International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 7 July 2015

Review on various security threats and there mitigation technique for mobile ad hoc network

Shraddha Gupta[1], Dharmendra Sharma[2]
SDBCE(Sushila Devi Bansal College Of Engineering)
shradha.gupta13@gmail.com[1], dharmu41180@gmail.com[2]

Abstract: *Ad hoc is wireless, in dependable infrastructure dynamic and self organize network create among different mobile host. Network generally exists in a Disaster recoveries, military activities emergency operation .Routing protocol have a major role in mobile network, which are affected from different attacks. Ad hoc on demand distance vector (AODV) routing protocol is suitable for routing protocol. Black hole attack is a serious hazard, in this attack a malicious node add spoof route and advertise shortest path to destination node and absorbs all data packet in it. In this paper, we have surveyed and compare the existing solution to black hole attack on AODV protocol and their demerit.*

Introduction:

Ad hoc network is a Multi hop wireless networks(MHWN).It is define as a collection fo nodes that connected each other through wirelessly by using radio signals with common channel.

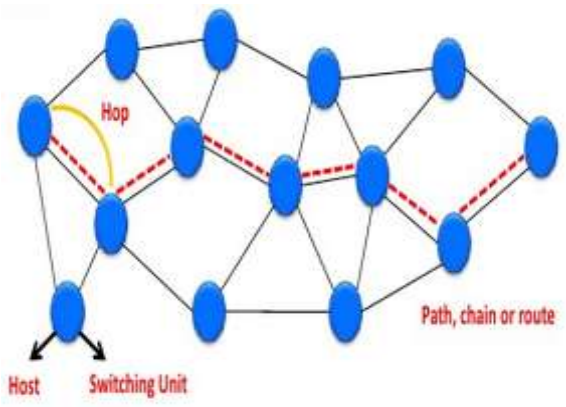

Fig. 1 Ad hoc Network

Ad hoc Network or Mobile Network. The node could be named Station or Radio Transmitters and receivers.

A mobile ad hoc network that frequently organizes in intimate and short lived network in different way. In the mobile ad hoc network, nodes can easily communicate with all the other nodes within their ranges. Changeableness of wireless connections between nodes. The wireless connection between mobile nodes in the ad hoc network is not regular for the communication participants. The nodes can regularly move into and out of the frequency range of the other nodes in the ad hoc network, and the routing information will be converting all the time because of the action of the nodes.

Ad hoc is generally used in military purpose, disaster area, personal area network and so on. In the absence of proper security mechanisms, an attacker node may join the network easily and act as an intermediate node which may be threat to security of data being exchanged.

Various problems related to security are as under:

1) Shared Broadcast Radio channel.

2) Insecure operational environment.

3) Lack of central authority.

4) Lack of association.

5) Limited resource availability.

Okoli Adaobi et. al worked to find the impact of black hole attack on the performance of MANET

and also found the impact of position of black hole node. According to them under the on

-demand routing protocol, the source of traffic is increase due to the closer of malicious node, the greater extent of damage inflicted on the network.

In this paper, we have surveyed and compare the existing solution to black hole attack on AODV protocal and their demerit

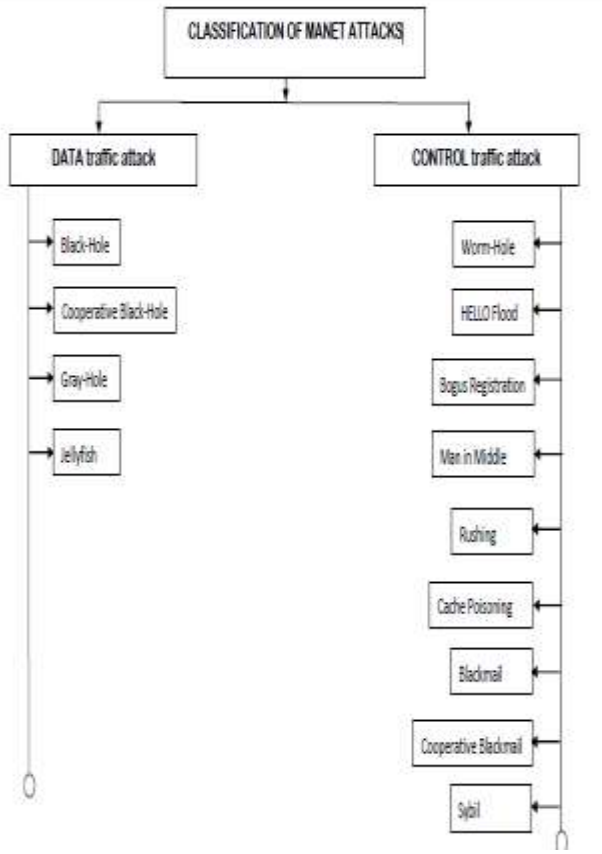

Fig. 2 Data Traffic Attack

1)Black Hole Attack: Black hole attack is malicious node and use same routing protocol that network used. The malicious node define in network that it is an only shortest path to the destination. The intention of the node may be to bottleneck the path finding process the packet being sent to destination.

