Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Basic Understanding of Routing Protocols for Mobile Ad-Hoc Network with a Security Threat: Black Hole Attack

Sidra Anam[1]
[1]M.Tech Scholar, CSE Department,
Pranveer Singh Institute of Technology,
Kanpur

Saurabh Gupta[2]
[2]Assistant Professor CSE Department,
Pranveer Singh Institute of Technology,
Kanpur

Abstract- The black hole problem is one of the security attacks that occur in mobile ad-hoc networks (MANETs). The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. It consists of mobile nodes that are free in moving in and out in the network. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc. Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. In this paper, we have studied the effect of black hole attack on different routing algorithms of MANET.

Keywords: Wireless Network, Mobile Ad-hoc Network, Black hole attack, Proactive protocols, Reactive protocols.

I. INTRODUCTION

The traditional routing protocols of the Internet have been designed for routing the traffic between wired hosts connected to a static backbone; thus, they cannot be applied to ad hoc networks because the basic idea of such networks is mobility with dynamic topology [11]. The two modes of operations in wireless networks are in the presence of Control Module (CM) also known as Base Stations and Ad-Hoc connectivity where there is no CM.

1.1 Ad-Hoc Networks

Ad-Hoc networks have no infrastructure where the nodes are free to join and left the network. The nodes are connected with each other through a wireless link. Whenever a node in the network is down or leaves the network that causes the link between other nodes is broken. The affected nodes in the network simply request for new routes and new links are established. Ad-Hoc network can be categorized in to static Ad-Hoc network (SANET) and Mobile Ad-Hoc network (MANET).

1.1.1 Static Ad-Hoc Networks

In SANET, the geographic location of the nodes or the stations is fixed. There is no mobility in the nodes of the networks, that's why they are known as static Ad-Hoc networks.

1.1.2 Mobile Ad-Hoc Networks

MANETs are a set of mobile nodes which are self-configuring and connected by wireless links automatically as per the defined routing protocol [12]. Mobile Ad-Hoc network topology is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. This property of the nodes makes it unpredictable from the point of view of scalability and topology.

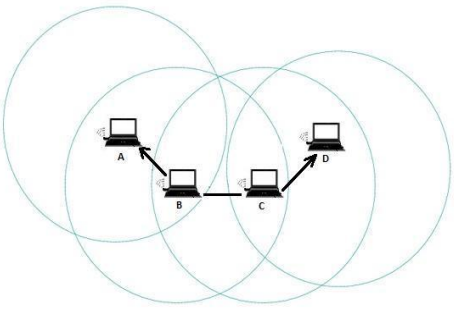

Fig.1 Mobile Ad-Hoc Network

II. MANETs ROUTING PROTOCOLS

Routing protocols in MANETs are classified into three different categories according to their functionality:

1. Reactive
2. Proactive
3. Hybrid

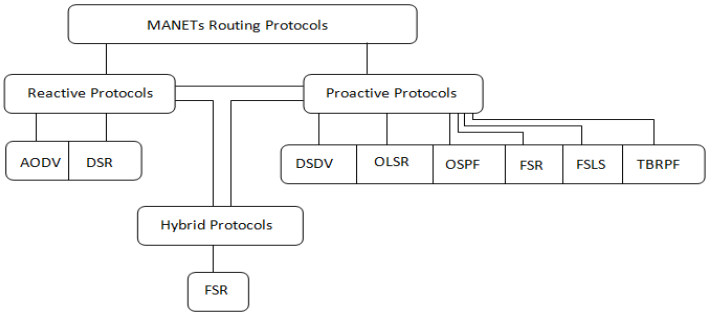

Fig. 2 MANETs Routing Protocols

2.1 Reactive Protocols

Reactive protocols also known as demand-driven reactive protocols. They do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. These protocols setup routes when demanded [3, 4]. When a node wants to communicate with another node in the network, and the source node does not have a route to the node it wants to communicate with, reactive routing protocols will establish a route for the source to destination node.

