Implementation of AODV Protocol and Detection of Malicious Nodes in MANETs

Savithru Lokanath[1], Aravind Thayur[2]

[1]Department of Electronics & Communication Engineering, DayanandaSagar College of Engineering, VTU, Bangalore, India

[2]Department of Computer Science and Engineering, Kammavari Institute of Technology, VTU, Bangalore, India

Abstract: ***Ad-hoc mobile networks are very dynamic, self-organizing; self-healing distributed networks which support data networking without an infrastructure. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other. Ad-hoc network is a self-organized, dynamically changing multi-hop network. All mobile nodes in an ad-hoc network are capable of communicating with each other without the aid of any established infrastructure or centralized controller. The user can use the network services efficiently and securely while moving. AODV (Ad-hoc On-demand Distance Vector) is a loop-free routing protocol for ad-hoc networks. It is designed to be self-starting in an environment of mobile nodes, withstanding a variety of network behaviors such as node mobility, link failures and packet losses. The AODV is a reactive protocol: the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up-to-date and to prevent routing loops.***

Keywords: MANET, AODV protocol, Attacks, Malicious nodes

1. Introduction

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile hosts without fixed network infrastructure and centralized administration. Communication in MANET is done via multi-hop paths. Lots of challenges are there in this area: MANET contains diverse resources; the line of defense is very ambiguous; Nodes operate in shared wireless medium; Network topology changes unpredictably and very dynamically; Radio link reliability is an issue; connection breaks are pretty frequent. Moreover, density of nodes, number of nodes and mobility of these hosts may vary in different applications. There is no stationary infrastructure. Each node in MANET acts a router that forwards data packets to other nodes. Therefore, selection of effective, suitable, adaptive and robust routing protocol is of utmost importance.

The research topics in MANETs include the various routing protocols to find the destination as fast as possible by efficiently utilizing the available resources in a network. The routing protocols can be broadly distinguished into proactive and reactive protocols. Each of them has different advantages in their own perspective, among which we are going to discuss about reactive routing protocol.

Another important research topic in MANETs is security issue. As MANETs are growing to a new heights even the breaching of network is also growing at the same rate. Since there is no centralized administration the attachment and detachment of a node in a network is become so easy because of which the MANETs are more vulnerable to attacks caused by the malicious nodes.

The different mechanisms have been proposed to fight against such breaching of network. In this report we are discussing few attacks and implementing the mechanism to fight against the *Blackhole Attack* and *Flooding Attack* which are one of the major attacks.

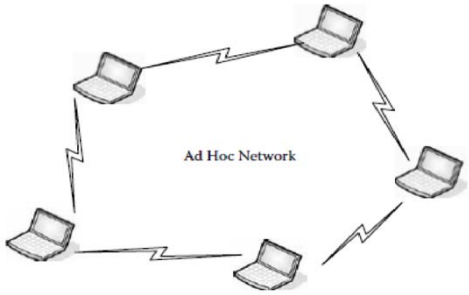

Figure 1: Ad Hoc Network

An ad hoc network is a collection of wireless mobile nodes (or routers) dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. The routers are free to move randomly and organize themselves arbitrarily; thus, the networks wireless topology may change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or may be connected to the Internet. Multi-hop, mobility, large network size combined with device heterogeneity, bandwidth, and battery power constraints make the design of adequate routing protocols a major challenge. Some form of routing protocol is in general necessary in such an environment, because two hosts that may wish to exchange packets might not be able to communicate directly, as shown in Figure 1.

2. AODV Protocol

Ad-hoc On Demand Distance Vector (AODV) is a reactive protocol that reacts on demand. It is probably the most well-known protocol in MANET. The demand on available bandwidth is significantly less than other proactive protocols as AODV doesn't require global periodic advertisements. It enables multi-hop, self-starting and dynamic routing in MANETs. In networks with large number of mobile nodes AODV is very efficient as it relies on dynamically establishing route table entries at intermediate nodes.

AODV never produces loops as there cannot be any loop in the routing table of any node because of the concept of *sequencenumber* counter. Sequence numbers serve as time stamps and allow nodes to compare how fresh information they have for other nodes in the network. The main advantage of AODV is its least congested route instead of the shortest path.

