Review Based on Black Hole Attack in MANET Environment

Hitesh Nagdev1st
Department of CSE
LNCTS (RIT)
Indore, India
E-mail: hiteshnagdev002@gmail.com

Mayur Rathi 2nd
Department of CSE
LNCTS (RIT)
Indore, India
E-mail: mayurrathi.31dec@gmail.com

Abstract: The routing protocol should detect and maintain a good route(s) between source and destination nodes in these dynamic networks. Many routing protocols have been proposed for mobile ad hoc networks, and none can be considered as the best under all conditions. This paper consist a systematic comparative evaluation of a new multipath routing protocol for MANETS should detect and maintain a various attack between source and destination nodes in these dynamic networks. Many routing protocols have been proposed for mobile ad hoc network (MANET). This paper consist a review of various attack on MANET.

Keywords: MANET, Black hole, Routing Protocol and IEEE 802_11.

I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are complimentary in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile [1]. These nodes can act as host/router or both at the same time.

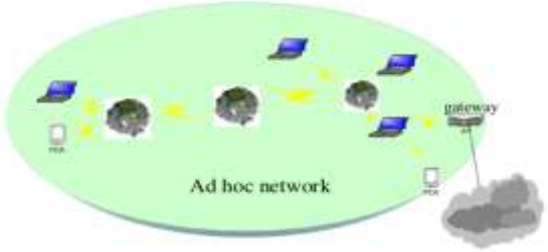

Figure1. Ad hoc Network

They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc.

II. SECURITY ISSUES IN MANET

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. 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.

In the last few years, security of computer networks has been of serious concern which has widely been discussed and formulized. Most of the discussions involved only static and networking based on wired systems. However, mobile Ad-Hoc networking is still in need of further discussions and development in terms of security [8]. With the emergence of ongoing and new approaches for networking, new problems and issues arises for the basics of routing. With the comparison of wired network Mobile Ad-Hoc network is different. The routing protocols designed majorly for internet is different from the mobile Ad-Hoc networks (MANET). Traditional routing table was basically made for the hosts which are connected wired to a non dynamic backbone [4]. Due to which it is not possible to support Ad-Hoc networks mainly due to the movement and dynamic topology of networks.

Due to various factors including lack of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are vulnerable to various attacks [2].

Major vulnerabilities which have been so far researched are mostly these types which include selfishness, dynamic nature, and severe resource restriction and also open network medium. Despite of the above said protocols in MANET, there are attacks which can be categorized in Passive, Active, Internal, External and network-layer attacks, Routing attacks and Packet forwarding attacks.

MANET work without a centralized administration where node communicates with each other on the base of mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker from inside the network. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [9]. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

III. FLAWS IN MANETS

MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is no main body that keeps watching on the nodes entering and leaving the network. All these weaknesses of MANETs make it vulnerable to attacks and these are discussed below.

Non Secure Boundaries:- MANET is vulnerable to different kind of attacks due to no clear secure boundary. The nature of MANET, nodes have the freedom to join and leave inside the network. Node can join a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes in the network. Due to no secure boundaries, MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. The links are compromised and are open to various link attacks. Attacks on the link interfere between the nodes and then invading the link, destroying the link after performing malicious behavior.

There is no protection against attacks like firewalls or access control, which result the vulnerability of MANET to attacks. Spoofing of node's identity, data tempering, confidential information leakage and impersonating node are the results of such attacks when security is compromised [3].

Compromised Node:- Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Mobile nodes in MANET are free to move, join or leave the network in other words the mobile nodes are autonomous [11]. Due to this autonomous factor for mobile nodes it is very difficult for the nodes to prevent malicious activity it is communicating with. Ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity. It can be seen that these threats from compromised nodes inside the network is more dangerous than attacking threats from outside the network.

No Central Management:- MANET is a self-configurable network, which consists of Mobile nodes where the communication among these mobile nodes is done without a central control. Each and every node act as router and can forward and receive packets [12]. MANET works without any preexisting infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for large scale Ad-Hoc network is very difficult due to no central management. When there is a central entity taking care of the network by applying proper security, authentication which node can join and which can't. The node connect which each other on the basis of blind mutual trust on each other, a central entity can manage this by applying a filter on the nodes to find out the suspicious one, and let the other nodes know which node is suspicious.

Problem of Scalability:- In traditional networks, where the network is built and each machine is connected to the other machine with help of wire. The network topology and the scale of the network, while designing it is defined and it do not change much during its life. In other words we can say that the scalability of the network is defined in the beginning phase of the designing of the network. The case is quite opposite in MANETs because the nodes are mobile and due to their mobility in MANETs, the scale of the MANETs is changing. It is too hard to know and predict the numbers of nodes in the MANETs in the future. The nodes are free to move in and out of the Ad-Hoc network which makes the Ad-Hoc network very much scalable and shrinkable. Keeping this property of the MANET, the protocols and all the services that a MANET provides must be adaptable to such changes.