2.1.1 Ad-Hoc On Demand Distance Vector Protocol (AODV)

It is a reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. It use control messages to find a route to the destination node in the network. There are three types of control messages in AODV which are discussed below [10].

Route Request Message (RREQ):

Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP):

A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply. RREP message is send back to the originator node.

Route Error Message (RERR):

Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

Route Discovery Mechanism in AODV:

When a node "A" wants to initiate transmission with another node "G" as shown in the figure 3, it will generate a route request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forwarded to the neighbors, and those node forward the control message to their neighbors' nodes. This process of finding destination node goes on until it finds a node that has a fresh enough route to the destination or destination node is located itself. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is established between "A" and "G", node "A" and "G" can communicate with each other [10]. Fig. 2.2 depicts the exchange of control messages between source node and destination node.

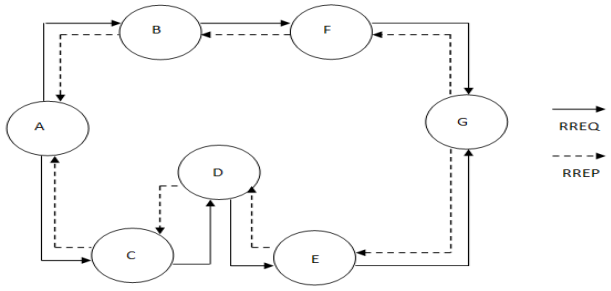

Fig. 3 AODV Route Discovery

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating the destination node i.e. from the node "A" to the neighbors nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error, where "A" is source node and "G" is the destination node. The scheme is shown in the figure 4 below.

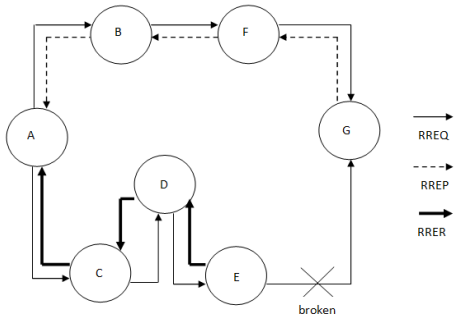

Fig. 4 Route Error Message in AODV

2.1.2 Dynamic Source Routing Protocol

Dynamic source routing protocol (DSR) is also a reactive protocol. DSR use to update its route caches by finding new routes. It updates its cache with new route discovered or when there exist a direct route between source and destination node. When a node wants to transmit data, it defines a route for the transmission and then starts transmitting data through the defined route [9]. There are two processes for route discovery and maintenance which are described below.

2.1.2.1 Route Discovery Process:

When a source node wants to start data transmission with another node in the network, it checks its routing cache. When there is no route available to the destination in its cache or a route is expired, it broadcast RREQ. When the destination is located or any intermediate node that has fresh enough route to the destination node, RREP is generated [1]. When the source node receives the RREP it updates its caches and the traffic is routed through the route.

2.1.2.2 Route Maintenance Process:

When the transmission of data started, it is the responsibility of the node that is transmitting data to confirm the next hop received the data along with source route. The node generates a route error message, if it does not receive any confirmation to the originator node. The originator node again performs new route discovery process.

2.2 Proactive Protocols

Proactive routing 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 [2]. Whenever there is a change in the network topology, these tables are updated according to the change. The nodes exchange topology information with each other; they can have route information any time when they needed [2].

2.2.1 Optimized Link State Routing Protocol (OLSR)

It is proactive routing protocol that is also known as table driven protocol by the fact that it updates its routing tables. It employs an efficient link state packet forwarding a mechanism called Multipoint relaying. OLSR optimizes the pure link state routing protocol. Conceptually OLSR topology discovery involves two phases: neighbor discovery and topology discovery. In the first phase, neighbor nodes are discovered by using Hello messages. The exchange of Hello messages in OLSR allows the selection of those MPR nodes. MPR nodes are responsible for broadcasting topology control (TC) message which would be flooded through the network in the second phase. OLSR has also three types of control messages which are describe below [7].

Hello

This control message is transmitted for sensing the neighbor and for Multi Point Distribution Relays (MPR) calculation.