3. Working of AODV Protocol

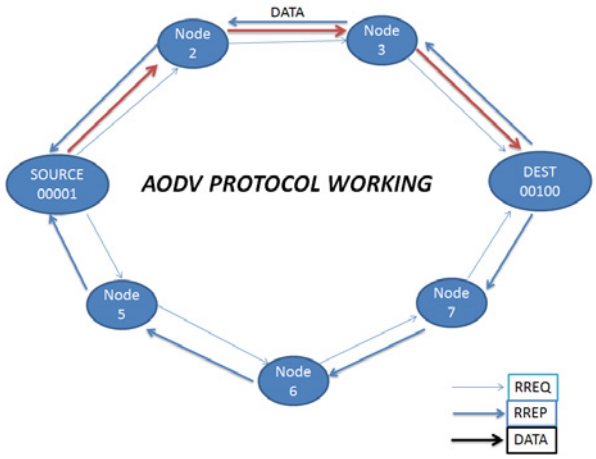

Figure 2: Working of AODV Protocol

We take an example of network topology as shown in the above figure. Here we shall consider that node 1(00001) wants to communicate with the node 4(00100).so source node(00001) first checks its routing table whether any route is available for destination node(00100) if any route exists it will send directly data packets to the destination node through the route available in the routing table. If no route available it will start route establishment phase. In our example let us consider there is no route available so source node broadcasts the RREQ packet to its neighboring nodes i.e. to node 2 and node 5.

Now the node 2 checks for the higher broadcast ID than in its Broadcast ID table and accepts only that packet.so this condition is helpful to discard any duplicate RREQ packets. Next it will check whether any route is available to destination if exists it will send the RREP packet to its previous node otherwise it will forward the RREQ to its neighbors. Here we assuming no route are initially available node 2 will forwards the RREQ to its neighboring nodes i.e. node 3.

Now node 5 also checks same as node 2 did and forwards the RREQ to is neighboring nodes i.e. node 6. Then now node 3 and node 6 will follow the same steps as node 2 did and node 3 will forward RREQ to the destination node (00100) and the node 6 will forward the RREQ to the node 7.Now the destination node will respond to the RREQ packet came from node 3 with a RREP packet and broadcasting them in the same route as the RREQ forwarded i.e. Destination node-node 3-node 2-source node. Now the node 7 will forward the RREQ to the destination node and the destination node will respond to it with a RREP packet and broadcasts in the route as the RREQ forwarded i.e. Destination node-node 7-node 6-node5-source node.

Since the Route 1(source node-node2-node3-destination node) has low hop count and reaches first to the source node, the source node will select that node as best node and sends the data packets to that route and will discard the other RREP's from other routes. After reaching of each data packet to destination, the destination node will send Acknowledgement to the source node through the same route.