IV. CLASSIFICATION OF ATTACKS

The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or/ as well as active or passive attack against the network.

External and Internal 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. While 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 behavior. Internal attack is more severe attacks then external attacks.

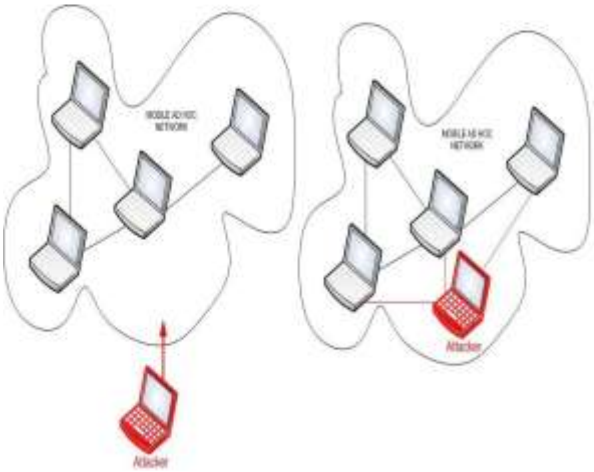

Figure2. External and Internal Attacks in MANETs

Active and Passive 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 [13]. 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. Attackers in passive attacks do not disrupt the normal operations of the network [8]. 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.

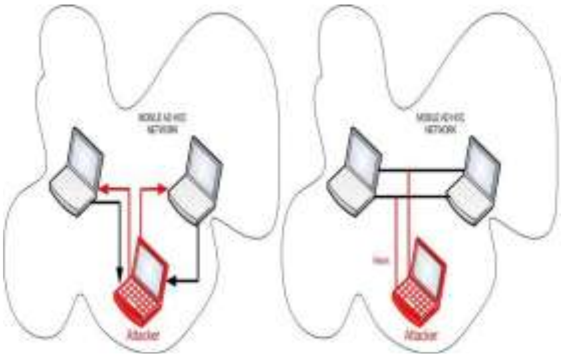

Figure3. Active and Passive Attack in MANETs

V. BLACK HOLE ATTACK IN MANET

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. These attacks are categorized in previous chapter “security issues in MANET” on the basis of their nature. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET). This chapter describes Black Hole attack and other attacks that are carried out against MANETs.

Black Hole Attack:- 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 [5]. 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].

The method how malicious node fits in the data routes varies. Fig 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.

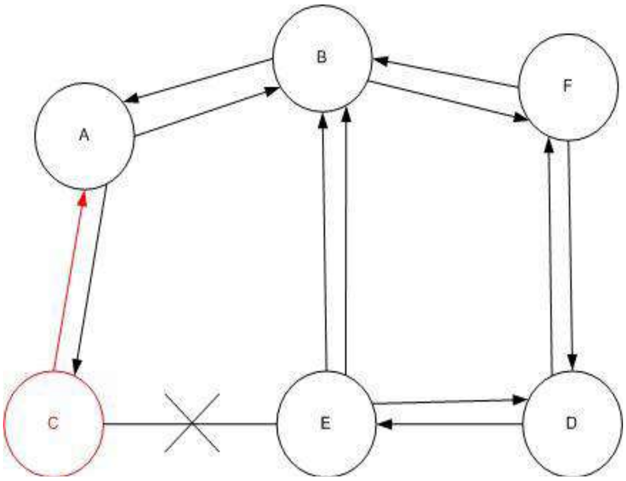

Figure4. Black Hole Problem

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. Internal 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. 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.

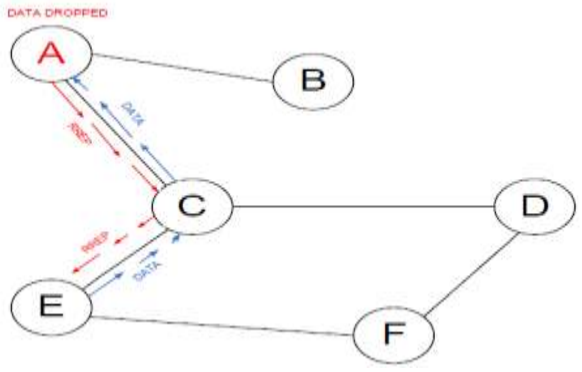

Figure5. Black hole attack specification

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.

Other Attacks on MANET

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. In the beginning the attacker nodes behaves normally and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets it starts dropping the packets and launch Denial of Service (DoS) attack. The malicious behavior of gray hole attack is different in different ways. It drops packets while forwarding them in the network. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [9]. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack [9].

Flooding Attack:- The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding [16]. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. This can be achieved by the attacker node by selecting such I.P addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker get into the network and set up paths between all the nodes in the network. Once the paths are established the attacker injects an immense amount of useless data packets into the network which is directed to all the other nodes in the network. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time.

