ISSN 2047-3338

# Securing AODV Routing Protocol from Black Hole Attack

Dr. S. Tamilarasan

***Abstract*– Ad-hoc networks are emerging technology, due to their spontaneous nature, are frequently established insecure environments, which makes them vulnerable to attacks. These attacks are happened due to the participating malicious nodes against different network services. Routing protocols, which act as the binding force in these networks, are a common target of these nodes. Ad hoc On-demand Distance Vector routing (AODV) is a widely adopted network routing protocol for Mobile Ad hoc Network (MANET). 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. In this paper we proposed a solution for identifying the malicious node in AODV protocol suffering from black hole attack.**

***Index Terms*– Ad-hoc AODV, Black Hole Attack, MANET and Destination Sequence Number**

## I. INTRODUCTION

WIRELESS networking is an emerging technology that allows users to access information and services electronically, regardless of their geographic position. Wireless networks have become increasingly popular in the computing industry. The applications of the ad hoc networks are vast. Mobile Ad hoc network (MANET) is a self-organized network because it is an infrastructure less feature of networks. MANET is a collection of nodes. Each node can connect by wireless communication links, without any fixed station such as base station. In MANET each node can act as a router and connectivity is achieved in the form of multihop graph between the nodes [1].

Due to the unique characteristics of MANET, developing an intrusion detection system (IDS) in this network is challenging. There is no centralized gateway device to monitor the network traffic. Since the medium is open, both legitimate and malicious nodes can access it. Moreover, there is no clear separation between normal and unusual activities in a mobile environment. Since nodes can move arbitrarily, false routing information can come from a compromised node or a legitimate node that has outdated information. Black hole or sequence number attack is one of the most common attacks made against the reactive routing protocol in MANETs. The black hole attack involves malicious node(s) fabricating the sequence number, hence pretending to have the shortest and freshest route to the destination. Numerous studies have attempted to devise effective detection methods for this attack. The aim of this paper is to investigate black hole & detection methods within the scope of ad hoc on demand distance vector (AODV) routing protocol [1], [2].

## II. AD-HOC ON DEMAND VECTOR PROTOCOL (AODV)

AODV combines some properties of both DSR and DSDV. It uses route discovery process to cope with routes on-demand basis. It uses routing tables for maintaining route information. It is reactive protocol; it doesn’t need to maintain routes to nodes that are not communicating. AODV handles route discovery process with Route Request (RREQ) messages. RREQ message is broadcasted to neighbor nodes. The message floods through the network until the desired destination or a node knowing fresh route is reached. Sequence numbers are used to guarantee loop freedom. RREQ message cause bypassed node to allocate route table entries for reverse route. The destination node unicasts a Route Reply (RREP) back to the source node. Node transmitting a RREP message creates routing table entries for forward route. Figure (Fig. 2) shows, AODV routing protocol with RREQ and RREP message [1]. If you want to submit your file with one column electronically, please do the following:

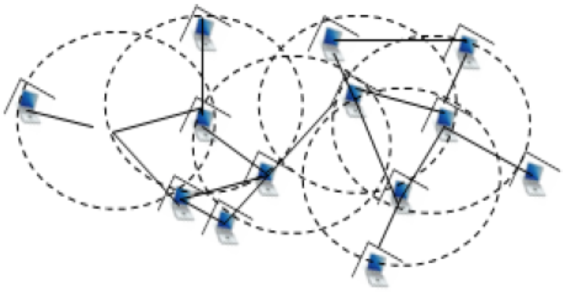

Fig. 1: Wireless Network Structures (Infrastructure less Networks)

Associate Professor cum HOD, Department of Information Technology, Loyola Institute of Technology & Management (LITAM), Dullipala (village), Sattenpalli (Mandal), Guntur, Andhra Pradesh, 522412, India (Email: stamilarasan74@rediffmail.com)

