A Fortify Approach to Secure AODV Protocol against Black Hole Attacks

Chanchal Lohi
Research Scholar
CSE Department
Oriental Institute of Science and Technology,
Bhopal

Sanjay Kumar Sharma
Assistant Professor
CSE Department
Oriental Institute of Science and Technology,
Bhopal

ABSTRACT
The advent of mobile and miniature devices in wireless technology gives rise to new paradigm called Mobile Ad-hoc Network (MANET). MANETs are self-maintaining, self administered dynamic network. MANETs are vulnerabilities in the MANET due to its intrinsic characteristic that make it insecure against various security threats.The black hole attack is forthcoming among them that are launched on AODV protocol. In these attacks, a malicious node disrupts data transmission by sending false routing information containing very high sequence numbers. To deal with these attacks, we proposed an incentive mechanism that protects network against this attack. This mechanism is integrated into route decision making process of the AODV protocol to defend the black-hole attack.

Keywords
AODV, Black hole attack, Gray-hole attack, security, sequence number.

1. INTRODUCTION
The proliferation of mobile devices leads towards the growth of Mobile Ad-hoc Network. MANET is a wireless network which does not require any infrastructure for establishing. It is a self configure, self administered network of mobile nodes which exhibit dynamic network topology. MANET also owns the characteristics of flexibility, distribution operation, addressing mobility, node to node connectivity, etc. for proper management and communication in MANET, special routing is required. A routing protocol for MANET is categorized in proactive, reactive and hybrid protocol respectively.

Due to openness, MANETs are vulnerable to security attacks. In such context, the selfish/ malicious nodes are more likely to appear. Some of the major attack are black hole attack, gray hole attack, wormhole attack denial of service attack. MANET requires a standard routing protocol to control and manage communication in a decentralized environment. AODV is the widely used protocol for communication in MANET.

This paper is organized as follows: sections II discusses AODV routing protocol, section III describe the black-hole attack, section IV presents the related work, section V explains proposed mechanism. Simulation results are presented in section VI and section VII consist of conclusion and future work.

2. AODV ROUTING PROTOCOL
AODV is Ad-hoc On demand Distance Vector routing protocol. It is a pure reactive protocol. When required, the route is established between the source and destination. [14]. The AODV protocol works in two phases: Route discovery and Route maintenance as described below

a) Route Discovery
A route discovery process is initiated whenever a node wants to send data to the destination and no route is available in its routing table. The source node broadcasts the RREQ packets to all neighbor nodes, which forward these RREQ packets to their neighbors. A node which is either a destination node or an intermediate node (with a fresh route to destination) replies by unicasting a RREP packet to the source node, on receiving the RREQ packet. When the RREP packet reaches the source node route is established. The complete scenario is shown in Figure 1.

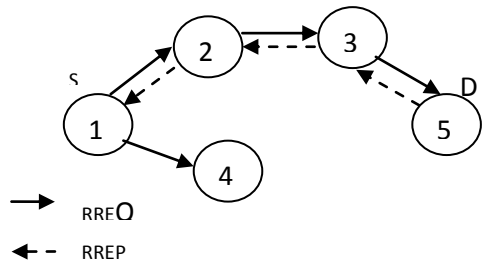

Fig 1: Route discovery process in AODV

In Figure 1, the source node 1 sends RREQ packets to all its neighbor nodes (node 2 and node 4). Subsequently node 2 forward this packet to its neighbor node, i.e. to node 3. On receiving the RREQ packet, destination node 5 responds. Thus, the route is established between source node 1 and destination node 5 via node 2 and node 3.

b) Route Maintenance
The source node maintains a route. When any link break and failure is detected, the route is declared as invalid and Route Error (RERR) packet is flooded in the network. These nodes in turn broadcast the RERR packet to their ancestor nodes and so on till the source node.

3. BLACK HOLE ATTACK
Black hole attack and gray-hole attack are network layer attacks. In black hole attack a Malicious node forcibly acquires the route from a source to a destination by the falsification of the sequence number and hop count of the routing message [18]. A Malicious node sends the RREP message to the source node to advertise itself for having the shortest route to the destination node.

A malicious node reply reaches first to requesting node. Hence route is created between malicious node and requesting node. Now malicious nodes start receiving data packets. Then a malicious node can intercept the data and perform eavesdropping, denial-of-service attack or man in the middle attack. Figure 2 illustrates how the black hole attack is conducted in MANET.

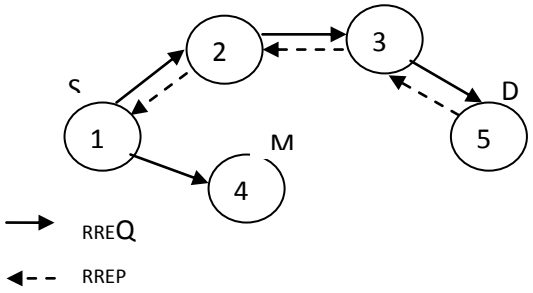

Fig 2: Black hole attack in AODV

In Figure2, node 1 wants to send some data to the destination node 5 and initiates the route discovery process by sending RREQ packets to all its neighbor nodes; node 2 and node 4. On receiving the RREQ packet, node 4 quickly sends false RREP packet to node 1 with the highest sequence number and less hop count and claim that it has the shortest route to the destination node. So the source node 1 assumes node 4 as a shortest route to reach the destination and sends data. Hence all the data will be trapped. In this case node 4 forms a black hole in the network.

