Survey of various Active Attacks in MANETS

MeenaBharti
PhD Candidate
PTU Jalandhar
Bathinda~Punjab
meenabharti89@gmail.com

Dr. Shaveta Rani
CSE Department
GZS,PTU Campus
Bathinda~Punjab
garg_shavy@yahoo.com

Dr. Paramjeet Singh
CSE Department
GZS,PTU Campus
Bathinda~Punjab
param2009@yahoo.com

Abstract*: Networks have flourished due to the advent of new technology. There is a mushroom growth in technology and day to day needs for communication which was never experienced before. A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can be internetwork in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. Various attacks needed to be detected on order to secure the wireless ad-hoc network. In this paper we are discussing various active attacks.*

Keywords: *MANET, Network Security, Active Attacks, Rushing Attack, Balckhole attack, Neighbor Attack, Sink hole Attack*

INTRODUCTION

In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges, or intermediate node(s) are used in order to communicate where the nodes are not in the direct communication range. As we can see that in these two situations, each node that has participated in the communication forms a wireless network automatically. Such type of communication in which each node participates to make a network can be viewed as mobile ad hoc network. Such a network features nodes that contain a wireless transmitter and receiver, using which node communicates with other nodes which are in its radio communication range. Sometimes a node has to communicate with some other nodes which are not in its radio range. In that case, a node takes cooperation of other nodes in the network [5]. Such type of communication is called multi-hop communication. So we can say that each node has to act as both a host and a router at the same time. As the nodes are mobile so these move in or out continuously form radio range of other nodes. So, the network topology changes frequently. This makes it more prone to attacks. To secure the wireless ad-hoc network, we need to detect the various attacks. These attacks can be categorized into two categories in MANET:

A. Passive Attacks

Here the data transmitted within the network is not altered by the attack rather it includes the unauthorized "listening" to the network traffic or accumulates data from it [1]. In case of passive attack, attacker does not disturb the operation of a routing protocol instead of it attacker tries to retrieve important information from it.

B. Active Attacks

Here the message flow between the nodes is prevented. Generally Active attacks are very severe attacks on the network. These types of attacks can be both external as well as internal [8]. In case of external active attacks, attacker nodes are not part of network; attacking nodes lies outside the network but in case of internal active attacks attacking nodes lies within the network. These kinds of attacks are difficult to detect.

CATEGORIES OF ACTIVE ATTACKS

Active attacks mainly have three categories

A. Dropping Attacks

Here all packets can be dropped by selfish nodes which are not destined for them [3]. In case of dropping attacks end-to-end communications between nodes is prevented.

B. Modification Attacks

Here packets are modified that disturb the overall communication between network nodes [3]. Sinkhole attack is the example of this kind of attack.

C. Fabrication Attack

Here fake messages are sent by the attacker to the neighboring nodes without receiving any related message.

TYPES OF ACTIVE ATTACKS

A. Neighbor Attack

Upon receiving a packet, an intermediate node records its ID in the packet before forwarding the packet to the next node [4]. But an attacker node, simply forwards the packet without recording its ID in the packet to make two nodes that are not within the communication range of each other believe that they are neighbors (i.e., one-hop away from one another), which results in a disrupted route.

B. Rushing Attack

Literally it means “a sudden attack”, or “to perform, accomplish, or complete with speed, eagerness, or violence”. “RUSHING ATTACK” is also called as “novel attack” or “denial of service” attack in networking [2].

In AODV routing protocol, when source nodes flood the network with route discovery packets (RREQ, RREP) in order to find routes to the destinations, every in-between node process only the first non replica packet and throw-outs any replica packets that arrive at a later time. A rushing attacker utilize this replica repression mechanism by quickly forwarding route discovery packets with a malicious RREP on behalf of some other node skipping any proper processing in order to gain access to the forwarding group [9]. In rushing attack, an intruder will “rush” (transmit early) the RREQ packet to suppress any later legitimate RREQs as shown in the Fig. 1. The source node S broadcasts a RREQ for node 3 and node 2. Now, on hearing the RREQ, the malicious node 3 rushes the RREQ to suppress the later legitimate RREQ. The rushing may in the following ways [9]. Malicious node 3 ignores the request forwarding delay (this is a randomized delay used by the routing protocol to avoid collision of broadcast packets).

