Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey of Behavior of MANET Routing Protocols Under Black-hole Attack

Jasvinder, Monika Sachdeva
CSE Department, SBSSTC Ferozepur,
Punjab Technical University(Punjab), India

Abstract:-Mobile ad hoc network (MANET) is a collection of communication devices and mobile nodes through an intermediary joint wireless to communicate with each other, without pre-defined infrastructure or central authority exists. . Lacking of central administration or fixed infrastructure in this case is a key feature of the network from intruders. Security issues in MANET at the present time are a difficult task. MANET likely due to the presence of a limited number of resources, the lack of a central authority and the positive and negative make it more vulnerable to attacks. Black hole attack, packets is dropped at the network layer, which reduces network performance. This paper identifies the black hole attack performance in the presence of ad hoc on demand distance vector (AODV) and optimized link state routing protocol (OLSR). We have a detailed analysis of the impact of such attacks, in order to show the necessary preventive measures to attack.

Keywords: Mobile Ad-Hoc Networks (MANETs), Black hole Attack, Ad-Hoc On Demand Distance Vector (AODV) , Dynamic source routing (DSR), Optimized Link State Routing (OLSR) Protocol

I. INTRODUCTION

Mobile network is a kind of network that of self-regulation by the mobile node, have the ability to help each other fixed of communicating condition. There are no dedicated routers, servers, access points, and base stations. If two mobile nodes are within each other's transmission range, they can communicate with each other directly. Otherwise, the nodes in between have to forward the packets to them from source node to the destination node. In such cases, every mobile node has to function as a router to forward the packets for others. So Mobility one advantage of wireless communications: gives a move freely, and are linked in a network environment. A Network dedicated to it is flexible that nodes can join and leave the network easily. However, this contract laptop flexibility of in a dynamic topology, in a safe position allocated guidance protocols. Security the serious problem makes the difficulties it very, the ad hoc nature of the network makes them vulnerable to malicious attack opponents . First, wireless links renders use ad hoc mobile networks are prone to various types of attacks - the black hole attack. The use of the wireless link, and the lack of fixed infrastructure and related articles of the custom dynamic topology network, which makes it impossible to use the wired network security mechanisms.

II. ROUTING PROTOCOL

The ad hoc routing protocol is a convention or standard that controls how the contract decides which way to route packets between mobile computing devices in peer networks. In ad hoc network main objective is to develop a routing protocol optimal path (minimum hop) with minimal overhead and minimal bandwidth consumption, so that timely delivery of packets between the source and the destination. MANET routing protocols currently available split to proactive routing protocols, reactive and hybrid [4]. Proactive routing protocol, each node of the other nodes in an active search, and periodically exchange routing information to ensure that the information contained in the routing table yet and correct, such as DSDV (Destination sequence distance carriers) OLSR (optimized link routing protocol) state. Routing protocols reactive, such a route, and established only when two nodes transmit data, and therefore, is also known as routing protocols based on demand, such as AODV (Ad-hoc on demand distance vector) or DSR (dynamic source routing) [5],[7] the source node broadcasts a request path is sent to flood through the entire network, to search for and secure a passage to the destination node. Organized contract guidance hybrid wireless set this idea, and then assigns a set of nodes outside different functionalities

Ad-Hoc on demand vector(AODV) routing protocol **:-**Allocated for consideration of ad-hoc on demand distance vector (AODV) is the protocol. In direct reaction of pure networks allocated using the AODV [1] protocol routing, in the hope of a mobile node with other nodes of the communication first broadcast RREQ (forwards the request) Message to find a new route to node. This discovery process the desired path is known, each one hop neighbor received the first broadcast RREQ, the RREQ keeping track sent along its routing table.