4. Architecture of AODV Protocol

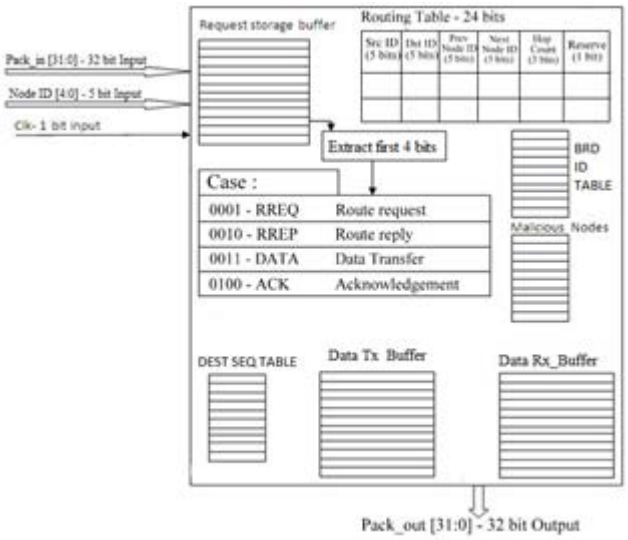

Figure 3: Architecture of AODV Protocol

5. Flowchart of AODV Protocol

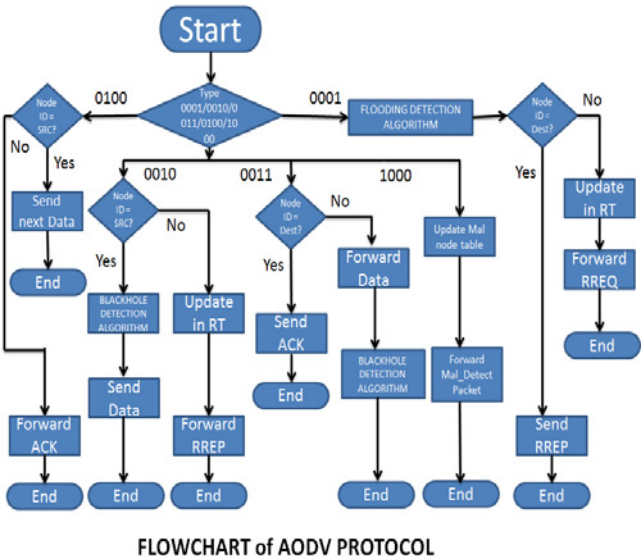

Figure 4: Flowchart of AODV Protocol

6. Attacks in MANETS

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired

network there are a number of attacks that affect MANET. These attacks can be classified into two types:

6.1 External and Internal Attack

External Attack:

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. This attack is same, like the attacks that are made against wired network. These attacks can be prevented by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated.

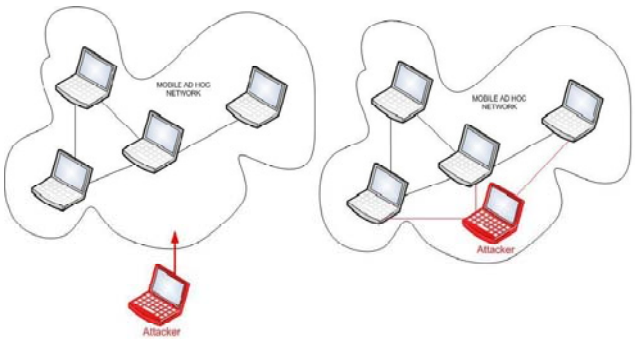

Figure 5: Showing external attack and internal attack

Internal Attack:

In internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behaviour. Internal attack is more severe attacks then external attacks.

6.2 Active and Passive Attack

Active Attack:

In active attack the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network. Active attacks can be an internal or an external attack. The active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network. Being an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service. This attack brings the attacker in strong position where attacker can modify, fabricate and replays the massages.

Passive Attack:

Attackers in passive attacks do not disrupt the normal operations of the network. In Passive attack, the attacker listen to network in order to get information, what is going on in the network? It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network.

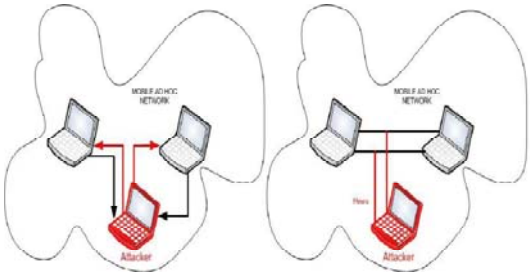

Figure 6: Showing active attack and passive attack

7. Blackhole Attack in MANETS

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept.

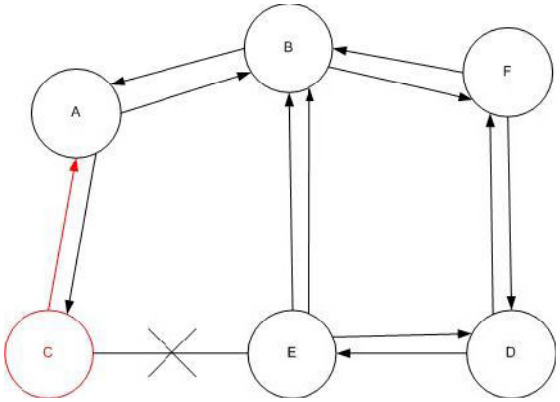

Figure 7: Black Hole Attack

This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

7.1 Detection of Blackhole Attack

Method 1:

Consider the above figure for detection of black hole attack, in which we are considering 'A' as source node and 'D' as destination node. The route has been already formed from A to D via A-B-F-D. Now the source node A sends the data to its neighboring node B. Now node B will store the Source ID, Destination ID, Data Packet No and Data in Malicious Detection Packet before forwarding the data to F, which we are considering here as black hole node.

Since node F is a malicious node it will alter the data sent by node B and it will forward the altered data to its neighboring nodes (i.e. node B and node D).

Now our aim is to detect the black hole node 'F', so we are using the Malicious Node Detection Procedure.

