Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Performance of AODV under Flooding Attack

Parbhat Verma
CSE Department & KUK
India

Seema
CSE Department & KUK
India

Komal Manocha
CSE Department & KUK
India

Abstract*— A Mobile Ad-Hoc Network (MANET) are future wireless networks consists of mobile nodes which communicate on-the-move without base stations. MANETS are mobile; it uses wireless connections to connect to various networks. This can be a standard LAN Network, or another medium, such as a WI-FI or satellite transmission. Some MANETs are allowing only local area of wireless devices (such as a group of LAN computers), while others may be connected to the Internet. Due to the dynamic nature of MANETs, they are not very secure, so it is important to be cautious what data is sent over a MANET. This can be improved by implementing various security concerns. MANET involves various attacks such as DoS, Brute Force attack etc. Here, we selected the flooding attack. The analysis performance of the routing protocols always degrades when the network is under the influence of any kind of denial of service attack. In this paper we have selected AODV routing protocol for our study. This paper guides about the performance of the AODV routing protocol under the flooding attack. To analyze how much the performance of the network deteriorates under the presence of attack we have taken the various network parameters via throughput, packet delivery ratio and end to end delay.

Keywords— ***Ad-Hoc Network (MANET),Throughput, packet delivery ratio, End to End delay Ad-hoc On Demand Distance Vector (AODV), Flooding Attack, Security***

I. INTRODUCTION

A Mobile Adhoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. Opposed to the infrastructure wireless networks where each user directly communicates with an access point or base station, a mobile ad hoc network, or MANET is a kind of wireless ad hoc network [1]. It is a self configuring network of mobile routers connected by wireless links with no access point. Every mobile device in a network is autonomous. The mobile devices are free to move haphazardly and organize themselves arbitrarily. In other words, ad hoc network do not rely on any fixed infrastructure (i.e. the mobile ad hoc network is infrastructure less wireless network. The Communication in MANET is take place by using multi-hop paths.

Nodes in the MANET share the wireless medium and the topology of the network changes erratically and dynamically. In MANET, breaking of communication link is very frequent, as nodes are free to move to anywhere. The density of nodes and the number of nodes are depends on the applications in which we are using MANET. Figure 1.1 shows a simple ad-hoc network

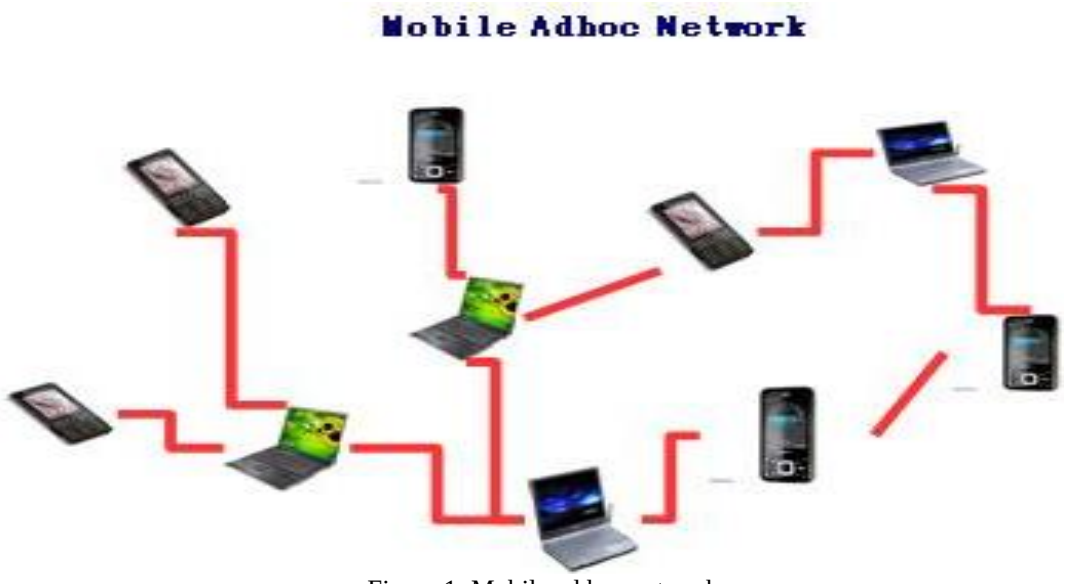

Figure 1: Mobile ad hoc network

MANET has given rise to many applications like Tactical networks, Wireless Sensor Network, Data Networks, Device Networks, etc. With many applications there are still some design issues and challenges to overcome [3,4]. Security is one of the most challenging and in request issue of ad hoc network. At the networking layer, the routing information must be protected from any attack against *confidentiality*, *authenticity*, *integrity* and *availability* of the information. Most of these are connected with encryption methods and access methods of the network. From the nature of ad hoc networks, these methods are not centralized, but rather distributed. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defence mechanism. [5,6]

