Performance Analysis of AODV under Black Hole and Flooding Attack in MANETs

Preeti Verma[1] Reena Rani[2]
[1]M. Tech. Scholar [2]Assistant Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]SDDIET, Barwala, India

Abstract— Mobile Ad-hoc Networks (MANETs) are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. The nodes can acts as host/router. The characteristics of MANETs such as dynamic topology, node mobility, self-organizing capability so that they can be deployed urgently without the need of any infrastructure. Due to security vulnerabilities of the routing protocols, however, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. On the basis of attack against MANETs may be classified into active and passive attacks. The attacks not only from outside but also from within the network. In particular, black hole attacks and flooding attacks can be easily deployed into the MANETs by the adversary. Our objective is to analyse the impact of black hole attacks and flooding attacks on MANETs performance using reactive routing protocol namely AODV (Ad hoc on Demand Distance Vector Protocol). We have used performance metrics i.e. Throughput, Packet Delivery Ratio and end to end delay to analyse the impact of both attacks on AODV Routing Protocol in MANET by using the network simulator NS-2.

Key words: Manet, NS2, Aodv, Flooding Attack, Black Hole Attack

I. INTRODUCTION

Wireless ad-hoc networks are composed of autonomous nodes that are self-managed without any infrastructure. They usually have a dynamic topology such that nodes can easily join or leave the network at any time and they move around freely which gives them the name MANETs. In MANETs the nodes can communicate with each other on the basis of mutual trust because it works without a centralised administration. This is because MANETs are more vulnerable to be exploited by an attacker inside the network. Thus security in MANETs is the most important concern for the functionality of the network. Attacks can be launched from all layers of the protocol stack but the routing layer attacks are the most damaging.

Routing layer attacks can be categorized as external attacks and internal attacks. The focus of this paper is to see how AODV can be misused and modified to work maliciously and an extensive simulation study of the modified NS-2 reflecting the following:

Flood attack greatly increases the routing overhead of the protocol.

Black hole attack drastically degrades packet delivery ratio and throughput and also increases the routing overhead.

This paper is organised in six sections. Introduction on MANETs is presented in section I. The overview of related work is described in section II. The AODV Routing protocol is discussed in section III. The possible routing attacks in MANETs are discussed in section IV. Experiments and Result lists in section V. Section VI conclude the paper.

II. PROPOSED WORK

In order to make security of the network unbeatable, it is essential to develop security schemes that can take care of malicious behaviour of internal nodes as well as deal with external attacks. Protection against these attacks is ensured only with a deep understanding of the attack launching methodology and attacker's perspective in MANETs. In recent years, various types of MANET attacks have been detected and analysed. We can divide the recent research into the following categories:

- Performance analysis of MANET reactive routing protocol AODV under two attack i.e. blackhole attack, flooding attack.
- Performance comparison of both attacks under single routing protocol.
- Then analyse which attack more affects the performance of the network.

III. AODV ROUTING PROTOCOL

Ad-hoc On Demand Distance Vector (AODV) is an on demand routing protocol which is used to find a route between the source and destination node as needed. It uses control messages such as Route Request (RREQ) and Route Reply (RREP) for establishing a path from the source to destination. When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. The route request reaches the destination and automatically creates the reverse path. Then RREP message follows the reverse path and as soon as source receives RREP message it can start sending the data packets.

IV. ROUTING ATTACKS IN MANETS

The attacks in MANET on the basis of behaviour of attack are categorized as passive attacks and active attacks. Passive attackers exchange the data in the network without disrupting the operation of a network. On the other hand active attackers destroy the data which is present in the network, thus affects performance of the network. The attacks further classify on the basis of sources of attack known as internal attacks and external attacks. Internal attacks are done by internal nodes in the network which are authorised whereas external attacks are done by the external nodes that are out of the network. Another classification of attacks is related to protocol stacks, for instance network layer attacks. The two main network layer attacks are discussed below:

All rights reserved by www.ijsrd.com

A. Black Hole Attack:

It is a kind of Denial of services (DoS) in MANETs. In this attack malicious nodes falsely claim a fresh route to the destination to absorb transmitted data from source to the destination and drop them instead of forwarding. Black hole attacks in AODV protocol are categorised as: Black hole attack caused by RREP, Black hole attack caused by RREQ.

B. Flooding Attack:

This attack is based on DoS in which the attacker node broadcast the false packet in the network. The aims of the attacker node to consume the available resources like bandwidth, battery power etc. so that legitimated users are not able to use these resources for valid communication. Flooding attack is easy to implement but it can cause severe damages.

