ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Detection of malicious packet droppers in MANET based on legitimate routing information

S.Madhurikkha*, R.Sabitha[2]
*Department of Computer Science and Engineering, Jeppiaar Engg College, Chennai, India
[2] HOD- IT Department, Jeppiaar Engg College, Chennai, India
***Corresponding author:madhurikkha@gmail.com**

ABSTRACT

Mobile Ad hoc Network (MANET) is the one of the types of Ad hoc Network which changes its location and configures itself when needed. It is a self-configuring network. It uses the wireless connections to connect to various other networks. Its mobile nature, decentralized control and frequent changing topology MANET is vulnerable to many attacks. It is very difficult to detect the attacks when it becomes part of network. Ad hoc on demand distance vector (AODV) is one of the routing protocols but exposed to well-known packet dropping attack, in which a malicious node intentionally and intentionally drops packets without forwarding them to destination. When groups of node act collaboratively in dropping packets in network, the information communication in network may be severely degraded and sometime completely disrupted. In this paper, we discuss about a security mechanism to defend against packet dropping attack in MANET.

KEY WORDS: Ad hoc Networks, Routing Protocols, AODV, Packet dropping Attack, MANET.

1. INTRODUCTION

Continuous progress has been made in securing MANETs via the development of secure routing protocols. MANET has mobile nodes which form on fly anywhere at any time due to infrastructure less and self-configuring characteristics. They have special features like wireless links, high mobility, multiple hops, dynamic topology & decentralized control which make them vulnerable to various attacks. Most of research work focus on prevention and detection of malicious nodes from network. Nodes cooperation is important in wireless network for routing packets but identifying and isolating attackers in such situation is a challenge. A set of nodes can be easily compromised such that detecting the malicious behavior is tedious. Such nodes flood other nodes with routing traffic; advertise non –existent links, drop packets, changes the contents of packets and thus inflicting failure in network.

One of the most popular routing protocol Ad hoc on-demand distance vector (AODV) is used in MANET. It is a source based routing protocol where routes are discovered only on demand. However, AODV is vulnerable to packet dropping attack. A malicious node wantedly drops all data packets or control packets without forwarding them to destination. A group of nodes can drop packets in collaboration in network at such a rate that message communication in network may get degraded or even disrupted. Unavailability of lack of physical protection and reliable mechanisms, packet dropping attack posts a serious threat to routing in MANETs. In (Jay dip Sen, 2011) authors have shown that black hole nodes (malicious node falsely advertise good route to destination on route discovery process) cooperate and work in groups in MANET and have proposed a solution to identify black and cooperative black hole attack. However their proposed security mechanism doesn't study to defend against packet dropping attack in MANET. In this paper the mechanism for cooperative black hole attack is proposed (Jay dip Sen, 2011) i.e., Data Routing information table and cross checking mechanism (Section V) are adapted to defend against packet dropping attack.

The rest of the paper is organized as follows. Section II discusses some related work in security methods for MANETs. Section III presents the overview of AODV routing protocol. Section IV describes about the packet dropping attack. Section V presents the methodologies adapted with its architecture to defend against the attack. Section VI gives the conclusion and future scope of work.

Related Work: A number of works have been done to enforce the security problem on the area of Ad hoc network community. This section lists some of these works.

In Muhammad (2008), proposed a two way solution to find out and identify malicious nodes in network by setting Tmax (maximum threshold) and monitoring nodes to state misbehaving nodes. But attacker in network in groups cannot be identified and isolated in this method.

In Jaydip sen (2007), proposed a cooperative scheme used to detect malicious node, as every node in network monitors the manners of its neighbors upon strange action. Distributed algorithm used to confirm attack in network. Since only trusted nodes are used for securing routing, it is an overhead and malicious nodes are not cut off in this method.

In Sirisha (2003), proposed a method where a discovery manager locates malicious nodes that drop packets in MANET by setting rules for nodes with low false positive rate. The detection manager fails to detect the misrouting behavior of the node in network.

In Marti (2000), proposed a mechanism watchdog and path rater to detect malicious node in MANETs. Nodes operate in a promiscuous mode in this scheme. Since watchdog technique may fall short to detect misbehaviors in presence of ambiguous collision, limited transmission power, false misbehaviors and partial dropping it lacks deficiency.