II. PROBLEM STATEMENT

We have selected AODV routing protocol for checking Performance. In our work we have analyzed the performance of the AODV routing protocol under the presence of flooding attack. To analyze how much the performance of the network deteriorates under the presence of attack we have taken the various network parameters via throughput, packet delivery ratio and end to end delay. We have taken five scenarios for our study. Keeping the total number of nodes to be fixed to 30 we have varied the number of attacker nodes firstly three then four then five and then six and then finally seven. From our network simulation we would try to analyze the impact of the increase in the number of attacker nodes in the network. The simulation work is carried out using the NS 2 simulator. We compared the results of these simulations to understand the network and node behaviours. The results of the simulation show that the packet loss increases in the network by increasing the number of flooding nodes. Mobile Ad hoc networks may also experience packet loss due to parameters employed. In our four simulations of network, we noticed that the variation of data loss due to network parameters such as the distribution of the nodes changed.

III. RESULTS

We compared the results of these simulations to understand the network and node behaviors. The results of the simulation show that the packet loss increases in the network by increasing the number of flooding nodes. Mobile Ad hoc networks may also experience packet loss due to parameters employed. In our four simulations of network, we noticed that the variation of data loss due to network parameters such as the distribution of the nodes changed.

Throughput:

The average rate at which the total number of data packet is delivered successfully from one node to another over a communication network is known as throughput. The result is found as per KB/Sec. It is calculated by Throughput= (number of delivered packet * packet size) / total duration of simulation

The results of the simulation show that the throughput in the network decreases by increasing the number of flooding nodes in the network. It is obvious that the throughput for the case with AODV, without attack, is higher than the throughput of AODV under attack as also shown in figure 2. The throughput keeps on decreasing as the numbers of malicious nodes are increased in the network keeping the total number of nodes constant in each scenario. This is because of the fewer routing forwarding and routing traffic. Here the malicious node discards the data rather than forwarding it to the destination, thus effecting throughput.

As throughput is the ratio of the total data received from source to the time it takes till the receiver receives the last packet. A lower delay translates into higher throughput. The overall low throughput of AODV is due to route reply. As the malicious node immediately sends its route reply and the data is sent to the malicious node which discard all the data. The network throughput is much lower.

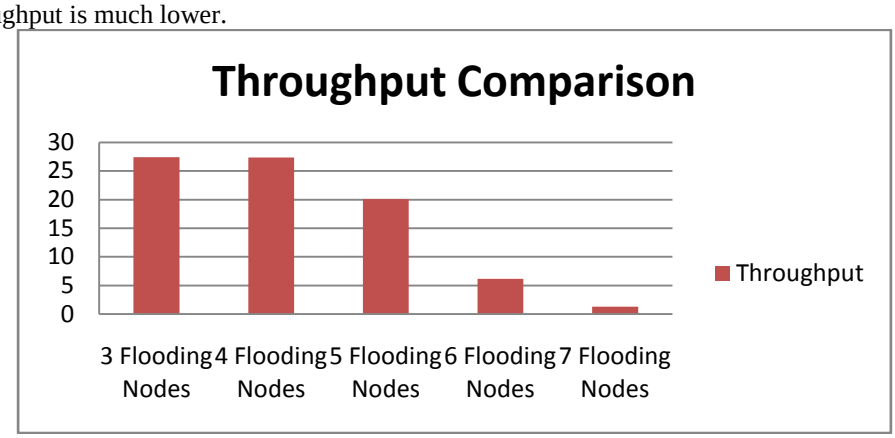

Figure 2: Throughput comparison with Flooding Nodes

Packet delivery Ratio (PDR) :

This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes throughout the simulation. It also describes the loss rate that of the packets, which in turn affects the maximum throughput that the network can support.

PDR= (Packets Received / Packets Sent)

This is due to increased congestion in the routes due to the false route requests generated in the network by the flooding attacker nodes. As the number of such nodes are increased in the network packet delivery ratio for AODV routing protocol decreases because of the increase in the false route requests generated in the network as shown in figure 3

