Secure Routing in Unsafe MANETs with Blackhole node by modification of AODV Routing protocol

Priyada Prakash [1], Anish Abraham[2]

[1]MTech Student, Department of Computer Science and Engineering, Government Engineering College ,
Thrissur, Kerala, India

[2] Assisstant Professer, Department of Computer Science and Engineering, Government Engineering College ,
Thrissur, Kerala, India

Abstract

Black hole attack which is a serious threat to the network security and information protection should be prevented at any cost. Black hole attack one of the denial of service attack sucks the data packets that are transferred through the network. The data packets that are received by the blackhole node will be eventually dropped by the node itself. The damages caused by the attack can be prevented by blocking the malicious node to be the intermediate node in communication within the network. The proposed method filters the original genuine RREP from the fake RREP created by the black hole node. This filtered RREP is only allowed to get transferred through the network. The identification of fake RREP is done using two factor that can determine the behavior of the node.

Keywords: AODV, Black hole, MANET, Wireless Network

1.INTRODUCTION

MANETs has become an inevitable part in field of wireless networking due to its ease of use, ease of implementation and its scalability . The security threats against the MANETs has also increased at a high rate. These security threats include both passive and active attacks. Blackhole attack is a Denial of Service attack that engulps every packet that it encounters. The data loss happens when a fake route is created between the source and the blackhole node and the data is transferred through this route. The fake route is created when the blackhole node forges a fake reply whenever a request is received.

In this paper we discuss a mechanism in which these fake replies can be filtered out. So that only the true replies reaches the destination. The behaviour of a node monitored by the neighbouring node helps in this filteration. Thus the fake replies are blocked and the route formation towards blackhole is hindered. Thus the influence of black hole in network can be decreased.

2.RELATED WORKS

Rutvij H. Jhaveri, Sankita J. Patel and C. Jinwala (2012) proposed an RAODV [1] in which the intermediate node also calculates a PEAK value dynamically in a certain interval of time and compares with the destination sequence number. Whenever an intermediate node receives a RREP, in normal AODV, it checks the destination sequence number in the RREP with destination sequence number of the same node in its routing table. If the destination sequence number in the RREP is greater than the destination sequence number in routing table then the RREP is valid and can be accepted or forwarded. In the modified AODV protocol the intermediate node also calculates a PEAK value dynamically in a certain interval of time and compares with the destination sequence number. The comparison is done to identify whether the RREP has been generated by a malicious node or not. The peak values is generated using three parameters, the RREP sequence number, the routing table sequence number and the number of replies received during this particular interval of time. The peak value represents the maximum possible value a RREP can have as its destination sequence number for its current state. Whenever a RREP with sequence number greater than PEAK value is encountered then the node that has generated that particular RREP is identified as a malicious node. The node is added to the malicious node list. That RREP is marked as DO_NOT_CONSIDER and is forwarded to the source node through the same path through which the RREQ came. Every node in the path that receives the RREP with a DO_NOT_CONSIDER mark updates its malicious node list with that node that generated the RREP. When the source node receives this RREP with a DO_NOT_CONSIDER mark ignores it and updates its malicious node list and wait for the next RREP. When the source node again send a RREQ it checks for the new entries in the malicious node list, if any it will be appended with the RREQ. Any node that receives this RREQ will also update its malicious node list with these entries in RREQ. This method uses RREQ and RREP packets to broadcast the malicious nodes identity in the network . The method helps to detect both black holes and the gray holes in the network [1].

Rutvij H. Jhaveri (2013) modifies the RAODV [1] by modifying the malicious node information broadcasting area. After calculating PEAK value, it is compared with the destination sequence number in the RREP. If the PEAK value is lesser than the destination sequence number then the node is malicious. The RREP is discarded and not send to the source node instead of broadcasting. The malicious node list of intermediate node is updated with the node that generated the RREP [2].

