# MS-AODV based Packet Delivery Monitoring while Pause Time and Speed in MANETs

S. Priya[1], Dr. P. Suganthi[2]
[1]Asst. Prof. Department of CS, Saradha Arts and Science College for Women, Perambalur
[2]Asst. Prof. Department of CS, N.K.R Gov. Arts College for Women,  Namakkal

**Abstract:-** The Mobile Ad hoc Network (MANET) has always shown its importance in various applications like military operations, disaster management, wireless mobile communications, etc. Since its applications are spread wide, it is most significant to control the traffic overhead introduced by the routing packets of such network. Also, the confidential information transmitted through these networks must be kept more secure and reliable. The proposed research work aims to find a solution for secure and reliable packet transmission in MANET. In this research work, Modified Secure AODV (MS-AODV) algorithm is used for optimal packet delivery ratio on pause time and speed.

Key words: Pause time, Modified AODV, Warm Hole, Black Hole and Delivery Ratio

## INTRODUCTION

In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created [7]. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can drop the packets between them to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

In Figure 1, let's say node 1 is the source and it wants to send data packets to the destination say node 6 and initiates the route discovery process. Assume that node 2 is a malicious node and it claims that it has route to the destination whenever it receives route request packets, and immediately sends the response to node S. If the response from the node 2 reaches first to node S then node S thinks that the route discovery is complete, then ignores all other reply messages and begins to send data packets to node 2 [4]. As a result all packets through the malicious node is consumed or lost.

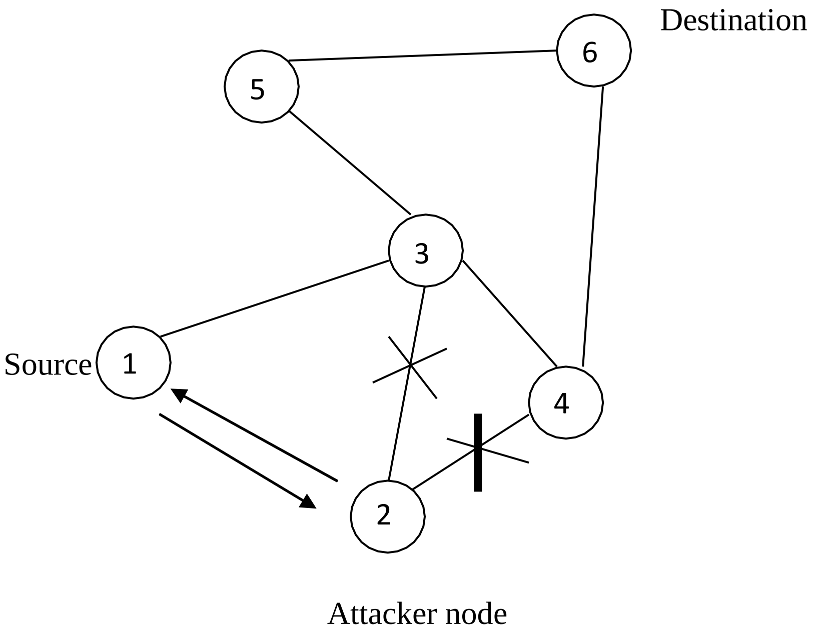

Figure 1 Black hole attack

Black hole attack in AODV protocol can be classified into two categories: black hole attack caused by RREQ and black hole attack caused by RREP. In most cases, the black hole attacker gains the route if the routing protocol does not protect itself [5]. This is because the black hole attacker does not follow the routing protocol rules by not spending a lot of time to reply. Hence black hole attacker replies quicker than the real destination node or any other nodes in the network.

## BLACK HOLE ATTACK CAUSED BY RREQ

An attacker can send fake RREQ messages to form black hole attack. In RREQ black hole attack, the attacker pretends to rebroadcast a RREQ message with a non-existent node address [6]. Other nodes will update their route to pass by the non- existent node to the destination node. As a result, the normal route will be broken down. Figure 2 shows the black hole attack caused by RREQ.

