Detecting and Isolating Malicious Node in AODV Routing Algorithm

Priyambada Sahu
Assistant Professor
C.V Raman Computer Academy
Bhubaneswar,Odisha

Sukant Kishoro Bisoy
Assistant Professor
C.V Raman College Of Engineering
Bhubaneswar,odisha

Soumya Sahoo
Assistant Professor
C.V Raman College Of Engineering
Bhubaneswar,odisha

ABSTRACT

A Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without using any centralized access point, infrastructure, or centralized administration. In MANET, Ad-hoc On-Demand Distance Vector (AODV) floods the control packets to discovery the route. Generally there is a limit on the number of these packets that can be generated or forwarded. Malicious node can disregard this limit and flood the network with fake control packets so that these packets have the limited bandwidth and processing power of genuine nodes in the network while being forwarded. Due to this, genuine route requests suffer and many routes either do not get a chance to materialize or they end up being longer than otherwise. This paper presents a simulation analysis of reactive routing protocol AODV in the presence of malicious attack under different Load. We present the simulations results based on packet delivery fraction, throughput, normalized routing load, and packet loss.

General Terms

AODV, Throughput, Normalized routing load, Packet loss, malicious node

Keywords

MANET, DSDV, AODV, PDF, NRL, NS2

1. INTRODUCTION

A MANET is a collection of mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration. Routing is a critical issue in MANET and hence the focus of this thesis along with the performance analysis of routing protocols. Different routing protocols are used in ad hoc wireless networks to update the routing information. Proactive (or table driven), reactive (on demand) and hybrid routing protocols are used for ad hoc wireless networks. Ad hoc on-demand distance vector (AODV) routing[1] , dynamic source routing (DSR) [2] and Destination sequence vector routing (DSDV) [3] protocols are the important routing protocols for ad hoc wireless networks. However, ensuring security in such networks is a big challenge because of the distributed nature of these networks and the assumption of mutual trust among participants. A broad overview of the security issues involved in Ad-hoc networks has been provided in [4]. Both data packets and control packets, as used by the routing protocol, are vulnerable to attacks.

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. Through simulation this paper shows that, under malicious attack the performance of AODV protocols decreses with the increase of number of malicoius node

2. PROBLEMS DUE TO ROUTE REQUEST FLOODING

Routing in MANET means to choose a right and suitable path from source to destination. Routing terminology is used in different kinds of networks such as in telephony technology, electronic data networks and in the internet network. Here we are more concern about routing in mobile ad hoc networks. AODV facilitates route formation using control messages RREQ (route request) and RREP (route reply). Each time a data packet is to be delivered by a node, the node checks whether it has a route to the destination. If it does not have a route, then a RREQ is broadcast to the neighbors. The neighbors rebroadcast the packet if they do not know the destination. In order to control the number of RREQ packets generated by a node, the AODV protocol put a restriction on parameter RREQ_RATELIMIT[5]. However, a malicious node can choose not to observe this limit and flood the network with a large number of fabricated RREQ packets which keep getting forwarded. This process continues, allowing the fake RREQ packets to propagate through the network. As the number of fabricated RREQ packets sent by the malicious nodes increases, the other nodes in the network use up their RREQ_RATELIMIT in forwarding these while other genuine RREQ packets are dropped.

The phenomenon explained above has various side effects ranging from inefficient routing to complete blocking of route formation. The route forming process is disrupted severely in the vicinity of the malicious node and the impact decays slowly as we move away from the malicious node. The fabricated RREQ packets to be processed at a given node outnumber the genuine RREQ packets, which increases the probability of the non-malicious RREQ not being forwarded because of the RREQ_RATELIMIT constraint. The non-malicious nodes do not form routes at all or end up forming longer routes as they try to avoid the high contention region near the malicious node [6].

Thus the effects of flooding [7] can be summarized as follows:

- Wastage of memory while maintaining routing table entries for malicious requests
- Wastage of battery power
- Denial of service to genuine nodes

- Creation of longer routes where short ones could have been possible leading to reduced throughput
- Consumption of limited processing power

It thus becomes very important to avoid or at least contain such flooding attacks so as to allow genuine routes to be formed in the network and also to conserve the limited resources available to the mobile nodes.

3. DETECTION OF MALICIOUS BEHAVIOR

In AODV routing protocol a malicious nodes can easily disrupt the communication. A malicious node that is not part of any route may launch Denial of Service (DOS) Attack. Also once a route is formed, any node in the route may turn malicious and may refrain from forwarding packets, modify them before forwarding or may even forward to an incorrect intermediate node. Such malicious activities by a misbehaving node cannot be checked for in pure AODV protocol [6].