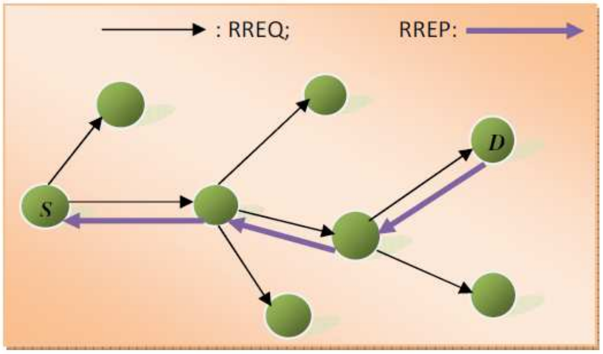

Fig. 2: AODV routing protocol with RREQ and RREP message

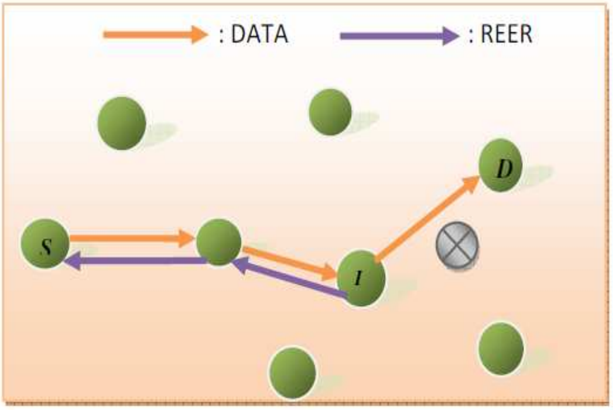

Fig. 3: AODV routing protocol with RERR message

For route maintenance nodes periodically send HELLO messages to neighbor nodes. If a node fails to receive three consecutive HELLO messages from a neighbor, it concludes that link to that specific node is down. A node that detects a broken link sends a Route Error (RERR) message to any upstream node. When a node receives a RERR message it will indicate a new source discovery process. Fig. 3 shows AODV routing protocol with RERR message [1].

## III. BLOCK HOLE ATTACKS

In a black hole attack, 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.

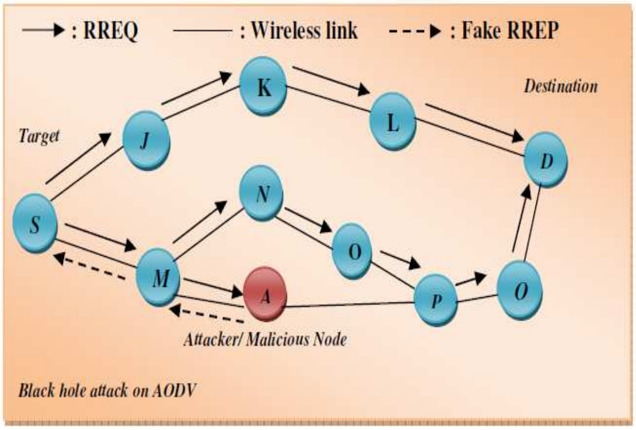

Fig. 4: Black hole attack on AODV

Fig. 4 shows an example of a black hole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A. However, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them on [2], [4].

## IV. EXISTING WORK ON BLOCK HOLE ATTACKS

In [4] Intrusion Detection Systems (IDS) are one of the primary techniques employed to thwart attacks against security threats. Intrusion detection can classified as network based and host based. Network based IDS installed on data concentration points of a network such as switches and routers. In the mobile ad-hoc networks we have no central device that monitors traffic flow so our proposed technique intrusion detection using anomaly detection (IDAD) uses host based IDS schema. IDAD assumes every activity of a user or a system can be monitored and anomaly activities of an intruder can be identified from normal activities. To find a black hole IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data collected and given to the IDAD system, the IDAD system is able to compare every activity with audit data. If any activity of a host out of the activity listed in the audit data, the IDAD system isolates the particular node from the network. In this algorithm they first broadcast RREQ for route discovery and then receive RREP and match the RREP with the audit data if they match save route to the route table and send the data otherwise discard the RREP and then again try.

In [2] [8], the authors introduce the route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the black hole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in

RREP and the one in CREP. If both are matched, the source node judges that the route is correct.

One drawback of this approach is that it cannot avoid the black hole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path.

