Performance Analysis of Secure AODV Routing in Mobile Ad-hoc Networks

Pallavi[1], Pooja Saini[2]
[1] Ambala College of Engineering and Applied Research/Computer Science, Ambala, India
[2] Ambala College of Engineering and Applied Research/Computer Science, Ambala, India

***ABSTRACT*- Wireless Mobile Ad Hoc Network is widely used network today but it suffers from various security problems like Worm Hole, Black Hole, Flooding, Sybil, Spoofing etc. These security problems can interrupt the operations of entire network and thus degrade the performance of the network in terms of Throughput, Packet delivery ratio, End to End delay, Routing Load, Bandwidth consumption. So there is a need to protect the network from these attacks. In this paper, we will review the black hole and flooding attack over the mobile ad hoc network and consider their impact over the network performance metrics Throughput and Packet delivery ratio.**

***Keywords*-** MANET, Black Hole, Wireless Security.

I. INTRODUCTION

Ad hoc networks are vulnerable to attacks due to many reasons. Amongst them are the absence of infrastructure, wireless links between nodes, limited physical Protection, and the Lack of a centralized monitoring or management, and the resource constraints. Goal of security is to provide security services to defend against all the kinds of threat explained in this chapter. Security services [1] include the following:

1) *Authentication:* ensures that the other end of a connection or the originator of a packet is the node that is claimed.
2) *Access control:* prevents unauthorized access to a resource.
3) *Confidentiality:* protects overall content or a field in a message. Confidentiality can also be required to prevent an adversary from undertaking traffic analysis.
4) *Privacy*: prevents adversaries from obtaining information that may have private content.
5) *Integrity:* ensures that a packet is not modified during transmission.
6) *Authorization:* authorizes another node to update information (import authorization) or to receive information (export authorization).
7) *Non-repudiation:* proves the source of a packet. Non-repudiation prevents the source from denying that it sent a packet.

Security issues in Mobile Ad Hoc Networks are as follows:

1. Minimizing resource consumption and maximizing security performance.
2. Network deployment renders more link attacks ranging from passive eavesdropping to active interfering.
3. In-network processing involves intermediate nodes in end-to-end information transfer.
4. Wireless communication characteristics render traditional wired-based security schemes unsuitable.
5. Node adding and failure make the network topology dynamic [1].

Security Attacks on Mobile Ad Hoc Networks

i. Passive Attacks

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of preventing such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard [1, 2].

ii. Active Attack

An active attack attempts to alter or destroy the data being exchanged in the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks [1, 2]. Black hole attack falls in this category.

In a black hole attack[3,4], a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic [5].

II. LITERATURE REVIEW

Various methods have been developed by different researchers to protect the network from Blackhole. Now we will discuss the recent solutions offered by researchers for this kind of attack.

Tan.S [6] proposed a Secure Route Discovery for the AODV protocol (SRD-AODV) in order to prevent black hole attacks. This mechanism requires the source node and the destination node to verify the sequence numbers in the Route Request (RREQ) and Route Reply (RREP) messages, respectively, based on defined thresholds before establishing a connection with a destination node for sending the data. Results show an improvement in the ratio of packet delivery for three different environments using our mechanism as compared to the standard AODV protocol.

Bindra G.S [7] proposed a mechanism to detect and remove the blackhole and grayhole attacks. They offered a solution for these attacks by maintaining an Extended Data Routing Information (EDRI) Table at each node in addition to the Routing Table of the AODV protocol. The mechanism is capable of detecting a malicious node. It also maintains a history of the node's previous malicious instances to account for the gray behavior. Refresh packet, Renew Packet, BHID Packet, Further request and further reply packets are also used in addition to the existing packets (RREQ and RREP). Our technique is capable of finding chain of cooperating malicious nodes which drop a significant fraction of packets.

Soni S.J et al. [8] presented a novel security mechanism that integrates digital signature and hash chain to protect the AODV routing protocol that is capable of defending itself against both malicious and unauthenticated nodes with marginal performance difference. The proposed security mechanism was also simulated in the Network Simulator 2 (NS2) to show marginal performance difference under attack.

Kshirsagar D. et al., [9] proposed a method to detect and prevent Blackhole attack by real time monitoring suspected node by its neighbor node. AODV routing protocol is modified to simulate the detection and prevention method. Node which replies to RouteRequest (RREQ) by source is monitored in promiscuous mode. Neighbor node of RouteReply (RREP) sender node is actually detecting malicious node.

Dangore, M.Y. [10] studied the effect of black hole attack in AODV based network. The network parameters like Throughput, Packet Delivery Ratio and Average End to End Delay are calculated for normal network (without black hole) and a network with one black hole. After detecting the black hole attack in order to resume data transmission, the black hole node is bypassed and the route to the genuine destination is resumed again. The performances of network parameters are compared in all the three scenarios.