During the judgment process the neighbors send their opinion about a node. When the node collects all opinions of neighbors, it decides about honesty of reply's sender node. The decision is based on the following rules which are used to judge about honesty of a node.

Steps to judge an honesty node

Rule 1: If a node delivers many data packets to destinations, it is assumed as an honest node.

Rule 2: If a node receives many packets but do not sent same data packets, it is possible that the current node is a misbehavior node.

Rule 3: When the rule2 is correct about a node, if the current node has sent number RREP packets; therefore surely the current node is misbehavior.

Rule 4: When the rule2 is correct about a node, if the current node has not sent any RREP packets; therefore the current node is a failed node.

In this paper, a proactive scheme is proposed to detect the above-mentioned malicious activities. A malicious node flooding the network with fake control packets, such as RREQs (Route Requests) causes congestion in the network. The processing of RREQ by the nodes in the network leads to further degradation in performance of the network. This abnormal behavior is handled in our scheme by ensuring a fair distribution of resources among all contending neighbors. Incoming RREQs are processed only if number of RREQs from the said neighbor is below RREQ ACCEPT LIMIT. This parameter specifies a value that ensures uniform usage of a node's resources by its neighbors. Another threshold RREQ BLACKLIST LIMIT determines whether a node is acting malicious or not. If the number of RREQs goes beyond RREQ BLACKLIST LIMIT then the node is blacklisted and all requests from it are blocked temporarily. Thus isolating the malicious node. Tampering of packets by a malicious node in the route can be detected by promiscuous listening by the other nodes that are part of the route. This type of moral policing, done by the nodes, ensures detection of any malicious activity taking place. To facilitate detection, extra information regarding route is exchanged while route formation. To provide security to it, promiscuous listening is proposed during the route formation also. Malicious nodes can easily disable RREQ_RATELIMIT and send out as many RREQ packets as possible. Not much can be done to stop the malicious node from doing this. However, the neighbors of this malicious node can work to control the number of fake RREQ packets that are sent, thus preventing the flood from crossing further hops.

4. ALGORITHM TO ISOLATE MALICIOUS NODE

Let L is the maximum limit each node having.

i.e L= RREQ_RATELIMIT

LT= RREQ_ACCEPT_LIMIT

M= RREQ_BLACKLIST_LIMIT

Upon the receiving the RREQ by a neighbor

Increment *rreq_count* for that neighbor

If rreq_count < LT

Process the RREQ

Else

If rreq_count > M

Black list the specifi node and declares it is malicious node

If the node behaves as malicious

Drop the data packets received by the malicious node.

Else

If the rreq_count > L

Ignore all route requests

Explanation of above algorithm.

Step 1: Source node sends the RREQ to the next neighbor node. If the route is found sends a RREP to the source node.

Step 2: if the route is established then source node sends data packet to the next node.

Step 3: if the intermediate node is a malicious node it will drop the packets which it receives from the neighbor node.

Step 4: The malicious node may send the fake RREQ to other nodes. So stop fake route request by ignoring the RREQ from the malicious node

5. PERFORMANCE METRICS

The following performance metrics are used to compare the performance of the routing protocols in the simulation:

Throughput: It is the amount of data per time unit that is delivered from one node to another via a communication link[9]. Throughput is expressed as bytes or bits per sec (byte/sec or bit/sec).

*Throughput = (Number of data packets Received * Packet size * 8) /Simulation Time*

Packet Loss: Mobility-related packet loss may occur at both the network layer and the MAC layer. In this work, packet loss concentrates for network layer.

Packet loss = Data Packet Sent – Data Packet Rec

Packet delivery ratio(PDF): it is ratio between number of packets received by destination and number of packet originated by application (CBR).

*PDF = (Data Packet Received / Data Packet Sent) * 100*

Normalized Routing Load (NRL): The number of routing packets transmitted per data packet delivered at the destination. This metric gives an idea of the extra bandwidth consumed by overhead to deliver data packet.

*NRL=((cp_sent + cp_forw) /DataAgtRec)*100*

cp_sent = rreq + rrep + rerr;

cp_sent =Controll Packets sent

cp_forw=Control packet forwarded

DataAgtRec=Datapacketsreceived

rreq= route request

rrep=route reply

rerr=routeerror

6. SIMULATION SCENARIO

We conducted the performance evaluation using the ns-2 simulator [8]. We adopted the "Random way-point" model to simulate nodes movement. Each node starts moving at random speed from its initial position to a random target position selected from within the simulation area. The speed is uniformly distributed from (0 to Vmax], where Vmax is the maximum speed of the simulation. When a node reaches the target position, it waits for a pause time period, and then selects another random target location and moves again. Therefore, we can simulate node mobility by varying the maximum speed and pause time.

