International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 6, June - 2013

Impact Of Node Mobility, Pause Time And RREQ Flooding Attack In MANET

Prof. Sunita Sahu
Assistant Professor, Indira College of Engineering and Management, Pune

Abstract

Mobile ad-hoc networks is a decentralized, infrastructure less network consisting of group of mobile nodes communicating with each other through wireless links. The performance of the mobile ad hoc network is highly affected by the traffic pattern like node mobility speed, pause time , mobility model etc. The paper analyzes the effect of varying traffic pattern like pause time and mobility speed in MANET. RREQ flooding is a distributed DOS type of attack which consumes the network resources. The paper also analyzes the effect of RREQ flooding in mobile ad hoc network with varying number of malicious node.

1. Introduction

A Mobile Ad-Hoc Network (MANET) is a collection of mobile nodes connected by wireless links, without the use of any infrastructure to form an arbitrary topology. The mobile node behaves like host to generate packets and router by forwarding packets to another node. In MANET, the nodes are free to move randomly. Thus the network's topology changes unpredictably and rapidly which make routing more difficult. Mobile ad hoc networks are mainly used in personal area networking, rescue operation, military environment and emergency operations.

A routing protocol is needed to transfer the packets from source to destination via number of nodes. Number of routing protocols has been proposed for Mobile Ad hoc networks. These protocols find a route for packet delivery and deliver the packet to the correct destination. Asymmetric link, dynamic topology, interference and routing overhead are the some of the problems in routing in MANET.

MANET routing protocols are broadly classified into two categories as: Proactive Protocols or Table Driven Protocols and Reactive Protocols On-Demand Protocols.

In proactive routing protocol every node maintains its own routing table to store routing information for every other possible node in the networks[1]. Routing tables is periodically updated as the network topology changes. Routing overhead is more in case of table driven routing protocol. Some of the proactive routing protocols are DSDV,WRP,STAR etc.

In reactive routing protocols, the route between source and destination node is searched only when needed using route discovery process[1]. Examples of reactive protocols are AODV, DSR, TORA etc.

This paper analyzed the impact of mobility speed, pause time and RREQ flooding attack in MANET. Many researchers have worked on the analysis of traffic patterns. In [1] the author's analyzed the impact of varying pause time on various routing protocol like DSR, AODV and DYMO and concluded that the DSR Routing gives better performance in varying pause time. In [2], the author compared the performance of AODV and AOMDV by varying pause time and network load considering CBR traffic. In [5] the author compared the performance of three random mobility models such as Random waypoint, Random walk and Random Directions under the constraints like packet-delivery fraction and End-to End packet delivery delay.

The rest of the paper is organized as follows: in section 2 the dynamic source routing protocol is discussed. The section 3 covers some commonly used mobility models and section 4 briefly covers the flooding attack. Section 5 covers the performance parameter followed by simulation results in section 6 and finally section 7 concludes the paper.

2. Dynamic Source Routing

The Dynamic Source Routing (DSR) protocol is a on-demand routing protocol [1,5]. DSR protocol maintains the route cache to store the route to the mobile node it is aware. This protocol composed of two major phases : route discovery and route maintenance. Whenever any node has the data to send, first it checks the route cache for the route to the destination. If it has the unexpired route, then it use it otherwise initiate a route discovery process by broadcasting the RREQ packet which contains the source address and the destination address. Whenever any intermediate node receives the RREQ, and it does not have the route to the destination it adds its own address in the route record and forward to its neighbor. RREP is generated whenever RREQ reaches to destination node or intermediate node which has the route to destination in its route cache. Route maintenance mechanism is used to detect whether the path to the destination exist or not. Route maintenance uses the route error message and acknowledgement Route error message is initiated whenever the destination's data link layer recognize any transmission error. DSR is suited for small to medium sized networks as its packet overhead (not packet data overhead) can scale all the way down to zero when all nodes are relatively stationary. The packet data overhead will increase significantly for networks with larger hop diameters as more routing information will need to be contained in the packet headers.

3. Mobility Models

Mobility models are used to represent the movement of mobile node and of their velocity ,location, acceleration with respect to time. Mobility model are very important and used to evaluate the performance of MANET protocols

3.1 Random Walk Mobility Model

In this model mobile node moves in random selected direction with selected speed .In this model each nodes movement changes either after constant time or after travelling constant distance[5]. For every movement the speed and direction are selected from predefined formula [minspeed, maxspeed] and [0.2*pi] respectively. While moving if mobile node reaches the boundary of simulation area, it bounces off the border by angle calculated from incoming direction. It is a memory less model resultant it generate unrealistic movement pattern.