Their are two type of Black hole attack can be described in AODV

Internal Black hole attack: Which fit in between the routes of gives source and destination.As soon as it get the chance this milicious node make itself an active data route element.

External Black hole attack: Physically stay outside of the network and deny access to network traffic .External attack become a kind of internal attack.

Black hole attack can be classified into to category:

1**)** Single Hole**:** In network one node is there which work as a malicious node.

2**)** Collaborative Black Hole Attack**:** More than one node work as a malicious node. Its also called attack with multiple malicious node.

3)Gray Hole Attack: Mislead the network by agreeing to forward the packet in the network's soon as it receive the packet from the neighbouring node, the attacker drop the packet .This is type of active attack. In the beginning the attacker nodes behaves normally and reply true RREP message to the started RREQ messages. When it receives the packets it dropping the packets and launch Denial of service attack. Drop packet while forwarding them in the network.

4)Jelly fish Attack: It is one of the denials of service attack and also a type of passive attack which is difficult to detect. It produces delay before the transmission and reception of data packets in the

Network. Applications such as FTP, HTTP and video conferencing are provided by UDP and TCP Jelly fish attack disturbs the performance these protocols. It is just as black hole attack but the difference is that the black hole attacker node drops all the data packets but jelly fish attacker node produces delay during forwarding packets. Jelly fish attack is categorized as Jelly fish reorder attack. Jelly fish attacks are targeted against closed loop. TCP has well known susceptibility to delay, drop and disorder the packets. Due to these nodes can change the sequence of the packets also drop some of the data packets. The jelly fish attacker

nodes fully accepts protocol rules, thus this attack is called as passive attack.

Control Traffic Attack

1) Wormhole Attack: Two attackers placed themselves strategically in the network. The attacker then keep on learning the network records the wireless data.

2) Hello Flood Attack: Some routing protocols in WSN require nodes to broadcast hello messages to announce themselves to their neighbours. A node which receives such a message may assume that it is within a radio range of the sender. In some cases this acceptance may be false; sometimes a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every other node in the network that the attacker is its neighbour.

3) Bogus Registration Attack: It is an active attack in which an attacker does a registration with a bogus care of address by masquerading itself as someone else. By advertising dishonest beacons, an attacker might be able to attract a mobile node to register with the attacker as if mobile node has reached home agent. Now, the attacker can arrest sensitive network data for the purpose of accessing network and may disturb the proper operation of network. It is difficult for an attacker to implement such type of attack because the attacker must have detailed information about the agent.

4)Man-in-Middle Atack:In cryptography and computer security, a man-in-the-middle attack (often abbreviated to MITM, MitM, MIM, MiM or MITMA) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

5)Rushing Attack:In an on demand routing protocol, a node a route require to a destination floods the network with REQUEST packets in an attempt to find a route to the destination for Route Discovery.If the Route Request for discovery forwarded by the attacker are the first to reach each neighbor of the target, then any route discovered by this Route Discovery will include a hop through the attacker

6)Cache poisioning Attack:The impact of a maliciously constructed response can be magnified if it is cached either by a web cache used by multiple users or even the browser cache of a single user. If a hit is cached in a web cache which is shared among another, such as those commonly begin in proxy servers, then all users of that cache will receive the malicious content until the cache entry is cleanup. If the hit is cached in the browser of an individual user, then that user will continue to receive the malicious content until the cache entry is cleanup, although only the user of the local browser instance will be affected

7)Black Mail Attack: At receiving a “route error” message, we look at the DRI table, if the rate is in [0, 0],we consider that this node is truly abnormal,otherwise we consider that this message was sent by an attacking node and we reject this message i.e. we will not let the Blackmail attack passed.

8) Sybil Attack: An ad hoc network is composed of mobile network, referred to as nodes that communicate only over a shared broadcast channel. A merit of such a network is that no fixed infrastructure is required: a network for routing data can be formed from whatever nodes are available. Nodes forward messages for each other to provide connectivity to nodes outside direct broadcast range.