Yaser khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer Bani Yasein (2011) proposed a method by modifing the AODV protocol by including a data structure referred as the trust table for every node and an extra field called trust field in the RREP. And also source node sends the its data only if the node replying with RREP is a reliable node. When a source node broadcast a RREQ the trust table of the nodes recieving the RREQ will get updated. Inorder for a node to become a trustworthy node and to get updated in the trust table of its neighbouring node it should pass a behavioural analysis filter. The filters considers the following aspects of the network such as continual change of neighbourhood, number of active connections that a node is part of, the link activity duration etc. Each node keeps a file of history registers informations about these aspects of its neighbours and is saved in the cache. This become the reference and support for the filter. When a source node broadcast a RREQ in the network, in order to be a trustworthy node the node should pass the filter. If it is able to pass then the neighbouring node will add the source node in its trust table. This process go on until the RREP is generated by a node. The replying node can be the destination itself, the intermediate node or the black hole node. The trust field in the generated RREP represents the reliability of the route. This field is initialized as 0 by replying node. The reliability of the route is estimated by the node reached in first hop from the replying node. When the next hop node receives the RREP the reliability or the trust factor is estimated and modified. The most critical stage in which the detection occurs is here. If the next hop node identifies the replying node as destination node then the trust value is changed from 0 to 2. If the replying node is not the destination but if it is present in the trust table of next hop node then the trust value is updated from 0 to1. If the replying node is neither the destination nor a trusted node then the trust value is not changed. As the RREP moves through the reverse path every node update the trust table with the previous node if the trust factor is 1 or 2. When the RREP reaches the source node data will be send only if the trust factor is 1 or 2 else it will be discarded and wait for next RREP [3].

Radha Krishna Bar, Jyotsna Kumar Mandal and Moirangthem Marjit Singh (2013) proposed a method in which the trustworthiness of a node is calculated by means of its ability to forward both the data packets and the RREQ packets. The method keep track of number of packets received and sent by each node. The factor W1 and W2 are calculated based on these counts. W1 represents the ability to forward the packets and is calculated as the ratio between Number of packet sent and Number of packet received.

$$W1 = \frac{Number\ of\ packets\ Sent}{Number\ of\ packets\ received} \qquad (1)$$

$$W2 = \frac{Number\ of\ RouteReply\ sent}{Number\ of\ RouteRequest\ received} \qquad (2)$$

The ptrust value is increased when threshold value is greater than the threshold value. Else decrease the ptrust value. The Trust Value is calculated as

$$Trust\ Value = W1 \square W2 \square ptrust \qquad (3)$$

Insert Trust value into Routing Table and the route establishment according to Routing Table [4].

3.PROPOSED METHOD

The proposed method is based on the assumption that the nodes overhear other nodes and keep count of the number of RREQ received by those nodes, the number of RREQ forwarded and the number of RREP created by that nodes. The routing table is updated for every node entry with these parameters. The RREP is added with a new field trust. Whenever a RREQ is broadcasted by the source node the newly added members of the blacklist will be added to the malicious node list [1][2]. Every intermediate node that receives the RREQ will update their black list based on the entries from the RREQ.

Whenever a destination node or an intermediate node responds to a RREQ with a RREP, the trust factor is set as 0. This RREP with trust value 0 is considered to be a unsafe RREP. The next hop neighbour that receives the RREP with trust factor 0 has the privilege to update the trust factor in the RREP as 1 based on the certain criteria. The intermediate node which is the first node to receive the RREP checks whether the RREP is created by the destination itself. Then the trust value can be updated as 1 and can be forwarded. If not the trustworthiness is calculated for the intermediate node that created the RREP. The trustworthiness of the node is calculated based on two factors w0, w1. These factors are calculated as

$$w0 = \frac{Number\ of\ RREQ\ forwarded}{Number\ of\ RREQ\ received} \qquad (4)$$

$$w1 = \frac{Number\ of\ RREP\ generated}{Number\ of\ RREQ\ received} \qquad (5)$$

For a black hole node the ratio between Number of RREQ forwarded and Number of RREQ received will be 0 since the number of any packets forwarded by the black hole node is always 0. Similarly the the ratio between Number of RREP generated and Number of RREQ received will be always equal to be 1, since the black hole replies to any RREQ it receives.

So the detection is accomplished by checking whether the parameter w0 is approximately equal to 0 and the parameter w1 is approximately equal to 1. If the condition fails then the RREP is updated with the trust factor 1 and forwarded. If the condition is satisfied for the black hole node the RREP can be a fake reply from the black hole. So further detection is done with the help of neighbouring nodes.

