A Survey of Attacks in Mobile Ad Hoc Network

Riteshkumar Vasava
P.G. Student
Department of Computer Science & Engineering
L.D. College of Engineering

Pradeep Gamit
Assistant Professor
Department of Computer Science & Engineering
L.D. College of Engineering

Abstract

This paper is a survey of attacks in Mobile Ad Hoc Network (MANET). A mobile ad hoc network is a self-constructed network. MANET is connected with mobile device. It's also called a node. All nodes pretend as both communications and router. MANET is an open network because there is an absence of centralized administration, due to these MANETs is attacks by malicious nodes. There are many attacks which are implemented by those malicious nodes like. Blackholl attack, Flooding Attack Replay Attack, Link Spoofing Attack. These research papers provide an overview of Attack in MANET.
Keywords: MANET, Link Spoofing Attack, Blackholl attack

I. INTRODUCTION

Wireless network is network in which device are connected without wired. The wireless network can be classified into two types: Infrastructure and Infrastructure less. In Infrastructure wireless net-work, the mobile node can move while communicating, the base stations are fixed and as the node goes out of the range of a base station. It gets into the range of another base station [1]. The fig.1 show Infrastructure wireless network.

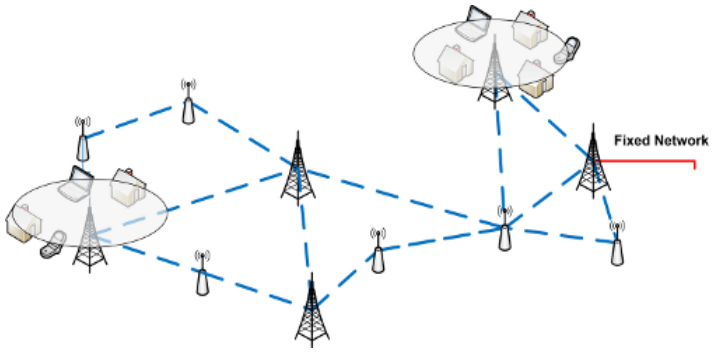

Fig. 1: Infrastructure Wireless Network

Infrastructure less or Ad Hoc Wireless Network. In the mobile node can move while them communing. There are no fixed base stations and all the nodes in the network act as router. It means Mobile ad hoc Network (MANET) is a collection of mobile devices which is a self-configuring network of nodes cooperatively in ad hoc manner without any fixed network infrastructure or centralized administration. In MANET each node is mobile and it's free to move in a random way. In addition to random move, a MANET can be constructed quickly. Because of this flexibility, a MANET is attractive for applications such as disaster relief, emergency operations, military service and etc. Fig. 2 show Infrastructure less Wireless Network.

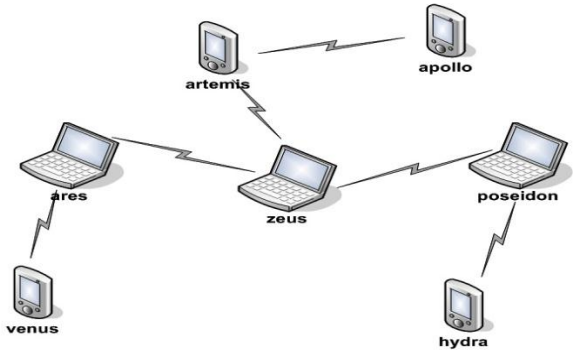

Fig. 2: Infrastructure less Wireless Network

A MANET is much more sensitive to attack as compare to a wired network due to some factored like. There is limited bandwidth and limited battery power. This factor makes routing in MANET an even more challenging task. Other is [2],

Transmission of routing and data packets is done in wireless medium, which is shared and generally unreliable and makes eavesdropping more likely. Even if the channel is reliable, the communication may still be unreliable due to the broadcast nature of MANETs. There is no central management point, which makes it difficult to ensure that all nodes participating in the network are polished. Last but not the least Mobility of nodes plays a very important role in the network, which makes routing even more challenging as the topology keeps changing regularly.

In Routing layer attacks there can be two type attackers; one is outsider attacks and second is insider attacks. In Outsider attacks in which the attacker has no authentication information about the control and data packets. Those attacks can easily detak using authentication and cryptography. Insider attack is most dangers attack. In these attacks cryptography may not help because the inside node already has all the cryptographic information.

