International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

A Survey Paper on Preventing Packet Dropping Attack in Mobile Ad-Hoc MANET

Arthi R, Siddique Ibrahim S P, Kirubakaran R
Department of Computer Science and Engineering, Kumarguru College of Technology, Coimbatore, TamilNadu, India

ABSTRACT

Mobile Ad-hoc Network (MANET) is collection of many wireless mobile nodes. In MANET any number of nodes can join to the network. Centralized administrator will not be there. All wireless devices under network can communicate with each other within a range. MANET is infrastructure less network so nodes are vulnerable to attacks. Packet dropping and bandwidth attacks are one of major concern in mobile ad-hoc network. When the packet move from source to destination in between some intermediate nodes behaving like malicious node they continuously drops all forwarding packets.This reduce the performance of the system. In this paper based on AODV (Ad-hoc On-Demand Distance Vector) routing protocol attacks are analysed and proposed node bypassing technique to identify and remove such kind of malicious node from the network.

Keywords : MANET, ADOV routing protocol, packet drop attack, malicious node, bypass technique, Route Request, Route Discovery.

I. INTRODUCTION

Wireless communication is rapidly growing technology. People are willing to use their devices anywhere and everywhere. Wireless connectivity gives freedom to move when they desire. Mobile Ad-hoc Network (MANET) is collection wireless network which include many mobile devices, laptop, Personal devices, etc...

In wireless network two classifications are there: one is nodes are interconnected with infrastructure and other is Ad-hoc wireless network which is infrastructure less network. Example for infrastructure network is GSM in this access point will be there it act as a router to forward the packets. But in Ad-hoc network central administrator will not be there. Topology of the network changes according to the nodes join or leave the network. This type of network will be used in military operations, emergency purposes.

In MANET security is the main issue. Any node can take routing decision due to absence of centralized administrator. Denial of Service (DOS) is an attack in which attacker makes the network inaccessible to the prospective user [1]. When packet forward from source to destination some intermediate nodes act like a malicious node [2] that continuously drop the packet and reduce the performance. Security need to be provided in order to identify the malicious nodes and remove it from the network.

Routing is the important part in MANET. Ad-hoc routing algorithm classified in to two types: proactive and reactive [4, 5]. In proactive routing algorithm it generates routing Table to route request. In reactive algorithm it establishes the path connection to destination whenever needed.

II. METHODS AND MATERIAL

1. AODV (Ad-hoc On-Demand Distance Vector) PROCESS

Reactive routing algorithm concept is used in AODV. Routes are established whenever source wants to send packet to the destination. AODV [3] maintain a table to store route information, which is useful in large networks. In this Route Request (RREQ), Route Reply (RREP), Route Error (RERR) is there.

A. Route Request

When source node want to send packet to destination node if node is not near to source then it send RREQ. Route Request is to find valid route to the destination. It is generated by source node RREQ and it broadcast RREQ to its neighbour nodes then neighbour node checks valid route to destination. If yes it sends a reply message to the destination. Otherwise it discards that path and finds other route. RREQ contain source IP, Destination IP, Current sequence number, destination sequence number, Hop count is initially zero it get incremented for each RREQ

B. Route Reply

After source node sends RREQ to its neighbour and it get reply when valid path is there to send packet see in figure 1. RREP contain destination IP address, Current sequence number, Source IP address. When multiple RREPs arrive to the source, then it takes the path with minimum hop counts or highest sequence number.

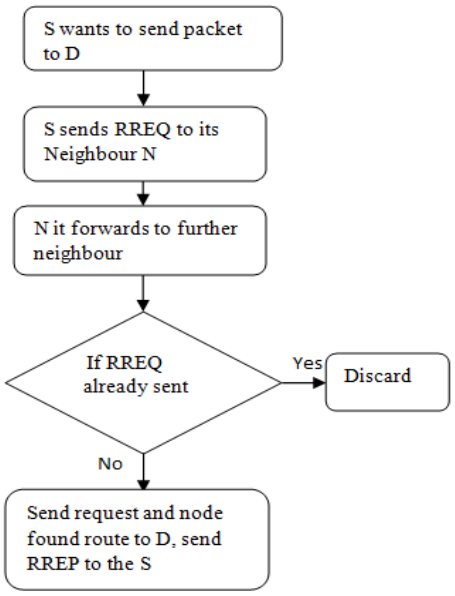

Figure 1. Flow chart for RREQ and RREP

C. Route Error

When some nodes are unable to forward the packets due to broken link it sends RERR [6] to the source. Once it arrive RERR source choose another way to send the packet to the destination.

