Performance Evaluation of AODV under Black Hole Attack in MANET using NS2

Dansingh Pradhan
B115025
Department of CSE
IIIT Bhubaneswar
b115025@iiit-bh.ac.in

Govind Rajendran
B115027
Department of CSE
IIIT Bhubaneswar
b115027@iiit-bh.ac.in

Franco Ekka
B115029
Department of CSE
IIIT Bhubaneswar
b115029@iiit-bh.ac.in

Aamaan Asif
B315061
Department of CSE
IIIT Bhubaneswar
b315061@iiit-bh.ac.in

ABSTRACT

Mobile ad hoc network(MANET)is a wireless infrastructureless network connected through a mobile device where the nodes connecting to this network does not requires to have the information about the network parameters before it is connected. Each node has the independence to move in any direction and start a network by connecting with other nodes. Devices connected in a MANET works as a router and should forward its data packets between the network. This type of network can be operated by themselves or by connecting to a larger internet where it may contain multiple transreceivers between nodes. As MANET is a wireless network it makes it more vulnerable than any wired network. Missing or absence of any part of the system can cost a huge risk to the network. Security of this network is very challenging and to have a safe and secure network there should be a good knowledge and understanding of possible forms of attack that can happen. In black hole attack, the malicious node spoofs it's identity and connects with the network. After the connection it starts misbehaving by it's actions while exchanging information. Instead of forwarding the routing packets to its neighbouring nodes it drops the packets which degrades the network communication between the nodes. Keywords- MANET; Mobilenode;Router; Routingprotocol;

1. INTRODUCTION

In our paper, we focused on the performance of AODV routing protocol between source node and destination node when there is a Black Hole attack in MANET.NS2 is used for the simulation and performance evaluation of routing.

Ad-hoc On Demand Distance Vector(AODV) is a reactive protocol which means whenever a node wants to send data to another node a route is constructed from source node to destination node. It does not go for any route searching if there is no data transfer between nodes. This routing protocol is very popular and widely used because of its on-demand establishment of routes and destination sequence number to determine the updated path to a destination. Route discovery mechanism of AODV are Route Request(RREQ) and Routing Reply(RREP).

RREQ: RREQ(Route Request) is a message broadcasted into the network which contains detail information on the path to get the node. This is done by keeping an ordered list of all the nodes it took to reach the current destination. It also contains details of the initial source and destination.

RREP: When the RREQ finally reaches the intended destination node, it sends a message to the source that the path has been found. The RREP(Routing Reply) message reaches the intended destination just by simply backtracking the RREQ list till it reaches the source.

HOP COUNT: Data passes through a number of nodes(Routers , Hub ,Bridges). To reach the intended destination and passing through each node is associated with a wait time and delay. Every time data passes through a node we call it hop. So a Special 8 Bit of data is reserved to mark the total number of hops known as Hop Count. It has maximum value of 225 and is decremented every time a hop occurs (Also known as TIME TO LIVE(TTL)).This is done so that in case of a networking failure the packet of data is not just bouncing around from node to node.

1.1 NETWORK SIMULATOR

We use NS2 to simulate wired or wireless network protocol(UDP , TCP) and study the behavior of those protocols.

NS2 provide us ns executable command which take TCL script language as input and gives a simulation trace file as output . The output is shown through animation using NAM or graph using Xgraph.

NS-2 has great advantages such as it is cheap , Complex scenarios can be easily tested . Results can be quickly obtained – more ideas can be tested in a smaller time frame . It supports various kinds of protocol such as AODV , DSDV

and many others ,Supported across various platforms such as Windows , Linux . NS-2 is highly modular and Popular

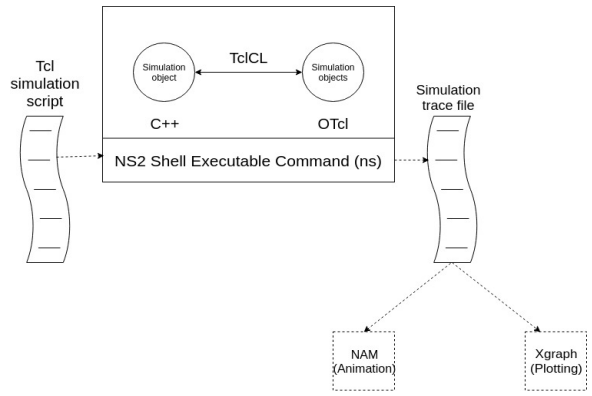

Figure 1: Architecture of NAM.

2. ATTACKS IN AD HOC NETWORKS

Attacks in Ad hoc network are mainly done to alter packets or drop packets or retransmit packets from the sender . As Ad hoc network are wireless , so Attacks in Ad hoc network are easy compared to wired network , Here attacker becomes invisible and just need to be in the range of the network to provide malicious node or make nodes malicious already present in the network . Two type of attack .They are:

1)External attack: Here external node is provided which interrupt in packet transferring in network. It spoof the start node that it has a better route to the destination and when packet is reached there it drop or alter those packets. ex :-Dos attack, Message Bombing etc.

