Attacks Finding and Prevention Techniques in MANET: A Survey

Bijender Bansal, Research Scholar, Gyan Vihar University, Jaipur, Rajasthan (India), bijender.vce@gmail.com

Pankaj Gupta Professor, VCE, MDU, Rohtak, Haryana (India), pankajgupta.vce@gmail.com

Neelam Sharma VCE, MDU, Rohtak, Haryana (India), sharma.neelam167@gmail.com

ABSTRACT - A Mobile Ad hoc Network (MANET) is a set of distributed sensor nodes . The nodes are connected in a self- configurable network in which they can add and join the network any time. Due to this kind of nature MANET is a collection of mobile nodes which is dynamically moves from one point to another. Due to this type of nature MANET is a weak network which suffers various kinds of attacks. There are many attacks in wireless Mobile Ad hoc Networks which disturb the network. MANETs suffers from attacks like packet dropping attack, Black Hole attack, Worm hole attack, denial of service attack etc. A Malicious node may or may not involve in route discovery mechanism with an intension to corrupt the overall network performance. These malicious nodes have serious impact on routing and delivery ratio of packets. Many researchers have discovered many types of techniques to propose different detection and prevention methods. In this paper a survey on different kinds of attacks and detection and prevention methods is presented.

Keywords **- Mobile Ad hoc Network, MANET, Security, Black hole attack, Gray hole attack, Worm hole attack, Byzantine attack, Jellyfish attack, Routing Protocol,**

1. Introduction:

Mobile Ad-hoc Networks (MANET) is the network of self configured network without any fixed infrastructure. It is a connection between computing devices which are wirelessly joined. MANET has some characteristics like in MANET there is no need of fixed road and rail network. The topology of the network is dynamic. MANET is less secure as compared to wired network. In MANET nodes can be contact directly if they are within radio range. MANET is an autonomous system of mobile node. It can operate in isolation or may have gateways to and interfaces with a fixed network. There are Bandwidth Constraints and Energy Constraints in MANET. MANET has distributed nature of operation for security, routing and host configuration. It provides high user density and large level of user mobility. MANET is more scalable than Fixed Network. In MANET every node act as both host and router[1].
There are some issues also occur in MANET like its randomly Changing Topology and Limited Energy. In MANET there is no centralized control and many threats from Compromised node inside network

2. Routing Protocols in MANET

Routing consists of two activity[2]:

1. **Routing** : It determining the optimal path from source node to destination node. It has two functions as path discovery and path maintenance.
2. **Packet forwarding**: In this data is carrying from the source node to destination node through intermediate nodes.

There are three types of routing protocol in MANET[3]:

2.1 Table driven routing protocol: This protocols are known as Proactive protocols. In these protocols every node maintains a constant route to all other nodes. In this every node has one or two table for record routing information and number of hops. In this every node keep up the network topology as tables After a time period , it is update the information in tables. It helps to provide a better shortest path. DSDV, WAR, OLSR are the types of proactive routing protocols.

2.2 On Demand routing protocol: This is also known as reactive routing protocol. In this each node keeps up data of just active routes to the destination node. These are designed to reduce the amount of overheads. It is source initiated protocol. The route is finding only when source node want to communicate with other node, shortest one selected. DSR,AODV,TORA protocols comes under this category.

2.3 Hybrid routing protocols: These protocols are the combination of both protocols. This protocol is used to provide hierarchical routing. Proactive protocol is used to collect the unusual routing information, then reactive is used to maintain the routing information when topology changes. TORA and ZRP are example of hybrid protocol.

3. SECURITY ATTACKS IN MANET

Security attacks can be External and Internal attacks. In External attacks the attacker node does not belong to the network but the Internal attacks the Attacker node belongs to that network. Internal attacks are more dangerous as compare to External attacks because attacker node knows all detail information and have access rights [4].

3.1. Internal Attacks:

1.Timing Attack 2. Modification Attack 3. Dropping Attack 4.Fabrication Attack

3.2. External Attacks

Active Attacks:

It problems or change the computer resources and involves change of the information flow. 1.Denial of Service Attack 2. Spoofing 3. Man-in-the-Middle 4. ARP poisoning 5. Ping Flood 6. Smurf Attack 7. Buffer Overflow 8. Heap Overflow 9. Formatting String Attack .

Passive Attacks: -

This type of attacks does not influence the system resource; they only watch or check the message. The plan of this type of attack is to find information that is being transmitted These can be following: 1. Wiretapping 2. Port Scan 3. Idle Scan

3.3 Layer attacks:
Attacks can also be classified on layered basis. Each layer has many types of attacks. There are some attacks on various layers[5].

Physical Layer: Jamming, Interceptions, Eavesdropping.
Data Link Layer: denial of service, traffic analysis, monitoring.
Network layer: Black hole, worm hole, sink hole , gray hole, flooding.
Transport layer: session hijacking.
Application layer: Denial of Service (DOS), code attack, viruses.

Various network layer attack types are considered [8][9][10]. There are some of them are discussed:

Black Hole Attack

In black hole attack a malicious node send a false route path to another node [11]. The source node starts to send data packets through the black hole node . In AODV , the malicious node send RREP message to source node that include a fake destination sequence number. That why source node select a route that passes through the malicious node. As the data transmission starts, malicious node drops the data packets that are needed to be forwarded to destinations. Malicious node can misuse the data packets. Black hole attack is more dangerous as compared to other attack.