3.2 Random Waypoint Model

The random way point mobility model was proposed by Johnson and Maltz . This model is widely used for mobile ad hoc network protocol simulation because of its simplicity and wide availability. In this model, node randomly chooses the destination and moves towards it with chosen velocity[2,5]. When node reaches the destination, it stops for the duration depending upon the specified "**pause time**". After this node again selects some random destination node and repeats the same procedure until the simulation ends. The major drawback of random way point mobility model is that nodes are not equally distributed in the entire simulation area they are more in centre area.

3.3 Random Point Group Mobility Model

In RPGM the logical centre are defined and every group have one group leader and group leader determines the mobility behavior of other node. The nodes in the group are randomly distributed around the reference point. This model represent the movement pattern of group of mobile node as well as individual mobile nodes within the group[6]. For each node, the mobility is assigned with a reference point that follows the group movement. Individual MN randomly moves based on its own predefined reference points, whose movements depend on the group movement.

3.4 Random directional mobility model

In random directional mobility model node selects the random direction in which to travel like random walk mobility model[5]. When a node reaches the boundary of the simulation area it pause for a specified pause time and again select the direction and continues the process. This model eliminates the drawback of random waypoint mobility model of clustering nodes in one part of the simulation area. Random directional model forces the mobile node to touch the network border before it changes its direction.

3.5 Gauss-Markov Mobility Model

The Gauss-Markov Mobility Model allows different levels of randomness via setting various parameters like speed and direction. Initially speed and direction are assigned to every mobile node. After fixed intervals of time speed and direction of

each mobile node is updated. Here the velocity of mobile node is modeled as a gauss markov stochastics process. Specifically, the value of speed and direction of every instance is calculated based on the basis of the value of speed and direction of previous instance.

4. Flooding Attack

Flooding attack is a denial of service type of attack in which the malicious node broadcast the large number of fake RREQ packet to the node which does not exist in the network or by sending large amount of irrelevant data to other node in the network[4][7][8] The main aim of flooding attack is to consume the available network resources so that valid or legitimated user can not able to use it. Because of the limited resource constraints in the mobile ad hoc networks resource consumption due to flooding attack reduces the throughput of the network [8].

Flooding attack can be categories in two category: Route request (RREQ) Flooding and DATA flooding

4.1 Route Request Flooding Attack

In the RREQ flooding attack, the malicious node generate large amount of RREQ packet and sends to the IP address which does not exist in the network[4]. Since the destination address is invalid no reply packet is generated by any node and hence attacker keep flooding the network by RREQ packets. As a result network gets congested by fake RREQ packets and valid data communication is not possible.

Various side effects of RREQ flooding attack are:

- Intermediate node's route table overflow
- bandwidth wastage
- node resources consumption

4.2 Data Flooding Attack

In data flooding attack the attacker first set up the path to all the nodes in the network. After setting the path it forwards the large amount of useless data packet to keep victim node busy in receiving useless packet. The intension is to exhaust the resources of the victim node so the node may get isolated from network[8].

5. Performance Matrix

Following performance matrix are used to evaluate the performance of our simulated mobile ad hoc networks.

5.1 Pause Time

Pause time is time duration for which mobile node hold the same position. Any node stays at same position for specified amount of pause time then node select some random direction. If the node pause time is 50 means node will not change its position for 50 seconds.

5.2 Mobility Speed

The nodes are free to move in any random direction inside the network. Mobility speed means average speed by which node moves in random direction in the simulation area[2]. Mobility speed have great impact on network topology; if the speed is more means more dynamic network.

5.3 Routing Overhead (ROH)

Routing overhead is the total number of control packets or routing packets generated by routing protocol during simulation.

6. SIMULATION RESULT

NS-2 simulator is used to analyze the performance of network. The DSR routing protocol is used for all the simulation and the other simulation parameters are shown in the table. The topology of the MANET depends on the pause time and mobility speed. It changes frequently when pause time is less and mobility speed is more.

