A Trust Based Cooperative Bait Detection Scheme to Prevent Blackhole Attack in MANET

Anu C
Department of Computer Science Engineering
Government Engineering Colllege, Mananthavady, Wayanad-670 644, Kerala, India.

Abstract-*Mobile Ad hoc Networks (MANETs) is a group of mobile nodes in which each node can cooperate with each other without the use of any predefined infrastructure. Nowadays MANET routing protocols are facing various kinds of security attacks. One of the major attacks is blackhole attack, in which a malicious node (blackhole node) that informing that it has the shortest path to reach the destination and then drops or holds the packets to the destination without forwarding them. In this paper, a dynamic source routing (DSR)-based security mechanism is proposed that detects and prevents blackhole attack. In this scheme, source node selects trusted neighbor node as bait node for sending fake route request. Any node other than bait node sends reply marked as a blackhole node. The secure mechanism increased the functioning of DSR routing protocol in terms of packet delivery ratio and throughput.*

Keywords-MANET, Blackhole attack, Dynamic source routing (DSR).

I. INTRODUCTION

A MANET is a set of mobile nodes in which each node can cooperate with each other without the use of any predefined infrastructure. MANET is a kind of ad-hoc network that can change locations, network topology and configure itself. So each node can play the function of router and host. In the case of data transmission, nodes need to cooperate among themselves to forward and receive the data packets, so forming a wireless network of local area. Therefore MANET is widely used in military operations, collaborative work crisis- management applications, personal area networking, bluetooth and so on.

MANET Characteristics are:

- Autonomous terminal: A node may fuction as both source and router.
- Dynamic network topology: As the network change rapidly,the mobile node dynamically establish routing among themselves.
- Distributed operation: There is no fixed network, control and management operation are distributed among the terminal.
- Multihop routing: Packet are to be delivered through one or more than one nodes.
- Light weight terminal: MANET terminals are light weighted because of its the small memory size, and less CPU processing capability of mobile nodes.

The routing protocol plays an important role in manet, in order to to transmit the data packet. But nowadays these routing protocols faces various kind of security attacks such as blackhole and gray hole. Here we discuss about the blackhole attack and prevention method using DSR routing protocol. Blackhole attack is one of among the major security attacks.

II. BLACKHOLE ATTACK

Blackhole Attack is one of the network layer type attacks in which malicious node advertise itself as a node which has the minimum path from the source to destination node. And collects all the packet from a source. Sometimes it holds or drops the packet without forwarding. When the node starts communication. First, it sends RREQ to the neighbor node. If there exists a route which is valid to reach the destination then it sends the packet through the path. If it does not have a route then it forwards the RREQ to the neighbor's node until reach the destination [1]. In Fig.1 the node F act as a fake node that sends RREP with highest sequence number before any other node response. And the Source node discards all reply packets and it assumes that the fake node is a node that has the minimum path to reach the destination. It sends all packet through that path. So the fake node F that collects all the packets coming from the source and drops all packets .

III. DYNAMIC SOURCE ROUTING PROTOCOL

Dynamic Source Routing protocol [2] is one type of reactiveprotocol. DSR maintain an updated route cache for finding new routes. Before data transmission, each node checks it route cache for the valid route. If there is a valid route then starts transmitting data through that route. Otherwise starts DSR route discovery process. Basically, it is has mainly 2 process.

Route Discovery

When a node initiates the data transmission, first it checks its route cache for the valid route. If a route to the destination is found then sent the packet through that route. But if the node does not contain a valid route, then it starts broadcasting RREQ packets. After receiving the RREQ intermediate node checks it route care whether it has a route. If intermediate node has an route then send the packet through that route. Otherwise, append its address to route request packet and

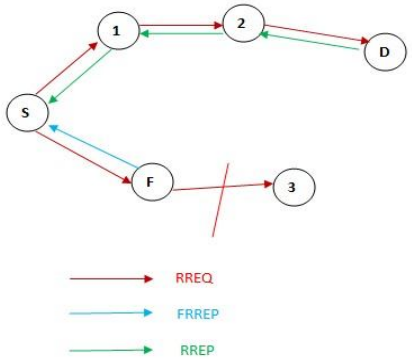

Fig. 1. Singleblackhole

forwards it to its neighbors until it reaches the sink node. When the RREQ message is received by the sink node, it will generate the reply packet and send that to the source node. After receiving the reply packet, source node starts the data transmission.