V. EXPERIMENTS AND RESULTS

Our work is to analyse the impact of Black hole attack and Flooding attack in AODV routing protocol based on parameters packet delivery ratio, throughput and end to end delay. We analysed the attacks by keeping the total number of nodes fixed with varying the number of Black hole nodes and Flooding nodes to analyse the performance of the network with AODV routing protocol without attack and under the attack.

A. Performance Metrics

1) Packet Delivery Ratio

It is the ratio of number of packets received at destination node to that of number of packets sent by the source node. It gives the reliability of the protocol for message deliver. It is affected by change in topology and node mobility. The PDR should be high.

2) Throughput

It is defined as total amount of data in terms of number of bytes received by the destination per second.

3) End-to-End Delay

It is the total time taken for the packet to reach from source to destination and it is measured in seconds. It includes all the delay in the network such as transmission time, buffer queues, delay induced by routing activities etc. Delay should be less for efficient packet transmission.

B. Simulation Details

To investigate the effects of Black hole attack and Flooding attack in AODV routing protocol by using Network Simulator (NS2), we have simulated the scenario of MANET with and without Black hole nodes and Flooding nodes. To test the protocol we used simulations of a network with 20 nodes. We have conducted four scenarios of the network with AODV routing protocol by increases the no. of blackhole nodes and flooding nodes firstly without any attacker nodes then two, four and finally six. We then compared the results of these simulations under various scenarios and then we use them for our result and discussion. The simulation details are given below in table 1.

Simulator	**NS-2 (ver. 2.33)**
Simulation Time	500(s)
Number of Mobile Nodes	20
Mobility Model	Random Waypoint Model
Black hole / Flooding Node	0,2,4,6
Topology	750m x750m
Transmission Range	250m
Routing Protocols	AODV
Traffic	Constant Bit Rate(CBR)
Pause Time	2(s)
Packet Size	512 bytes
Data Rates	10 Kbits

Table I: Simulation Setup

C. Results and Discussions

We compared the results of these simulations to understand the network and node behaviours. The results of the simulation show that the packet loss in the network increases with increase in number of attacker nodes. This is due to increase congestion in the routes towards the attacker nodes. MANET may also experience packet loss due to parameters employed. In our four simulations of network, we noticed that the data loss due to network parameters such as the distributions of the nodes changed.

1) Throughput

It is obvious that the throughput for AODV is sometime high and sometimes low. The malicious nodes discard the data rather than forwarding it to the destination, thus effecting throughput.

The result of the simulation show that the throughput in the network decreases by increases the number of blackhole nodes and flooding nodes in the network. But the impact of blackhole attack is more severe than the flooding attack. The performance of the network degrades much higher in presence of blackhole attack as compared to flooding attack as shown in figure 1 below:

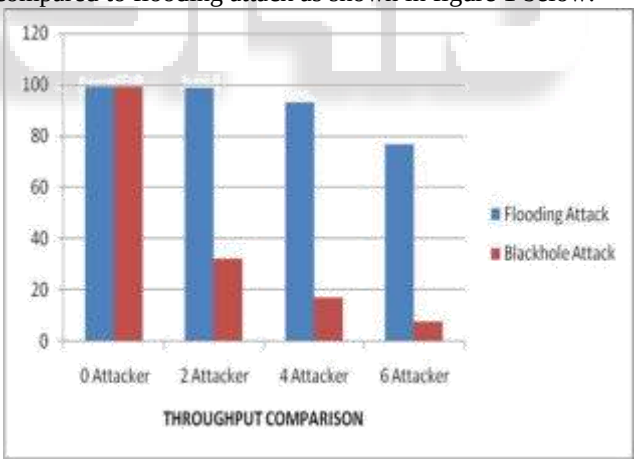

Fig 1: Throughput for AODV Protocol with Black Hole Node/Flooding Node

2) Packet delivery Ratio (PDR)

The results of the simulation show that the number of packets successfully delivered in the network with a Black hole node/Flooding node decreases by increasing the number of attacker nodes in the network. The malicious node discards the data rather than forwarding it to the destination. In the presence of more flooding attacker nodes the congestion in the network increased. As such nodes are increased in the network more and more packets are discarded thus affecting the delivery ratio of the network.