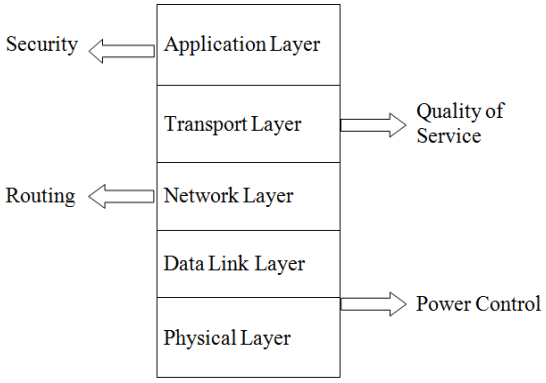

Fig. 3: an attacking layer in MANET

In [3], the authors survey attacks and their countermeasures in mobile ad hoc network for five layers: application, transport, network, data link layer, and physical. For attacks against the network layer, the authors survey countermeasures for impersonation attacks, modification attack, wormhole attacks, and blackhole attacks. However, new attacks and counter-measures against a network layer attack, such as withholding of routing traffic have not been discussed in the paper. Figure 3 show challenging layer in MANET.

II. ROUTING PROTOCOLS IN MANET

MANET is continuously changing network. For that to finding a correct route for a specific node is some changing task. MANET has many topologies to discover the most recent. MANET routing protocols can mainly classified into two categories:

A. Table Driven or Proactive Protocols:

It is also called a Proactive Protocols. They attempt to maintain consistent up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view [4]. Some of the table driven Protocol are: Distance vector routing protocol (DSDV) [5], [7] is based on the classical Bellman-Ford routing mechanism, DBF [6].

B. On Demand or Reactive Protocols:

It is also called a Reactive Protocol. In these routing is source initiated routing. Routes are created as when it required. When a node required a route to a destination, it invokes a route discovery process within the network. In [4], this process is completed once a route is found or all possible route permutations have been examined. The route remains valid till destination is achieved all the communications (packages) between sender and destination or until the route is no longer needed. Some of the On Demand protocol is: Dynamic Source Routing protocol (DSR) [8], [9], AODV [10], [11].

III. ROUTING ATTACK IN MANET

A. Selective Forwarding:

In selective forwarding attacks, a malicious node selectively forwards messages to other nodes and drops a fraction of messages. The number of packets dropped depends on the configuration by the adversary and sometimes, the malicious node is configured to drop only those packets that are destined for a specific node. Selective forwarding attack is effectively launched when the attacking node is effectively includes on the route of a data flow. This type of attack is difficult to detect. It can degrade the performance of the routing protocol, especially when it is used in combination with other attacks such as wormhole attacks [12].

B. Blackhole Attack:

In Blackhole Attack, one malicious node sends wrong information about routing in to the neighbour's node and also claiming that it has a lowest optimum route. Means node advertises its availability of fresh routes (short path) without checking its routing table. For that reason all node send all data packets to through this malicious node. Now it's up to the configuration of that malicious node whether it drops all the packets or performs some other action [13]. If the node drops all the packets then it calls a blackhole attack.

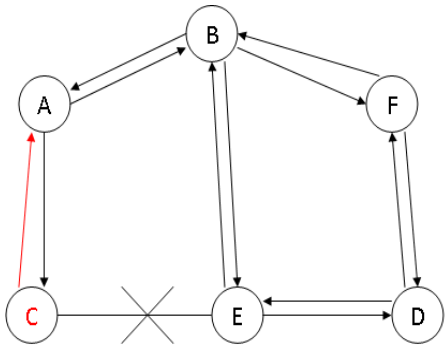

Fig. 4 Blackhole attack in some MANET

Figure 4 show that how blackhole attack work. In this network node "A" wants to send data packets to node "D" and start the route discovery process. If node "C" is a malicious node then it will claim that it has route to the specified destination. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the shortest route and 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.

C. Flooding Attack/ Data Flood attack:

In these attack, the aim of the flooding attack [14] is to exhaust the network resource, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routeing operation to cause severe degradation in network performance. The flooding attack [15] may be RREQ flooding or data flooding attacks. In RREQ flooding attack, the attackers generate many RREQ packets in unit time to unknown IP address. As the priority of RREQ packets is higher than data packets, the RREQ are handled first and this scenario becomes a honey pot for an attacker. In data flooding, the attacker first maintains the routes to the destination node and then frequently sends useless data packets, which engage the network and stop the processing of legitimate data packets [15].

