Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Attack in MANET

[1]Aarushi*, [2]Harish Bedi
[1]Department of computer science and engineering, BRCM, Bahal, Bhiwani, India
[2]Department of computer science and engineering, BRCM, Bahal, Bhiwani, India

Abstract: ***MANET is an infrastructure less network with mobile nodes. Due to mobility provided to the node i.e. dynamicity of the network the network is prone to various attacks. This paper describes various attacks and specially focuses on the wormhole attack and its variants. The paper also describes the AODV routing protocol with its packet format. The paper also describes how wormhole attacks works in AODV.***

Keywords*: MANET, AODV, Wormhole Attack*

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an ―infrastructure less network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves. Message routing is a problem in a decentralize environment where the topology fluctuates. While the shortest path from a source to a destination based on a given cost function in a static network is usually the optimal route, this concept is difficult to extend in MANET. The set of applications for MANETs is diverse, ranging from large scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to malicious attacks [1]

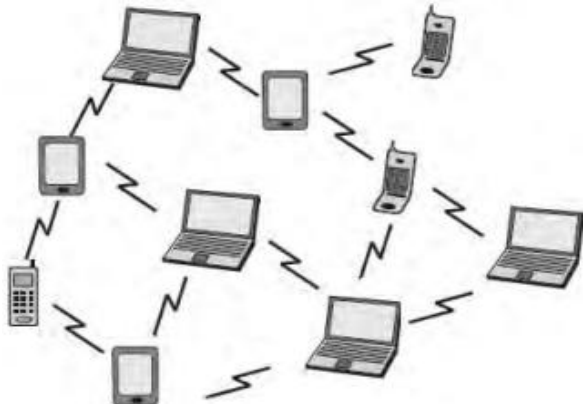

Fig. 1. MANET [2]

II. ATTACKS IN MANET

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

1. External Attack: External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

2. Internal Attack: Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities [1].

Security Attacks

Routing is one of the most vital mechanisms in the ad hoc networks. Improper and insecure routing mechanisms will not only degrade the performance of the ad hoc networks, but will also render such networks vulnerable to many security attacks. Most of the attacks is on the message, which is used to establish and maintain relationships between nodes in the networks. Attacks against the routing messages could be launched in many forms and may include all the characteristics described earlier. Information or messages could be deviated from the normal operation flow using modification, interception, interruption or fabrication attacks [3].

In a more severe case, attackers also might use any combination of these attacks to disrupt the normal information flow. As far as their concern, this study is the first to address security attacks against the ad hoc networks routing messages.

Modification

In a message modification attack, attacker makes some changes to the routing messages, and thus endangers the integrity of the packets in the networks. Since nodes in the ad hoc networks are free to move and self-organize relationships among nodes at some times might include the malicious nodes. These malicious nodes might exploit the random relationships in the network to participate in the packet forwarding process, and later launch the message modification attacks. Examples of attacks that can be classified under the message modification attacks are impersonation attacks and packet misrouting [3]

Impersonation Attacks

Impersonation attacks are also called spoofing attacks. The attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes. Usually this would be one of the first steps to intrude a network with the aim of carrying out further attacks to disrupt operation. Depending on the access level of the impersonated node, the intruder may even be able to reconfigure the network so that other attackers can (more) easily join or he could remove security measures to allow subsequent attempts of invasion. A compromised node may also have access to encryption keys and authentification information. In many networks, a malicious node could obstruct proper routing by injecting false routing packets into the network or by modifying routing information [3].

Jamming

In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered [1].

Man- In- The- Middle Attack

An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender [1].

Black hole Attacks

In this attack, malicious nodes trick all their neighboring nodes to attract all the routing packets to them. As in the wormhole attacks, malicious nodes could launch the black hole attacks by advertising themselves to the neighboring nodes as having the most optimal route to the requested destinations. However, unlike in the wormhole attacks where multiple attackers colluded to attack one neighboring node, in the black hole attacks, only one attacker is involved and it threatens all its neighboring nodes [3].

Wormhole Attacks

In the wormhole attacks, a compromised node in the ad hoc networks colludes with external attacker to create a shortcut in the networks. By creating this shortcut, they could trick the source node to win in the route discovery process and later launch the interception attacks. Packets from these two connections to create the fastest route from source to the destination node. In addition, if the wormhole nodes consistently maintain the bogus routes, they could permanently deny other routes from being established. As a result, the intermediate nodes reside along that denied routes are unable to participate in the network operations.