In Bhalaji (2009), proposed an association based routing using DSR protocol to enhance security against selective packet drop attack which is based on trust value and threshold parameters between nodes. But the cost of maintaining the association table for each node is not evaluated.

In Liu (2007) proposed a two hop acknowledgement scheme to prove that wireless node has actually forwarded packets to next hop, receiver sends acknowledgement in reverse direction for multiple hops to achieve the goal. But well behaved nodes can become a part of malicious link and may result in losing good routes in network.

Overview of Aodv Routing Protocol: Ad hoc On Demand (AODV) is a descendent of Destination Sequenced Distance Vector (DSDV) routing protocol. It is a reactive type of routing protocol which establish route to destination only when there is a demand. All nodes in Ad hoc network maintain a routing table which lists the next hop node information for a route to destination. AODV utilizes destination sequence number in routing table to ensure loop-free routing and to avoid count-to-infinity problem. It tells the novelty of the route to destination. Whenever source node wishes to route packets to destination, it first checks it's possessing routing table to determine whether a route to destination is already available. If so, it routes the packets to destination. If not, the source nodule initiates a route discovery process (figure 1) where it broadcasts a route request (RREQ) message to its neighbors which is extra propagated until it reaches an intermediate node with fresh route to destination node or destination node itself.

The intermediate nodes on receiving RREQ make an entry in their routing table for the node (which forwarded RREQ message) and source node. If the destination sequence number present in routing table is minor than or equal to number present in RREQ packet, the node relays an additional request to its neighbors. If the Sequence number is superior, it denotes a "fresh route" and packets can be sent through this route. The intermediate node or the destination node with fresh route to destination unicasts route reply (RREP) message to neighboring nodes from which it received RREQ. All neighboring nodes on the turnaround path make entry of the nodes from which it received RREP. The source node on receiving the updated route to destination node starts routing data packets through neighboring nodes that responded it first with RREP. During this routing if any node identifies a link crash it sends a Route error (RERR) message to all other nodes that uses this link for their communication. This message is sent to the source node to update its route to the destination and to avoid denial of service. Since AODV doesn't incorporate any security mechanisms, nodes misbehavior can perform many attacks like dropping packets, altering contents of packets, IP spoofing etc., However AODV protocol achieves limited security and lacks scalability and latency time.

Packet Dropping Attack: In a Packet dropping attack, a malicious node purposely drops the packets they receive. To conduct its attack, the malicious node must initially fit in to the route and then it starts the action which is the data dropping Bhalaji (2009). The manner with which the malicious node fits in the data route differs. The packet dropping attack can be of any one way given below.

- Dropping Control Packets
- Selectively Dropping Packets
- Group of nodes collaboratively drop packets

We shall discuss the above mentioned ways of dropping packets using AODV protocol in MANET.

Control Packet Dropping: A malevolent node drop control packets like RREQ, RREP or RERR packets to keep use of failed routes, which results in a denial of service (Djamel Djenouri, 2007). Dropping RREQ packets will exclude the malicious node from routes and avoid receiving data packets to forward from it. So, malicious node mainly drops RERR (route error) packets to gain routes.

In figure 2, node S is source node and D is the destination node. Nodes 1 to 5 acts as intermediate nodes, M acts as malicious node. In this example the node 5 moves from the path and sends a Route Error (RERR) message to source through intermediate nodes. On receiving the RERR message node 4 forwards it to malicious node M, but it drops the control packet (RERR) without forwarding it to source node.

The Source node is not updated with the RERR message and it sends packets to destination which is accepted by the malicious node. Now the malicious node gains the route and initiates a denial of service.

Selective data packet dropping: A Malicious node becomes separately of routing data to destination node and starts receiving data packets and drops them selectively and forwards the rest of packets to its neighbors Bhalaji (2009). It is difficult to isolate such nodes in the network. In figure 3, S is the source node and D is the destination node. Nodes 1 to 5 act as intermediate nodes. Node M is malicious. The source node (S) starts a route discovery process by transmit RREQ packets to neighboring nodes. The malicious node is a part of network (M) receives RREQ. The source node starts forward the data packets after receiving the RREP message from the Destination node (D). As

malicious node M being part of routing data packets, starts dropping some data packets and forwards others to next hop node. The packet dropping is shown with lines in the figure 3. This is difficult to detect since it drops the packets selectively.