D. Link Spoofing Attack:

In a link spoofing attack, a malicious node advertises fake links with non-neighbours to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbours. This causes the target node to select the malicious node to be its multipoint relay (MPR). As an MPR node, malicious node can then manipulate date or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks [16].

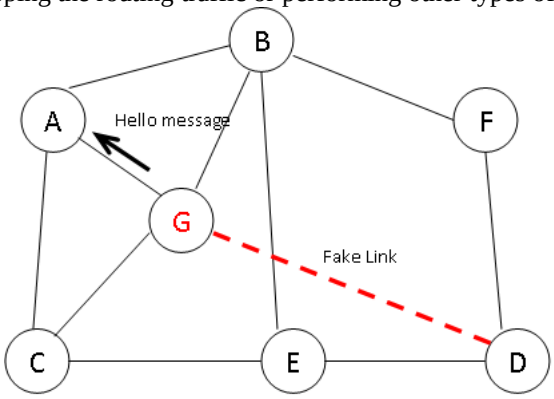

Fig. 5: A Link Spoofing attack

Figure 5 shows an example of the link spoofing attack in an OLSR MANET. In the figure, we assume that node G is the attacking node, and node A is the target to be attacked. Before the attack, nodes B, C and G are MPRs for node A. During the link spoofing attack, node G advertises a fake link with node A's two-hop neighbour, that is, node D. According to the OLSR protocol, node A will select the malicious node G as its only MPR since node G is the minimum set that reaches node A's two-hop neighbours. By being node A's only MPR, node G can then drop or withhold the routing traffic generated by node A [16].

E. Replay attack:

In a MANET [16], topology frequently changes because of node mobility. It means that current network topology might not exist in the future. In a replay attack [17], a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale router. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

F. Worm Hole Attack:

A wormhole attack [18] is one of the most sophisticated and severe attacks in MANETs. In this attack, two nodes collude to create a tunnel or out-of-band connection with each other and modify the routing messages to attract all the traffic towards them. The possible aims of the wormhole attacker could be eavesdropping, damaging the network performance by partially or completely dropping packets, modifying data packets, or launching denial of service attack by isolating the nodes.

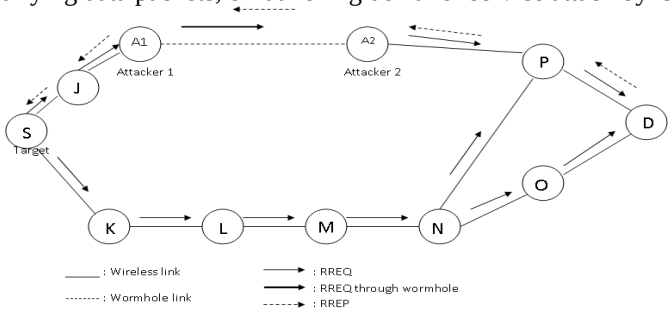

Fig. 6: wormhole attack on reactive routing

Figure 6 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes A1 and A2 are two colluding attackers and that node S is the target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to destination node D, its neighbours J and K forward the RREQ as usual. However, node A1, which received the RREQ, forwarded by node J, records and tunnels the RREQ to its colluding partner A2. Then, node A2 rebroadcasts this RREQ to its neighbour P. Since this RREQ passed through a high-speed channel, this RREQ will reach node D first. Therefore, node D will choose route D-P-J-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-J-P-D that indeed passed through A1 and A2 to send its data [16].

G. Colluding Misrelay Attack:

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog and pathrater [19].
Figure 7 shows an example of this attack. In these figure both node B and C are attacker. Consider the case where node B forwards routing packets for node S. In the figure, the first attacker B forwards routing packets as usual to avoid being detected by node S. Means it woke as selfish node. Selfish node work as they wants' which time node work as attacker or safe node that not

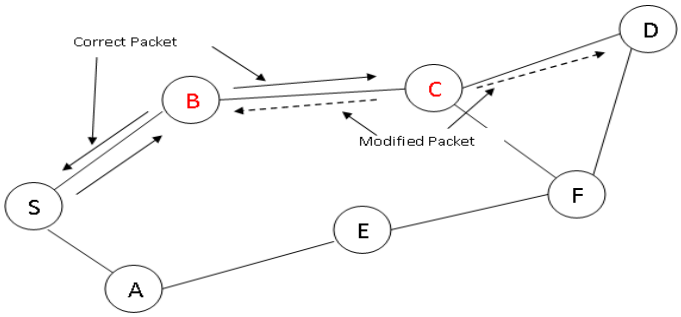

Fig. 7: colluding misrelay attack

fixed in every condition. However, the second attacker C drops or modifies these routing packets. In [20] the authors discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.