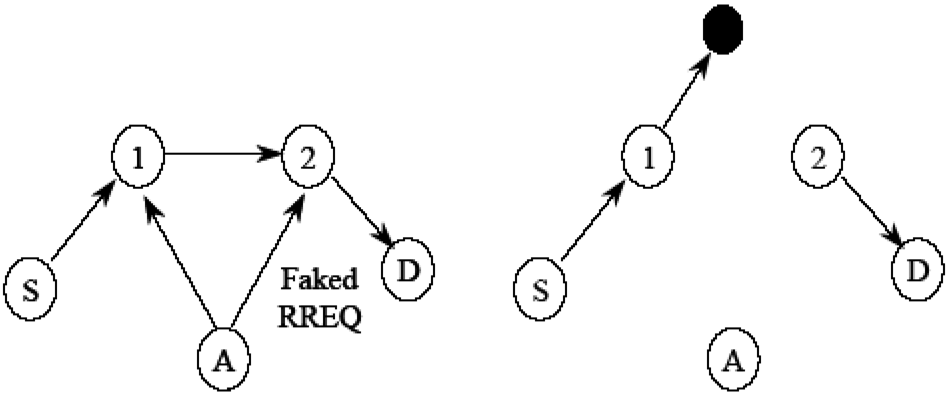

Figure 2 Black hole attack caused by RREQ

The attacker uncast the faked RREP message to the originating node. When the originating node receives the faked RREP message, it updates its route to destination node through the non-existent node. Then the RREP black hole is formed.

## RELATED WORKS

The analysis of the existing system revealed that in some techniques to combat the black hole, the source negotiates with the neighbors before deciding on which route it should use to send the data. This actually delays the actual time and data transfer can take place after the route discovery phase. This in turn means that they rely on the neighbors to identify the attackers in the network. This does not become reliable especially in the case when more black hole nodes available in the network. Also in such a method, the overhead of the network is also increased due to the use of additional check messages with the neighbors.

Some methods like the Data Routing Information makes use of complex check tables to determine the black hole in the network. Such methods are effective but they consume more memory due to the use of such tables [8]. Here the scalability of the network is affected since the number of nodes in the network increases. The size of the routing information tables created for additional check also increases. This again increases the memory consumption and also delay the data transfer to take place after the route discovery phase.

Mainly all these methods use the neighbor’s view of the network to detect black hole nodes. This is not that much effective when compared with a direct negotiation with the destination node since the path from a source to a particular destination may not be always reliable.

Amish et al. proposed Ad hoc on-demand Multipath Distance Vector (AOMDV) protocol to detect and prevent wormhole attack in MANET. In AOMDV protocol sender verifies whether route is available in the routing table or not. If it is not available, then it will broadcast the packet to its neighbor nodes. Here source node will note down the sending time and receiving time. For every route round trip time is computed to calculate final threshold round trip time. If threshold round trip time is more than 2, then wormhole attack is detected. It was observed that AOMDV protocol has low routing overhead and delay.

Robinson et al. prevented wormhole attack in mobile commerce based wireless networks. Cryptographic techniques are used to nullify the wormhole attack. During the route request process, powerful servers are used to parallelize the heavy computation and during route reply process, only limited source node decrypts all the cipher text transmitted by neighbor nodes and not every neighbor node execute cryptographic computations. Secure transaction protocol designed here contains three stages namely preparation stage, transaction stage and post operation stage. Performance was evaluated in terms of cryptographic parameters.

Saini et al. proposed an algorithm based on the distance and in case of attacks, the location of the intruder is the most important thing. So it was easy to find the location of the node. Attaching each node with the global positioning system increases the cost of the system and to overcome this, receiver node is attached with the global positioning system to know the position of the neighbor node. The special antenna is used to collect the information about the relative nodes and with the help of the relative nodes, they can find from where the data has been sent. The main disadvantage of using the special antenna or global positioning system is its high cost. The usage of global positioning system or special antenna reduces the battery life of the system. By using the location that has a detection mechanism, it may increase the false positive rate since the location of node is not static in MANET.

## PORTRAYAL OF MODIFIED SECURE AODV PROTOCOL

In the proposed model the system is designed such that it makes use of the destination unique identifier to detect the black hole in the network and then isolate this black hole node from the path between the sender and destination nodes. Here unlike the existing methods, the dependency of the source on the neighbor and even the further neighbor is avoided. The route checks are done by the direct negotiation with the destination rather than with the neighbors.

Here in addition to the direct negotiation the route is verified by comparing it with the various other routes the sender receives as a response to the normal AODV route request message. Thus the overhead is reduced by reducing the number of extra messages sends out to verify a particular route. The same sequence number based route selection of AODV is still preserved here and also the routing table is kept simple and similar to that of the normal AODV protocol.