For the simulations, 20 nodes were initially positioned at random locations over 1000 m x 1000 m area. After that 40, 60, 80 and 100 number of nodes have been created for the simulation. Each simulation is 120 seconds long. We have created 2, 4, 6, 8, 10 numbers of malicious nodes in the network. Additionally, every node has a radio range of 250 meters and the IEEE 802.11 WLAN MAC protocol was used. The parameter used in the simulation is shown in table-1. We modified aodv.cc file to implement our malicious node attack. For those two malicious nodes is created for our network. The basic goal of our malicious node is to drop the packet so that there do not have any communication between source and destination. We added following things to modify our code.

```
// if I am the malicious node
if (malicious == true ) {
drop(p, DROP_RTR_ROUTE_LOOP);
// DROP_RTR_ROUTE_LOOP is added for no reason.
}
```

Table-1: PARAMETER USED IN SIMULATION

PARAMETER	VALUE
Channel type	Wireless channel
Number of nodes	20,40,60,80,100
Pause time	10 Sec
Traffic type	CBR
Data Payload	512 bytes/packet
MAC Types	802_11
Node Placement	Random
Mobility	Random way point
Transmission range	250m
Speed	0-20 m/s
Area of simulation	1000m X 1000m
Seed	1
Number of Maliciuos attacks	2, 4, 6, 8, 10
Time of simulation	120 msec.

7. RESULT ANALYSIS

In this an attempt has been made to find impact of malicious node in AODV routing protocol under different density of node with number of malicious attack. Inorder to find the performance of AODV under malicious attack we designates few nodes as malicious node. Initialy we measure throughput, packet delivery ratio (PDR), packet drop and normalized routing load (NRL) by varying number of nodes. So we fix the number of malicious node to 6 and pause time 20 m/s. Fig. 2 indicates that throughput of AODV routing protocol increases with increase of number of nodes. But under malicious attacks throughput of AODV is less as compared to normal AODV.

As Fig.3 suggest, under attack PDR of AODV limits to 84 - 92% but PDR increases for both with increase of number of nodes. AODV drops more packets under malicious attacks as compared to normal under varying number of nodes (see Fig.3).

It is concluded from Fig.4 that normal AODV (without malicious attack) have more NRL as compared to AODV with malicious attack because under attacks it does not allow the more packets to pass to their neighbor nodes.

Then we measured PDR and packet drop of AODV protocol by implementing 2, 4, 6, 8 and 10 nodes as malicious node. As Fig. 5 and Fig. 6 indicates PDR of AODV decreases drastically with the increses of number of malicious node and drops more packets because it doesn't allow the packet to flow further.