Route Maintenance

Route Error packet and Acknowledgments (ACK) are the two mechanisms for route maintenance. The node ACK mes- sage to source node only when successfully delivery of the packet. If there is any link breakage then sends error message.

IV. LITERATURE REVIEW

In recent year many researches has done in the detection of a malicious node in the MANETs. Most of this detection is used to detect single or cooperative blackhole attack. But there are lots of time and cost needed for detecting this blackhole attack [8]. Detection mechanism can be two types proactive and reactive. In case of proactive scheme, a node constantly watch nearby nodes. But there is no malicious node present in the network, the overhead is created for this detection, and the resource is also wasted. It avoids and prevents an attack in the earlier stage. The second one is reactive detection schemes. In this scheme detection start only when the packet delivery ratio below some threshold value.

In [4] Liu et al. proposed a security mechainsm (2ACK) for the detection of malicious node. In this method, First node starts to sends the data packet to its next-hop neighbor. If next-hop receives the packet, it sends the acknowledgement to the source node indicate that packet is successfully received. If any attacker present between this two-hop, it holds or drops the packets. So the next-hop node does not forward the acknowledgement towards the source node. That time the source realizes that an attacker presents in the network and takes immediate action. Only a small amount of datapackets is used for the acknowledgement, in order to reduce the additional overhead. In this scheme, detection delay will be increased since the detection process is invoked based on ACK. This method is under the category of the proactive method and produces additional overhead in the absences of the malicious node.

In [5] Xue and Nahrstedt proposed a security mechanism (BFTR) for detecting the malicious node. In this scheme, first monitor the route that is chosen by the destination. For the detection it uses the end to end acknowledgment. The source node calculates the packet delivery ratio. If packet delivery ratio drops in some threshold value then source node uses a new route. But attacker node may still present in the new route. Source node wants to find new route again which leads to continues route discovery process. This method is under the category of the reactive method. Here the detection start or source find new path only when packet delivery ratio is below some threshold value.

In [3] G.Vennila, Dr.D.Arivazhagan proposed a prevention mechanism that using a Cryptographic Algorithm. This approach is used to secure the DSR protocol. The proposed solution uses RSA cryptographic algorithm and sequence number calculation to eliminate the blackhole node. In route discovery process, the RREQ is encrypted at the sender side and it forwards to the neighbor's node. If the node knows the key value, decrypt the RREQ and it generates RREP. After receiving the RREP in a source, it computes the threshold difference. If the difference of sequence value is below the some threshold value, then the node is a legitimate node. Otherwise, the node is considered a malicious node. This method prevents cooperative blackhole attack. In this method is under the category of the proactive method. If there is no attacker node present in the network, produces additional routing overhead.

In [6] Tsou, Chang, Lin, Chao and Chen proposed a BDSR scheme, This scheme is used for the detection and prevention of blackhole attack and The aim of this method is to sending fake request and catch the blackhole node. First, it

selects the virtual and random address. And use this address as sending fake RREQ. Any node replies this request considered a mali- cious node. Then put this node into blackhole list. Initially, it is a proactive scheme. Then detects the attacker node, reactive detection is starts. The first source node sends the packet. After data transmission, calculate the packet delivery ratio. If it is below some threshold value then detection starts again. Initial stage it is a proactive detection and finally, it becomes reactive detection. In BDSR, RREP and RREQ packets are modified. This method combines both reactive and proactive detection scheme. First, it acts as the proactive then detects malicious node . After the malicious node detection, Then starts the second type of detection. Ie.reactive.But this approach uses a virtual bait id, which is not presented in the network. But how to select virtual destination address to bait the malicious node is not specified. Here there is a chance for entering a real node with the same baited into the group. Then all nodes who is near to the destination gives RREP to the source, in this case the source will treat the replied nodes are malicious nodes and put them into blackhole list. Hence the proper functioning of the group is not working. This methods detect only single blackhole attack.