The algorithm follows the basic AODV protocol with a modification in the route reply collection stage. When a node needs to transmit data, it first sends out the Route Request (RREQ) message. This RREQ is received by all nodes including the black hole node due to its broadcast nature. Destination node when it receives the RREQ message responds to it by generating the Route Reply (RREP) in the case of normal AODV. But here we modify the RREP message in normal AODV to include the unique ID of the destination itself to find the black hole node RREP and this is termed the modified RREP (MRREP).Hashing of this MRREP is done to enhance security. This can be done because the black hole nodes don’t have any knowledge of the unique ID of the destination.

The algorithm works as follows. As in normal AODV the source node broadcasts the RREQ message. As a result of this broadcast multiple RREQ reaches the destination node. As stated above, the destination node broadcasts out MRREP message which reaches the source through many nodes. Now the source is configured to accept many MRREP messages and store them into a table say Reply Collect Table (RCT). Now taking into consideration large scenarios collection of all MRREP is time consuming and has memory constraints. In order to filter out the MRREP we set up a timer at the source whose run time decides the number of MRREP collected. The MRREP are then compared by checking the unique ID field for similarities.

Taking into consideration the fact that the black hole node always tries to send a fake RREP with a highest sequence number and also it cannot fake the unique ID of the destination. We can find out the black hole node easily using the comparison method. The identified black hole entries are then removed from the RCT and it is rearranged in the decreasing order of sequence number. The highest sequence number route in the filtered RCT is used to send the data.

## WORKING PROCEDURE OF MODIFIED SECURE AODV PROTOCOL

As depicted in Figure 3, source node S initiates a route discovery process. Since node S doesn’t have a route it sends RREQ packet to all the neighbor nodes. The neighbor nodes 1, 2 and M receive the RREQ packet. The node 1 and 2 processes the route request packet but malicious node M immediately replies to source node with a higher destination sequence number. The route reply also contains the unique identifier of the destination. Source node won’t send the data packet immediately through node M. Instead it waits for the reply from the other nodes. For filtering delayed replies, a timer has been included. So the route replies during the run time of the timer is collected by the source node and stored in a table. After some time it will receive the reply from node 1 as (1 – 3), and node 2 as (2 – 3). According to this proposed solution, it first rearranges all replies in the decreasing order of sequence numbers and then compares the unique identifier in all the route replies. If any identifier differs then that reply is considered fake and the node is considered malicious. Alarm messages are then sent out to inform the other nodes of this discovery. The sender then uses the next highest sequence number route to transfer the data.

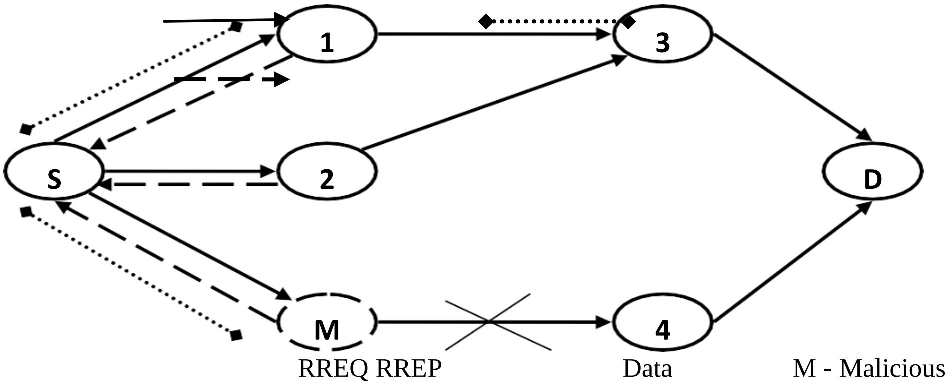

Figure 3 Modified Secure AODV protocol

Finally if the route S - 1 – 3 – D has the highest sequence number after the removal of the fake RREP, then this route will be used by the sender node S to transfer data to the Destination Node D. So to an extent this algorithm can combat the Black Hole in MANET.

## SIMULATION OF MODIFIED SECURE AODV

To evaluate the performance of the secure AODV protocol, simulation was done in NS-2.Here modification is done in the AODV protocol and it is named as secure AODV protocol. CBR packets with 512 bytes are transmitted. The number of malicious nodes is assumes as two. The performance Secure AODV is evaluated with the following performance metrics and is also compared to AODV protocol with black hole nodes.

Table 1 Modified Secure AODV protocol

| Source | Intermediate Node | Destination |
|---|---|---|
| S | M – 4 | D |
| S | 1 – 3 2 – 3 | D |

**Packet delivery ratio:** It is the ratio of total number packets received to the total number of packets sent.

PDR=total number of packets received/total number of packets sent (1)

**Throughput:** It is the total number of packets/bytes received by the source node per unit time.

Throughput=total number of packets/bytes received/unit time. (2)

**End to end delay:** It is an overall time taken for a packet to be transmitted from source to destination.

The parameters used for the simulation was summarized in Table 2.