- When node sends or forward the data packet to its neighbouring node, first it will store the Source ID, Destination ID, Data Packet No and Data in Malicious Detection Packet.
- If the next node is the malicious node then it will alter the data and forward that packet to its neighbouring nodes.
- The previous neighbouring node which has forwarded the data packet to malicious node will now receive the packet emitted by the malicious node and compares its data by considering the
- Source ID, destination ID and packet number mentioned in Malicious Detection Packet.
- Since the data emitted by the malicious node is altered, previous node will detect that node as the malicious node.

Method 2:

In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

In this method we are detecting the Blackhole attack during route discovery phase, mainly during route reply phase. When the malicious node sends the route reply saying that it has fresh enough route to destination and it advertise the source node by including high destination sequence number in RREP packet. When the malicious node sends the RREP packet, its previous node has to check the destination sequence number present in RREP packet and the threshold value. If the value present in the RREP packet is greater than the threshold value the previous node will note its ID and consider it as malicious node. Otherwise the previous node will forward the RREP packet to its previous node and the process will continue.

7.2 Flowchart for the Detection of Blackhole Attack

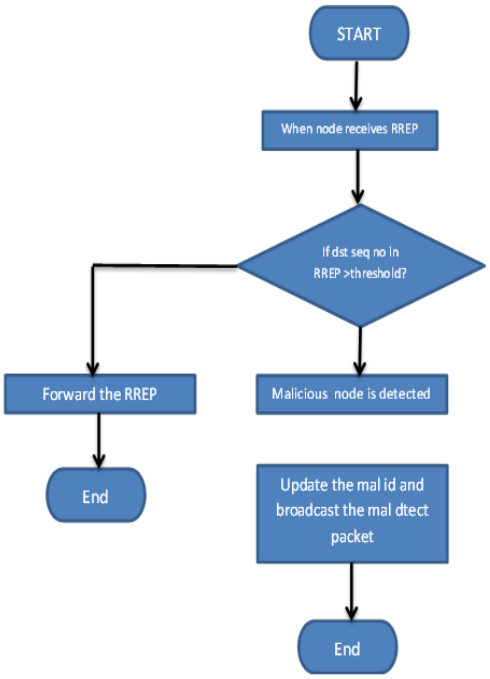

Figure 8: Flowchart of Blackhole attack

8. Flooding Attack in MANETS

Flooding attack is a denial of service type of attack in which the malicious node broadcast the excessive false packet in the network to consume the available resources so that valid or legitimated user can not able to use the network resources for valid communication. Because of the limited resource constraints in the mobile ad hoc networks resource consumption due to flooding attack reduces the throughput of the network. The flooding attack is possible in all most all the on demand routing, even in the secure on demand routing SRP, SAODV, ARAN, Ariadne etc. Depending upon the type of packet used to flood the network, flooding attack can be categorized in two categories.

- RREQ flooding
- DATA flooding

RREQ Flooding

In the RREQ flooding attack, the attacker broadcast the many RREQ packets per time interval to the IP address which does not exist in the network and disable the limited flooding feature. On demand routing protocols uses the route discovery process to obtain the route between the two nodes. In the route discovery the source node broadcast the RREQ packets in the network. Because the priority of the RREQ control packet is higher then data packet then at the high load also RREQ packet are transmitted. A malicious node exploits this feature of on demand routing to launch the RREQ flooding attack.

Data Flooding

In the data flooding, malicious node flood the network by sending useless data packets. To launch the data flooding, first malicious node built a path to all the nodes then sends

the large amount of bogus data packets. These useless data packet exhausts the network resources and hence legitimated user can not able to use the resources for valid communication.

8.1 Detection of Flooding Attack

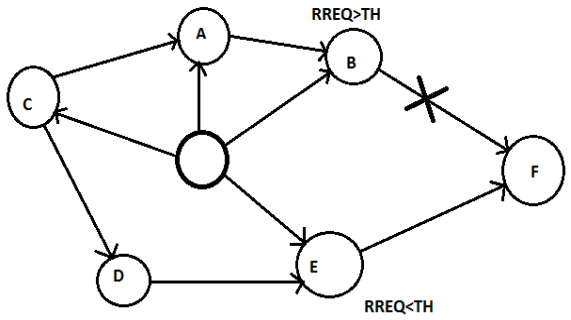

Figure 9: Flooding attack

To detect the RREQ flooding, the "Neighbor suppression method" is used. In this method a fixed threshold value is defined for every node in the network. If any node receives the RREQ flooding packet more than the threshold value then the sender is assumed as a attacker and all the packets from attacker is discarded by the receiver node. A node gets higher priority if it sends less numbers of RREQ packets.