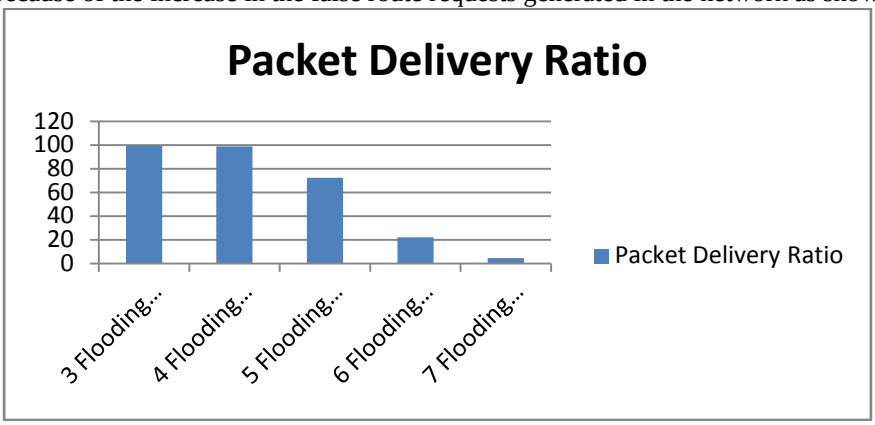

Figure 3: Packet Delivery ratio with Flooding Nodes

End to End delay

End-to-end Delay: the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

$\sum$ (arrive time – send time) / $\sum$ Number of connections

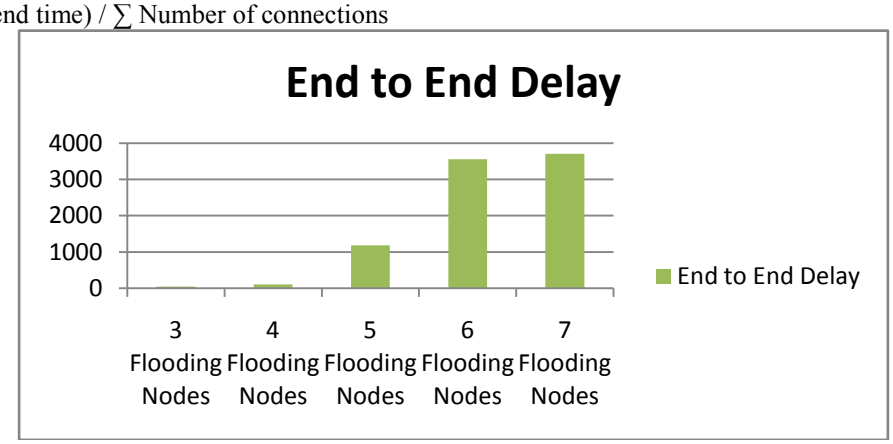

Figure 4: End to End Delay with Flooding Nodes

The results of the simulation show that the number of packets successfully delivered in the network decreases by increasing the number of attacker nodes in the network. This is due to the fact that more and more number of packets is dropped because of the increased congestion created by the flooding nodes. Since the packet drop is increased the more and more retransmissions are required for the successful delivery of the packets. More and more retransmissions leading to more end to end delay.

IV. PROPOSED WORK

Generally, it is the case that a node does not send a message to a specific node, because of network topology discovery purposes. Then the transmission is done primarily by using flooding technique. That is the transmission of the message without designating a destination node and sending to any available node at the transmission range of the sender. This technique is very useful method for neighbour discovery. Neighbour nodes for a node S are the nodes that S can send/receive message directly.

V. CONCLUSIONS AND FUTURE SCOPE

We simulated the Flooding Attack in the Ad-hoc Networks and investigated its affects. In our study, we used the AODV routing protocol. The other routing protocols could be analysed as well. All routing protocols are analysed produces different results. So, the optimized routing protocol for reducing the Flooding Attack may be determined. While Determining the Flooding Attack, we observed increased packet loss in the ad-hoc network. The overall end to end delay is also increased in the network. If the number of Flooding Attack Nodes is increased then the data loss would also be expected to increase. Thus from our simulation study we conclude that the flooding attack degrades the performance of the network. The more the number of attacker nodes the more severe the impact of attack.

In our thesis, we try to simulate the flooding attack effect in the network. But detection of the Flooding Attack Node is another future work. There are many Intrusion Detection Systems (IDS) for ad-hoc networks. These IDSs can be analysed to determine which one is the best to detect the Flooding Attack. Additionally, we used UDP connection to be

able to count the packets at sending and receiving nodes. This would be another solution for finding the Flooding Attack Node. This takes place after the route determination mechanism of the AODV protocol and finds the route in a much longer period. Finding the Flooding Attack node with connection oriented protocols could be another work as a future.

REFERENCES

[1] Y. Zhou, Y. Fang and Y. Zhang, "Securing wireless sensor networks: a survey", *IEEE Commun. Surveys Tutorials*, vol. 10, num. 3, pp. 6-28,2008.

[2] Priyanka Goyal, Vinti Parmar and Rahul Rishi, *"MANET: Vulnerabilities, Challenges, Attacks, Application",* IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011. S. Bouam and J. B. Othman,

[3] Swati Jain, Dr Naveen Hemrajani, Dr. Sumit Srivastava "Simulation And Analysis Of Performance Parameters For Black Hole And Flooding Attack In MANET Using AODV Protocol" International journal of scientific & technology research volume 2, issue 7, July 2013

[4] Mobile Ad Hoc Networking Working Group – AODV http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv

[5] IETF Manet Working Group AODV Draft http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-08.txt

[6] A. Jamalipour, "Self-organizing networks [message from the editor-in-chief]," IEEE Wireless Communications, vol. 15, no. 6, pp.2-3, Dec. 2008.