In [7] Vaishali B. Mewada, Viral Boris agar, proposed a modified DSR for mitigating Black hole Impact in MANET. In this approach, a source node uses available path in its route cache and sent first data packet and waits for the acknowledgment (ack). If ack comes within a certain time, then this route is considered as safe and succeeding packets are sent along this same route otherwise start to identify the presence of malicious node. A fictive route request is sent along the available route with the destination address as a fictive address which is not present in the network. The node that replies to this fictive route request is listed as a black hole and added in the blackhole list. If the route reply is from destination node then the route is the safe route. This scheme In this scheme, packet delivery ratio and throughput can be achieved same as DSR based MANET without a malicious node. As the pause time increases, performance parameters remain same as the simple DSR protocol performance. This is a proactive method. Sometimes in this network there is no malicious node is presented, that time overhead is created, a resource used for detection is wasted. This method detects single blackhole attacks.

V. PROPOSED METHOD

In this proposed method (TCBDS) modified the DSR routing protocol to detect and prevent blackhole attack. In this scheme source node selects trusted neighbor node as bait node for sending fake route request and catch the malicious node. The Fig.2 shows the block diagram of proposed method. Proposed security mechanism has three steps [9]: 1) Trust based bait step; 2) Reverse tracing step; and 3) DSR route discovery process.

Trust based Bait Step : its one hope neighbor node as a testing destination (bait node). That is its address is used to send fake route request. Based on the trust value of the neighbor node, source node selects it as a bait node. Trust is calculated using the formula, ratio of a number of the packets forwarded to the number of packets received. Higher the trust, select it as a testing destination. Trust is evaluated for the nodes by establishing the communication from the source. Source selects its one-hop neighbor based its trust value. Then source node sends baited route request to all nodes. Then original destination and malicious node reply this request. This would indicate that malicious node present in the route reply. Then starts the next step.

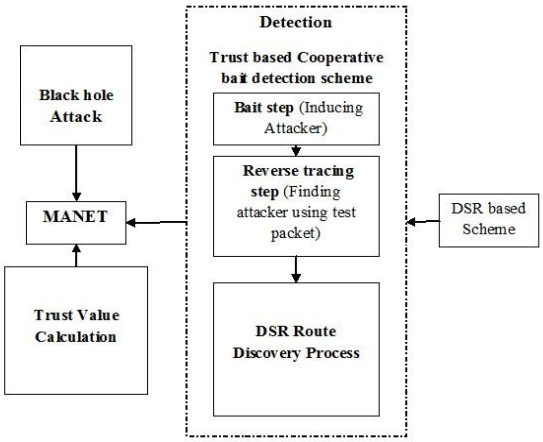

Fig. 2. Block diagram of TCBDS

node (blackhole node). After the source node broadcast the fake RREQ. The blackhole node replies with false RREP. Then source node forwarded the test packet towards the blackhole node. If malicious node (blackhole node) received these packet it does not forward to the destination. So the attacker node is detected.

Then source node broadcast the alarm packets. And inform all other nodes to the presence of this malicious node and stop communication with this node.

DSR route discovery process : In this step source node starts to find the new route. Then forwarded the packet towards the destination using this new route.

VI. SIMULATION RESULT

The simulation is done using NS2 (Network Simulator). To evaluate the performance of proposed method the metrics given below are used:

Packet Delivery Ratio: It represents the ratio of the number of packets received to the number of packets forwarded.

The Fig.3 shows the variation of time, the packet delivery ratio value is increased in the black hole attack prevention technique when compared to the black hole attack scenario.

Throughput : This metric represents the number of bits transmitted per second.That is number of successfully received packets in a unit time and it is represented in bps.