The Gray-hole attack is a special case of a black hole attack. In gray-hole attack node drops intercepted packet with some probability. A gray-hole attack exhibits its malicious behavior in different ways. It may drop packet coming from certain specific node(s) in a network while forwarding all packet from other nodes. Another type of gray-hole node may behave maliciously for sometime duration by dropping packets, but may switch to normal behavior later [10]. A gray hole may also exhibit a behavior which is a combination of above two. This attack is more difficult to detect then black hole attack.

4. RELATED WORK

In [6], the author proposed Local Intrusion Detection mechanism in which intrusion detection is performed locally using the previous node. Each intermediate node buffers the RREQ packet and send Further Route Request packet (FRREQ) to the next hope node via a new path. The next hop node sends Further Route Reply (FRREP). When the previous node receives FRREP from the next hope node it extracts the information. If the information in FRREP and RREP matches it discard the FRREP packet, and transmit the RREP packet. Otherwise , it discards the RREP packet and produce alarm.

In [11] the requesting node waits for another route reply with next hope details from other neighboring nodes for some time period. After the timer expires, it checks the collected route replies with repeated next hop node and if any repeated node is present in the reply path it assume the path is correct and selects it as a route to transmit data to the destination.

In [7], the authors proposed Enhanced Route discovery AODV (ERDA). The ERDA introduces three elements: rrep_table, mali_list and rt_upd. By default the value of rt_upd is true and it allows updating the routing table when a RREP is received by the source node. On receiving the RREP packet from destination node, rt_upd value is set to false and all RREP packets come after this is denied. Then a rrep_tab is analyzed to determine malicious node with a very high sequence number.

In [8] authors proposed Forced Routing Information Modification Model (FRIMM) to prevent black hole attack. The authors assume the network is centralized and constructed on three basis; server, access point and nodes. The server and access point are fixed while the nodes are on ad-hoc basis. Nodes can only communicate with the access point. To detect black hole attack, access point scans the network to check whether the requesting node become victim of black hole attack. If yes, then it fetches the MAC address of malicious node and attacks on malicious node with the help of another access point and forces victim to divert traffic via an access point.

In [5], the author proposed secure AODV protocol. The new protocol mitigates black hole attack by taking feedback from the network before forwarding data. In secure AODV whenever a node receives RREQ/RREP packets, its weight is incremented in the routing table. The ratio of RREQ/RREP reflects the participation of node in the routing process. Secure AODV takes decisions based on the number of route request and replies forwarded by the node.

In [5], the authors proposed Generalized Intrusion Detection and Prevention Mechanism which monitors network layer characteristics and performance statistics. GIDP uses a combination of anomaly based and knowledge based Id to protect MANET.

Monika Wahengham and Ningrinla Marchang [4] proposed IDS using Fuzzy logic. The IDS monitors the network traffic and identify the attacker node based on threshold value. IDS incorporate fuzzy logic to handle imprecise information. In black hole attack node drops all the packets and total number of packets dropped should be greater than the threshold value. In gray hole attack towards the source, the node drop the packet coming from the particular source and the total number of dropped packets should be greater than the threshold.

K. S. Sujatha et. al. [3] explained genetic algorithm based IDS. IDS transform the network in population by considering various networking parameters like packet drop, request forwarding rate, request receive rate, etc. the population is encoded by using binary values. Each chromosome is then evaluated for an objective function. The threshold is determined by calculating the average of individual network parameter and then mapped the individual based on fitness criteria. The survival nodes are the malicious nodes.

5. PROPOSED TECHNIQUE

We proposed a technique to secure AODV protocol against black hole attack. We modify he default working of recvreply() function of the AODV protocol by adding our proposed mechanism. The proposed mechanism detects the black hole attack in network and prevents them to communicate with other nodes in a network.

The proposed algorithm uses two new variables to detect black hole node. They are additive value (€) and adaptive sequence number (α). Adaptive value is calculated for each received RREP packet to check whether it is from the normal node or from a black hole node. The proposed algorithm is described below

Step 1: Initialize the source node, destination node & intermediate nodes in the network.

Step 2: Source node broadcast its RREQ packets to communicate with the destination.

Step 3: destination node, malicious node and intermediate nodes send the reply.

Step 4: on receiving a reply at destination node D, D calculates the additive value (€).

Step 5: calculate Adaptive sequence no. (α) =

α = Routing table sequence number + € ;

Step 6: if (adaptive sequence no < RREP sequence no.)