Table 1: Simulation Parameters

No. of nodes	50
Simulation time	300 sec
Mobility speed	20/50 ms
Pause time	0/50/ 150 ms
Routing algorithm	DSR
Mobility model	Random waypoint
Simulation area	1500 X 300
Packets Rate	4/sec
Packet size	512
Traffic type	CBR(UDP)
No. of malicious node	1 to 10

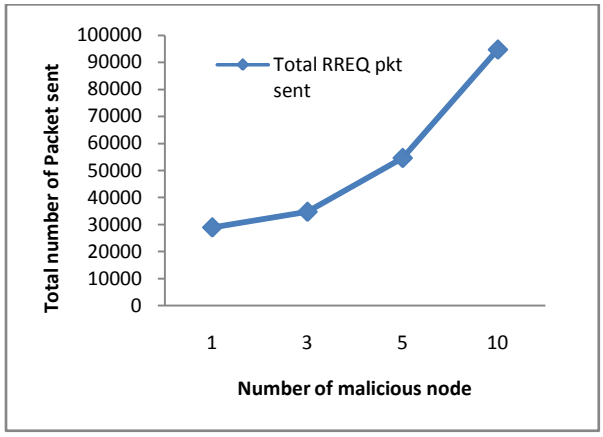

Figure1: Effect of Route Request Flooding

Total number of route request send and receive are used to analyze the performance of the network.
Figure 1 shows the effect of flooding attack in the network of 50 nodes with mobility speed 20 ms and pause time 0.

Figure 1 shows that the fake route request packets and hence total RREQ packets increases drastically as number of malicious node increases .Because of this more number of routing entries are created in the routing table of every node and hence increases the routing overhead. This type of route request flooding attack also consume the valuable resources of the nodes and hence decreases the network performance.

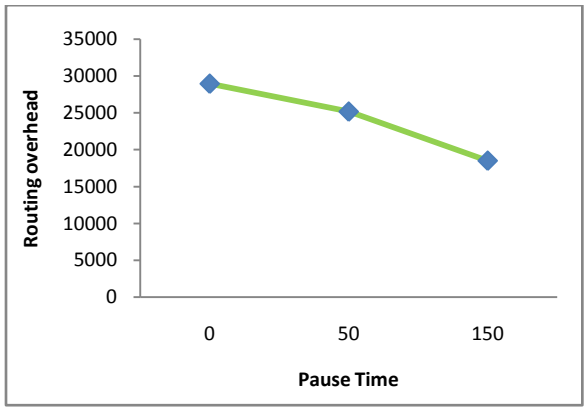

Figure2: Effect of pause time

Figure 2 shows that the effect of pause time in the network. Pause time zero mean nodes are continuously moving and hence number of RREQ packets per unit time. As we increase the pause time means network is less dynamic leads to less number of RREQ packet per unit time.

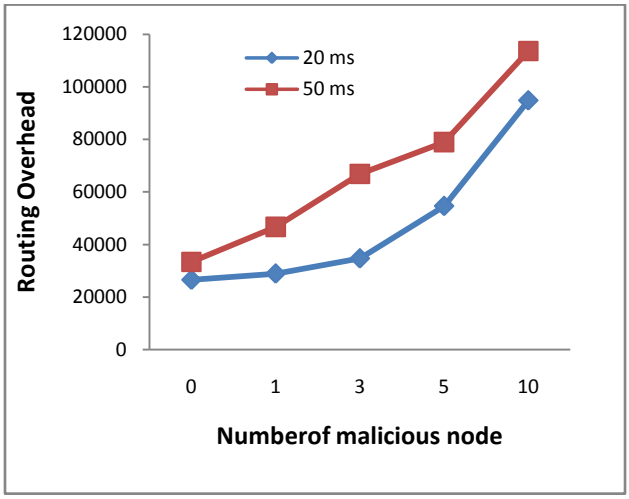

Figure3: Effects of flooding in different mobility speed with pause time 0(sent)

The figure 3 shows the impact of flooding attack in different mobility speed . Routing overhead increases with the number of malicious node drastically and exhaust the network resources. The graph also shows that with same number of malicious node ,the routing overhead is more when mobility speed is high.In case of high mobility the routing overhead is more because route breaks very often.

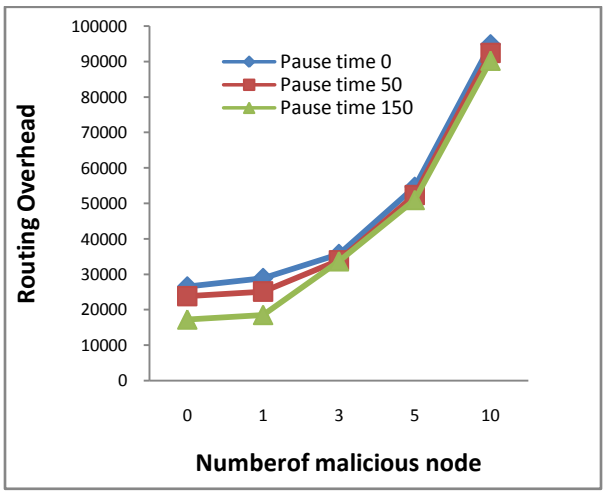

Figure 4: Effects of flooding in different pause time keeping mobility speed 20 ms

