is big problem for wireless networks. Jamming decreases the overall- performance of network by effecting their throughput, network load, end to end delays etc.[3]

4 .Literature Survey:

- Gurpinder singh, Asst. Prof. Jaswinder Singh(2012) discussed that OSPF, DSR, AODV, TORA, OLSR and DSDV on the basis of quantitative and qualitative metrics.TORA create less network load and throughput is high for AODV using OPNET 14.5 and Network Load, Throughput like matrices in paper titled" MANET: Issues and Behavior Analysis of Routing Protocols".
- Pankaj Palta, Sonia Goyal (2012) discussed that OLSR is better in those scenario where bandwidth is large as it always updated their nodes so large bandwidth is used than TORA on same conditions using OPNET simulation tool and throughput, delay, data dropped, Retransmission attempts like metrices in paper" Comparison of OLSR and TORA Routing Protocols Using OPNET Modeler".
- Sumit Mahajan, Vinay Chopra(2013), studied that TORA the finest suited for MANET protocol in dense population of nodes and scale well with large and small sized whereas AODV has very poor QoS in high populated node networks with GSM voice traffic data. OLSR outperforms in terms of throughput jitters and gets the same low delay as OLSR using OPNET and performance matrices namely Delay, Network Load Throughput, Jitter, MOS Value in paper" Performance Evaluation of MANET Routing Protocols with Scalability using QoS Metrics of VOIP Applications".
- Snehita Modi, Dr. Paramjeet Singh, Dr. Shaveta Rani(2014), Integrated approach includes a network with high mobility, IEEE 802.11g standard with max data rate, heavy traffic (FTP, video conferencing) improved AODV increased drastically buffer size and the media access delay while reduces the network throughput, retransmission attempts, while the media access delay decreases. The overall performance of network increases except the network load which is increased by the proposed mechanism. Using OPNET 14.5/ Media Access Delay, Retransmission attempts, Network Load, Throughput in paper entitled" Performance Improvement of Mobile Ad hocNetworks under Jamming Attack".
- 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".

- Alaa Zain,Heba A. El-Khobby, Hatem M. Abd Elkader, Mustafa M. Abdeln discussed that OLSR, GRP and AODV, that have more severe effect when there is a higher number of malicious nodes and delay under attack in case of OLSR is more than in case of AODV. In case of network load, however effect on AODV by the malicious node is less as compare to OLSR.AODV is less vulnerable to denial of service attack than DSR, GRP and OLSR using OPNET 17/Delay, Data loss,Packed end to end delay, Network Load,Throughput in paper "MANETs performance analysis with DOS attack at different routing protocols".
- 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".

5. Conclusion and Future Scope

This paper deals with all the aspects of routing Protocols such as TORA, OLSR and GRP. In this paper we describe that dos attack can effect the performance of MANET network and also we have describe that dos attack is a type of jamming attack with the help of Point coordination function (PCF) techniques we can reduce the impact of jamming attack on any network For future references we will create the network with these routing protocols and then on one of the network we will implement the jamming attack .and after that we will implement the PCF so we can reduce the effect of jamming attack .for all this we will use OPNET tool.

6. References:

[1]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.

[2] 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.

[3] 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 .

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

[5] 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.

[6] 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

[7] 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.

[8] 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.
Vol. 30 No.1, August 2011, pp. 55 – 67.