A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORK

Nidhi Choudhary
Dept.of Computer science
UCE, Rajasthan Technical University
Kota,India

Dr.Lokesh Tharani(associate proffesor)
Dept.of Electronics and communication
UCE, Rajasthan Technical University
Kota,India

***Abstract*— Mobile ad hoc networks (MANET) are collections of self-organizing mobile nodes with dynamic topologies and have no fixed infrastructure. MANET do not have centralized administration, here nodes act as both host as well as router and communicate by forwarding packets for each other in multi hop way, because of the fundamental characteristics like, the open medium, dynamic network topology, lack of centralized monitoring and management these networks are particularly vulnerable to various types of attacks. Many secure and robust routing protocols have been designed and many security schemes have been recommended to tackle these security issues. In MANET, due to presence of malicious nodes routing attacks are particularly severe. In this paper, we present a survey of security threats in MANET and examine routing threats based on whether they are dependent or independent of routing protocol.**

Keywords- *MANET,AODV, OLSR, security threats.*

I. INTRODUCTION

A mobile ad hoc network (MANET) represents complex distributed system that consists of collection of wireless mobile nodes, which are connected through wireless links. MANET does not rely on any fixed infrastructure and has dynamic topologies. Here nodes can communicate directly if they are within each other range; however nodes have to rely on other nodes to forward messages if they are not in each other range. Construction of MANET does not need any existing network infrastructure and this result in a low cost network, which even provides freedom of mobility. Due to low cost and mobility, a MANET is suitable for applications such as disaster relief, vehicle networks, casual meetings, campus networks, robot networks, emergency operations, military service, maritime communications, and so on. Unlike the conventional network, a MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes [1]. When compared with conventional wired network it is somewhat difficult to perform routing in MANET due to its dynamic nature. Considering this structure now, several efficient routing protocols have been proposed. These routing protocols can be mainly classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol [2], nodes request for and find routes only when required. In proactive routing protocols, such as the Optimized Link State Routing (OLSR) protocol [3], nodes obtain routes by periodic exchange of network topology information.

II.SECURITY GOALS

Security issues of ad hoc networks are same as that of other systems. The main requirement of these security policies is to protect communicated information from intruders and to utilize the resources in a proper way without letting them get misused. Some of the main issues that security policies must cover are explained in the following:

1. Authentication: ensures that the other end of a connection or the originator of a packet is the node that is claimed.
2. Confidentiality: ensures certain information is never disclosed to unauthorized entities.
3. Integrity: ensures that a packet is not modified during transmission.
4. Availability: ensures that network resources are available all time and also ensures the ability to sustain the networking functionalities without any interruption due to security threats.

III .SECURITY THREATS

Mobile ad-hoc networks are more vulnerable to be attacked than wired network due to their characteristics. For example in mobile communication routing messages are an essential component , as for nodes that are not in range each packet is to be passed through the intermediate nodes to traverse the packets from source to destination. We can distinguish two main categories of attacks: Routing protocol dependent and routing protocol independent attacks. Routing protocol dependent attacks are the attacks which are prone to occur on specific routing protocols, such as DSR, AODV. Blackhole attack(AODV) targets ad hoc on-demand routing protocol, link withholding attack, link spoofing attack

(OLSR) and colluding misrelay attack(OLSR) targets Optimized Link State Routing protocol. Routing protocol independent attacks are attacks which are not prone to occur for specific routing protocol these attack can take place irrespective of the routing protocol used like wormhole attack, DOS (denial of service) attack, replay attack. These attacks are discussed in detail.

IV. ROUTING PROTOCOL DEPENDENT ATTACKS IN MANET

A. Blackhole Attack (AODV)

AODV [2] is a reactive routing protocol. In AODV, when a source node S wants to forward a data packet to a destination node D and does not have a direct route to D, it initiates route discovery by broadcasting a route request Packet (RREQ) to its neighbors and if the neighbor is a intermediate node and does not have direct route to destination then intermediate node also rebroadcast the route request packet. This process is repeated until the RREQ reaches the destination node. When the first RREQ arrives, the destination node sends a route reply (RREP) to the source node through the same path from which the (RREQ) arrived. If the same RREQ arrives later then it will be ignored by the destination node.

In a blackhole attack, a malicious node sends fake routing information, and claims that it has shortest path to the destination with an intension to interrupt the continuity of communication. It does so by causing the other good nodes to route the packets through this malicious node. In AODV, the attacker can send a false RREP packet in response to the RREQ packet forwarded by the source node, claiming that it has a sufficiently shortest route to the destination node. This lets the source node to select a path which passes through the malicious node and therefore all traffic will be routed through this node. The attacker node then drops some packets from the traffic, due to which the communication fails. Figure.1 shows an example of a blackhole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently shortest route than other nodes to the destination node. The source node S will choose the route that passes through node A, since the attacker's advertised sequence number is higher than other nodes' sequence numbers.