2. PACKET DROPPING ATTACK IN MANET

In MANET packet dropping attack is the major concerns see in figure 2. When packet forward from source to destination some intermediate node act like a malicious node drops the entire packet instead of forwarding to the destination so network performance get reduce. There are various reasons for packets dropping [7] are there.

1. Packet may get dropped due to bandwidth attack. For each node bandwidth is assigned to forward data. Hackers may hack the bandwidth limit and drop the packet.
2. Due to network broken link, nodes can't able to forward the packet. Lack of energy resources also leads to packet dropping.
3. Due to malicious node packet dropping attack take place. Malicious node will send false information to the source that it has shortest distance to destination.

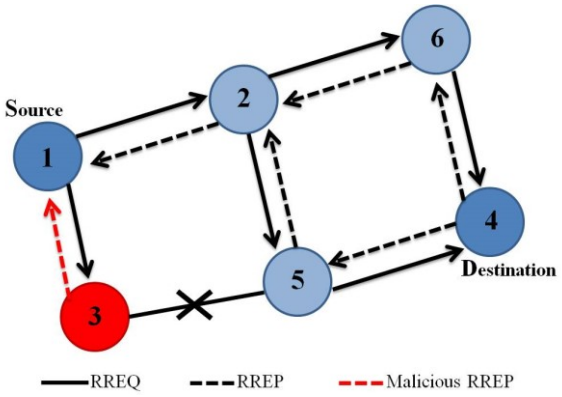

Figure 2. Packet dropping attack

III. RESULTS AND DISCUSSION

TECHNIQUE FOR DETECTING MALICIOUS NODE IN THE NETWORK

When a source node wants to send packet to other node which is not near then it sends an RREQ packet to all its neighbours. If a neighbour knows route to destination of this packet then it sends an RREP packet that contains the next hop address to which neighbour node will forward the packet.

1. Source forward RREQ and set timer to receive acknowledgement from the neighbour node.
2. If receiver didn't send acknowledgement means then it is consider as half-trusted node otherwise it is consider as trusted node.
3. Once again RREQ is send to half-trusted node; again it does not provide RREP means it is consider as malicious node. New route will be discovered and remove that malicious node.

By Route discovery and Monitoring phase selfish nodes are identified,

Route Discovery

Sender first send the trap RREQ to its entire neighbour which contains destination address which does not exists in the network. So when malicious node receive RREQ they doesn't check own routing table and immediately send reply to source node that it is the shortest distance, after receiving the Fake RREQ response sender node record the fake RREP and add it to his malicious list. After it inform to all nodes in the network.

Monitoring Phase

Each node in the network monitor the neighbour node each has neighbour id if any malicious node identified it does not forward data to next node so his forwarding ratio is decreasing if this ratio is less than threshold value the monitoring node immediately send alert message to source node then source node discard his entry from routing table.

Packet also get drop due to bandwidth attack by attackers also known as DOS attack see in figure 3.

1. Bandwidth is assigned to each node in the network and each has unique id.
2. Source Sends route request RREQ and receives route reply RREP from its neighbours. If any attacker nodes are identified make it as invalid path and inform to all the node in the network.
3. When source node IP Address and destination node IP are same it is consider as attacker node then discarded.
4. If the RREQ and the RREP is same, then it is consider as attacker node bypass node to step 2. Otherwise add the nodes to the network.
5. Then check latest two times if the node consume more bandwidth as compared to the assigned bandwidth, if no then not an attack, if yes then there may be possibility of attack.
6. Then check if the node, who require more bandwidth is a request bandwidth from the neighbour node, if yes then not an attack because the source node knows the location of neighbour node. If no, then it is attacker node.
7. Restore the assigned bandwidth.
8. Then simply bypass the node that is request for the bandwidth other than the neighbour node.
9. Then redistribute the bandwidth to the nodes in the network, except the attacker node.