To resist the RREQ flooding, they defined the neighbor suppression method which prioritizes the node based on the number of RREQ received. A node gets higher priority if it sends less numbers of RREQ packets and defined the threshold value.In this method a fixed threshold value is defined for every node in the network. If any node receives the RREQ flooding packet more than the threshold value then the sender is assumed as a attacker and all the packets from attacker is discarded by the receiver node. A node gets higher priority if it sends less numbers of RREQ packets.

8.2 Flowchart for the Detection of Flooding Attack

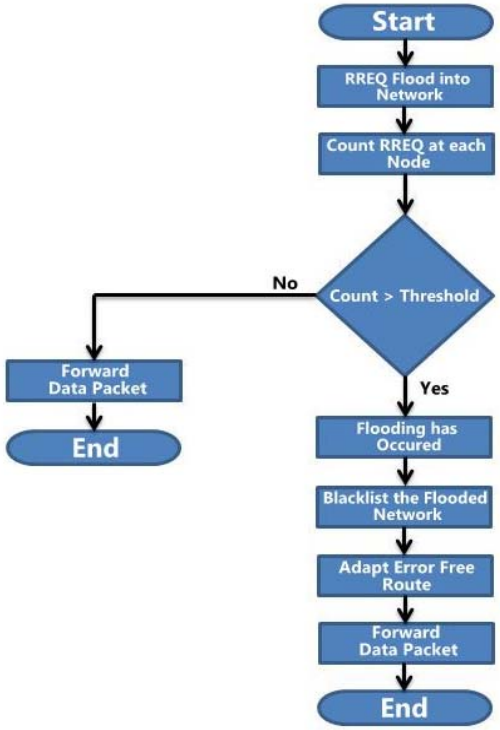

Figure 10: Flowchart of flooding attack

9. Conclusion

MANETs is a network technology which is based on self-organization of mobile nodes. Due to the random movement of nodes the network topology is a continuously changing one. Due to this characteristic of MANETs achieving a higher stable route which is free from malicious attacks is a challenging task in MANETs. In summary, the secure ad hoc on demand Distance vector algorithm suitable for use with ad-hoc networks.

AODV avoids problems with previous proposals (notably DSDV) and has the following features:

- Nodes store only the routes that are needed
- Need for broadcast is minimized
- Reduces memory requirements and needless duplications
- Loop-free routes maintained by use of destination sequence numbers
- Scalable to large populations of nodes.

Here AODV protocol is implemented on the Spartan 3 device from Xilinx family, using the VHDL, which provides stable route for longer duration and also fights against flooding and Black hole attack .In this paper, we present a distributive approach to detect and prevent the RREQ flooding attack. The effectiveness of the proposed technique depends on the selection of threshold values. Although, the concept of delay queue reduces the probability of accidental blacklisting of the. Further the proposed method can be extended to prevent data flooding also.

Hardware implementation of protocol provides efficient utilization of resources and battery power can be used

effectively. The protocol can be designed to fight against other attacks as well.

References

[1] C. Siva Ram Murthy and B.S Manoj "Ad-hoc Wireless Networks, Architecture and Protocol"
[2] Komala CR, Srinivas Shetty, Padmashree S., Elevarasi E., "Wireless Ad hoc Mobile Networks", National Conference on Computing Communication and Technology, pp. 168-174, 2010
[3] Samir R. Das, Charles E. Perkins and Elizabeth M. Royer, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks"
[4] David B. Johnson, David A. Maltz and Josh Broch," DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks",
[5] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu and Jorjeta Jetcheva, "A Performance Comparison of Multi-hop Wireless Ad Hoc Network Routing Protocols"
[6] C.M Barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in
Mobile Ad-Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

Author Profile

Savithru Lokanath obtained his B.E degree in Electronics & Communication Engineering from Dayananda Sagar College of Engineering, Bangalore, India in 2013 under the Visvesvaraya Technological University.

Aravind Thayur obtained his B.E degree in Computer Science Engineering from Kammavari Sangha Institute of Technology, Bangalore, India in 2013 under the Visvesvaraya Technological University.