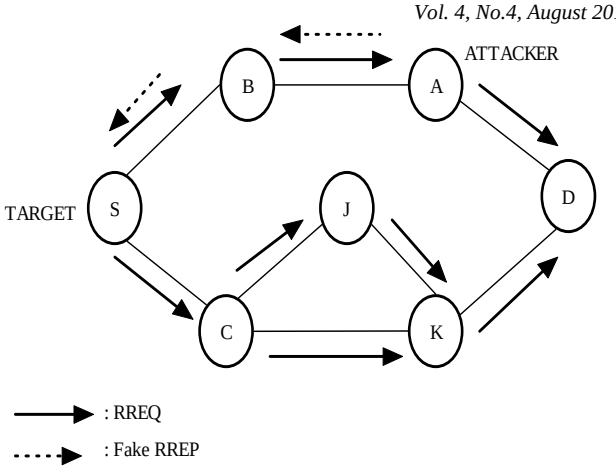

Figure 1. Example of black hole attack on AODV.

B. Link Spoofing Attack (OLSR)

OLSR [3] is a proactive routing protocol, that is, it is based on periodic exchange of topology information. OLSR make use of multipoint relay (MPR) to implement an efficient flooding mechanism by efficiently decreasing the number of transmissions needed. In OLSR, each node selects its own MPR from its neighbors.

In a link spoofing attack, to disrupt the routing operations a malicious node announces fictitious links with non-neighbors. The OLSR protocol constitute a typical example, by advertising fake links with the targets two hop neighbors the malicious node can convince a target node to select him as an MPR. As an MPR node, a malicious node can then misuse data or routing traffic to disrupt the communication, for example, dropping or modifying the routing traffic or accomplish other kind of DoS(denial of service) attacks. Figureure.2 shows an example of the link spoofing attack in an OLSR MANET. In the Figure, node A is malicious node and node S is target node to be attacked. Before the attack both nodes B and J are MRPs for node S. During the attack, node J advertise false link with target node S's two hop neighbor, which is, node A. Now according to OLSR routing protocol malicious node will be selected as only MPR as it is the minimum set that reaches target node S two hop neighbors. As now malicious node can withhold the traffic generated by target node S[11].

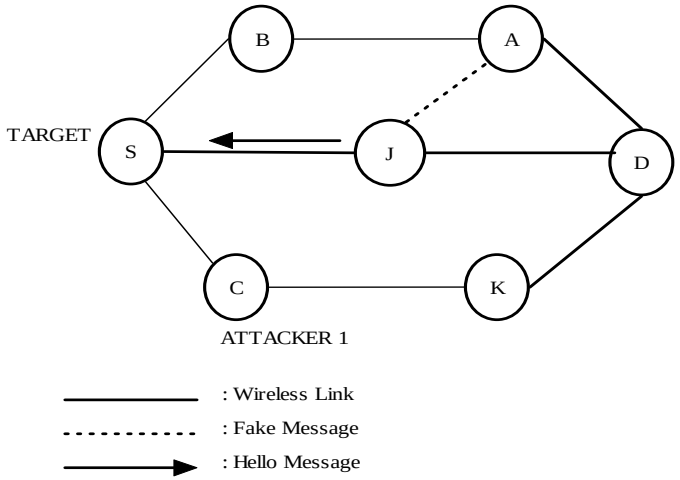

Figure 2. Example of link spoofing attack on OLSR

C. Colluding Misrelay Attack

In this attack, multiple attackers work in collusion to drop or modify routing packets to disturb routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog[10]. For example consider the case where malicious node (A1) forwards routing packets for a node T. The first attacker node (*A*1) relay routing packets as usual to avoid being noticed by node T.
However, the second malicious node (A2) drops or modifies these routing packets. A combination of malicious nodes can interrupt up to 100 percent of data packets in the OLSR MANET.

V. ROUTING PROTOCOL INDEPENDENT ATTACKS

A. Wormhole Attack

A wormhole attack [7] is also known as tunnelling attack and is one of the most severe and sophisticated attacks in MANETs. A wormhole attack is composed of colluding attackers and a wormhole tunnel. To establish a wormhole attack two or more colluding attackers records packets at one point in network and tunnels them to another point through wormhole tunnel which can be wired link, a high-quality wireless out-of-band link, or a logical link. The latter node then replays these packets to the other nodes in the network in its vicinity. The attack is severe as it creates loophole in communication that provides authenticity and confidentiality. The packets that are tunneled arrive much earlier than the packets through other route. Therefore these malicious nodes are with greater probability to be included in the route and take an advantage for further attacks. Figure 3 shows an example of wormhole attack A1 and A2 are malicious nodes S is the target node. When S broadcast a RREQ packet, its neighbor forwards it. However when RREQ packet arrives at malicious node it records and tunnels this RREQ to its colluding partner A2 through a high speed channel. Then node A2 rebroadcast this to its neighbor, through this tunneled route RREQ reaches first to destination node D then from other routes. Therefore D selects the route which includes attackers to unicast an RREP[11].