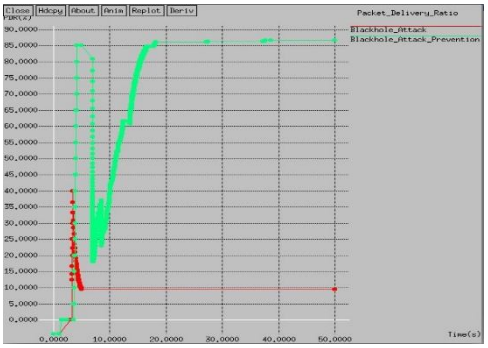

Fig. 3. Comparison of Packet Delivery Ratio

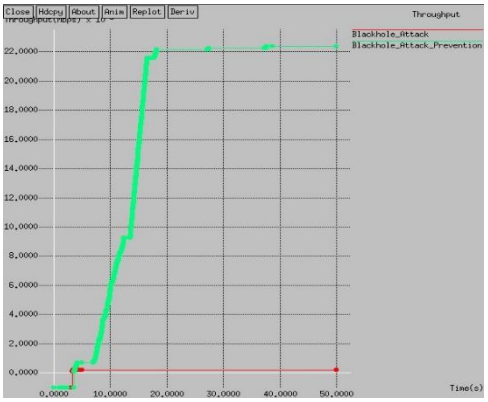

Fig. 4. Comparison of Throughput

In Fig.4 shows the variation of time, the throughput value is increased in the black hole attack prevention technique when compared to the black hole attack scenario.

Routing Overhead: It represents the amount of routing- related control packet transmissions divided by the amount of data transmissions.

In Fig.5 shows the variation of time, the overhead value is increased in the black hole attack prevention technique as it involves number of control packets to ensure the presence of attacker when compared to the existing black hole attack scenario.

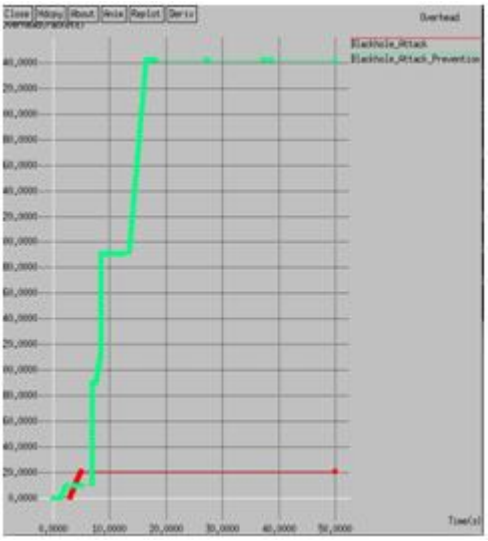

Fig. 5. Comparison of Routing Overhead

VII. CONCLUSION AND FUTUREWORK

Blackhole attack is a major security threat in the routing protocols. It effect its performance badly. So proposed a mechanism to detect and prevent blackhole attack. In this scheme source node select trusted neighbor node as bait node for sending fake route request. Any malicious node is detected, then sent the alarm packet to all other node in the netwrok to stop communicating with this blackhole node. Simulation results of proposed method shows the better result in terms of packet delivery ratio, throughput.

In future work, proposed security mechanism can be modi- fied for detect and prevent grayhole attack. Grayhole attack is a one type of blackhole attack. In which an attacker node selectively drops the packets. Initially it acts as legitimate node. Later it drops the packet selectively.

REFERENCES

[1] A. Baadache, and A.Belmehdi, ”Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks”, International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[2] Durgesh Kumar Mishra Mahakal Singh Chandel, Rashid Sheikh. ”Secu- rity Issues in MANET: A Review”

[3] N. M. G.Vennila, Dr.D.Arivazhagan, ”Prevention of co-operative black hole attack in manet on dsr protocol using cryptographic algorithm”, IJET,2013.

[4] K. Liu, D. Pramod, K. Varshney, , and K. Balakrishnan, ”An acknowl- edgement based approach for the detection

of routing misbehavior in manets", IEEE Trans. Mobile Comput., vol. 6 pp. 536-550, 2007.

[5] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments", Wireless Pers.Commun., vol. 29, pp. 367-388, 2004.

[6] P. C. Tsou, J. M. Chang, Y. suan Lin, H. C. Chao, and J. L. Chen,"Developing a bdsr scheme to avoid black hole attack based on proactive and reactive architecture in manets", ICACT, 2011.

[7] Vaishali B. Mewada, Viral Boris agar, "Modified DSR for Mitigating Black hole Impact in MANET", International Journal for Technological Research in Engineering Volume 1, Issue 9, May-2014 ISSN Online: 2347-4718

[8] Neha1, Manmohan Sharma, "A Survey on Black Hole Attack Detection and Prevention Techniques", International Journal for Research in Applied Science and Engineering Technology (IJRASET), Volume 3 Issue IV, April 2015.

[9] Jian-Ming Chang, , Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks by Ma- licious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE Systems Journal, 2015.