III. PROBLEM FORMULATION

MANET is the networks of mobile nodes with limited resources like computation power, communication range and storage capabilities, shared channel, usually for economical reasons. Nodes can join and leave the network any time. So if any malicious node joins the network then it is very difficult to trace that node which greatly affects the security of the network. So it is necessary to detect and isolate that node from entire network for smooth operations. To secure the communication over MANETs there must be a method which can ensure the detection and prevention from the attacks like Black Hole. Here, we will develop a method which can prevent the network from this attack by identifying the malicious nodes using sequence numbers.

IV. PROPOSED SCHEME & ENVIRONMENT

In our proposed scheme, receiver monitors the sequence number in the packet against a sequence number threshold. If current sequence number is much higher than the expected sequence number then, receiver start a filter to trace all the sequence number in network and finally nodes do not respond, if they receive the packet which is quite higher than the expected threshold. The idea can be explained by the following steps:

Proposed Algorithm:

```
While(communication)
    If filter is false, network is open to attack
        If there is any change in the seq. no, change the counter value
    Else filter is true then ignore the request and reply that having unexpected seq. no. and finally update the routing table information.
```

We are considering the wireless environment having 30 nodes arranged in the area 1200*1200. Omni directional antennas are used for the transmission of 1000 bytes packets. CBR traffic type is used.

Here, we are taking three scenarios one for AODV without attack with 30 nodes, second for AODV with Blackhole attack having 1 selfish node and third for AODV with Blackhole attack Prevention with 1 selfish node.

The parameters for the implementation of these scenarios in ns2 are shown in Table 1 below:

Parameter	Value
Simulator	Ns2
Routing Protocol	AODV
Channel	Wireless
No. of Nodes	30
Topology Dimension	1200m*1200m
Traffic Type	CBR
Mac Type	802.11 MAC Layer
Packet Size	1024 bytes

Antenna Type	Omni Direction
Interface Queue Type	Droptail
Selfish Node	1
Node Placement	Random
Simulation Time	10ms

Table 1: Simulation Parameters

V. Results And Discussion

For the first scenario, two dimensional XGraph is drawn. Along Y axis, the packet lost and received parameter is taken and along X axis, time is taken. In the following graph green line show the Packet loss and red line show the Packet received during the transmission.

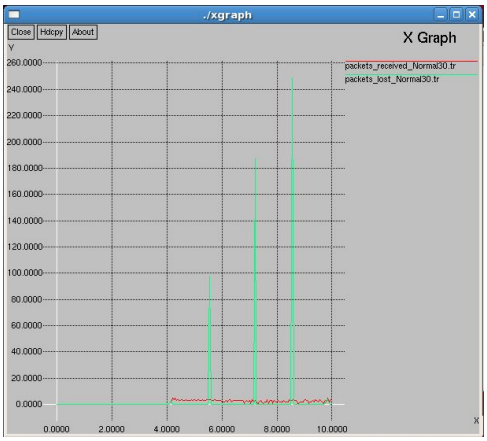

Figure 1 : Performance of AODV without attack

Fig. 2 shows the network performance under blackhole attack. In this graph, packet loss ratio is increased and thus degrades the PDR and throughput.

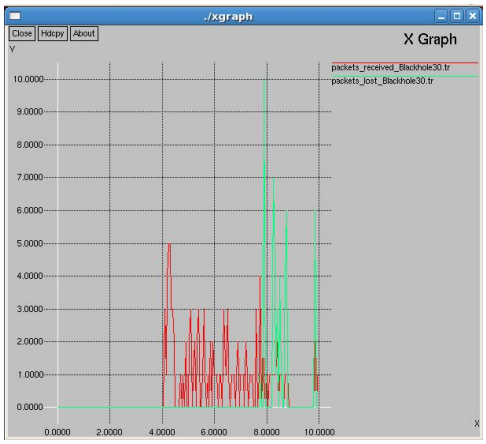

Figure 2: AODV Performance under Blackhole Attack

After applying the above mentioned algorithm, packet loss ratio is reduced which is shown in Fig. 3 and thus improves the network throughput and PDR.

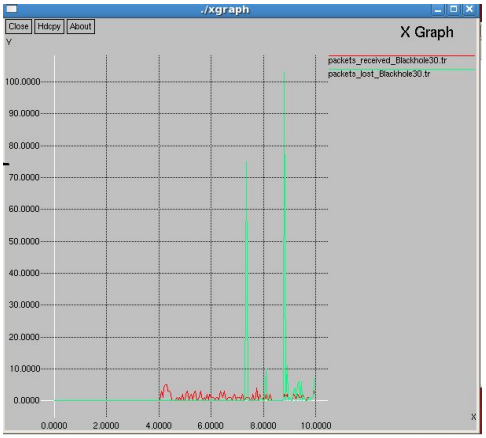

Figure 3: AODV performance after recovering from Blackhole Attack

Protocols	Received (Packets/Second)	Sent (Packets/Second)
AODV(Without attack)	540	806
AODV(With Blackhole attack)	340	806
AODV(With Blackhole Attack Prevention)	349	806

Table 2: Total packets Sent/Received

Protocols	Throughput	PDR
AODV (Without Attack)	54	66.99751861
AODV (With BlackHoleAttack)	34	42.18362283
AODV (With BlackHoleAttack Preventation)	34.9	43.30024814

Table 3: AODV performance

When there is only one attacker node present in the network then Simulation results are shown by Throughput and Packet Delivery Ratio graphs.