Topology Control (TC)

These are link state signaling that is performed by OLSR. MPRs are used to optimize these messaging.

Multiple Interface Declaration (MID)

MID messages contains the list of all IP addresses used by any node in the network. All the nodes running OLSR transmit these messages on more than one interface.

2.2.1.1 Working of OLSR

Multi Point Relaying (MPR)

OLSR diffuses the network topology information by flooding the packets throughout the network. The flooding is done in such way that each node that received the packets retransmits the received packets. These packets contain a sequence number so as to avoid loops. The receiver nodes register this sequence number making sure that the packet is retransmitted once. The basic concept of MPR is to reduce the duplication or loops of retransmissions of the packets. Only MPR nodes broadcast

route packets. The nodes within the network keep a list of MPR nodes. MPR nodes are selected with in the vicinity of the source node. The selection of MPR is based on HELLO message sent between the neighbor nodes. The selection of MPR is such that, a path exist to each of its 2 hop neighbors through MPR node. Routes are established, once it is done the source node that wants to initiate transmission can start sending data.

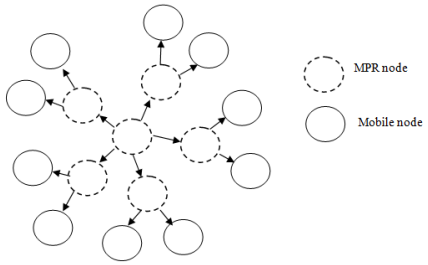

Fig. 5 Flooding Packets using MPR

The whole process can be understood by looking into the figure 6 below. The nodes shown in the figure are neighbors. "A" sends a HELLO message to the neighbor node "B". When node B receives this message, the link is asymmetric. The same is the case when B send HELLO message to A. When there is two way communications between both of the nodes we call the link as symmetric link. HELLO message has all the information about the neighbors. MPR node broadcast topology control (TC) message, along with link status information at a predetermined TC interval [7].

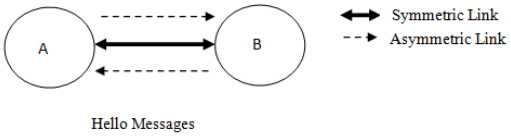

Fig. 6 Hello Message Exchange

2.3 Hybrid Protocols

Hybrid protocols exploit the strengths of both reactive and proactive protocols, and combine them together to get better results.

2.3.1 Zone Routing Protocol (ZRP)

The network is divided into zones, and use different protocols in two different zones i.e. one protocol is used within zone, and the other protocol is used between them. ZRP uses proactive mechanism for route establishment within the nodes neighborhood, and for communication amongst the neighborhood it takes the advantage of reactive protocols. These local neighborhoods are known as zones, and the protocol is named for the same reason as zone routing protocol. Each zone can have different size and each node may be within multiple overlapping zones. The size of zone is given by radius of length P, where P is number of hops to the perimeter of the zone [3].

2.3.2 Secure Zone Routing Protocol (SZRP)

A secure hybrid ad hoc routing protocol, called Secure Zone Routing Protocol (SZRP), which aims at addressing the above limitations by combining the best properties of both proactive and reactive approaches. The proposed protocol is based on the concept zone routing protocol (ZRP). It signature and both the symmetric and employs an integrated approach of digital asymmetric key encryption techniques to achieve the security goals like message integrity, data confidentiality and end to end authentication at IP layer [8].

III. SUMMARY TABLE

We have discussed different MANETs Routing Protocols. All of these can be summarized in the following table:

MANETs Routing Protocols	Routing Algorithm	Messages	Description	References
Reactive (demand-driven)	AODV	RREQ	When a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network.	[10]
		RREP		
		RERR		
	DSR	RREQ	DSR use to update its route caches by finding new routes. It updates its cache with new route discovered or when there exist a direct route	[9]
		RREP		