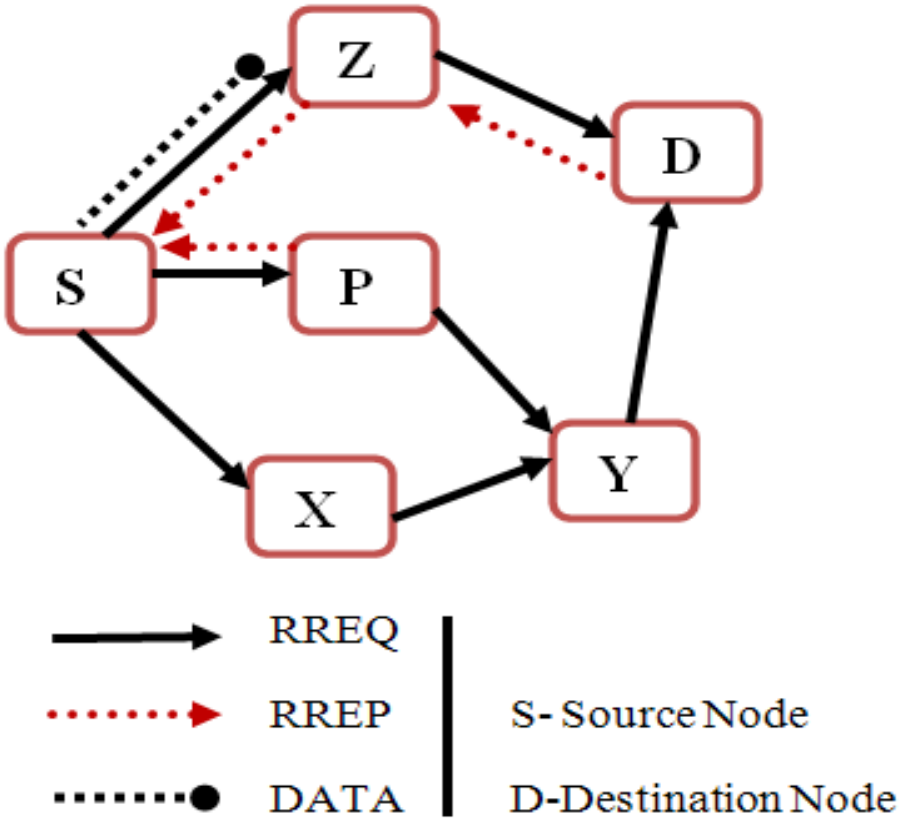

Fig 1. Propagation of RREQ and RREP from A to E

It checks later in its routing table to see if he has enough of a new road to the destination node provided in the freshness RREQ Message. The road indicated by the sequence number a destination the attached to it. If you find a way node fresh enough, it unicasts (Post Road) RREP message back along the path saved to the source node or re-broadcast the message RREQ otherwise. Continue same process even message RREP from the destination node or a node argument which has routes to fresh destination node is received by the node source [11].

Dynamic source routing (DSR) Routing Protocol **:-** Simple process each node in the network maintains a route cache in which it caches roads has learned that. To send data to another node, if it is found on the road in its path cache, the sender puts this road (a list of all the intermediate nodes) in the packet header and forwards it to the next stage in the path. Each intermediate node examines head and retransmits to the node indicated after its ID in the path the packet. If there is no route is found sender stores the packet and the gets track using the discovery process track is described below.

Route maintenance and discovery to find a route to the destination, broadcast source a route request packet to all nodes within radio transmission. In addition to the source addresses and destination decade, path packet contains the requested track record, which contract record of that accumulated at the request of the package track visited. When a node receives a request path, it does the following. If the destination address of the request matches the address its own, it's the destination. Track record in the package contains on the route there quest by reaching this node from the source. This route is sent back to the source package in the way of reply following the same route in reverse order. (We assume bidirectional links. Not be considered an alternative response mechanism for unidirectional links here.) Otherwise, it is an intermediate node. If you do not see this request before the knot and contains the path to the destination table in its cache, it creates a route reply packet with the road from the cache, and send it to the source [4] [9]. These responses are called intermediate node responses, and if it does not have a track, it appends its own address to the road record, and hop count increases by one, and re-broadcast the request. When it receives a reply source path, it adds this path to the cache and sends any pending data packets. If any link is broken on the path to the source (detected by the MAC layer of the transmitting node), an error packet is generated in the path. And unicasted error way back to the source using part of the road has passed so far, and erases all entries that contain the broken link in the road caches along the way[10].

*Optimized Link State Routing Protocol (OLSR)***:-** Optimized Link State Routing Protocol (OLSR) [6] declaration of advanced mobile networks allocated. It acts as a Spreadsheet, which turned positive agreement network information regularly topology with other nodes. OLSR is Mobile ad hoc network routing protocols active. Agreement will inherit the stability of a link-state algorithm, and Methods available immediately, if needed, because of its positive advantages. OLSR is optimized in the classic link-state protocol, designed to declare the ad hoc mobile networks. OLSR reduces the overhead of flooding using only selected nodes, called MPRs, retransmission control information, traffic control.

