ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Detection of Black Hole Attack With Improved AODV Protocol in Manet

Lalita Prajapati[1], Anurag Singh Tomar[2]

P.G. Student, Department of Computer Engineering, Lovely Professional University, Punjab, India[1]

Assistant Professor, Department of Computer Engineering, Lovely Professional University, Punjab, India[2]

ABSTRACT:Ad-hoc network is a collection of dynamic nodes it means any node can join the network and leave the network any time. Wireless communication is less secure than wired communication and that's why it is the vulnerability of mobile ad-hoc network and any threat can easily affect the communication. Many types of attacks are developed today which badly crash the network and make the communication performance degrade. So for avoid these vulnerabilities and make network secure we propose the technique on SECURITY of mobile ad-hoc network. To provide the security of mobile ad-hoc network we generate new techniques for detection of black hole attack. Black hole attack is type of malicious node who drops the packet instead to send that packet to their destination.

KEYWORDS:MANET, Malicious node, AODV, RREQ, RREP, MDSR, Pdr (packet Delivery Ratio)

I. INTRODUCTION

MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology. They can act as both routers and hosts. Their ability to self-configure makes this technology suitable for provisioning communication, for example disaster-hit areas where there is no communication infrastructure or in emergency search. In MANET routing protocols for both static and dynamic topology are used. An ad hoc network is a wireless network describe by the nonexistence of a centralized and fixed infrastructure. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks. Mobile ad-hoc network is a collection of dynamic nodes, it means in MANET any node can enter the network any time and join the network any time. There is no effect if any node can automatically leave the network. We can say that it is a form of wireless network. Because it is ad-hoc means temporary nodes stable in network. In MANET there is no access points and infrastructure. There is no coordinator who coordinates the system. It is autonomous and self-organizing wireless communication network. All devices are connected to each other without base station and access points and these are connected to each other on temporary basic.

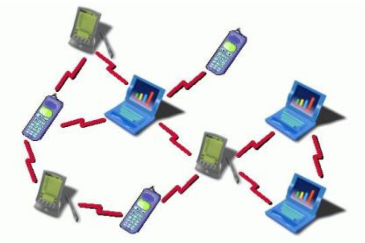

Figure 1Mobile Ad-hoc Networks

1.1 Major Issues in MANET: There are some issues in MANET. These are as follow:

1. **Infrastructure less-** The first challenge in Mobile ad- hoc networks is the infrastructure less environment so designing new network design is challenges.
2. **Dynamic Environments**- The other issue in the mobile ad-hoc networks is the dynamic environments means changing topology affect the communication of source to destination.

DOI: 10.15680/IJIRSET.2015.04050119

3. **Power issue**-The other issue in the Manet is the limited battery life and power so this reason it consumes lots of resources and increase the overhead.
4. **Autonomous nature**-Due to the absence of the admin there is no central coordinator to control the function of the mobile nodes due to this reasons the mobile nodes move in network and fails to configure that proper.
5. **Device Discovery**- When the new node comes in the network than this very important to update their existence to all nodes in the networks

1.2 Black Hole Attack in MANET:

Black whole attack is a type of MANET attack which present in a network and act as a true node but the true definition of black hole attack is a malicious node. Malicious node act as false node in the network and show that node has the best path for send the packet or says that it having fresh route to the destination. Source node broadcasts RREQ packet and further forwarded to intermediate nodes to search the best and short path. If the malicious is present in the network and if that node receive RREQ packet, it's immediately sends false RREP packet with high sequence number. In this the false node claims that node has the best path for send the packet Thus the false node drops instead send the packet to its destination.

In this Figure 2 the Black hole attack explains, the source node is node 1 and destination node is 4 and 3 is a malicious node who act as an honest node. When source node send the request packets to all nodes than malicious node first of all give the reply and take the packet from source and drop the packet instead send that packet to destination node.