2)Internal attack. Here the malicious node is the node already present in the network. At First it helps in transferring packets between network and after some time it misbehaves and then start in dropping packets.

3. BLACK HOLE ATTACKS

A sequence number is a number associated with the each entry in the routing table, Higher priority sequence numbers have higher priority ie they imply that they have a more up-to-date path to the destination, the sequence number of incoming RREQ is compared with the intermediate node's sequence number to determine the shortest path.

MANET network is capable of changing its structure and is made of multiple mobile infrastructures, further all of the transmissions take place in a wireless medium this places a serious threat of interception of data by malicious nodes that were not a problem in previous wired networks(as there is a fundamental difference of static spine as compared to the dynamically changing topology that the ad-hoc network was designed for).A node in a ad-hoc network can be a computer, a router or even a switch.

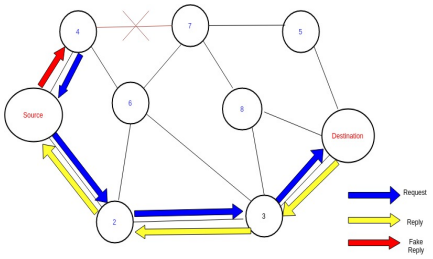

Figure 2: Black hole attack

A malicious or misbehaving node does not do its normal function of forwarding data packets to intended destination rather drops the packets of data of performs an man-in-the-middle-attack .

Man in the middle attack is where an attacker intercepts the data transmission between source and destination ,The attacker can choose to relay the message by modifying it or even keeping a copy of he essential data.

Ad-hoc networks are popularly used in military purposes and personal area networks due to is dynamic nature but he above attacks can compromise data and privacy of the message a black hole attack is when an malicious node brings it self into the path of transmission of the data so it can execute an denial of service attack and man in the middle attack .It achieves this by changing the parameters such as sequence numbers and hop count. When a RREQ message is received by the compromised node it disguises itself as the having a fresh route to the destination and now receives data from the source which can be forwarded of dropped based on frequency of packets received or a fixed time interval.

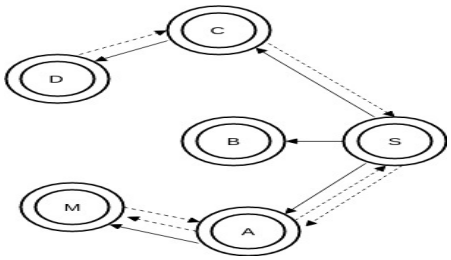

Figure 3: example of Black hole attack and its effect on the network

4. ANALYSIS OF BLACK HOLE ATTACK

Analysis of Black hole attack was done by entering malicious nodes in the network . and different parameters were analyzed such as Packet Delivery ratio, Packets dropped and Throughput .

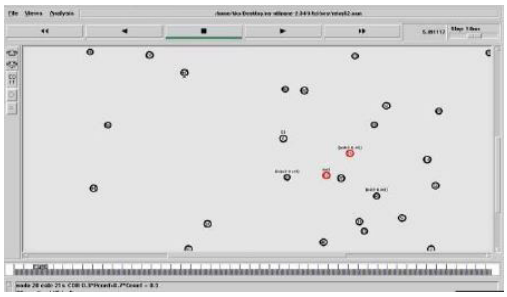

Figure 4: Network containing 2 malicious nodes

5. PERFORMANCE METRICS

Typically, the body of a paper is organized into a hierarchical structure, with numbered or unnumbered headings for sections, subsections, sub-subsections, and even smaller sections.

5.1 PACKET DELIVERY RATIO (PDR)

It is the ratio of number of packets reaching the destination to the number of packets sent from the source node.

lets say ,

PDR :- Packet delivery ratio

pr :- Sum total of all the packets reached the destination

sr :- Sum total of all the packets sent from the source

So,

PDR = pr/sr

No of nodes in network	PDR for 0 malicious node	PDR for 1 malicious nodes
6	93.18	75
15	17.2	7.82

Table 1: PDR for zero and one malicious nodes

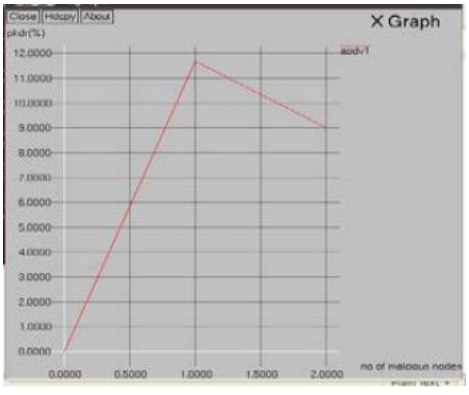

Figure 5: Graph depicting Packet delivery ratio in the presence of malicious nodes