Packet dropping in groups: Groups of malicious node collaboratively drop the packets without forwarding it to the destination. This activity makes the network to break from message communication between nodes and even disrupt the whole topology.

In figure 4, Node S is source node and D is the destination node. Nodes 1 to 4 act as intermediate nodes. Node M and N are malicious nodes which collaborate with each other in the network. As an example, when source node S wishes to transmit data packets it send an RREQ massage to its neighboring nodes. The malicious nodes M and N being part of RREQ, respond with an RREP to source node. It is said that the malicious nodes respond even faster than rest of the nodes in network.

Now on receiving the RREP from M, source node transmits the data packets. On the receipt of data packets, malicious node M simply drops them or forwards all data packets to malicious node M which in turn drops all packets without forwarding to intended destination. The destination node doesn't know any message on what is happening in the path as the malicious nodes completely block it. When malicious nodes form groups they degrade the whole network and stop the communication between the nodes. All these attacks lack security mechanism to defend against them which will be discussed in the next session.

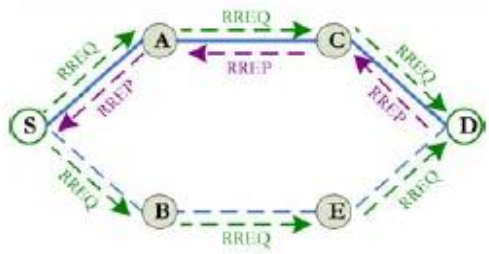

Figure.1. AODV – Route Discovery

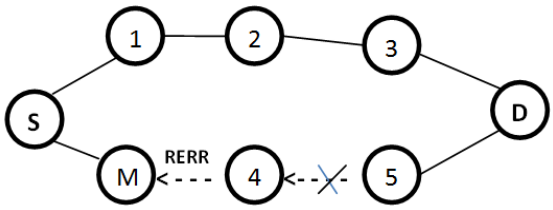

Figure.2. Control packets dropping

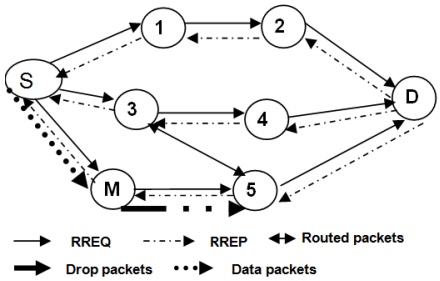

Figure.3. Selective packet dropping

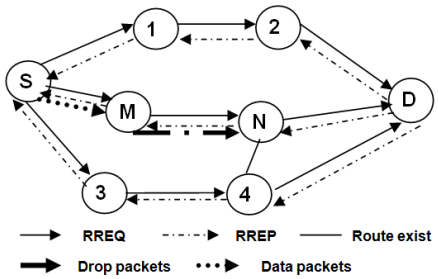

Figure.4 Collaborative packet dropping

METHODS AND MATERIALS

Methodologies Adapted: In this section, the proposed methodologies for defending against packet dropping attack are discussed. The mechanism proposed modifies the standard AODV protocol by introducing two techniques namely,

- Data Routing Information (DRI) table
- Cross Checking

These two concepts were implemented in (Jay dip Sen, 2011) to defend against cooperative black hole attack. The authors in (Jay dip Sen, 2011) have concluded that these mechanisms can be used to secure against packet dropping attack also.

Data Routing Information (DRI): In this method during route discovery process, the nodes which react to RREQ message of source node must send two-bits of additional information. Each node must maintain an additional DRI table in which bit '1' stands for 'true' and bit '0' stands for 'false'. The first bit 'from' denotes whether any data packets routed from the nodes in node ground. The second bit 'through' stands for routing data packets through the node in the node field. For example from figure 5 a sample database maintained by node 5 is shown in table 1.

The entry 1 0 for node 4 implies that node 5 has routed data packets from 4 but has not routed any data packets through 4.

The entry 1 1 for node D imply that node 5 has routed data packets from and through node D. The 0 0 entries for node M denotes that node 5 has not in flight from and through node M.