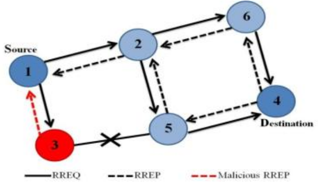

Figure 2 black hole attacks

The black hole attack is very serious type of attack that direct effect on the communication and packet delivery ratio and delay with throughput. Their different types of black hole attacks like as the cooperative black hole attack and single black hole attack

II. BACKGROUND AND RELATED WORK

In [1], authors have proposed a dynamic learning system against black hole attack in AODV based MANET (Payal. N. Raj and Prashant B. Swades,2009) presented the method to detect the black hole method with comparing of intermediate sequence number and source sequence number and after check the threshold limit and check the black hole node and if node detect than reject and block that node with alarm message.

In [2] , authors have presented Preventing AODV routing protocol from black hole attack (L.Himral, V.Vig, 2011) presented that to find the black hole node to safe the routing protocol by check the sequence number of source node or intermediate node those give the reply back or we can say that RREP packet send by those nodes.

In [3] , authors have presented Secure AODV against maliciously Packet dropping (Mohamad Taqi Soleimani, 2011) presented the purpose to stop the packet dropping and designed to detect the black hole attack through neighbor's information. When node receiving the RREP packet after that to check the validity of packet, the source node will broadcast the NREQ packets to all its two hops neighbours to check that is there any destination node or suspicious node.

In [4] authors have presented PPN: Prime Product Number based Malicious Node Detection Scheme for MANET (Sapna Gambhir, Saurabh Sharma, 2012) presented the method to detect the malicious nodes with the help of prime product number and using the concept of AODV protocol and the cluster head. According to the researchers they can detect the malicious nodes with prime product number it means in the network every node has its prime identity and it cannot be modified.

In [5] authors have presented Modified DSR Protocol for Detection and Removal of Selective Black Hole Attack in MANET (Mohanpriya and Llano Krishnamurthy, 2013) to detect the black hole attack. In this proposed method used the Modify DSR protocol and the source node broad cast the route request packets to all nodes The requested destination or any intermediate node having the path can send back the reply to source node.

In [6] authors have presented Optimized positioning of multiple base stations for black hole attacks (Anurag Singh Tomar and Gaurav Kumar Tak 2014) presented the approach to specify the preventation of black hole attack by deploying the multiple base stations. For this reason they use the concept of genetic algorithm and with the help of this easy find out the optimized position.

In [7] authors have presented Enhanced multiple approach for preventation and elimination of black hole attack in mobile ad-hoc networks considering the enhancement of network throughput (Maninder pal Singh, Man Mohan Sharma 2014) presented the technique to prevent the black hole attack with consider the network throughput and used the opnet simulator for the result

III. PROBLEM FORMULATION AND OBJECTIVES

In study done by M. Mohanpriya, they have proposed a modified DSR routing protocol which defines a threshold value and compare the ratio of number of packets received at the destination to the number of packets sent by the destination. If the number of packets received at the destination are less than 80 precent of the packets sent by the source it initiates the process to detect the malicious node? However this approach detects black hole node only after the attack has occurred. This approach may lead to loss of some useful information to the destination and loss the data packets. With this approach the data packet is very much loss and end to end delay is increase. The routing overhead is very much due to MDSR because in MDSR for transmission of QREQ, QREP, MNREQ and ALARM packets. So reduce all these problems, it is very important to consider some steps that eliminate the effect of black hole attack. In recent years, the end to end delay was very high between source to destination due to packet dropping if black hole node between devices in the network. So, due to this network performance was degraded but now the end to end delay will be less with the proposed algorithm. Earlier the packet drop rate was very high but with the proposed algorithm packet drop rate will be reduced. The Proposed algorithm will detect the black hole attack very efficiently in terms of packet drop rate and bandwidth.