IV. CONCLUSION

MANET is an emerging network technology. MANET is an Infrastructure less network for that MANET can be deployed quickly and creates a network. MANET has advantage like create a network at disaster place etc. But MANT also has weaknesses like limited bandwidth, computational power and centralized administration. Existing security for wired network

cannot apply directly for MANET network. In this paper, we reviewed that which attacks are applied in MANET network. How these attack work in MANET. In my way the blackhole attack is dangers. And Future research should be focused in blackhole attack. And find out solutions to the blackhole attack.

REFERENCES

[1] Sunil Taneja, Ashwani Kush, "A Survey of Routing Protocols in mobile Ad Hoc Network", International journal of Innovation, vol. 1, No. 3, August 2010
[2] Humaira Ehsan, Farrukh Aslam Khan, "Malicious AODV", International Conference of Security and Privacy in Computing and Communications, 2012 IEEE
[3] B. Wu et al., "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Network," wireless/Mobile Network Security, Springer, vol. 17, 2006.
[4] Hongmei Deng, Wei Li, Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, October 2002
[5] C.E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computer", Proceeding of ACM SIGCOMM 94, 1994, pp. 34-244
[6] D. Bertsekas and R. Gallager, "Data Network", Prentice Hall Publ., New Jersey, 2002
[7] P. Chema Reddy, Dr. P. Chandrasekhar Reddy, "Performance Analysis of Adhoc Network Routing Protocols", Academic Open Internet Journal, SSN 1311-4360, Volume 17,2006
[8] D. B. Johnson, D. A. Maltz, Y. C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Network (DSR)", IETF Draft, April 2003, work in progress. http://www.ietf.org/internet-drafts/draft-itef-mamet-der-09.txt
[9] D. B. Johnson, D. A. Maltz, "Daynamic Source Routing in Ad Hoc Network", Mobile Computing, T. Imielinski and H. Korth, Eds., Kulwer Publ., a996, pp. 152-81.
[10] C. Perkins, E. B. Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing – Internet Draft", RFC 3561, IETF Network Working Group, July 2003
[11] C. E. Perkins, E. M. Royer, "Ad-Hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing System and Applications (WMCSA), New Orleans, LA, 1999, pp. 90-100
[12] Agrawal, S., Jain, S. And Sharma, S. "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Network", Journal of Computing, 3(1), 2011, 41-48
[13] Johnson D.B., Maltz D.A., "Dynamic Routing in Ad Hoc Wireless Networks", Mobile Computing, 1996, ch.5, 153-181.
[14] P. Yi et al., "A New Routing Attack in Mobile Ad Hoc Network", Int'l. J. Info. Tech., vol.11, no. 2, 2005.
[15] Shandilya S. K., Sahu S., "A trust based security scheme for RREQ flooding attack in MANET", International Journal of Computer Applications, 5(12), 2010, 4-8
[16] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Abbas Jamalipour, "A Survey of routing Attacks in Mobile Ad Hoc Network", IEEE Wireless Communications, October 2007
[17] C. Adjih, D. Raffo, P. Muhlethaler, "Attacks Against OLSR: Distributed Key Management for Security", 2nd OLSR Interop/Wksp., Palaiseau, France, July 28-29, 2005
[18] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Network", IEEE JSAC, vol. 24, no. 2, Feb. 2006.
[19] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Network", 6th MobiCom, Boston, MA, August 200
[20] B. Kannhavong et al., "A Collusion Attack Against OLSR-Based Mobile Ad Hoc Network", IEEE GLOBECOM '06
[21] Th. Clausen et al., "Optimized Link State Routing Protocol", IETF Internet draft, draft-ietf-manet-olsr-11.txt, July 2003