Wormholes and Its Variants

In wormhole attack where two colluding nodes that are far apart are connected by a tunnel giving an illusion that they are neighbors. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network from there. By using this additional tunnel, these nodes are able to advertise that they have the shortest path through them. Once this link is established,

the attackers may choose each other as multipoint relays (MPRs), which then lead to an exchange of some topology control (TC) messages and data packets through the wormhole tunnel. Since these MPRs forward flawed topology information, it results in spreading of incorrect topology information throughout the network . On receiving this false information, other nodes may send their messages through them for fast delivery. Thus, it prevents honest intermediate nodes from establishing links between the source and the destination. Sometimes, due to this, even a wormhole attacker may fall victim to its own success. In , a particular type of wormhole attack known as "in-band wormhole attack" is identified. A game theoretic approach has been followed to detect intrusion in the network. Presence of a central authority is assumed for monitoring the network. This is a limitation in wireless scenario such as military or emergency rescue. No experimental result is reported in.

In the wormhole attacks are classified as 1) In-band wormhole attack, which require a covert overlay over the existing wireless medium and 2) Out-of-band wormhole attack, which require a hardware channel to connect two colluding nodes. The in-band wormhole attacks are further divided in as 1.1) Self-sufficient wormhole attack, where the attack is limited to the colluding nodes and 1.2) Extended wormhole attack, where the attack is extended beyond the colluding nodes. The colluding nodes attack some of its neighboring nodes and attract all the traffic received by its neighbor to pass through them. In the second type of wormhole attacks, the intrusions are distinguished between a) hidden attack, where the network is unaware of the presence of malicious nodes and b) exposed attack, where the network is aware of the presence of nodes but cannot identify malicious nodes among them [4].

III. ROUTING PROTOCOLS

The nature of MANET's makes simulation modeling an important tool for understanding the operation in these networks. Multiple Ad-hoc network routing protocols have been developed in the recent years, in order to find an optimized Routes between source and destination. To make data transmission possible between two nodes, multiple hops are required due to the limited transmission range of the nodes. Due to the Mobility of the nodes the situation becomes even more complicated. Routing protocols can be categorized in three category named as proactive, reactive and hybrid protocols. Proactive routing protocols are typically table-driven such as Destination Sequence Distance Vector (DSDV). Reactive routing protocol does not regularly update the routing information. Information is updated only when there is some data need to be transmitted. Examples of reactive routing protocols are Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols are the combination of both reactive and proactive approaches such as Zone Routing Protocol (ZRP) [5].

Ad-Hoc on Demand Distance Vector Protocol

Ad-hoc On Demand Distance Vector (AODV) is a reactive protocol that reacts on demand. It is probably the most well-known protocol in MANET. It is a modification of DSDV. The demand on available bandwidth is significantly less than other proactive protocols as AODV does not require global periodic advertisements. It enables multi-hop, self-starting and dynamic routing in MANETs. In networks with large number of mobile nodes AODV is very efficient as it relies on dynamically establishing route table entries at intermediate nodes. AODV never produces loops as there cannot be any loop in the routing table of any node because of the concept of sequence number counter borrowed from DSDV. Sequence numbers serve as time stamps and allow nodes to compare how fresh information they have for other nodes in the network. The main advantage of AODV is its least congested route instead of the shortest path[6].

Routing information is stored in source node and destination node, intermediate nodes dealing with data transmission. This Approach reduces the memory overhead, minimize of the network resources, and runs well in high mobility scenario. The communication between nodes involves main three procedures known as path discovery, Path establishment and path maintenance. Three types of control messages are used to run the algorithm, i.e. Route Request (RREQ), Route Reply (RREP) and Route Error (RERR). The format of RREQ and RREP packet are shown in Table 1 and Table 2.

Table 1: RREQ Field

Source address	Source Sequence	Broadcast Id	Destination Address	Destination Sequence	Hop Count

Table 2: RREP Field

Source address	Destination Address	Destination Sequence	Hop count	Lifetime

When the source node wants to send some data to the destination node, Source will issue the route discovery procedure. The source node will broadcast route request packets to all its accessible neighbors'. The intermediate node receiving request (RREQ) will check the request whether he is destination or not. If the intermediate node is the destination node, will reply with a route reply message (RREP). If not the destination node, the request will be forwarded to other neighbor nodes. Before forwarding the packet, each node stores the broadcast identifier and the node number from which the request came. Timer is used by the intermediate nodes to delete any entry when no reply is received for the request. The broadcast identifier, source ID are used to detect whether the node has received the route request message previously or not. It prevent from the redundant request receiving in same nodes. The source node may receive more than one reply, in that case it will determine later which message will be selected on the basis of hop counts. When any link breaks down due to the node mobility, the node will invalidate the routing table. All destinations will become unreachable because of loss of the link. Then it will create a route error (RERR) message. The node sends the RERR upstream to the source node. When the source receives the Route reply message, it may reinitiate route discovery if it still requires the route [5].