IV. PROPOSED DESIGN

The detection of black hole attack will work on different stages .Packet delivery ratio check on destination node In this step first of all we will deploy the nodes in the network and make a network. The source will start the communication and send the route request packets to all neighbouring nodes and after receiving route reply packets to all nodes send the data packets to all nodes, But after some time when destination node release that the packets comes from source node very less. Than check the threshold limit and according to this the threshold limit is below 10-20 packets .The basis of this suspense the destination node check or we can say calculate the packet delivery ratio and try to reach the final result. This packet delivery ratio checks if the total packets counts less than 20 than the destination node check the packet delivery ratio. The check packet delivery ratio we have the formula that destination node use. Total packets send by the destination by received by the destination node and we can find out the packet delivery. The check packet delivery ratio we use the probabilities. The probability checks by the destination node on the basis of two time slots. The reason behind this is the destination node analyse two time slot for detect the malicious node that t1 and t2. On the time of t1 first destination node check how many packets are successfully received out of total packets. Let's 2 out of 10 data packets are receive at time t1.The first condition of probability apply here. The destination nodes have some doubts on that path and have suspected about the malicious node. This doubt clearance the destination node waits for t2 time slot. The time t2 again start to check the successful packets and behaviour of malicious node. The time t2 the successful packets received 4 out of 10 packets but other packets are not receive to destination node. These analyses confirm the destination node about the malicious node and apply the second conditions of probability here. The task for packet deliver ratio performs on the basis of these probabilities. We get two conditions of probabilities to check the malicious node:-

a) 20% chances the node that is not a black hole node but 80% chances that is black hole node. Now we check the probability of 80% that is 80/100 means 0.8 chances that is black hole node.

b) 25% chances are the node that is not a black hole but 75% chances we are sure that this is black hole node. Now we check the probability of 75% that is 75/100 means 0.75 chances that is not a black hole node. But if we combine together both assumptions then we can check the total probability of malicious node.

DOI: 10.15680/IJIRSET.2015.04050119

c) After this calculation we can see that there is 60% chances that node is the black hole and 40% chances that is not black hole. Now we have suspect that the node is malicious. For confirm this we check the forwarding ratio of route request packets by source node. In this confirmation the source node check that route which is suspected by Destination node. The destination node sends the negative acknowledgement or dummy packet to source via alternative path.

The next Detection Step performs by source node. The malicious node reply backs itself but in case of AODV protocol the other nodes reply come from the destination node. This would mean that other nodes have forward the request packets, so for them forwarding ratio will not be infinite. However the black hole node doesn't forward the route request message. It's ratio of number of request packet forward by the node to the request packets received by the node. Now table for ratio of request messages for each node will be looked up. The node for which the ratio is infinite will be detected as malicious node. We can find out this by received route request message by forward route request message and find out the result. After that the source node checks the packet sequence number or we can this Verification Step Where we can compare sequence no. of the route reply messages sent by genuine and malicious node. The sequence number sent by malicious node is always higher. Those becomes the malicious node and now for isolate the malicious node in the network and check the final confirmation of genuine node and malicious node use the concept of prime number. Now we Difference of genuine node and malicious node with prime number by source node and find out the real malicious node. For the difference of genuine node and malicious node we use the concept of prime number and in this network every node has prime number. Now the malicious node act as the genuine node and due to this reason that malicious node also use a prime number. So for avoid this problem and make the difference of honest and malicious node the source node broadcast fake packet and this packet contains the message that all nodes send their prime numbers for new network. Because the malicious node also the part of this network so that node also receives this message and thinks this message not only for me and for all nodes that is the part of this network or route. So, when the source number has the primary product numbers of any two nodes who are also give participation in past communication. The source node sends the dummy packet to all nodes which has the information is that the source node wants to create new session so send the prime number. When the malicious node receives this packet and query message than immediately attach its prime number with that prime product number and dummy packets. After receiving the prime number of that malicious node the source node try to divide that number to prime product number. If the number is not divisible to prime product number than this thing proper confirm that is malicious node and the source node blocks that black hole node and update this to all nodes.