The next hop node that initiates the detection process broadcast a Test Route Request (TRREQ) with the suspected node ID. The neighbouring nodes that keeps the track of the suspected node will reply with a Test Route Reply (TRREP). The TRREP contains the count of number of RREQ received, number of RREQ forwarded and the number of RREP generated. From these details the intermediate node that performs the detection process calculates the parameters w0 and w1.

The figure 1 shows the scenario of the communication in which SN denotes the source node, IN the intermediate node, DN the destination node, MN the malicious node and ON the overhearing neighbour node. The ON node is in the vicinity of the nodes MN, IN. When the source node initiate the route discovery procedure by broadcasting the RREQ with the destination field set as DN. The RREQ reaches the nodes in the network either from the source node SN or forwarded by an intermediate node IN.

The nodes IN, ON which has a route to the destination will reply to the RREQ without broadcasting the RREQ . Similarly the destination node which receives the RREQ will also reply to the RREQ. But when a malicious node MN receives the RREQ it will surely reply with a fake reply even though a route is not present to the destination node. It is assumed that the any node that create a RREP should reply with the trust factor 0. Only the next node that first receives the RREP has the privilege to update the trust factor as 1.

The first node to receive the RREP which is an intermediate node will initiates the detection procedure. The RREP from the destination node will be updated with a trust value 1 by the intermediate node since the replying node itself is the destination node. When the RREP is updated by a trust factor 1 the RREP will be forwarded. Once the RREP is updated with a trust factor of 1 then every other intermediate node will be forwarding the RREP towards the source node SN.

The RREP with trust factor 0 created by any intermediate node will subjected to the detection process by the first neighbour node receiving the RREP. The neighbour node IN will check the routing table entry of the replying node. Based on the routing table entries fields line number of RREQ received, number of RREQ forwarded, number of RREP generated the trustworthiness of the replying node is calculated by finding the w1 and w0 values. If the replying node is found to be trustworthy then the trust field in the RREP will be updated to 1 and then forwarded. Since the node

IN figure 1 is a non malicious node the RREP is forwarded with trust value set as 1.

If the intermediate node IN itself cannot determine the trustworthiness of the replying node then the intermediate node seeks the help of the other neighbouring nodes. This is done by broadcasting the TRREQ with the replying node IP address as the suspected node. The neighbour nodes ON which is monitoring the malicious node MN will retrieves the routing table entry for the suspected node MN and send the field entries number of RREQ received, number of RREQ forwarded, number of RREP generated to the intermediate node that has broadcasted the TRREQ. These data are send by embedding them in TRREP.

After receiving the TRREP the intermediate node that has initiated the detection process again checks for the trustworthiness of the replying node. If the trustworthiness of the replying node is still not determined then the RREP will be discarded.