Selfish Node:- In MANETs the nodes perform collaboratively in order to forward packets from one node to another node. When a node refuse to work in collaboration to forward packets in order to save its limited resources are termed as selfish node, this cause mainly network and traffic disruption [16]. The selfish nodes can refuse by advertising non existing routes among its neighbor nodes or less optimal routes. The concern of the node is only to save and preserves it resources while the network and traffic disruption is the side effect of this behavior. The node can use the network when it needs to use it and after using the network it turn back to its silent mode. In the silent mode the selfish node is not visible to the network.

The selfish node can sometime drop the packets. When the selfish node see that the packets need lot of resources, the selfish node is no longer interested in the packets it just simply drop the packets and do not forward it in the network.

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. The fig below shows the two attackers placed themselves in a strong strategic location in the network.

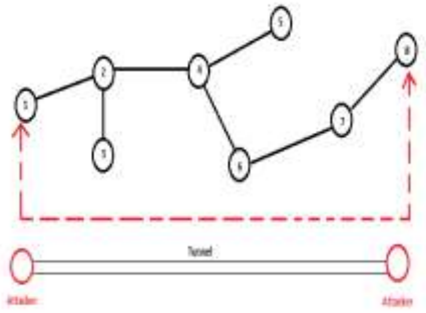

Figure6. Wormhole attack

In wormhole attack, the attacker gets themselves in strong strategic location in the network. They make the use of their location i.e. they have shortest path between the nodes as shown in the Fig. 4.5 above. They advertise their path letting the other nodes in the network to know they have the shortest path for the transmitting their data. The wormhole attacker creates a tunnel in order to records the ongoing communication and traffic at one network position and channels them to another position in the network [12].When the attacker nodes create a direct link between each other in the network. The wormhole attacker then receives packets at one end and transmits the packets to the other end of the network. When the attackers are in such position the attack is known as out of band wormhole [17].

The other type of wormhole attack is known as in band wormhole attack [17]. In this type of attack the attacker builds an overlay tunnel over the existing wireless medium. This attack is potentially very much harmful and is the most preferred choice for the attacker.

Sleep Deprivation Torture Attack:- One of the most interesting attack in MANETs, where the attacker tries to keep the nodes awake until all its energy is lost and the node go into permanent sleep. This attack is known as sleep Deprivation torture attack [18]. The nodes operating in MANETs have limited resources i.e. battery life, the node remain active for transmitting packets during the communication. When the communication cease these nodes go back to sleep mode in order to preserve their resources. The attacker exploit this point of the nodes by making it busy, keeping it awake so as to waste all its energies and make it sleep for the rest of its life. When nodes went to sleep for ever an attacker can easily walk into the network and exploit rest of the network.

Jellyfish Attack:- In jellyfish attack, the attacker attacks in the network and introduce unwanted delays in the network [19]. In this type of attack, the attacker node first get access to the network, once it get into the network and became a part of the network. The attacker then introduce the delays in the network by delaying all the packets that it receives, once delays are propagated then packets are released in the network. This enables the attacker to produce high end-to-end delay, high delay jitter and considerably affect the performance of the network.

Modification Attack:- The nature of Ad-Hoc network is that any node can join freely the network and can leave it. Nodes which want to attack join the network. The malicious node then later exploits the irregularities in the network amongst the nodes. It participates in the transmission process and later on some stage launches the message modification attack [9]. Misrouting and impersonation attacks are two types of modification attack.

VI. CONCLUSION

In this paper we discussed classification of detection mechanisms for black hole attack in static MANET. Distributed detection approach is more advantages than centralized approaches since single point failure. In witness based strategy of distributed approaches, randomness introduced in choosing witnesses at various levels like whole network and limited to geographical grids to avoid prediction of future witnesses. If chosen witness node itself captured information then detection of black hole attack is uncertain. There may be trade-off between memory, communication cost overhead and detection rate. All the approaches dealt with MANET. With the deployment knowledge (like order, neighborhoods, and group members with locations) all the nodes in the network should know highest deployed generation which impractical and can move join other groups since neighbours vary. Some MANET application requires mobile nodes. The entire approaches become complex when considering for mobile nodes which dealt with location claims(only) and Deployment knowledge are suitable for mobile MANET, since location changes time to time in mobile ad hoc network. And some other approaches for MANET have been discussed.

REFERENCES

[1] D.B.Roy, R.Chaki and N.Chaki, “A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Neworks,” International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.

[2] N.Shanti, Lganesan and K.Ramar, “Study of Different Attacks On Multicast Mobile Ad-Hoc Network”.

[3] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, “A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks,” Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[4] S.Marti, T.J.Giuli, K.Lai, M.Baker, “Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks”.

[5] 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.

[6] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, “A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks,” Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[7] V.Mahajan, M.Natue and A.Sethi, “ Analysis of Wormhole Intrusion attacks in MANETs,” IEEE Military Communications Conference, pp. 1-7, Nov, 2008.

[8] F.Stanjano, R.Anderson, “The Resurrecting Duckling: Security Issues for Ubiquitous Computing,” Vol. 35, pp. 22-26, Apr, 2002.

[9] H.L.Nguyen,U.T.Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks,” International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.