Impact of Black Hole attack on Mobile Ad-hoc Networks (MANETS) Ad-hoc Demand Routing (AODV) protocol

Miss Ruchika S. Gole
Department of Information and technology
Prof Ram Meghe Institute of technology
& Research Badnera-Amravati

Miss Vasanti Y. Gaud
Department of Information and technology
Prof Ram Meghe Institute of technology
& Research Badnera-Amravati

ABSTRACT:

In this paper we have discussed some basic routing protocols from Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to that of the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack others nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. Main objective of writing this paper is to address some basic security concerns in MANET, operation of blackhole attack and securing the wellknown routing protocol Ad-hoc On Demand Distance Vector.

Keywords: MANET, AODV, DSDV, TORA, Security, Attacs, Black Hole

I. INTRODUCTION:

An ad-hoc network is a collection of wireless mobile hosts forming a temporary networkwithout the aid of any stand-alone infrastructure or centralized administration[10].

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. The Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. It represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary. Mobile ad-hoc network is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. This property of the nodes makes the mobile ad-hoc networks unpredictable from the point of view of scalability and topology.

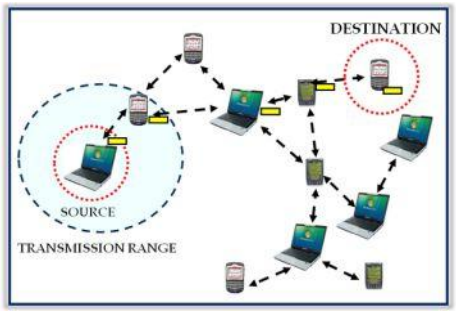

Figure 1: Mobile ad-hoc Network (MANET)

When a node wants to send data to another node, the destination node must lies within the radio range of the source node that wants to initiate the communication [1]. The intermediate nodes within the network aids in routing the packets for the source node to the destination node. These networks are fully self organized, having the capability to work anywhere without any infrastructure. Nodes are autonomous and play the role of router and host at the same time. MANET is self governing, where there is no centralized control and the communication is carried out with blind mutual trust amongst the nodes on each other. The network can be set up anywhere without any geographical restrictions. One of the limitations of the MANET is the limited energy resources of the nodes.

II. MOBILE AD-HOC NETWORKS ROUTING PROTOCOLS

MANETs routing protocols are categorized into three main categories . These are proactive routing protocols, reactive on-demand routing protocols and hybrid routing protocols as shown in fig (2). When a mobile node receives new routing information then it checks if it has a similar kind of information in its routing table. If the node already has that routing information then it compares the sequence number of the received information and the one it has. If the sequence number of the information it has is less than that of the received information then it discards the information with the least sequence number. If the both the sequence numbers are the same then the node keeps the information that has the shortest route or the least number of hops to that destination.

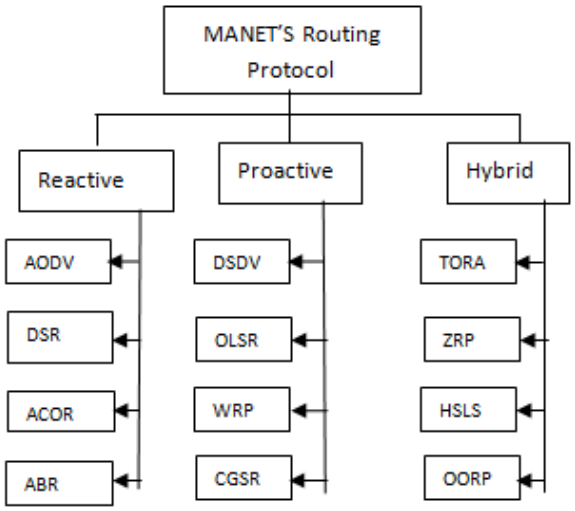

Figure 2: MANETs Routing Protocol

***2.1Reactive routing protocol*:** These protocols are also called as proactive protocols since they maintain the routing information even before it is needed [12]. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. As the routing information is usually maintained in tables, so these protocols are also called *table-driven* Protocols

2.2Proactive routing protocol: These protocols constantly maintain the updated topology of the network. Every node in the network knows about the other node in advance, in other words the whole network is known to all the nodes making that network. All the routing information is usually kept in tables [6]. Whenever there is a change in the network topology, these tables are updated according to the change.