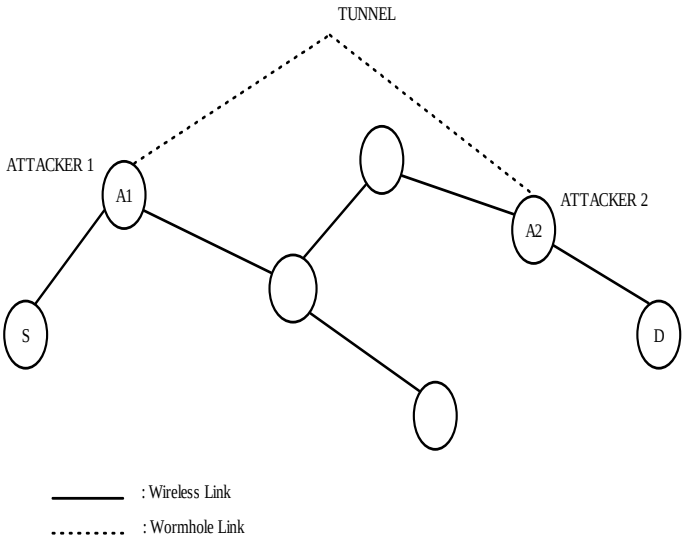

Figure 3. Example of wormhole attack on reactive routing.

B. Flooding Attack

This is also known as resource consumption attack[9], it gives rise to DOS(denial of service) when used against on-demand ad hoc routing protocols. Its main aim is to unnecessarily consume bandwidth and nodes resources to disrupt the routing operation. Flooding attack occurs due to unregulated forwarding of packets in network. In this attack a malicious node either floods the network with a lot of route request packets for a node ID which does not exist in network or may stream large volumes of useless data packets so as to consume the bandwidth and congest the links. Due to this the legitimate node will be busy in receiving useless packets from malicious node and this leads to wasting of node resources. It severely degrades the network performance

C. Sybil Attack

In Sybil attack, a attacker node behaves as if it were a group of nodes by showing multiple addresses. There are, basically two ways by which a Sybil node can get an identity; abducting other node's identity or constructing false identities. The malicious node prevents other nodes from using these addresses by impersonating a large number of nodes in the network, it can "out vote" the well-behaved nodes, and can save itself from detection systems in collaborative tasks such as Byzantine failure defenses. This attack can severely disrupt geographic routing protocols, and can even affect multiple path routing schemes and node localization [5].

VI. CONCLUSION

MANETs are vulnerable to routing security attacks due to its distributed nature, so it is vital to protect them. In this paper we categorize the attacks as routing protocol dependent attacks and routing protocol independent attacks, here we highlight some of the attacks which lie in these categories. MANET security composed of challenging and complex area, in which further research is still being performed and will results in finding of new threats.

REFRENCES

1. S. Ci *et al.*, "Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks," *IEEE Trans. Vehic. Tech.*, vol 55, no. 4, pp. 1302–10 July 2006.
2. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.
3. Th. Clausen *et al.*, "Optimized Link State Routing Protocol," IETF Internet draft, draft-ietf-manet-olsr-11.txt, July 2003.
4. Y.C. Hu, A. Perrig, and D.B Johnson, "Wormhole attacks in wireless networks," Selected Areas in Communications, IEEE Journal on, vol. 24, no.2, pp. 370-380,Feb. 2006,..
5. Y.C. Hu, A. Perrig and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," Proc. 2nd ACM workshop on Wireless security (WiSe '03), pp. 30-40, 2003,.
6. Amara korba, Abdelaziz, Mehdi Nafaa, Ghanemi Salim," Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks**,"** 2013 UKSim 15th International Conference on Computer Modelling and Simulation
7. Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attack in Wireless Networks," *IEEE JSAC*, vol. 24, no. 2, Feb.2006.
8. Bounpadith kannhavong, hidehisas nakayama, yoshiaki nemoto, and nei kato**,"** A Survey Of Routing Attacks In Mobile Ad Hoc Networks," IEEE wireless communications • october 2007
9. P. Yi *et al.*, "A New Routing Attack in Mobile Ad Hoc Networks," *Int'l. J. Info. Tech.*, vol. 11, no. 2, 2005.
10. S. Marti *et al.*, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," 6th MobiCom, Boston, MA, Aug. 2000.
11. Amara korba Abdelaziz, Mehdi Nafaa, Ghanemi Salim"Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks**"** UKSim 15th International Conference on Computer Modelling and Simulation 2013 IEEE.