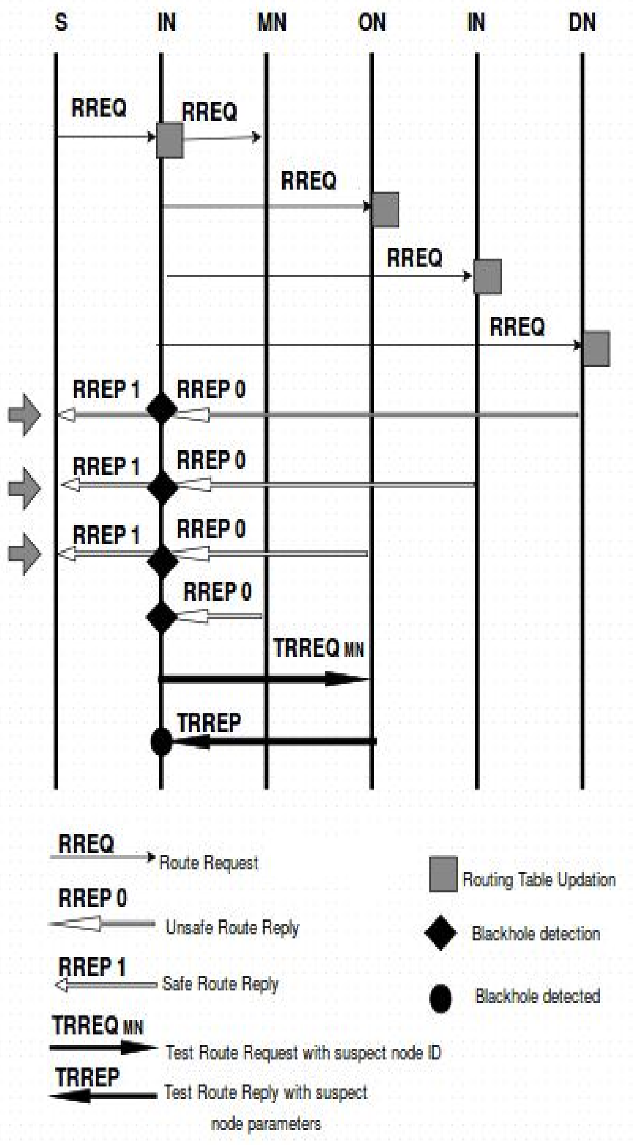

Figure 1 Modified AODV

It is assumed that only the RREP with a trust factor of 1 always reaches the source node. The other RREP with trust factor 0 will be filtered and ignores , thus preventing it from further broadcast. It is also assumed that the intermediate node that first receives the RREP is responsible for the detection process. But there are circumstance when the source receives the RREP with trust value 0 as in figure 2. This is because the replying node itself become a neighbour of the source node. In that case the source node will act a s the intermediate node that first received the RREP and initiates the detection procedures.

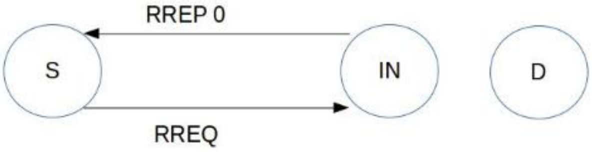

Figure 2 Scenario when the RREP 0 is received

So a source node always checks whether the trust factor in the received RREP is 0 or 1. The trust factor 0 represents that the replying node is the neighbour of source node and it indicates that the source node should initiates the detection procedure by calculating the trustworthiness of the replying node and if needed by the means of TRREQ.

4.Simulation results and Analysis

4.1 Experimental Setup

The simulation has been implemented in NS 3.21. The node mobility patterns is emulated by the random way point mobility model in ns3 with a topology of 1000m by 1000m. The underlying traffic protocol is UDP/CBR with a packet size of 1024 bytes and AODV is the base routing protocol.

Table 1: Parameter specifications

Parameter	Value
Grid size	1000m X 1000m
Routing Protocol	AODV, MAODV, BAODV
Number of nodes	20
Mobility model	Random Way Point
Mobility range	2,4,6,8 … 20
Packet traffic	CBR/UDP
Packet size	1024 bytes
Simulation time	100 s
No of Communications	10, 20, 30 , … , 100
Pause Time	0
Data rate	250 Kbps

4.2 Performance Metrics

PDR is the ratio between the number of packets transmitted by a source and the number of packets received by a destination. PDR value determines the number of packets successfully delivered to the destination node.

$$PDR=\frac{Number\,of\ packets\,received}{Number\,of\ packets\,received} \qquad (6)$$

4.3 Results and Analysis

The performance of the Modified AODV is evaluated by varying the parameters like number of communications and mobility. In each communication source sends five packets of 1024 bytes to the destination. The number of communication or flow is varied from 10 to 100 and the average PDR is calculated for AODV and MAODV separately. The analysis and the results are depicted in the figure 3 . The performance of modified AODV is better than AODV.