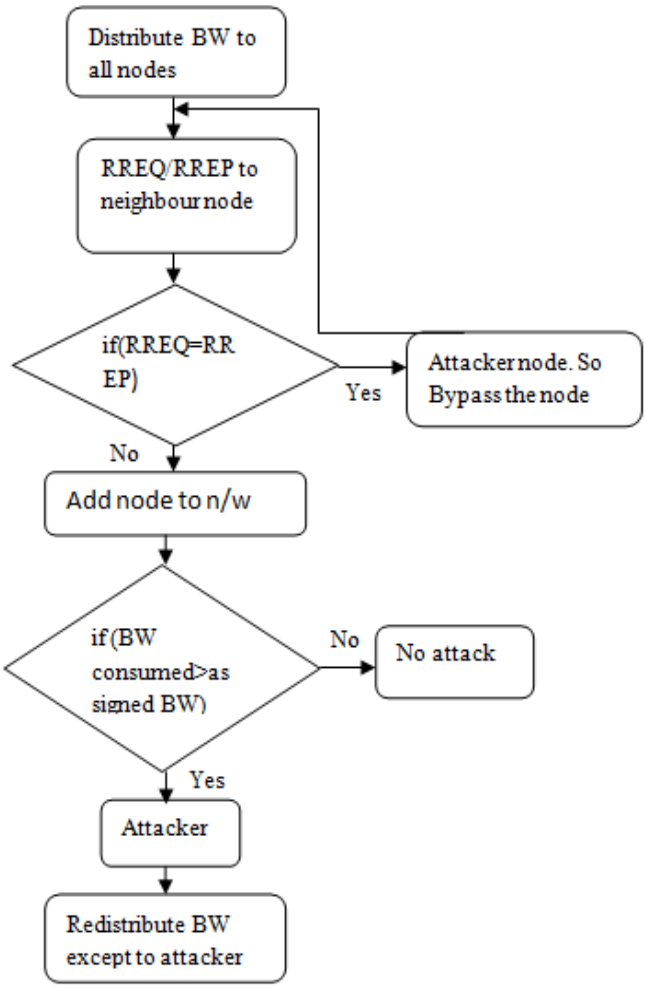

Figure 3. Flow Chart to Detect Bandwidth Attack

IV.CONCLUSION

When network is under attack, it will reduce the performance of the system. So misbehaving nodes are identified and removed from the network. This paper surveyed to prevent pack dropping and bandwidth attack in MANET. Further all possible attacks are detected and improve reliability, effectiveness and provide security to the MANET wireless system.

V. REFERENCES

[1]. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad-hoc networks: A survey" in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012.

[2]. Rasika Mali, Sudhir Bagade, "Techniques for Detection of Misbehaving Nodes in MANET: A Study" International Journal of Scientific & Engineering Research, Volume 6, Issue 8, August-2015

[3]. Gaurav Sharma, Ashish Roberts "An Overview of AODV Routing Protocol" International Journal of Modern Engineering Research (IJMERS) Vol.2, Issue.3, May-June 2012.

[4]. C. Siva Ram Murthy, B. S. Manoj, "Ad-hoc Wireless Networks Architecture and Protocols", 2nd Pearson Education, 2005.

[5]. E. Perkins, "Ad -Hoc Networking", Addison Wesley, 2001.

[6]. Anjuman Ranavadiya, Shreya Patel, " A Survey Paper on AODV Routing Protocol for MANET" IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 10, 2014

[7]. Neema Soliyal, Alok Tomar "Survey of effect of packet dropping attack in AODV routing And detection of such nodes in MANET" IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.6, No 2, Mar-Apr 2016

[8]. Vrinda Tokekar "Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks" International Conference on Pervasive Computing (ICPC) 2015.