Step 7: malicious node detected;

Step 8: drop RREP packet;

We incorporate above algorithm in the route discovery phase, so detect and eliminate black hole attack in the network.

6. EXPERIMENTAL SETUP AND ANALYSIS

We implement our mechanism using network simulator NS-2 version 2.25. NS is an event driven network simulator program developed at the University of Berkley, which includes many network objects such as protocols, applications and traffic source behavior [13]. NS is an event driven network simulator program developed at the University of Berkley, which includes many network objects such as protocols, applications and traffic source behavior [13].

We have taken 20 second of simulation time for simulation purpose. Each particular traffic have 5 seconds of traffic to avoid traffic disturbance. We are taking four traffic scenarios in simulation using CBR (Constant bit rate) Model. Number of nodes are taken 25.We have defined maximum 100 nodes that can be allowed in this scenario.

Table 1: Simulation Parameter

Parameter	**Values**
Simulator	NS-2(Version – 2.25)
Simulation time	20 seconds
Number of nodes	25
Routing protocol	AODV
Traffic Model	CBR`
No. of Source	04
Transmission range	250m
No. of black hole nodes	03

Network information includes complete detailed analysis of the number of packets send, received by all the nodes which are involved in the communication with the help awk script. We use different awk script to trace different information.

Table 2: Throughput of Network in Different Cases

No. of packets	**Normal scenario**	**BH attack scenario**	**After detection**
Source node sent -	264	252	240
Destination node Received-	257	2	194
% of packet received	98	Approx 0	82.3

The above table shows the throughput of the network. The throughput is highest in the normal working of the network. On the other hand it falls to zero in presence of attack. The propose algorithm detects and prevent the attacker to harm the network. Hence, performance is increased to 82%.

7. CONCLUSION AND FUTURE WORK

The default AODV routing protocol is easy to breach. Hence AODV protocol is vulnerable to various DoS attacks, including black-hole and gray-hole attack. By studying the limitations of previous proposed solutions to these attacks, we proposed a novel approach to prevent and block black-hole. We implemented the approach in network simulator ns-2 and compare the results using various metrics like PDR, routing overhead, End to End delay.

We also emphasize that though the proposed algorithm is implemented and simulated for the AODV routing algorithm, it can also be further extended for use by other routing algorithms, as well.

8. REFERENCES

[1] S. J. Patel et. al. "A Novel Approach to Gray-hole and Black-hole Attacks in Mobile Ad-hoc Networks" Second International Conference on Advanced Computing & Communication Technologies, Pp 556-560.

[2] R. H. Jhaveri, "MR-AODV: A Solution to Mitigate Black-hole and Gray-hole Attacks in AODV Based MANETs" Third International Conference on Advanced Computing & Communication Technologies, Pp. 254-260.

[3] K.S. Sujatha et. al. "Design OF Genetic Algorithm based IDS for MANET" ICRTIT-2012, IEEE, Pp 28-33.

[4] M. Wahengbam and N. Marchang, "Intrusion Detection in MANET using Fuzzy Logic", 2012, Pp 456-460.

[5] Rajesh Yerneni and A.K. Sarje "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks" ICCCNT'2012, pp. 248-252.

[6] Maha Abdelhaq et. al "A Local Intrusion Detection Routing Security over MANET Network" 2011 International Conference on Electrical Engineering and Informatics, 2011.

[7] Kamarularifin Abd Jalil et. al. "Securing Routing Table Update in AODV Routing Protocol" IEEE conference on Open Systems, 2011, pp. 116-121.

[8] Muhammad Raza and Syed Irfan Hyder "A Forced Routing Information Modification Model for Preventing Black Hole Attacks in Wireless Ad Hoc Network" Proceeding of 2012 9th International Bhurban Conference on Applied Science & Technology, 2011, pp 418-422.

[9] Adnan Nadeem and Michael Howarth "A Generalized Intrusion Detection & Prevention Mechanism for Securing MANETs" 2009.

[10] Jaydip sen et. al "A Mechanism for Detection of Gray Hole Attack in Mobile AD Hoc Networks" ICICS 2007.

[11] Latha Tamilselvan and V. Sankaranarayanon "Prevention of Blackhole Attack in MANET" The 2nd International Conference on wireless Broadband and Ultra Wideband Communications, 2007.

[12] Harmandeep Singh and Manpreet Singh, "Securing MANETs Routing Protocol under Black Hole Attack" , International Journal of Innovative Research in Computer and Communication Engineering, June 2013, pp 808-813.

[13] K. Mahalakshmi et.al. "Intrusion Detection System Based MANET Security Against Selective Black Hole Attacks" International Journal of Research in Computer Engineering and Electronics, June 2013.

[14] Jaspal Kumar et. al. "Effect of Black Hole Attack on MANET Routing Protocols" I.J. Computer network and Information security, April 2013, pp 64-72.

[15] Nital Mistry et. Al. "Improving AODV Protocol against Blackhole Attacks" International MultiConference of Engineering and Computer Scientists 2010.