In [5] authors have mentioned the AODV protocol and Black hole attack in MANETs and proposed a feasible solution for the black hole attacks that can be implemented on the AODV protocol. The Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET. As future work, author intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like packet delivery ratio (PDR), mean delay time, packet overhead, memory usage, mobility, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes.

In [5], the authors proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive.

In [10], the authors analyzed the black hole attack and showed that a malicious node must increase the destination sequence number sufficiently to convince the source node that the route provided is sufficiently enough. Based on this analysis, the authors propose a statistical based anomaly detection approach to detect the black hole attack, based on differences between the destination sequence numbers of the received RREPs.

The key advantage of this approach is that it can detect the attack at low cost without introducing extra routing traffic, and it does not require modification of the existing protocol. However, false positives are the main drawback of this approach due to the nature of anomaly detection.

In [14], according to author solution, information about the next hop to destination should be included in the RREP packet when any intermediate node replies for RREQ. Then the source node sends a further request (FREQ) to next hop of replied node and asks about the replied node and route to the destination. By using this method we can identify trustworthiness of the replied node only if the next hop is trusted. However, this solution cannot prevent cooperative black hole attacks on MANETs. For example, if the next hop also cooperates with the replied node, the reply for the FREQ will be simply “yes” for both questions.

Then the source will trust on next hop and send data through the replied node which is a black hole node.

## V. PROPOSED SOLUTION

The solution, which is proposed to prevent the black hole attacks in the MANET. This solution is basically to modify the working of the source node without alternating intermediate nodes and destination nodes by using a method

- A new table RR-Table (Request Reply),
- A timer (Waiting Time), and
- A variable MN-ID (Malicious Node ID).

In this method we can checking whether there is large difference between the sequence number of source nodes or intermediate node who has sent back RREP or not. Typically, the first routes reply in the RR table which is from the malicious node with high destination sequence number. Now, we can compare the first destination sequence number with the source sequence number. If there is existing much more differences between source and destination sequence number, then the destination node is malicious node, then we could immediately eliminate that entry from the RR-Table.

The destination sequence number is a 32 bit integer associated with every route. This number is used to find the route as fresher. If the destination sequence number is larger than others, then this DNS from the malicious node. Now, N3 will send RREQ message to the source and noted it to D, they would again broadcast the RREQ control message. RREQ control message broadcasted by node N3, the malicious node M also received the RREQ. The malicious node generate fake RREP message and send it to node N3 with very high destination sequence number. Then the node N3 would send it to source node S. Typically, in AODV, as the destination sequence number is high, the route node N3 will be considered to be fresher and hence node S would start sending data packets to node N3. Hence in our proposed algorithm, AODV before sending data packets firstly source node will check the difference between sequence numbers. If it is too larger, the node will be malicious one, and it will be isolated from the network.

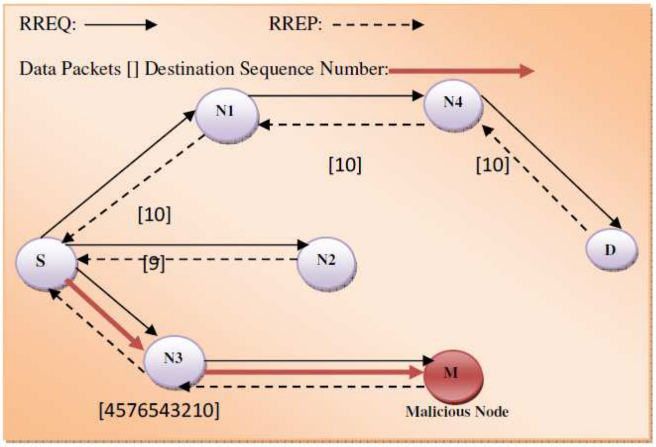

Fig. 5: traversal of Control Messages in AODV

*Algorithm: Prior_ReceiveReply (RREP) Method*

Parameters: Destination Sequence Number (DNS), Node ID (NID), Malicious Node ID (MN_ID)

*Step 1:* Initialization Process:
Start discovery phase with the source node S.

Assign current time and time required to execute the Prior-ReceiveReply (RREP function.

*Step 2:* Storing Process:

To store all the Route Replies DSN and NID in the RR (Request Reply) Table.