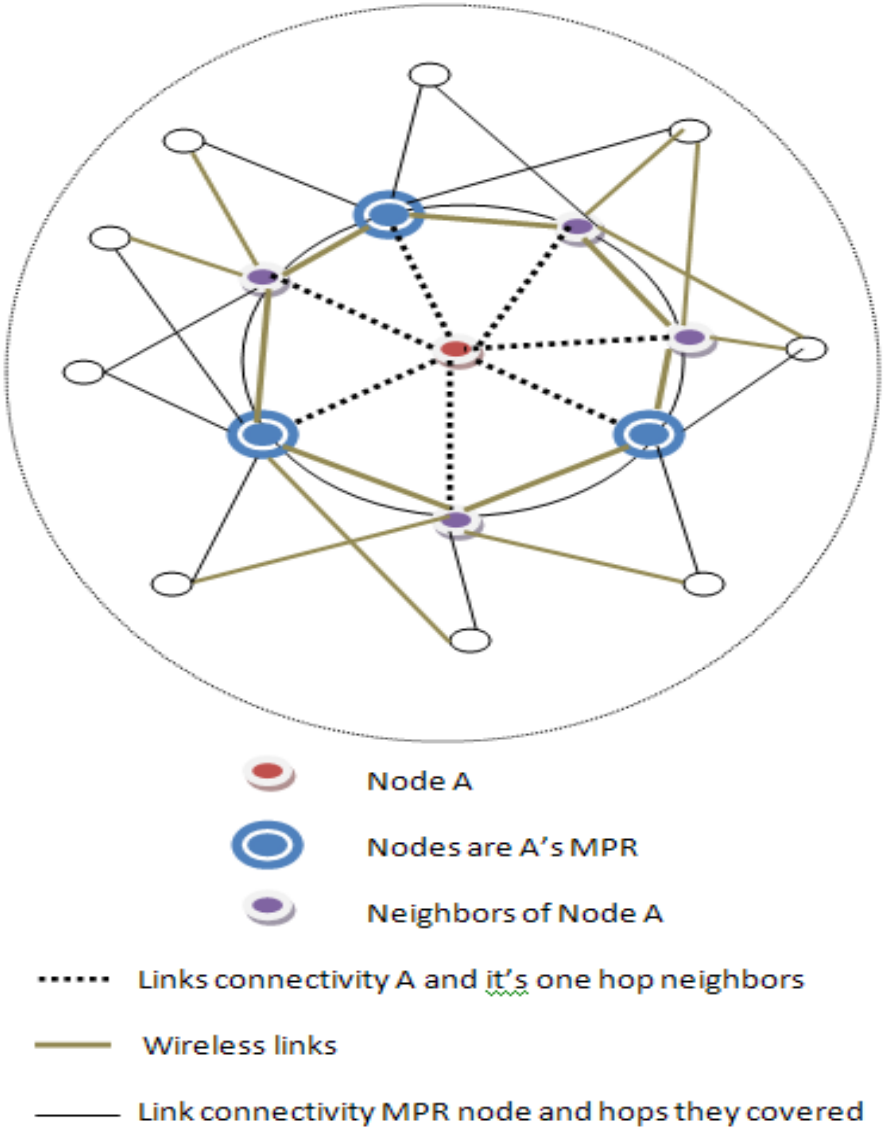

Fig 2: OLSR Working in MANET

This method significantly reduces the need to flood a message to all nodes in the number of retransmissions Network. Secondly, OLSR only partially submerged link state, to provide the shortest route. That Must be a small group of link state information needed, all nodes, named MPRs, to announce the MPR has links Specified. Additional topology information, if it exists, it can be used, such as redundancy purposes. OLSR is designed Work in a fully distributed, does not rely on any central entity. Does not require the agreement Reliable transmission of control messages: each node sends a control message on a regular basis, it cannot be maintained some of these messages reasonable wear and tear. These losses occur frequently due to collision or other wireless network Transmission problems. In addition, OLSR does not require a sequence of messages. Each message contains control Increase for each message sequence number. Therefore, the receiver control message, if necessary, it can be easily To determine what the most recent information - even if the rearrangement of the message, and the sending process.