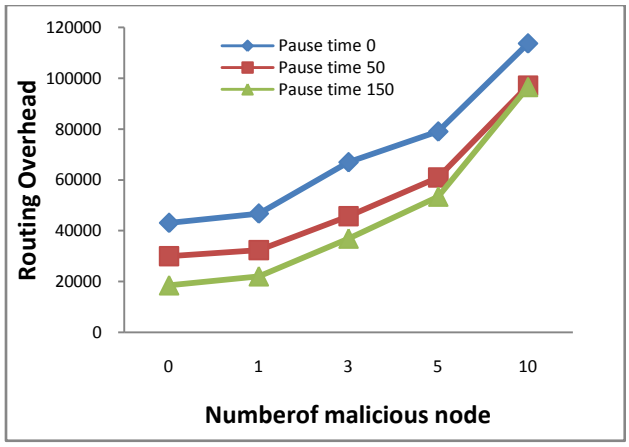

Figure 5: Effects of flooding in different pause time keeping mobility speed 50 ms

From figure 4 and 5 it is clear that pause time inversely effects the routing overhead in the network. Less pause time means more dynamic network as nodes keeps continuously moving; generate more routing overhead and vice versa.

7. Conclusion

This paper provide the simulation analysis of network with different mobility speed and pause time. Mobility is a very important characteristic of the MANET which determines the link stability of the network. If the node mobility is more means less link stability and hence more dynamic network topology. The results shows that the network performance varies with pause time and mobility speed. In this paper we have used DSR routing protocol for simulation as it gives better performance in high mobility condition. This paper also covers analysis of effects of RREQ flooding attack in the network and the results shows that RREQ flooding highly degrades the performance of the network by generating large number of routing overhead which in terns consume networks valuable resources.

References

[1]. Dhananjay Bisen, et al." Effect of Pause Time on DSR, AODV and DYMO Routing Protocols in MANET"

[2]. P.Periyasamy, Dr.E.Karthikeyan" Impact of Variation in Pause Time and Network Load in AODV and AOMDV Protocols" *I.J. Information Technology and Computer Science*, 2012, 3, 38-44 Published Online April 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijitcs.2012.03.06

[3]. B. Divecha et al, "Impact of Node Mobility on MANET Routing Protocols Models", Journal of Digital Information Management, February 2007.

[4] Ai-Fen Sui, Dai Fei Guo, Dong-Sheng Zhao "An Effective Method to Mitigate Route Query Floods in MANETs", 978-1-61284-307-0/11/$26.00 ©2011 IEEE

[5] M.K.Jeya Kuma, R.S.Rajesh **"**Performance Analysis of MANET Routing Protocols in Different Mobility Models", IJCSNS International Journal of Computer Science and Network 22 Security, VOL.9 No.2, February 2009

[6] K.Muthumayil, V.Rajamani, S.Manikandan and M.Buvana "Performance Analysis of Reference Point Group Mobility model,Random Mobility models in Associativity Based long-lived Routing(ABR) protocol"

[7] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang "Resisting Flooding Attacks in Ad Hoc Networks" Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) 0-7695-2315-3/05 $ 20.00 IEEE

[8] Revathi Venkataraman, M. Pushpalatha, Rishav Khemka and T. Rama Rao "prevention of flooding attack in mobile ad hoc network". International Conference on Advances in Computing, Communication and Control (ICAC3'09).

[9]Shishir K. Shandilya, Sunita Sahu "A Trust Based Security Scheme for RREQ Flooding Attack in MANET" *International Journal of Computer Applications (0975 – 8887) Volume 5– No.12, August 2010*

[10] Elizabeth M. Royer, C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communications, pp.46-55, April 1999.

[11] Mohd Izuan Mohd Saad, Zuriati Ahmad Zukarnain,"Performance Analysis of Random-based MobilityModels in MANET Protocols", European Journal of Scientific Research, Vol. 32(4), pp. 444-454,2009.

[12] Sunita Sahu, Shishir K. Shandilya" a comprehensive survey on intrusion detection in manet**"** *International Journal of Information Technology and Knowledge Management July-December 2010, Volume 2, No. 2, pp. 305-310*

[13] The Network Simulator ns-allinone-2.34, http://www.isi.edu/nsnam/ns/

[14] Kevin Fall, K. Varadhan, "The ns Manual",University of Southern California, Information Sciences Institute (ISI), http://www.isi.edu/nsnam/ns/ns-documentation.html.

[15] NS-2 with Wireless and Mobility Extensions, http://www.monarch .cs.cmu.edu.