Algorithms Steps

1. Source node sends the route request messages to all the nodes and gets reply and start communication.
2. Destination node receives packets less compare than a threshold limit and start check the packets counts.
3. Destination node performs the function of packet delivery ratio (pdr) with the total number of counts of source node.
4. Now destination node finds the pdr on the basis of probability or percentage of black hole node or not in network with two conditions.

The probability checks by the destination node by two time slots and on the basis on that the destination node checks the step of packet delivery ratio.

5. The source node check the forward packets ratio of every node which send their message forward for the path with which node not send the forward message and calculates the results .
6. Than verification the sequence number high of nodes. Any node have sequence number high than suspect but not sure about black hole.
7. Now the source node sends the dummy packet with the message for new session creation with the two prime products of two nodes and asks to send that prime number.
8. After receive the prime number of suspect node than try to divide that with the prime product of two nodes.
9. If divide than genuine otherwise it will malicious node.

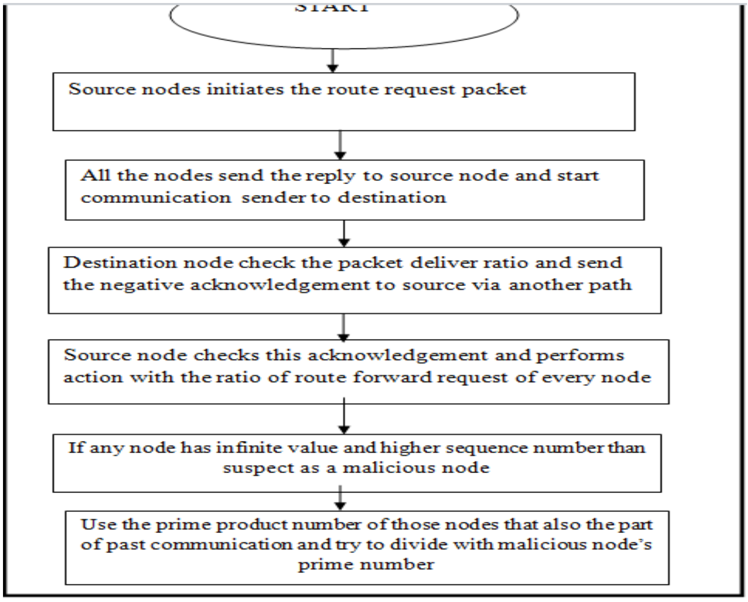
START
Source nodes initiates the route request packet
All the nodes send the reply to source node and start communication sender to destination
Destination node check the packet deliver ratio and send the negative acknowledgement to source via another path
Source node checks this acknowledgement and performs action with the ratio of route forward request of every node
If any node has infinite value and higher sequence number than suspect as a malicious node
Use the prime product number of those nodes that also the part of past communication and try to divide with malicious node's prime number

Figure 3 Flow chart of proposed design

V. PERFORMANCE EVALUATION

1. Simulation Configuration:

Our Simulation is conducted within the network Simulator (NS) 2.35 environments and Ubuntu 13.10.Simulation is being done by improvedAODV routing. We generate the result in NS-2. The graphs are used to signify the variation in throughput and end-to-end delay using the proposed method. Red line shows the old result and the green colour represents the new result by improved AODV protocol.The Throughput can be defined as the number of packet data received per unit time or average time means how much the nodes take for send to receive packets and send. The end-to-end delay defined as the time taken between sending of a packet and it's receiving on the destination or the time gap between the sender and the destination that takes by the intermediate nodes.