The main concept of this agreement is the use of "multi-point relay (MPR). Each node adjacent to the group of their choice MPR node [3],[8]. Node only, select this MPRs, responsible for the generation and transmission of information topology, Used to spread to the entire network. MPRS flooded topology information to provide an effective mechanism for Reducing the required number of transmissions. Agreement is the most suitable for large-scale and high-density network technology MPRs work well in this context. The basic tasks include OLSR neighbor's sensor, multi- Relay selection, topology and routing table published account.

III. 3. Black Hole attack

Black hole attack in AODV:-Black hole attack [1] [2], is a denial of service attack, a malicious node can attract fresh path to the destination lied to all of the data packets. In for forwarding them is shown below in Figure 3, imagine node "M" a malicious.When the node "S" radio node "Z" and "X" and "M" package a RREQ, accept it. "M" node, a malicious node does not check its routing table to route requests to the node "D". Thus, it immediately sends back pack RREP, claiming a route to the destination. Of "M", "S" node receives the RREP advance RREP of "Z" and "X".

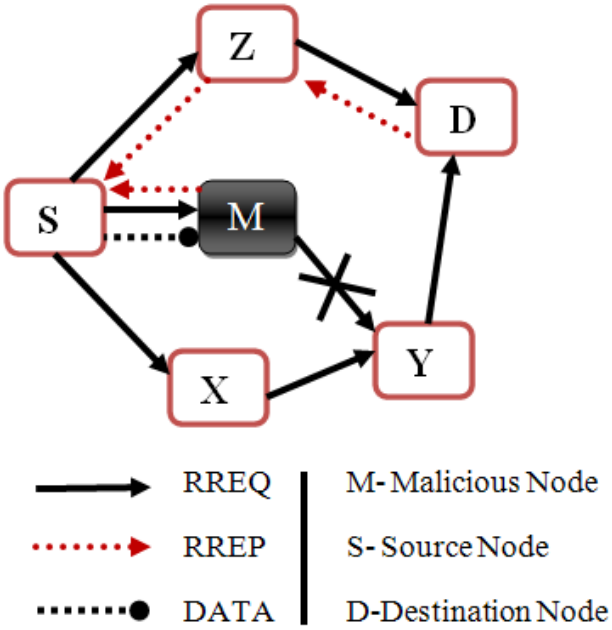

Fig.3. Black hole Attack in AODV

Suppose that the node "S", "M" is the shortest road route and send any data packet's destination through.

Black Hole Attack in OLSR:-In order to run DOS attack OLSR send HELLO and / or TC(Topology control) false messages to the nodes , which is reasonable, because it is used to provide basic network connectivity. The first possibility is to send the only TC fraud message. This is reasonable because it is through the local validation [8], and failed to detect fake messages TC. The second possibility is both messages Welcome false and TC. This is not specified method, in this work, as it gets on one node message TC, including its IP address, regardless of the originator, the neighbors will be able to detect attacks. We have implemented a third way. As the black hole node sends welcome messages and a fake TC. In this process, the attack messages, which requires actually more neighbors. Consequently, there is a high probability; the node is selected as MPR by its neighbors.