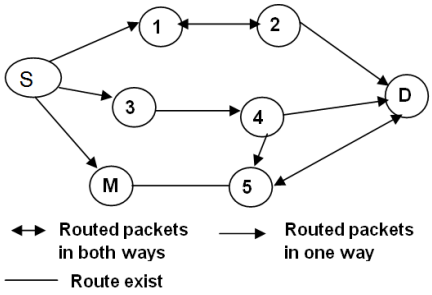

Figure.5. Sample Network for DRI Table entry

NODE #	DRI	
	FROM	THROUGH
4	1	0
M	0	0
D	1	1

Table.1. DRI table of node 5

Cross Checking: The proposed system relies on reliable nodes i.e. Nodes through which data packets are routed previously by source node is known to be trustworthy. The proposed model is depicted in figure 6. In the modified protocol, source node broadcasts RREQ message to discover route to destination node. The intermediate node (IN) on its RREP provides facts regarding its next hop node (NHN) and its DRI table entry for that NHN. On receiving the RREP from IN, source node checks its own DRI table to verify whether IN is reliable node.

If source node has already routed data through IN, it is reliable and source node starts routing through IN otherwise, IN is unreliable. Now source node sends '*further request'* (FRq) message to IN's NHN to check the identity of IN. The cross checking is to gather information from NHN by asking following question to it.

- Has IN routed any data packets through NHN?
- Who is current Next Hope Node's next hop (neighbor) to destination node?
- If current Next Hope Node routed data through its own next hop?

The NHN responds to source node with '*further reply'* (FRp) message including the following.

- Data routing information table entry for Intermediate node
- The information regarding Next Hope Node's next hop (neighbor)
- DRI table entry for NHN's next hop.

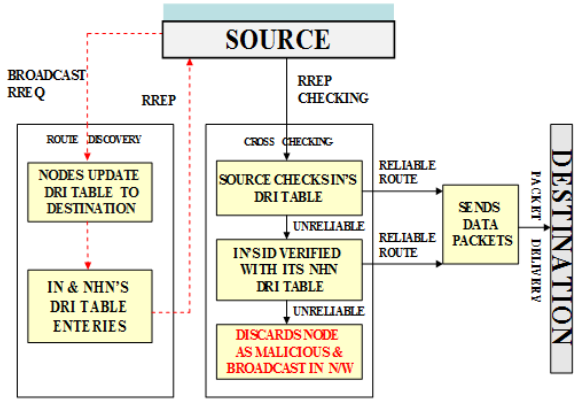

Figure.6.Proposed model for packet dropping attack in MANET

RESULTS AND DISCUSSION

On viewing the Frequent Replies message from Next Hope Node, source node checks whether NHN is reliable. If source node has routed through NHN already it is reliable otherwise NHN is unreliable. If Next HN is reliable, the source node checks whether IN is an malicious node i.e., if the first bit of DRI table entry for IN in NHN table is 0 (NHN has not routed data from IN) and the second bit of DRI entry for IN in NHN table is 1 (IN has routed data through NHN) then Intermediate is a malicious node. IF Intermediate node is not a malicious node, Next HN is reliable node then the route is secured and source node update its DRI entry for IN with 0 1. If IN is malicious node, then source node identifies all nodes in reverse path from IN to the node which has generated RREP as malicious nodes. The source node further broadcasts the list of malicious nodes in the network. If the NextHN is unreliable, source node checks the identity of Next HN by treating it as Intermediate and sends Frequent Rq to the IN's next hop node. This goes on like a loop until the source node finds a secure route to destination. Since it is a one-time procedure and it is affordable for the security purpose.

As an example, consider figure 3, when source node sends an RREQ packet, the malicious node M replies with an RREP message with its Data RI table entry and its next hop node (i.e., if M has routed data packets through node 5).The source node on receiving the RREP from M, checks its own Data RI table whether it has routed data packets through M it sends an FRq message to IN's Next HN (node 5) to check the identity of M. The source node enquires node 5 through an alternative path S-3-5.

- Whether node 5 has routed any data from M.

- Who is node 5's next hop and
- Whether node 5 has routed data packets through its

Next hop node.