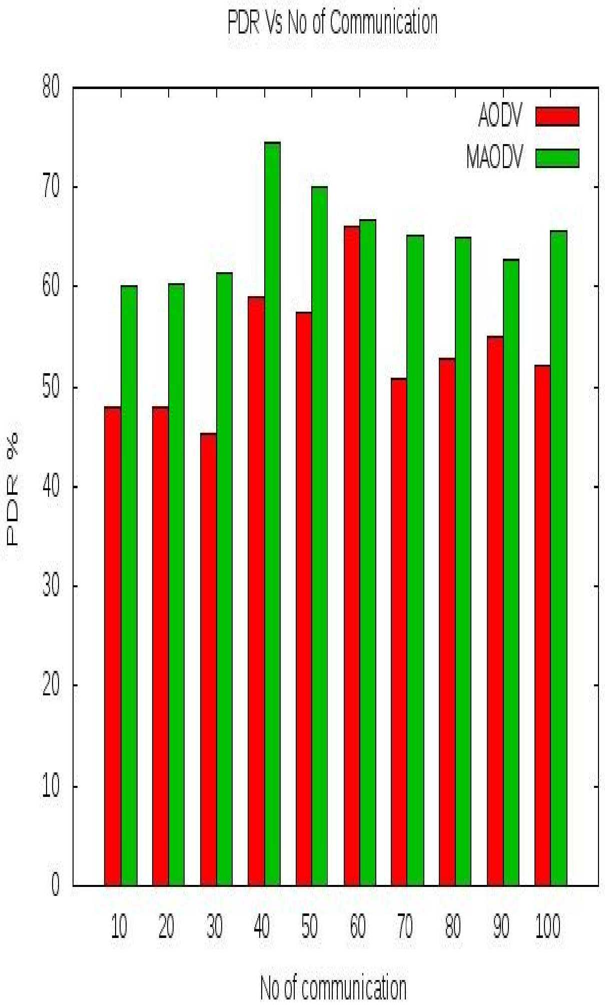

Figure 3 Comparison of PDR by varying number of communication

By keeping the number of communication same the mobility is varied from 10 to 100 and the average PDR is calculated for AODV and MAODV in separative. The analysis is done and the results are shown in figure 4. It is found that the PDR value is better for Modified AODV when comparing with AODV.

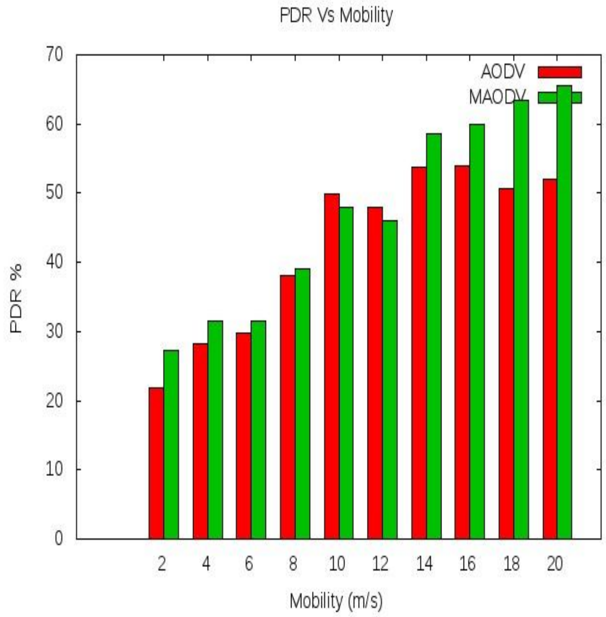

Figure 4 Comparison of PDR by varying mobility

5.CONCLUSION

The proposed method has effectively achieved the objective to block the false RREP created by the black hole node. As a result the fake route creation to the black hole node is blocked. Since data is not transmitted to the black hole node the packets lost is minimum. There is an increase in the PDR value in the modified AODV. By blocking the fake RREP the black hole is prohibited to be the intermediate node in a route. Thus the black hole node have only negligible influence in the network.

References

[1] Rutvij H. Jhaveri , Sankita J. Patel and Devesh C. Jinwala, “A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks,” Second International Conference on Advanced Computing & Communication Technologies, 2012.

[2] Rutvij H. Jhaveri, “ MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs,” Third International Conference on Advanced Computing & Communication Technologies, 2013.

[3] Yaser Khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer Bani Yasein, “A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks ,” International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011

[4] Radha Krishna Bar, Jyotsna Kumar Mandal and Moirangthem Marjit Singh, “QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack,” International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA), 2013 .

AUTHOR

Priyada Prakash is M Tech Student in the Department of Computer Science, Government Engineering College Thrissur, Kerala, India. She received B Tech Degree of Computer Science and Engineering in 2013 from Vidya Academy of Science and Technology, Thalakkottukkara, Thrissur, Kerala, India. Her research interests are Network Security and Cryptography.

Anish Abraham is working as Assistant professor in department of computer science at Government Engineering College Thrissur. He has completed M.E computer science from PSG College of technology Coimbatore. He completed his B.Tech from Model Engineering College Kochi. His research interests are in the areas of machine learning and Bioinformatics.