***2.3Hybrid routing protocols*:** It is the combination of both proactive and reactive routing protocols i.e. temporary ordered routing algorithm (TORA), zone routing protocol (ZRP), hazy sighted link state (HSLS) and order one routing protocol (OOPR).

III. WORKING OF AODV:

The Ad-hoc On-demand Distance Vector (AODV) routing protocol is a reactive MANET routing protocol. AODV combines the features of proactive and reactive protocol i.e. Destination Sequenced Distance Vector (DSDV) and Dynamic Source Routing (DSR) protocols. The route discovery and maintenance process in AODV is similar to that in DSR. To explain this

We take an example of five mobile nodes as shown in Figure-3. The circles indicate the range of communication for the nodes. As each node has a limited communication range, it can communicate with its neighbor nodes only. At an instant, Node 4 wants to communicate with Node 3, but it is uncertain of the route. Node 4 broadcasts RREQ that is received by its neighbors Node 1 and Node 5. Node 5 doesn‟t have any route to Node 3 and therefore it rebroadcasts RREQ that is received back by Node 4. Node 4 drops it. On the other side, if Node 1 has a greater sequence number than RREQ, it discards RREQ and replies with RREP. If not, it updates the sequence number in its routing table and forwards RREQ to Node 2. As Node 2 has a route to Node 3, it replies to Node 1 by sending an RREP. Node 1 sends RREP to Node 4 and route Node 4-Node 1-Node 2-Node 3 is confirmed to send data packets. Node 4 can now send data packets to Node 3 through the specified route. Imagine a Node 6 in the communication range of Node 1 and Node 2. As shown in Figure-4, Node 1 moves out of network. Suppose Node 6 detects it first by not getting any HELLO message from Node 1and marks the respective route table entry for route as invalid. It sends out an RERR with the invalid route which is received by Node 2. This is how Node 2 comes to know from Node 6 that Node 1 is no longer its neighbor.

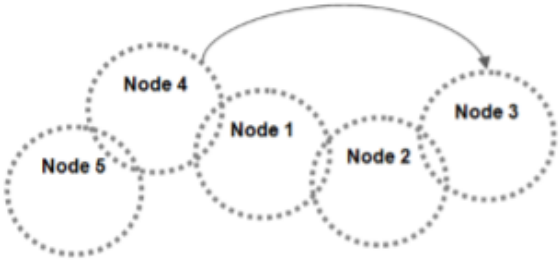

Figure-3 Communication between nodes in a Mobile Ad-hoc Network

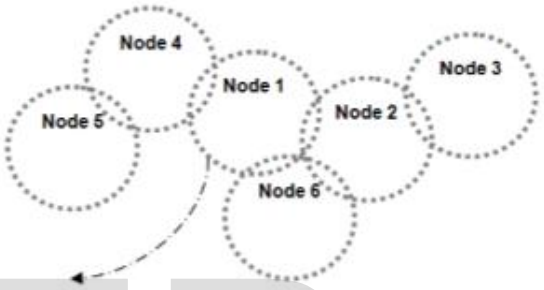

Figure-4 Node 1 moves out of communication range

IV. ATTACKS IN MANET:

As MANETs are unwired network with dynamic topology. Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic utility of network. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats [4]. There can be two kinds of attacks: passive and active. A passive attack does not disturb the normal network operation while an active attack does it. In passive attack, attacker sneaks data without altering it. Passive attacks are difficult to detect as there is no change in the functionality of the network. Active attacks can be internal or external. Internal attacks are carried out by nodes within the network

while external attacks are carried out by nodes outside the network. Modification, Impersonation and Fabrication are some of the most common attacks that cause a big security concern for MANET

4.1 Black hole Attack

In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol [9]. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device has been able to insert itself between the communicating nodes.