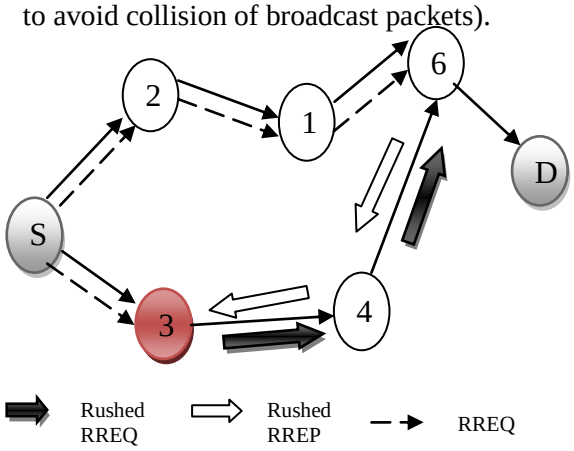

Fig 1: Rushing Attack

Malicious node 3 rushes the RREQ with a higher source sequence number. This rushed RREQ from Malicious node 3 arrives first at node 6, and therefore node 6 will discard the legitimate RREQ from node 1 when it arrives later via 1, as shown in Fig. 1. Due to duplicate suppression, the actual valid RREP message from valid node will be discarded and consequently the attacking node becomes part of the route. In rushing attack, attacker node, send packets to proper node after its own filtering is done, so from outside the network, the nodes behaves normally and nothing was happened [4]. But it might increase the delay in packet delivering to destination node [2].In this section it is briefly detailed about the active attacks on the network layer with the examples. These researches on attack are concluded that the attacks degrade the performance of the network as fit as data

packet transmission. In the next section it is discussed about development of the detection mechanism by various researchers to defend against the attacks.

C. Blackhole Attack

A blackhole attacker first needs to invade into the multicast forwarding group in order to intercept data packets of the multicast session [6, 8]. Then it starts to drop some or all of data packets it receives instead of forwarding them to the next node on the path which results in very low packet delivery ratio, e.g. in Fig. 2 source node S wants to send data packets to destination node D and initiates the route discovery process. Consider that node 2 is a malicious node and it claims that it has route to the destination whenever it receives route request packets, and send response to node S immediately. As node S will receive first reply from node 2 so it will ignore replies from other nodes and starts to send packets through node 2 which results in sending of all packets through the malicious node which can be consumed or lost.

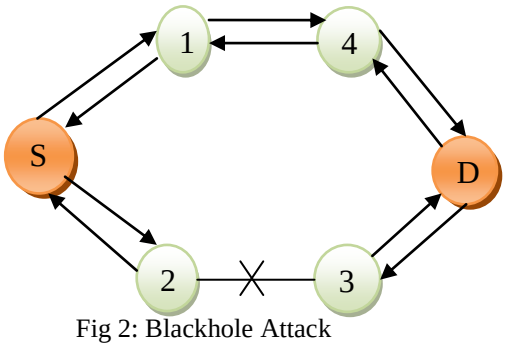

Fig 2: Blackhole Attack

D. Byzantine Attack

Here the attack is made by single node or multiple nodes. Packets are forwarded through non-optimal paths that can create routing loops or can drop selective packets resulting in disruption or degradation of routing services in a network [10].It is also called as impersonation attack because the malicious node might imitate another normal node. It also sends false routing information for creating an anomaly update in the routing table. In addition to this, the attacker may get unauthorized admission to resources and sensitive information.

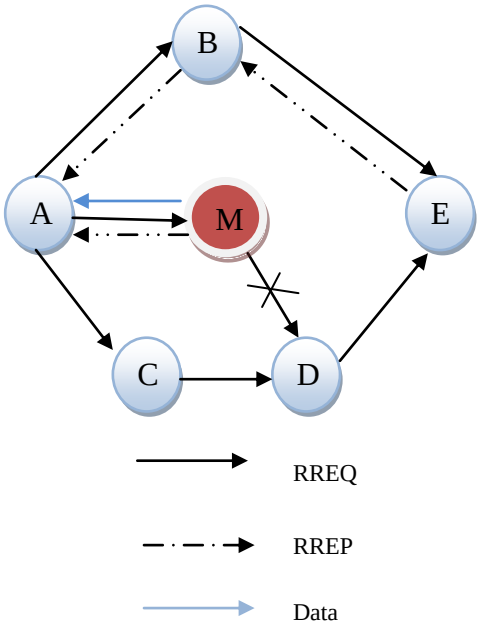

Fig3: Byzantine attack

In the above figure, the malicious node M receives route request from source node A. But, M selectively drops certain data packets or it just forwards the data packets to a non optimal route [11].

E. Blackmail Attack

Here the target is routing protocols which use mechanisms for their cognition of malicious nodes and broadcast the messages which try to blacklist the offender [7]. An attacker might blackmail a legitimate node by adding other legitimate node to their blacklists. Thus the nodes can be avoided in those routes.

F. Sybil Attack

Here the case is of multiple identities pretended by the attacker [7]. A malicious node can be had as if it were a larger number of nodes either by impersonating other nodes or simply by claiming false identities. There are three categories of this attack: fabricated/stolen identity, direct/indirect communication and simultaneity.

G. *Misrouting Attack*

In the misrouting attack, a non-legitimate node redirects the routing message and sends data packet to the wrong sink [10]. This type of attack is made by modifying the final destination address of the data packet or by forwarding a data packet to the wrong next hop in the route to the destination.

H. Resource consumption Attack

In this attack, a malicious node deliberately tries to consume the resources [8] (e.g. bandwidth, battery power, etc.) of other network nodes. The attacks could be in the form of very frequent generation of beacon packets unnecessary route request control messages, or forwarding of stale information to nodes.