Table 2 Modified Secure AODV simulation parameters

| **Parameter** | **Value** |
|---|---|
| Simulator | NS 2.35 |
| Simulation area | 750m * 750m |
| Number of nodes | 50 |
| Number of malicious nodes | 2 |
| Payload size | 512 bytes |
| Antenna type | Omni Antenna |
| Channel | Wireless channel |
| Propagation | Two way ground |
| MAC | MAC 802.11 |
| Routing protocol | AODV |
| Traffic type | CBR |
| Interference queue length | 150 |
| Interference Queue | Queue/ Droptail/ PriQueue |

## RESULTS AND DISCUSSION

Figure 4 shows the packet delivery ratio obtained with a scenario consisting of 50 nodes where 2 nodes acted as the black hole node. Pause time is varied from 10 to 50 seconds. The Secure AODV protocol with black hole nodes is compared with AODV protocol with black hole nodes. Packet delivery ratio of AODV protocol with black hole nodes is in the range of 50 to 60%. But Secure AODV protocol provides the packet delivery ratio in the range of 90 to 95% .The simulation results shows that Secure AODV protocol provides a higher packet delivery ratio in presence of black hole nodes compared to AODV protocol with black hole nodes.

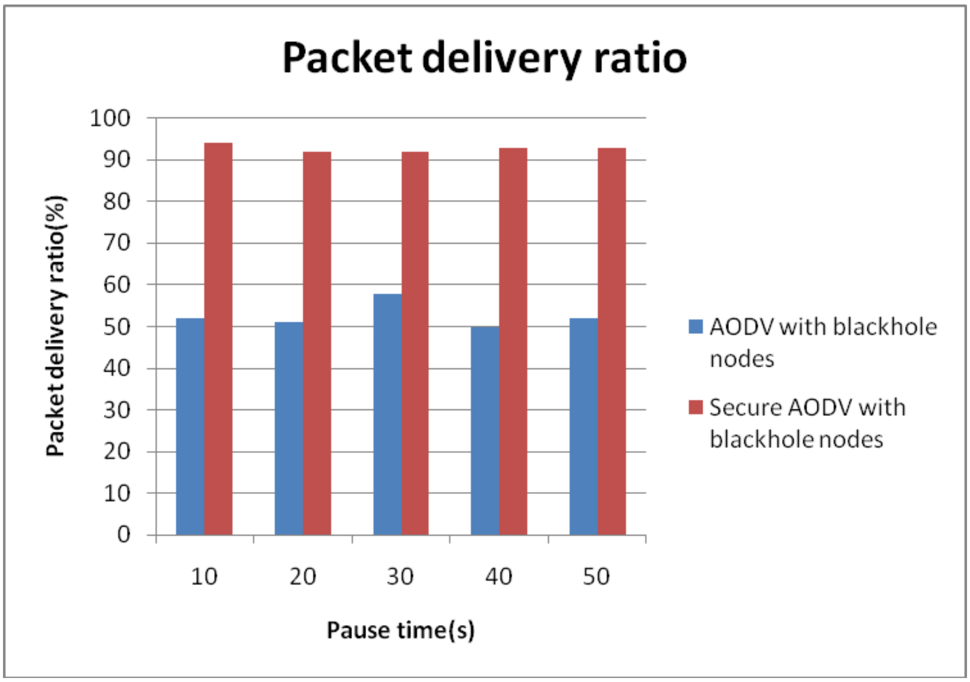

Figure 4 Effect of packet delivery ratio on pause time

Figure 5 shows the packet delivery ratio against increasing speed. Speed is varied from 10 to 50 m/s. The proposed Secure AODV protocol is compared with AODV protocol with black hole nodes. Results show that the packet delivery ratio decreases with increased mobility. This is because routes are subject to breakage as the speed increases. In presence of 2 black hole nodes, packet delivery ratio of AODV protocol with black hole attack is in the range of 50 to 60%. But Secure AODV protocol provides the packet delivery ratio in the range of 90 to 95%. The simulation results show that our Secure AODV protocol provides a higher packet delivery ratio in presence of black hole nodes.