4.2 Gray Hole Attack

In this kind of attack the attacker misleads the network by agreeing to forward the packets in the network. As soon as it receive the packets from the neighboring node, the attacker drop the packets. This is a type of active attack.

4.3 Wormhole Attack

Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then keep on hearing the network, record the wireless data. In wormhole attack, the attacker gets themselves in strong strategic location in the network.

V. IMPACT OF BLACK HOLE ATTACK ON AODV:

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack [5].

5.1 Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination [9]. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

5.2 External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network [4]. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized in following points

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route.

In AODV black hole attack the malicious node “A” first detect the active route in between the sender “E” and destination node “D” [5]. The malicious node

"A" then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node "C".

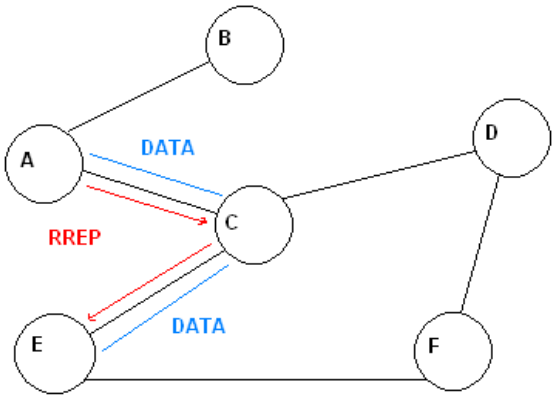

Figure 5: Black hole Attack in detail

This node "C" forwards this RREP to the sender node "E". Now this route is used by the sender to send the data and in this way data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack [9].

VI. CONCLUSION & FUTURE SCOPE:

This paper shows practically how to perpetrate black hole attacks in ad-hoc networks. After the evaluation of this use case for the protocol further performance enhancements are planned. One of the most important issues has been the research on security for MANETs. Since securing MANETs is a very challenging task no final overall solution has been developed so far. Many different approaches exist that can be applied to specific scenarios. Some of them have been described in this paper. Future work should also concentrate on the combination of security protocols in order to develop a secure MANET environment

REFERENCES:

[1] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah," MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.
[2] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhanng, "Security on Mobile Ad-hoc Networks: hallenges and Solutions" 1536-1284/04/IEEE Wireless Communications Feb., 2004.
[3] 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.
[4] M.Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile ad-hoc networks"
[5] Irshad ullah, Shoaib rehman," Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols".
[6] M.Abolhasan, T.Wysocki, E.Dutkiewicz, " A Review of Routing Protocols for Mobile Ad-Hoc Networks," Telecommunication and Infromation Research Institute University of Wollongong, Australia, June, 2003. [7] Douglas E. Comer Internetworking with TCP/IP Volume 1 Principles, Protocols, and Architecture. Prentice-Hall, Inc.
[8] Chia-Ching Ooi, N. Fisal, "Implementing a small scale MANET testbed based on Geocast enhanced AODV bis routing protocol.
[9]http://www.docstoc.com/docs/30136052/Study-of-Secure-Reactive-Routing-Protocols-in-Mobile-Ad
[10] David B. Johnson and David A. Maltz. Dynamic source routing in ad hoc wireless networks. Technical report, Carnegie Mellon
[11] Md. Golam Kaosar, Hafiz M. Asif, Tarek R. Sheltami, Ashraf S. Hasan Mahmoud," Simulation-Based Comparative Study of On Demand Routing Protocols for MANET".
[12] Charles E. Perkins. Ad Hoc Networking. Addision Wesley, 2001. University, 1996.