		RERR	between source and destination node. When a node wants to transmit data, it defines a route for the transmission and then starts transmitting data through the defined route.	
Proactive (table-driven)	OLSR	Hello TC MID	It employs an efficient link state packet forwarding a mechanism called Multipoint relaying. OLSR optimizes the pure link state routing protocol.	[7]
Hybrid	ZRP	Hello	It uses proactive mechanism for route establishment within the nodes neighborhood, and for communication amongst the neighborhood it takes the advantage of reactive protocols.	[3]
	SZRP		It employs an integrated approach of digital signature and both the symmetric and asymmetric key encryption techniques to achieve the security goals like message integrity, data confidentiality and end to end authentication at IP layer	[8]

Table 1: Summary table of MANETs Routing Protocols

IV. SINGLE BLACK HOLE ATTACK IN MANET

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. 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 [4]. 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 [5]. The method how malicious node fits in the data routes varies. Figure 7 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

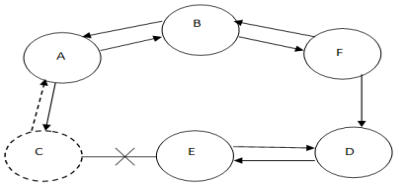

Fig. 7 Single Black Hole Problem

4.1 Black hole attack in AODV

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

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. 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 [13]. This attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

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. It can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET [13].

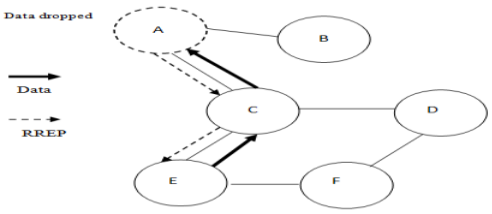

Fig. 8 Black hole attack specification

In AODV black hole attack the malicious node "A" first detect the active route in between the sender "E" and destination node "D". 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". 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.

3.2 Black hole attack in OLSR

Here a malicious node forcefully selects itself as MPR. Malicious node keep its willingness field to Will always constantly in its HELLO message. So in this case, neighbors of malicious node will always select it as MPR. Hence the malicious node earns a privileged position in the network which it exploits to carry out the denial of service attack. This attack is much vulnerable when more than one malicious node is present near the sender and destination nodes.

V. CONCLUSION AND FUTURE SCOPE

In this paper we have studied the working of different MANETs routing algorithms like AODV, DSR, OLSR, ZRP and SZRP. These routing algorithms are prone to many security attacks. We have seen the effect of Black Hole attack on AODV and OLSR. The analysis has proved that the vulnerability of two protocols OLSR and AODV have more severe effect when there is higher number of nodes and more route requests. In this paper we have studied only single node black hole attack to be in the route. The future work can be based on the group attack for this problem.

REFERENCES

[1] Zhu, C. Lee, M.J.Saadawi, T., "RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing Protocols", IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.

[2] 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.

[3] http://www.netmeister.org/misc/zrp/zrp.html#SECTION00041000000000000000

[4 K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology, Sweden, 22nd March 2007.

[5] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006.

[6] Park V, Corson S (1998) Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification. Internet Draft, Internet Engineering Task Force MANET Working Group.

[7] T.Clausen, P. Jaquet, IETF Request for Comments: 3626 Optimized Link State Routing Protocol OLSR, October 2003.

[8] Niroj Kumar Pani, "A Secure Zone-based Routing Protocol for Mobole Ad hoc Networks", Partial thesis, NIIT, Rourkela, Orissa 769008, India May 2009.

[9] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Comp. Commun. Rev., Oct., 1994, pp. 234–44.

[10] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector routing", In IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100,
Feb. 1999.[11] Janne Lundberg, Helsinki University of technology, "Routing Security in Ad Hoc Networks", **http://citeseer.nj.nec.com/400961.html**.

[12] Pradeep Kumar Sharma, Shivlal Mewada and Pratiksha Nigam, "Investigation Based Performance of black and gray hole attack in Mobile Ad hoc Network", ISROSET, Volume-01 , Issue-04.

[13] Chanchal Aghi and Chander Diwaker, "Black hole attack in AODV routing protocol: A Review", IJARCSSEE, Volume 3, Issue 4, April 2013.