Repeat the above process until the time exceeds.

```
While ((current time <= (current time + wait time))
{
  Store the route replies DNS and NID in the RR-Table.
}
```

*Step 3:* Identify and Remove Malicious Node:

Retrieve the first entry from RR Table.

Check the DNS with SSN, if DNS is greater than SSN, then discard the first selected entry from the RR Table.

```
If (DNS > SSN)
{
  MN_ID = NID;
  Discard entry from table
}
```

*Step 4:* Node Selection Process:

Sort the contents of RR Table entries according to the DNS.

Select the NID having highest value of DNS among the RR Table entries.

Continue step 3 and step 4 until we have to find the destination node.

*Step 5:* Continue Default Process:

Call Receive Reply method of default AODV Protocol.

The above algorithm is identified the malicious node and removed from the table. The routing table does not maintain the malicious node in the path. In addition, the control messages from the malicious node, too, are not forwarded in the network. Moreover, in order to maintain freshness, the RR-Table is flushed once a route request is chosen from it. Thus, the operation of the proposed protocol is the same as that of the original AODV, once the malicious node has been detected. The main benefits of proposed solution are: 1) The malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process, 2) With no delay the malicious node are easily identified i.e., as we said before all the routes has unique sequence number. Generally the malicious node has the highest Destination Sequence number and it is the first RREP to arrive. So the comparison is made only to the first entry in the table without checking other entries in the table, 3) No modification is made in other default operations of AODV Protocol, 4) Better performance produced in little modification, and 5) less memory overhead occurs because only few new things are added.

## VI. RESULTS

*Packet delivery ratio (PDR):* The percentage of data packets delivered to destination with respect to the number of packets sent. This metric shows the reliability of data packet delivery.

*Packet Loss:* This metric informs us about the amount of control packets fails to reach its destination in a timely manner.

Performance comparison is made on the basis of above two metrics between existing AODV and proposed AODV.

*1). Packet Delivery Ratio (PDR):* PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. The Fig. 6 shows that PDR of AODV is heavily affected by the malicious nodes where as the PDR of Proposed AODV are immune to it. According to our result, the proposed AODV is secure against black hole attacks.

This is mainly due to the fact that our protocol detects the attacker and allows the source nodes to avoid it. By avoiding the attacker, our protocol finds shortest paths, and so, delivers more packets. On the other hand, the PDR decreases in the case of AODV that is subject to an attack. This is due to the fact that the number of correctly received packet is very less than the number of transmitted packets. Indeed, with the increase of the source nodes, the probability of intrusion increases, and the malicious node absorbs all the data packets passing through it.

*2). Packet Loss:* Clearly, the percentage of packets dropped increases as both the speed and the number of nodes increases. As speed increases, the position of a node will clearly change more rapidly. A source node will still use the last route it has for a destination (if it didn't expire yet), but

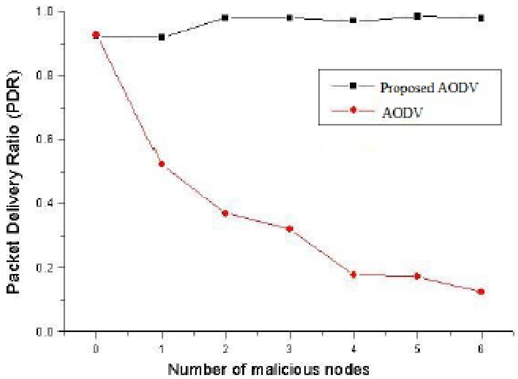

Fig. 6: PDR (Packet Delivery Ratio)

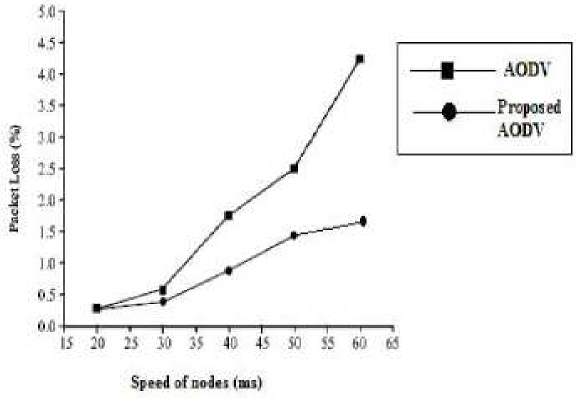

Fig. 7: Packet Loss

due to the fast mobility pattern, this route will frequently be invalid which causes the packet to be dropped. This will cause more and more packets to time out before reaching their destinations. This was also noticed in our simulation as shown in the Fig. 7. The graph concludes that there is very less packet lost percentile in the proposed AODV as compared to the AODV.