Since node 5 is a reliable one, it sends FRp message stating that DataRI entry for the IN (i.e. M) is 0 1 and it also sends the Data RI table of its next hop. On receiving the FRp message, the source node decides that M is a malicious node and it ignores any other RREP from that node and broadcasts the list in the network. Thus, the packet dropping in the route is detected by isolating the malicious node before routing data packets. Now for packet dropping in groups let us consider figure 4, using the proposed Mechanism. When node M responds to source node with RREP message, it provides its next hop N and Data RI table entry. Here node M is a malicious node which lies about using the path by replying with DRI equal to 0 1.On receiving RREP message from M source node checks its own Data RI table to see whether M is a reliable node. Since source node has never sent any data through M before, M is not a reliable node to source node. Therefore source node sends FRq to N via S-3-4-N and asks about the same three questions mentioned above. Since N is maliciously

Collaborating with M, it replies positively to all the three questions and gives node 2 (chosen randomly) as its next hop. When source node contacts node 2 via path S-1-2 to cross check validity of node N, node 2 responds negatively. The Data RI table for node 2 shows the entry for node N as 0 0. Based on this information source node infers that node N is a malicious node. If node M has really routed data packets through node N before, it should have validated the node N. Since node N is invalidated through node 2, source node infers that node M is maliciously cooperating with node N. Hence node M and N are marked as malicious nodes and this information is propagated through network. Source node discards any further response from node M and N, chooses an alternative path to route D. Thus packet dropping in groups and even control packet dropping can be detected using this mechanism.

4. CONCLUSION AND FUTURE WORK

In this paper one of the attack namely packet dropper attack is studied in MANET. A security protocol has been proposed to make out the ways of packet dropping nodes in MANET and thereby making a secure routing path from source node to the destination node avoiding the malicious nodes. As a future scope of work, packet dropper attack can be discussed with different routing protocols in MANET and the results can be compared with the proposed security mechanism and may be evaluated by implementing it in the network simulator *ns*-2.

REFERENCES

Bhalaji N & Shanmugam A, Reliable Routing Against Selective Packet Drop Attack in DSR Based MANET, Journal of Software, 2009.

Djamel Djenouri, On Securing MANET Routing Protocol Against Control Packet Dropping, IEEE 2007.

Hongmei Deng, Wei Li and Dharma Agrawal P, Routing Security in Wireless Ad Hoc Network, IEEE 2008.

Hongmei Deng, Wei Li and Dharma P, Agarwal, Routing Security in Wireless Ad Hoc Networks, University of Cincinnati, IEEE Communications magazine, 40(10), 2002.

Jay dip Sen, Sripad Koilakonda, Arijit Ukil, A mechanism for detection of cooperative black hole attack in Mobile Ad hoc Networks", Proceedings of IEEE International conference on Intelligent systems, Modeling & Simulation 2011

Jaydip Sen , Girish Chandra P, A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks, Proceedings of IEEE International conference on Telecommunication, 2007.

Liu K. Deng J, Varshney P, balakrishnana K, An acknowledgment based approach for the detection of routing misbehaviour in MANETs, IEEE Transaction on mobile computing, 2007.

Marti S, Giuli T, Lai K and baker M, Mitigating routing misbehaviour in mobile ad hoc networks, proceedings of international conference on mobile computing and networking, 2000.

Michiardi P and Molva R, Preventing denial of service and selfishness in adhoc networks, In Working Session on Security in Ad Hoc Networks, Lausanne, Switzerland, 2002.

Muhammad Zeshan, Shoad, khan A, Adding Security Against packet dropping Attack in Mobile Ad hoc Networks, Proceedings of ACM International Seminar on Future Information Tech & Mgmt Engg, FITME 2008.

Perkins C.E, Belding-Royer E and Das S.R, Ad hoc On demand Distance Vector (AODV) routing, IETF RFC 3561, 2003.

Rao R and Kesidis G, Detecting of malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited, in Proc. IEEE GLOBECOM, 2003, 2957–2961.

Sirisha R, Medidi, Muralidhar Medidi & Sireesh Gavini, Detecting Packet-dropping Faults in Mobile Ad-hoc networks, IEEE 2003.

Yi S, Naldurg P and Kravets R, Security-Aware Ad Hoc Routing for Wireless Networks, Proceedings of ACM MOBIHOC, 2001, 299-302.

Zhang Y and Lee W, Intrusion detection in wireless ad-hoc networks, in Proc. ACM MobiCom, 2000, 275–283.