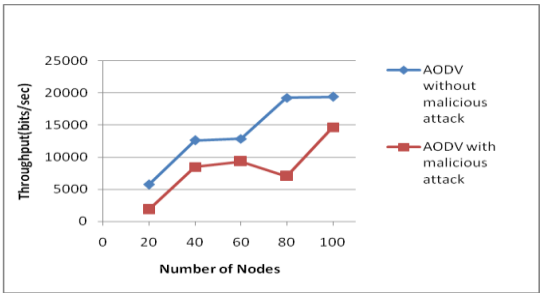

Fig. 1: Throughput of AODV with and without malicious attack

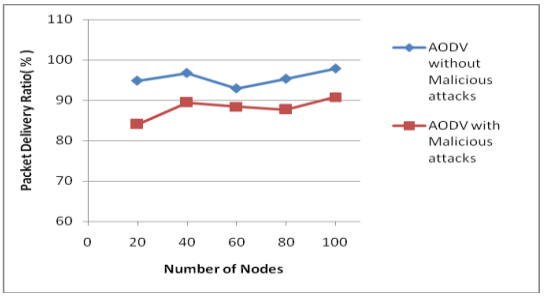

Fig. 2: Packet Delivery Ratio of AODV with and without malicious attack

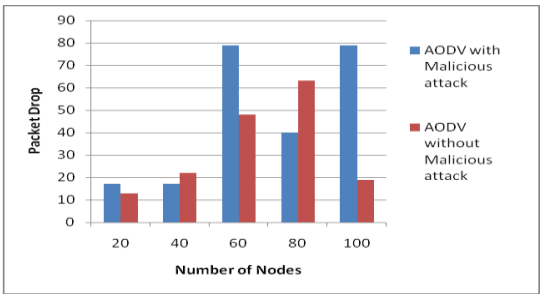

Fig. 3: Packet Drop of AODV with and without malicious attack

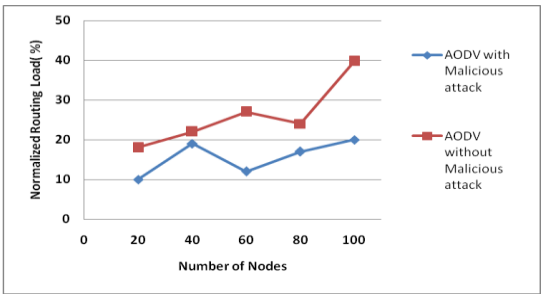

Fig. 4: Normalized Routing Load of AODV with and without malicious attack

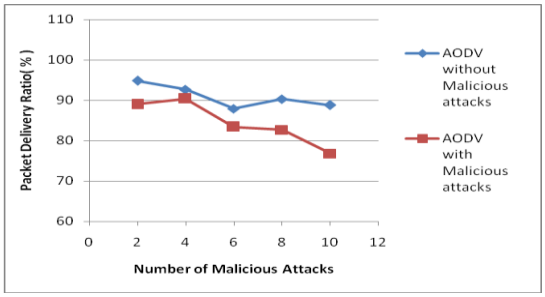

Fig. 5: Packet Delivery Ratio of AODV under Number of malicious attack

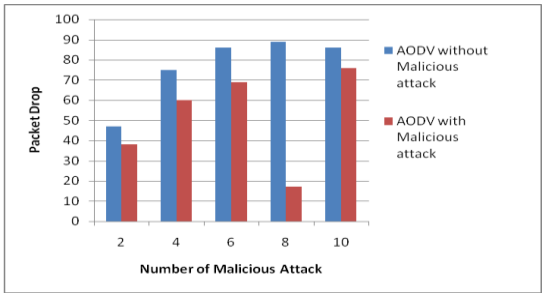

Fig. 6: Packet Drop of AODV under Number of malicious attack

8. CONCLUSION

Security is an essential requirement in mobile ad hoc network (MANETs). Malicious attack will disrupt the performance of the network almost completely which may not forward any traffic at all to neighbor node. So detection of the malicious node and isolation of malicious node will stop sending fake request call. In this an attempt has been made to find impact of malicious node in AODV routing protocol under different density of node with number of malicious attack. Result shows that throughput and packet delivery ratio of normal AODV is much better than AODV with malicious attack. Under malicious attack AODV drops more packets with increase of number of attacks. It is found that performance of routing protocol (AODV) degrades by introducing malicious nodes but have less routing overhead as compared to normal AODV.

9. REFERENCES

[1] C. Perkins, E. Royer, "Ad-hoc On-Demand Distance Vector Routing", Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications, 1999, pp. 90-100.

[2] D. Johnson, D. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless Networks", Mobile Computing, Editors: T. Imielinski and H. Korth, pp. 153 – 181, Kluwer, 1996.

[3] C. Perkins, P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers", in: ACM SIGCOMM_94 Conference Communications Architectures, Protocols and Applications, 1994, pp. 234–244.

[4] P. Ning, K. Sun, "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad hoc Routing Protocols", Proceedings of the 2003 Annual IEEE Information Assurance Workshop, June, 2003, pp. 60 – 67.

[5] Perkins C.E., Terminology for Ad-Hoc Networking, Draft-IETF-MANET-terms-00.txt, November 1997.

[6] Sugata Sanyal, Ajith Abraham, Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia and Nirali Mody, "Security Scheme for Malicious Node Detection in Mobile Ad Hoc Networks", 6th International Workshop on Distributed Computing (IWDC-2004), A. Sen et al (Eds.), Springer Verlag, Germany, Lecture Notes in Computer Science, Vol. 3326, ISBN: 3-540-24076-4, pp 541-542, 2004

[7] Jayesh Kataria, P.S. Dhekne, and Sugata Sanyal, "A Scheme to Control Flooding of Fake Route Requests in Ad-hoc Networks", International Conference on Computers and Devices for Communications, CODEC-06, December 18-20, 2006, Kolkata, India.

[8] The network simulator—ns-2. Available from http://www.isi.edu/nsnam/ns/

[9] Z.Alexander, Performance Evaluation of AODV Routing Protocol: Real-Life Measurements, SCC,June 2003.