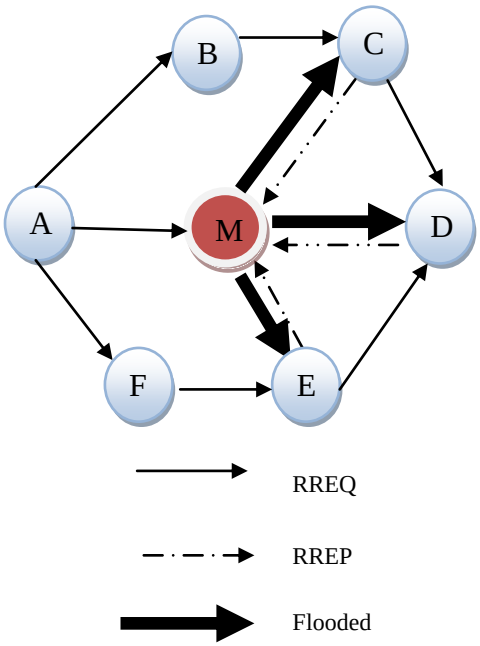

Fig 4: Resource Consumption Attack

In the above figure, where M is the malicious node, which keeps on sending excessive requests to the victim nodes C, D and E. This results in the decrease in battery power of the nodes.

I. Sinkhole Attack

In sinkhole Attack, a compromised node or malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. After this, it modifies the secret information, such as modifying data packet or drops them to which arise complications in the network. A malicious node attempts to attract the secure data from all neighboring nodes. In this type of attack, the malicious node advertises wrong routing information to produce itself as a specific node and receives the whole network traffic [11].

It modifies the data packets by changing the sequence number or drops them. Hence, the path through malicious node "M" appears to be the best available path.

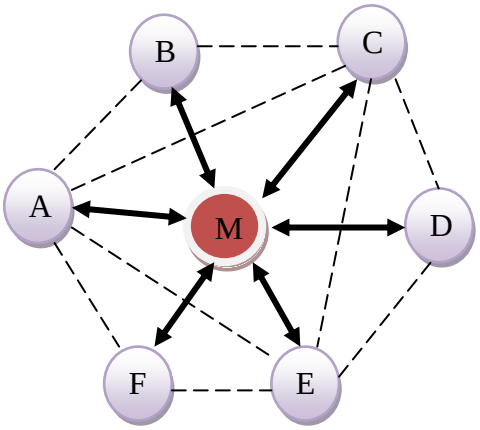

Fig 5: Sinkhole Attack

J. Denial of Service (DoS)

It includes the prevention of authorized access to resources or the delaying of time-critical operations [10]. A denial of service (DoS) attack is characterized by an attempt by an attacker to prevent legitimate users of a service from using the desired resources and attempts to "flood" a network, and thus prevents authorized network traffic.

K. Jelly fish (JF) Attack

A jellyfish attacker first needs to intrude into the multicast forwarding group [3]. After this, it delays data packets unnecessarily for some

amount of time before forwarding them to next node. This results in high end-to-end delay and thus degrades the performance of real-time applications.

CONCLUSION AND FUTURE SCOPE

As, in Mobile Adhoc NETwork (MANET) various nodes moves continuously, so entering or exiting radio range of other nodes frequently. So, it is more prone to attacks. In this paper various attacks are studied. These attacks make network complicated by choosing non-optimal routing path. Some attacks consume resources of other nodes of network like battery life and bandwidth. It is very necessary to detect these attacks and to take some preventive measures. In future work can be done to study various prevention and detection techniques of these attacks.

References

[1] K, PrasanaVenkatesan T, Ramkumar R.," Security Attacks and Detection Techniques for MANET" Discovery, Volume 15(42), 89-93, April 10, 2014.

[2] R. Kravets, S. Yi, and P. Naldurg, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks", In ACM Symp. on Mobile Ad Hoc Networking and Computing, 2001.

[3] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing", Kluwer Academic Publishers, Vol 353, 1996, pp. 153-181.

[4] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75

[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, volume 5, Number 3, 2007, pp 338-346.

[6] Payal N. Raj and PrashantB.Swadas, "DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[7] MahaAbdelhaq, Sami Serhan, RaedAlsaqour and Rosilah Hassan "A local Intrusion Detection Routing Security over MANET Network", IEEE, July 2011, Bandung, Indonesia

[8] Gajendra Singh Chandel and RajulChowksi, "Study of Rushing attack in MANET," International journal of ucterion (IJCA), Vol. 79, No. 10, Oct. 2013.

[9] ShobhaArya and ChandrakalArya, "Malicious Nodes Detection in Mobile Ad Hoc Networks", Journal of Information and Operations Management,Vol.3, No.1, 2012, pp. 210-212.

[10] NiteshFunde& P. R. Pardhi, "Analysis of Possible Attack on AODV Protocol in MANET" International Journal of Engineering Trends and Technology (IJETT) – ISSN: 2231-5381 Volume 11 Number 6 – May 2014

[11] Gwalani, S. ; Srinivasan, K. ; Belding-Royer, E.M. ; Kemmerer, R.A., " An intrusion detection tool for AODV-based ad hoc wireless networks" IEEE - Computer Security Applications Conference, 2004. 20th Annual, ISSN : 1063-9527 Page(s): 16 – 27, Dec. 2004