## VII. CONCLUSION

In this paper we analyzed the security system with our proposed AODV algorithm. This method is very simple and efficient approach for defending the AODV protocol against Black Hole attacks. The Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET by indentifying the node with their sequence number; check is made for whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not? Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. In addition, the proposed solution may be used to maintain the identity of the malicious node as MN-Id, so that in future, it can discard any control messages coming from that node. Now since malicious node is identified, the routing table and the control messages from the malicious node, too, are not forwarded in the network.

*Future Work:* As future work, research work intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead, memory usage, mobility, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes and also focusing on resolving the problem of multiple attacks against AODV.

## REFERENCES

[1] Tamilarasan-Santhamurthy; "A Comparative Study of Multi-Hop wireless Ad-Hoc Network Routing Protocols in MANET", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011, PP: 176-184.ISSN(online):1694-0814.

[2] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato; "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS", IEEE Wireless Communications • October 2007.PP: 85-90.

[3] S.ciet al; "Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks" IEEE Trans.Vehic Tech. vol: 55, No: 4, July2006, PP: 1302-1310.

[4] Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection by Yibeltal Fantahum Alem & Zhao Hheng Xaun from Tainjin 300222, China 2010, IEEE.

[5] Modified AODV Protocol against Blackhole Attacks in MANET by K. Lakshmi1, S.Manju Priya2 A.Jeevarathinam3 K.Rama, K.Thilagam, Lecturer, Dept. of Computer Applications, Karpagam University, Coimbatore. International Journal of Engineering and Technology Vol.2 (6), 2010.

[6] An Adaptive Approach to Detecting Black Hole Attacks in Ad Hoc Network 2010 24th IEEE International Conference

[7] Modified AODV Protocol against Blackhole Attacks in MANET by K. Lakshmi1, S.Manju Priya2 A.Jeevarathinam3 K.Rama4, K.Thilagam5, Lecturer, Dept. of Computer Applications, Karpagam University, and Coimbatore. International Journal of Engineering and Technology Vol.2 (6), 2010.

[8] Seungjoon Lee, Bohyung Han, Minho Shin; "Robust Routing in Wireless Ad Hoc Networks" 2002, international Conference.

[9] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park "Black Hole Attack in Mobile Ad Hoc Networks" ACM SouthEast Regional Conference 2004.

[10] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007, PP:338-346.

[11] X. Wang, T. Lin and J. Wong, "Feature selection in intrusion detection system over mobile ad-hoc network," Technical Report, Computer Science, Iowa State University, 2005.

[12] M. Hollick, J. Schmitt, C. Seipl and R.Steinmetz, "On the effect of node misbehavior in ad hoc networks", Proc. Of IEEE Intl Conference on Communications (ICC'04), Paris, June 2004, pp. 3759-3763.

[13] Dokurer .S, Y. M. Erten , Can Erkin Acar "Performance analysis of ad-hoc networks under black hole attacks", Turkey

[14] Weerasinghe.H. "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", IEEE Student Member

**S. Tamilarasan, PhD**: He is received the B.E (CSE) degree from Madras University, Chennai, Tamilnadu, India, M.E(CSE)degree from AnnaUniversity, chennai, India, PhD(CSE) from Maghatma Gandhi Kashi Vidyapeeth University, Varanasi,U.P. Currently working as Associate Professor in Information Technology, LITAM, Sattenapalli, A.P.

*Specialization*: Mobile computing, Advanced Data Structure, Design and analysis of algorithm, Computer networks, His interesting research field is Mobile Ad-Hoc Networks.