5.2 PACKETS DROPPED

Packets dropped is the count of number of packets that do not reach the destination

lets say ,

pd :- packets dropped

ps :- number of packets send from the source

pr :- number of packets that actually reached the destination

So,

pd = ps - pr

No of nodes in network	packets dropped for 0 malicious nodes	packets dropped for 1 malicious nodes
6	12	44
15	32	57

Table 2: Packets dropped by zero and one malicious nodes

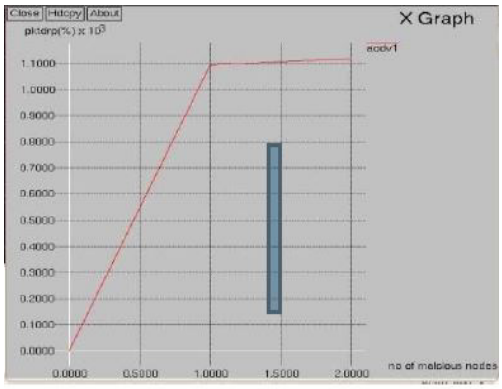

Figure 6: Graph depicting packets dropped in the presence of malicious nodes

5.3 THROUGHPUT

It can be defined as the average number of packets being received by the destination per second

lets say ,

tput :- throughput

rp :- packets received

ts :- time required for simulation

So,

tput = rp/ts

No of nodes in network	Throughput for 0 malicious nodes	Throughput for 1 malicious nodes
6	243	196
15	34	23.62

Table 3: Throughput for zero and one malicious nodes

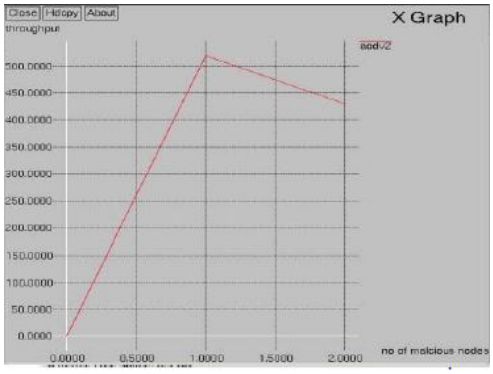

Figure 7: Graph depicting throughput in the presence of malicious nodes.

6. CONCLUSIONS

Black hole attack are very dangerous for network , since the efficiency of network degrades with the income of malicious node in the ad-hoc network. The sending of packets is hampered very heavily due to Black Hole attack.

Black hole attack is one of the severe security threats in Ad-hoc networks which can be easily employed by exploiting vulnerability of on-demand routing protocols such as AODV.

Performance parameters of the network can be improved such as throughput and PDR(packet delivery ratio) can be increased packet drop rate can be reduced greatly by using the following techniques . IDAD (Intrusion Detection using anomally) to prevent Black Hole attacks imposed by both single and multiple malicious nodes . Apart from that several new threshold - based black hole attack prevention method can be employed to increase the efficiency of the network.

Another detection technique is by using Intrusion Detection System (IDS) that uses data mining techniques for the detection of a Denial of service (DOS) attack , the so called Black hole attack.

References

1. Nadia Boumkheld , Mounir Ghogho , Mohammed El Koutbi . Intrusion detection system for the detection of blackhole attacks in a smart grid. *DOI - 10.1109/ISCBI.2016.7743267*. IEEE , Olten, Switzerland, *Date Added to IEEE Xplore* - 17 November 2016 , *Date of Conference* - 5-7 Sept. 2016 .

2. Taku Noguchi , Takaya Yamamoto . Black hole attack prevention method using dynamic threshold in mobile ad hoc networks. *DOI: 10.15439/2017F101*. IEEE , Prague, Czech Republic, *Date Added to IEEE Xplore* - 13 November 2017 , *Date of Conference* - 3-6 Sept. 2017.

3. Yibeltal Fantahun Alem , Zhao Cheng Xuan . Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection. *DOI: 10.1109/ICFCC.2010.5497455*. IEEE , Wuha, China , *Date Added to IEEE Xplore* - 28 June 2010 , *Date of Conference* - 21-24 May 2010.

4. Gayatri Bendale , Sameeksha Shrivastava . An improved blackhole attack detection and prevention method for Wireless ad-hoc Network. *DOI: 10.1109/ICTBIG.2016.7892702*. IEEE , Indore, India , *Date Added to IEEE Xplore* - 06 April 2017 , *Date of Conference* - 18-19 Nov. 2016.

5. Monika Y. Dangore , Santosh S. Sambare . Detecting and Overcoming Blackhole Attack in AODV Protocol. *DOI: 10.1109/CUBE.2013.23*. IEEE , Pune, India , *Date Added to IEEE Xplore* - 09 January 2014 , *Date of Conference* - 15-16 Nov. 2013.