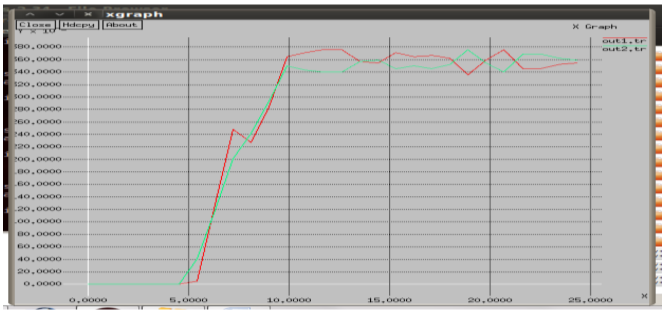

Figure 4 Throughput comparison

In figure 4 we can see the comparison of the throughput. In red line out1.tr show the throughput less but in the green line out2.tr see the throughput high as compare to out1.tr.

DOI: 10.15680/IJIRSET.2015.04050119

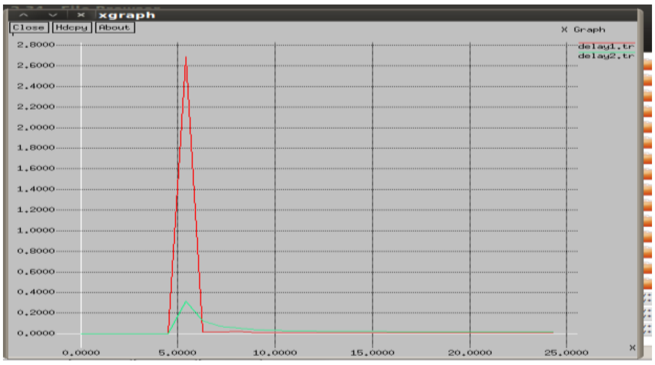

Fig 5: comparison of end to end delay

In figure 5graph the red line delay1.tr show the end to end delay very high but in the green line delay2.tr see the result that the end to end delay very less.

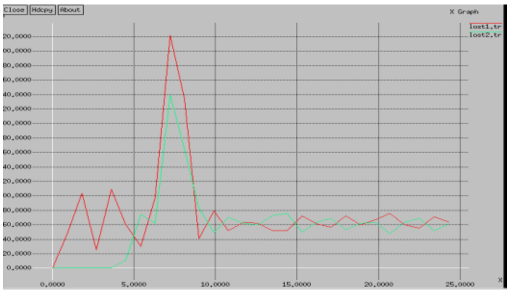

Figure 6 comparison of Packet loss

We can see the result of packet loss in this figure 6 where the red line shows the conventional result and the green line show the new result. The green line show us that packet loss very less compare than the red lone.

VI. CONCLUSION

In this paper am using improved AODV and result are come positive but we can do the better improvement for detect the black hole attack thus it detect already when any malicious enter in the networks and cannot receive the request messages from source and cannot capable to compromise any node for attack the networks. Here need to improve the throughput better in future and use the novel technique for detects the black hole attack.

REFERENCES

[1] Payal. N. Raj & Prashant B. Swades "A Dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues, volume.2, p 54-59, 2009.

[2] L. Himral, V.Vig "Preventing AODV routing protocol from black hole attack", International Journal of Engineering Science and Technology (IJEST), volume.3,2011.

[3] Mohammad Taqi Soleimani "Secure AODV against Malicious Packet Dropping ", Institutes of Electrical and Electronics Engineer-IEEE,2011

[4] Sapna Gambhir, Saurabh Sharma "PPN: Prime Number based Malicious Node Detection Scheme for MANET", IEEE international advance computing conference (IACC), 978-1-4673-4529/S 31.00,2013.

[5] Mohanpriya & Lingo Krishnamurthy "Modified DSR Protocol for Detection and Removal of Selective Black hole Attack in MANET", Computers and Electrical Engineering, 2013.

[6] Anurag Singh Tomar and Gaurav Kumar Tak "Optimized positioning of multiple base stations for black hole attack", International journal of advanced research in computer engineering and technology, volume3,issue 8,August 2014.

[7] Man Mohan Sharma and Maninder pal Singh "Enhanced multiple approaches for preventation and elimination of black hole attack in mobile ad-hoc networks considering the enhancement of network throughputs", International journal of engineering science and research technology ,ISSN:2277-9655,may 2014.