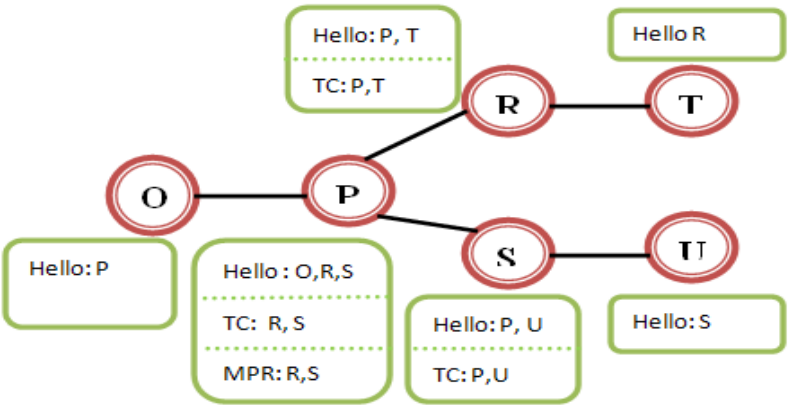

Figure 3: (a). OLSR without Blackhole

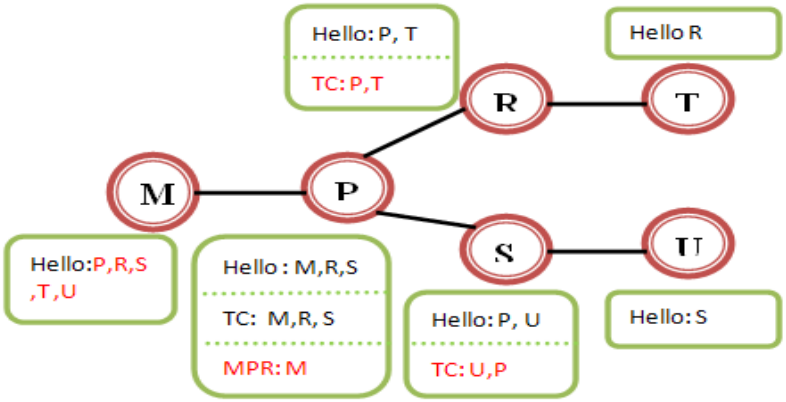

Figure 3: (b). OLSR with Blackhole

More neighbors attack requires more likely impact attacks. From very little or on TC news, select the empty set since MPR spread the message of false attack, in the vicinity of the forged message TC. Therefore, the attacker is able to capture the track. Figure 3 (b) is shown in Figure 3 (a) of the network OLSR. This time the node M has taken over and used as a black hole. This causes some changes in the network. In this figure, only latitude from the network node P. Changes in the node the for the black hole the hello message is false. Did not specify the node and R, S, which sends does not contain TC package node P [12]. Moreover, R, respectively, sending a packet node T. U, via node S, node attempts to send these packets through a black hole Node. And therefore, has been to control the black hole to connect from P to T and U.

IV. Conclusion

Ad hoc networks based on service and development of in computing environment has improved. In this paper, we study three major routing protocols AODV, DSR and OLSR. Ad hoc wireless networks vulnerable to various attacks because of the physical and environmental characteristics of the node. One type of attack, the black hole, it can be easily deployed on MANET described. In the future; we intend to develop routing protocol performance simulation and analysis of the proposed solutions based on different criteria, such as packet delivery ratio (PDR), and the average delay, guidance pregnancy and productivity.

References

1. Medadian M.;Mebadi,A.; Shahri, E.," Combat with Black Hole attack in AODV routing protocol", Communications (MICC),2009 IEEE 9th Malaysia International Conference on, pp.530-535, 15-17, Dec.2009.
2. H. Weerasinghe and H. Fu, "Preventing cooperative black hole attacks in mobile ad-hoc networks: simulation, implementation and evaluation," International Journal of Software Engineering and Its Applications, *Vol. 2, No. 3* (2008) pp. 39-54.
3. Anuj Gupta, Navjot Kaur, Amandeep Kaur , "A Survey on Behaviour of AODV and OLSR Routing Protocol of Manets under Black Hole Attack" IJCST Vol. 2, Iss ue 4, Oct . - Dec. 2011 ISSN : 0976-8491 (Online) | ISSN : 2229-4333(Print)
4. Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, 2002.
5. Nor Usop, A.Abdullah "Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7, July 2009
6. http://www.ietf.org/rfc/rfc3626.txt/optimized link state routing protocol, Apr, 2013.
7. http://en.wikipedia.org/wiki/Mobile_ad_hoc_network , Apr, 2013.
8. M. Wang, L. Lamont, P. Mason, and M. Gorlatova, "An effective intrusion detection approach for OLSR MANET protocol," Proceedings of 1st IEEE ICNP Workshop on Secure Network Protocols, 2005.
9. Miss. Bhandare A. S, Dr.Mrs. Patil S.B"Study of Protocols (AODV, DSR) Of MANET (Mobile ad-hoc network)& Black hole attack in AODV" IOSR Journal of Electronics & Communication Engineering (IOSR-JECE) ISSN : 2278-2834, ISBN : 2278-8735, PP : 50-53
10. R. Boppana, A.Mathur"Analysis of the Dynamic Source Routing Protocol for Ad Hoc Networks" Workshop on Next Generation Wireless Networks, December 2005
11. A. Dande, Dr. A. A. Gurjar "Black Hole Attack in Manet's: A Review Study" International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 2, No. 3, March 2013
12. L. Sridhran R, Ali hussain & K. Satya rajesh "A Study on Black hole attack against olsr based manes" International Journal of Computer Networking,