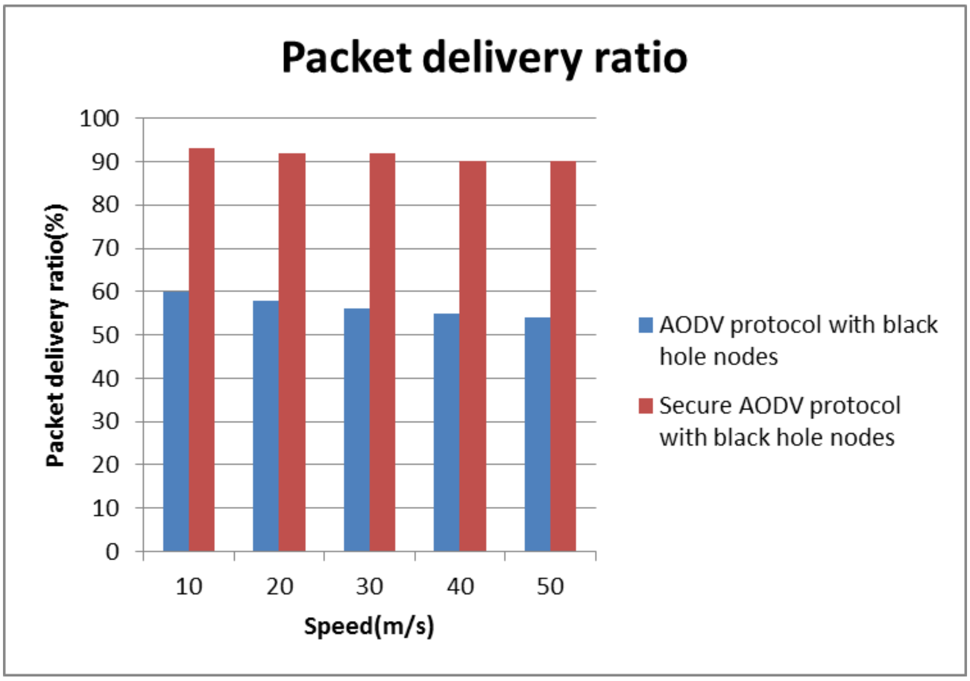

Figure 5 Effect of packet delivery ratio on speed

## CONCLUSION

Modified Secure AODV routing protocol to combat black hole attack in MANET. The Secure AODV protocol follows the basic AODV protocol with modification in the route reply collection stage. When a node needs to transmit data, it first sends out the Route Request (RREQ) message. This RREQ is received by all nodes including the black hole node due to its broadcast nature. Destination node when it receives the RREQ message responds to it by generating the Route Reply (RREP) in the case of normal AODV. But here we modify the RREP message in normal AODV to include the unique ID of the destination itself to find the Black Hole node RREP and this is termed the modified RREP (MRREP).Hashing of this MRREP is done to enhance security. By using this protocol black hole attacker node is identified and eliminated from the network.

## REFERENCES

[1] P Amish and V.B.Vaghela, Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol, Procedia Computer Science, 79(2016),700-707.

[2] Robinson, Y. H., Krishnan, R. S., Julie, E. G., Kumar, R., & Thong, P. H. (2019). Neighbor knowledge-based rebroadcast algorithm for minimizing the routing overhead in mobile ad-hoc networks. Ad Hoc Networks, 93, 101896.

[3] Saini, T. K., & Sharma, S. C. (2019). Prominent unicast routing protocols for Mobile Ad hoc Networks: Criterion, classification, and key attributes. Ad Hoc Networks, 89, 58-77.

[4] Robinson, Y. H., Julie, E. G., Saravanan, K., & Kumar, R. (2019). FD-AOMDV: fault-tolerant disjoint ad-hoc on-demand multipath distance vector routing algorithm in mobile ad-hoc networks. Journal of Ambient Intelligence and Humanized Computing, 10(11), 4455-4472.

[5] Robinson, Y. H., & Julie, E. G. (2019). MTPKM: Multipart trust based public key management technique to reduce security vulnerability in mobile ad-hoc networks. Wireless Personal Communications, 109(2), 739-760.

[6] Sharma, V. K., Verma, L. P., & Kumar, M. (2019). CL-ADSP: Cross-Layer Adaptive Data Scheduling Policy in Mobile Ad-hoc Networks. Future Generation Computer Systems, 97, 530-563.

[7] Balaji, S., Julie, E. G., Robinson, Y. H., Kumar, R., & Thong, P. H. (2019). Design of a security-aware routing scheme in mobile ad-hoc network using repeated game model. Computer Standards & Interfaces, 66, 103358.

[8] Shams, E. A., & Rizaner, A. (2018). A novel support vector machine based intrusion detection system for mobile ad hoc networks. Wireless Networks, 24(5), 1821-1829.