Throughput: It refers to how much data can be transferred from sender to receiver in a given amount of time. It is measured in bps. It is calculated by:

$$\text{Throughput} = \frac{\text{No.of packets received}}{10}$$

Throughput of the three scenarios can be compared by the bar chart shown in Fig. 4.

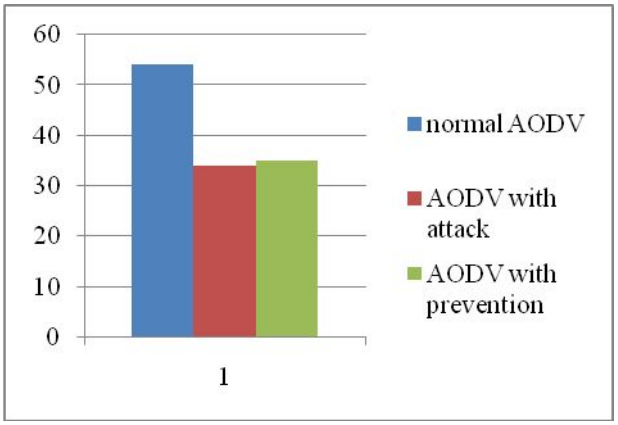

Figure 4: Throughput

Packet Delivery Ratio: It is the ratio of the number of delivered data packets to the destination. It is calculated by:

$$PDR = \frac{\text{No.of packet received}}{\text{No.of packets sent}} * 100$$

PDR for the three scenarios can be compared by the bar chart in Fig. 5.

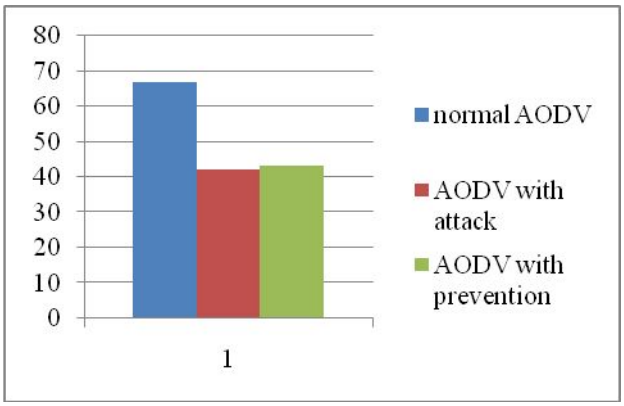

Figure 5: Packet Delivery Ratio

VI. CONCLUSION

In this paper, we explore a different method to detect and prevent the black hole attacks over the MANETs. This attack can degrade the performance of entire network so it is very important to control this attack. This attack reduces the throughput of AODV from 54% to 34% and PDR is from 66% to 42%. After detecting and preventing the network from this attack, throughput and PDR is increased up to 1%. We used NS-2 for implementation and results show the effectiveness of our proposed scheme.

VII. REFERENCES

1. Erdal Çayırcı et al.,"Security in Wireless Ad Hoc and Sensor Networks", A John Wiley and Sons, Ltd, Publication, 2009.

2. Chen X. et al., "Sensor Network Security: A Survey", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 2, SECOND QUARTER 2009.

3. Songbai Lu,"A MANET Routing Protocol that can Withstand Black Hole Attack", IEEE Computer Socity, 2009.

4. V. Palanisamy1, "Impact of Black Hole Attack on Multicast in Ad hoc Network", IEEE, 2010.

5. Tamilarasan S., "Securing and Preventing AODV Routing Protocol from Black Hole Attackusing Counter Algorithm", IJERT-2012, Vol. 1 (5), pp 1-6.

6. Tan.s, "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs" ,ICTC, 2013, pp 1027 – 1032.

7. Bindra G.S et al.,"Detection and removal of co-operative blackhole and grayhole attacks in MANETs", ICSET-2012, pp 1-5.

8. Soni, S.J et al. , "Enhancing security features & performance of AODV protocol under attack for MANET", ISSP-2013, pp 325 – 328.

9. KSHIRSAGAR, D. ET AL., "BLACKHOLE ATTACK DETECTION AND PREVENTION BY REAL TIME MONITORING", ICCCNT-2013, PP 1-5.

10. DANGORE, M.Y. ET AL., "DETECTING AND OVERCOMING BLACKHOLE ATTACK IN AODV PROTOCOL", CUBE-2013, PP 77-82.