Operation of Wormhole Attack in AODV

Wormhole attack is a kind of replay attack that is particularly challenging in MANET to defend against. Even if, the routing information is confidential, encrypted or authenticated, it can be very effective and damaging. An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value. Thus it prevents any other routes from being discovered. It may badly disrupt communication as AODV would be unable to find routes longer than one or two hops. It is easy for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route for tunneled distances longer than the typical transmission range of a single hop. Malicious nodes can retransmit eavesdropped messages again in a channel that is exclusively available to attacker. The wormhole attack can be merged with the message dropping attack to prevent the destination node from receiving packets.

Wormhole attack commonly involves two remote malicious nodes shown as X and Y in Figure-2. X and Y both are connected via a wormhole link and they target to attack the source node S. During path discovery process, S broadcasts RREQ to a destination node D. Thus, A and C, neighbors of S, receive RREQ and forward RREQ to their neighbors. Now the malicious node X that receives RREQ forwarded by A. It records and tunnels the RREQ via the high-speed wormhole link to its partner Y. Malicious node Y forwards RREQ to its neighbor B. Finally, B forwards it to destination D. Thus, RREQ is forwarded via S -A-X-YB-D. On the other hand, other RREQ packet is also forwarded through the path S-C-D-E-F-G-D. However, as X and Y are connected via a high speed bus, RREQ from S-A-X-Y-B-D reaches fist to D. Therefore, destination D ignores the RREQ that reaches later and chooses D-B-A-S to unicast an RREP packet to the source node S. As a result, S chooses S-A-B-D route to send data that indeed passes through X and Y malicious nodes that are very well placed compared to other nodes in the network. Thus, a wormhole attack is not that difficult to set up, but still can be immensely harmful for a MANET. Moreover, finding better techniques for detection of wormhole attacks and securing AODV against them still remains a big challenge in Mobile Ad-hoc Networks [7].

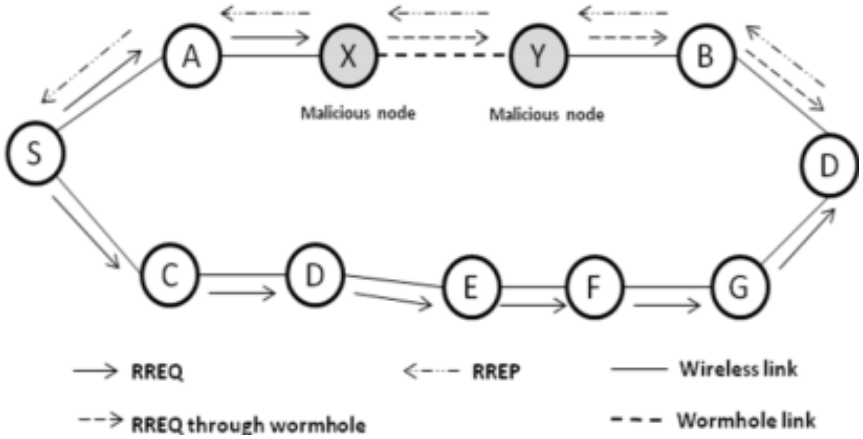

Fig. 2. Wormhole attack on AODV in MANET

IV. CONCLUSION

The paper describes the AODV routing protocol in MANET along with the wormhole attack and its operation with AODV routing protocol. The wormhole attack in the AODV routing protocol degrades the network performance. The wormhole attack must be detected and prevented to enhance the performance of the network. The technique must not increase any cost i.e. the technique must not use any extra hardware.

REFERENCES

[1] Priyanka Goyal, Vinti Parmar, and Rahul Rishi. "Manet: vulnerabilities, challenges, attacks, application." *IJCEM International Journal of Computational Engineering & Management* 11 (2011): 32-37.

[2] Mohit Kumar, and Rashmi Mishra. "An Overview of MANET: History, Challenges and Applications." *Indian Journal of Computer Science and Engineering (IJCSE),* (2012): 0976-5166.

[3] Mohd Faisal, M. Kumar, and Ahsan Ahmed. "ATTACKS IN MANET." *International Journal of Research in Engineering and Technology*, (2012): 2319-1163.

[4] Reshmi Maulik, and Nabendu Chaki. "A study on wormhole attacks in MANET." *International Journal Computer Information System Ind Manag Appl* (2011): 271-279.

[5] Achint Gupta, Priyanka VJ and Saurabh Upadhyay. "Analysis of Wormhole Attack in AODV based MANET Using OPNET Simulator." *International Journal* (2012), 1(2): 241-247.

[6] Jhaveri, Rutvij H., Ashish D. Patel, Jatin D. Parmar, and Bhavin I. Shah. "MANET routing protocols and wormhole attack against AODV." *International Journal of Computer Science and Network Security*, 10, no. 4 (2010): 12-18.

[7] Jhaveri, Rutvij H., Ashish D. Patel, Jatin D. Parmar, and Bhavin I. Shah. "MANET routing protocols and wormhole attack against AODV ." *International Journal of Computer Science and Network Security* 10, no. 6 (2010): 12-18.