All rights reserved by *www.ijsrd.com*

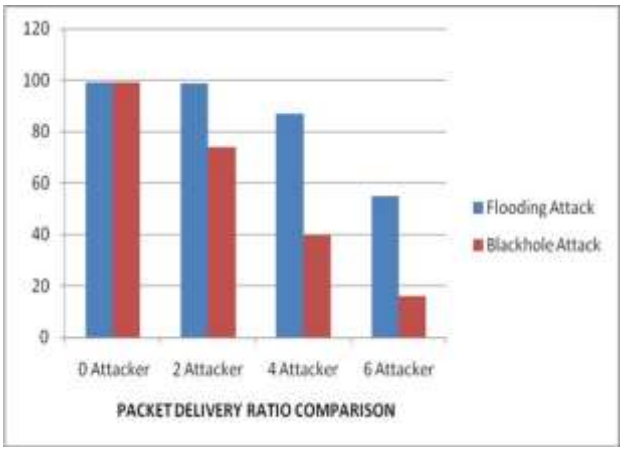

Fig 2: Packet Delivery Ratio for AODV Protocol with Black Hole Node/Flooding Node

3) End to End Delay (E2E delay)

It refers to the time taken for a packet to be transmitted across a network from source to destination. This metric includes all possible delay that may be caused by buffering during route discovery, propagation and transfer time etc. The results of the simulation show that the end to end delay keeps on increasing as the number of attacker nodes are increased in the network. The attacker nodes exist in the network drop the packets and hence a retransmission is required. As such nodes are increased in the network the probability of the packet being getting dropped also increases thus more and more retransmission are required and thus increasing the overall end to end delay with the increase in attacker nodes.

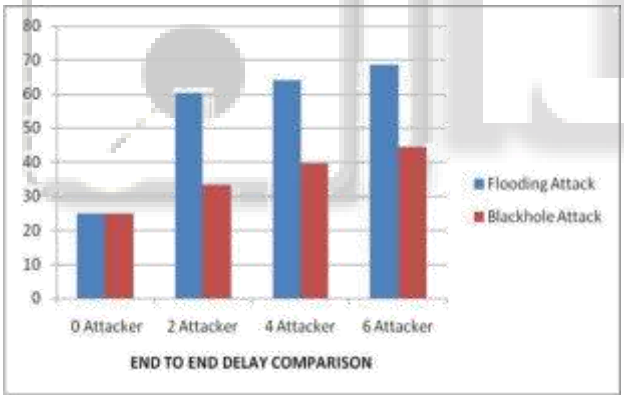

Fig 3: End to End Delay for AODV Protocol with Black Hole Node/Flooding Node

VI. CONCLUSION

Security of MANET is the most important features for its deployment. In this paper, we analysed the impact of Black hole attack and Flooding attack with respect to the performance parameters like throughput, PDR and end to end delay. We have analysed that vulnerability of the protocol AODV has more severe effect when the number of black hole nodes is increased. We have shown in simulations that the all these parameters with the Black hole attack and Flooding attack in the network decreases. But we conclude from our study that the performance of the network degrades to a much higher extent in the presence of Black hole attack as compared to Flooding attack.

REFERENCES

[1] Soufiene Djahel, Farid Naıt-abdesselam, and Zonghua Zhang, "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges", IEEE communications surveys & tutorials, vol. 13, no. 4, fourth quarter 2011.
[2] www.ebookbrowse.com , www.docstoc.com
[3] Monika Roopak, Proff. BVR Reddy, "Blackhole Attack implementation in AODV Routing Protocol", International Journal of Scientific & Engineering Research, Vol. 4, Issue 5, May-2013.
[4] Mr. L Raja, Capt. Dr. S Santhosh Baboo, "Comparative Study of Reactive Routing Protocol (AODV, DSR, ABR and TORA) in MANET", International Journal of Engineering and Computer Science , Vol. 2, Issue 3 March 2013.
[5] Priyanka Goyal, Vinti Parmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.
[6] Anuj Gupta, Navjot Kaur, Amandeep Kaur, "A Survey on Behaviour of AODV and OLSR Routing Protocol of MANETs under Black Hole Attack", IJCST Vol. 2, Issue-4, Oct - Dec. 2011.
[7] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012.
[8] Akshai Aggarwal, Savita Gandhi, Nirbhay Chaubey, Naren Tada, Srushti Trivedi, "NDTAODV- Neighbour Defense Technique for AODV to Mitigate Flood Attacks in MANETS", International Journal of Computer Networks & Communications (IJCNC) Volume-6, No.1, January 2014.
[9] 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 Science & Technology Research, Volume-2, Issue-7, July 2013.
[10] Adnan Nadeem, Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Comm. Surveys & tutorials, Vol. 15, No. 4, Fourth Quarter 2013.
[11] Jiajia Liu, Xiaohong Jiang, Hiroki Nishiyama, Nei Kato, "Throughput Capacity of MANETs with Power Control and Packet Redundancy", IEEE Transactions on wireless communications, Vol. 12, No. 6, June 2013.

All rights reserved by *www.ijsrd.com*