AODV: Ad hoc On Demand Network

The Ad hoc On-Demand Distance Vector (AODV) protocol used when two end point do not have a valid active route to each other .It is dynamic, multi hop routing among mobile nodes wishing to establish and maintain an ad hoc network. AODV allows for the construction of routes to specific destination and does not require that nodes keep these routes when they are not in active communication .AODV avoid the “counting to endless” problem by using destination sequence number This make AODV lop off. The following type of message is in AODV:-

1) RREQ: Route Request Message-used to initiate the route finding Process.

2) RREP: Route Reply Message-messages are used to conclude the routes.

3) RERR : Route Error message-messages are used to notify the network of a link

breakage in an active route.

LITERATURE SURVEY

1) Raja Mohmood,R.A;Khan, A.I: According to these author the source node send two RREPs message, but selectively picking any consecutive RREP packets. This approach will likely appropriate in cases where a Black Hole node is located nearer to a source node and likely to under perform when it is located many hops away from the source node.A proposal that a source node waits for a predisposed time value to receive other RREPs with next hop details from the other neighbouring nodes, without sending the DATA packets to the early RREP node.Simultaneous the expiry of the timer, it checks in CRRT table to find out any repeated next hop node. The chance of malicious path is limited if any repeated next hop node is present in the RREP paths. And simultaneous comparison of the received RREPs, selects a neighbour which has the same next hop as other alternative routes to send the data packets. This solution adds a delay and decreases throughput as more RREPs are waited for, and the process of finding repeated next hop is an extra computation overhead.

2)Hao Yang,Haiyun Luo: They observe that how the AODV routing protocol works and then implemented black hole attack on it at the same time a trust based mechanism for its prevention. The trust based detection method has the better packet delivery ratio and correct black hole node detection probability, but suffered from the higher routing overhead due to the periodically broadcast packets. The other proposed method which is reactive detection method eliminates the routing overhead problem from the on demand way of route generation. Our complete implementation reveals that the proposed method of trust mechanism when applied on AODV protocol gives better results in all the cases for MANET as compared with normal AODV in case of black hole attack.

3) Xiao Yang Zhang;Sekiya; Y.,Wakahara. Y.: Analyze the impact of the presence of the black hole nodes on the MANET performance. They found that as the percentage of black hole nodes increases, the network performance degrades.

4)Okoli Adaobi [04] et al worked to find the impact of black hole attack on the performance of MANET and also found the impact of position of black hole node. According to them under the on-demand routing protocol, the closer a malicious node is to the source of traffic, the greater extent of damage inflicted on the network.

5)N.Balaji,A Shanmugam,"A Trust Based Model to mitigate Black hole attacks:In this paper we have presented a trust based routing model to deal with blackhole and cooperative blackhole attacks that are caused by malicious nodes. We believe that fellowship model is a requirement for the formation and efficient operation of ad hoc networks. The paper represents the first step of our research to analyse the cooperative black hole attack over the proposed scheme to analyse its performance. The next step will consist of analyzing the protocol over Grey hole and cooperative grey hole attacks.

CONCLUSION

In this paper, we studied the problem of black hole attacks under MANET Scenario. Due to the unspecified design there are many limitations of routing protocol in MANETs; many researchers have conducted various techniques to suggest different types of prevention mechanisms from black hole problem under MANET scenario. The proposals are proposed in a illogical order and divided into single black hole and cooperative black hole attack. According to this work, we observe that how the AODV routing protocol works and then implemented black hole attack on it at the same time a trust based mechanism for its prevention. The trust based detection method has the better packet delivery ratio and correct black hole node detection probability, but suffered from the higher routing overhead due to the periodically broadcast packets. The other proposed method which is reactive detection method eliminates the routing overhead problem from the on demand way of route generation. Our complete implementation reveals that the proposed method

of trust mechanism when applied on AODV protocol gives better results in all the cases for MANET as compared with normal AODV in case of black hole attack.

REFERENCE

[1] Raja Mahmood, R.A.; Khan, A.I.; , "A survey on detecting black hole attack in AODV-based mobile ad hoc networks," High Capacity Optical Networks and Enabling Technologies, 2007. HONET 2007. International Symposium on , vol., no., pp.1-6, 18-20 Nov. 2007

[2] Hao Yang; Haiyun Luo; Fan Ye; Songwu Lu; Lixia Zhang; , "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE , vol.11, no.1, pp. 38- 47, Feb 2004.

[3] N. Bhalaji, A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based MANET", European Journal of Scientific Research, Vol.50 No.1, pp.6-15, 2011.

[4] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol 3, No 5, 13-20, May 2008

[5] Songbai Lu; Longxuan Li; Kwok-Yan Lam; Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," Computational Intelligence and Security, 2009. CIS '09. International Conference on, vol.2, no., pp.421-425, 11-14 Dec. 2009.