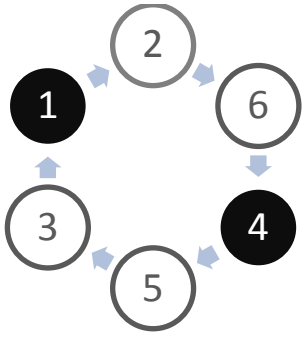

Figure 1

In the following the malicious node is act as like a intermediate node. Node 6 want to send data packet to node 2 but in between node 4 and node 1 is a malicious node. It will act like a active node. Node 4 receiving RREQ from the node 6 and send response to the node 6. Node 6 is think the route is a active and start to send data packet. But data packets are received by node 4 and node 6 does not know about the data packet. All data packet are lost. The Black hole attack is an active insider attack. A black hole is a node that always responds with a RREP message to every RREQ, even though it does not actually have a legal path to the desire node.
Black hole attacks are classified into two categories: 1) Single black hole attack 2) collaborative black hole attack.

1)Single black hole attack: In single hole attack only one node acts as malicious node on path.

Figure 2.

2.Collaborative Black hole attack: In collaborative attack more than one nodes act as malicious node. It is also known as multiple malicious nodes attack.

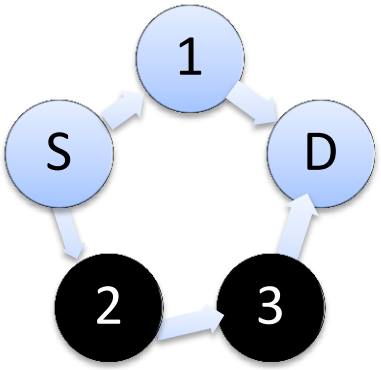

Figure 3

Malicious nodes respond to the source node but these nodes do not refer routing table. The source node assumes that route discovery is complete, ignore other RREP messages and select the route through malicious node. The attacker node drops the received messages. Attacker node attacks all RREQ messages this way and takes over all routes. So all packets are sent to a path, that are simply dropped and will not be reached to appropriate destination.

Flooding Attack

In flooding attack attacker node exhausts the network with the unnecessary data packets and consumes node's resources like battery power. It disturbs the routing function and degrades the network performance. The victim nodes are not able to receive or forward any data packet because services of network become so weighed down with unnecessary packet.

Byzantine Attack

In this attack an intermediate malicious node works in mutual agreement. That node create a routing loop to non optimal path or selectively drop the packets. Such attacks are difficult to identify.

Wormhole Attack

In this attack a attacker node record packets at one location in the network after that replay them at another location in the network using private network [12]. Due to this nature the attacker may create a wormhole for those packets also that does not belong to him.

Replay attack:

Due to changeable topology of MANET current network topology might not exist after some time. In replay attack , attacker node record other node's message and resend to destination. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions [8]

Gray Hole Attack

This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In this kind of attack a hateful node does not participate in route discovery mechanism that is initiated by other nodes and is therefore not a part of active route. Such hateful nodes would increase the route discovery failure and harm the overall network performance [9].

Rushing Attack

Two colluded attackers use the tunnel method to form a attack. When attacker node receives any request packet for path discovery then it sends the packet in the network before any other node forward the request packet. Due to this if same demand packet send by approved node to already received nodes then they judge packet as replica and reject it. In this way attacker will always be part of the route and it is really not easy to identify such hateful node. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne[14].

Sink Hole Attack:

In this attack a compromised node tries to magnetize the data to itself from all adjoining nodes. So, the node eavesdrop on all the data that is being communicated between its adjoining nodes. It can also be implemented on Adhoc networks such as AODV by using flaws such as maximizing the succession number or minimizing the hop count, so that the path accessible through the malicious node appears to be the best available route for the nodes to communicate.

Spoofing Attack:

In this attack, the attacker assumes the identity of other node in the network, hence it receive the messages that are meant for that node. usually , this type of attack is launched in order to gain access to the network so that further attacks can be launched , which could seriously cripple the network.

Selfish Behavior

In this attacker node selfish participate in route discovery mechanism and become a part of an active route. As it becomes the part of an active route, the attacker nodes would start dropping data packets that are not related to him with an intension to conserve energy which is required to forward data packets that belongs to other nodes.

Jellyfish Attack

Jellyfish attack is somewhat different from Black- Hole & Gray-Hole attack. Instead of blindly dropping the data packets, it delays them before finally delivering them. It may even scramble the order of packets in which they are received and sends it in random order. This disrupts the normal flow control mechanism used by nodes for reliable transmission. Jellyfish attack can result in significant end to end delay and thereby degrading QoS.

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.

Sybil attack:

The Sybil attack specially aims at distributed system. The attacker tries to perform as numerous dissimilar nodes rather than one. This allows him to copy the outcome of a selection used for entrance safety methods. Since ad hoc networks depend on the message between nodes, many systems affect unnecessary algorithms to guarantee that the data gets from source to destination. A result of this is that attackers have a harder time to destroy the reliability of information

Desynchronization attack:

In this attack, the challenger constantly forges communication to one or both end points which demand series of missed frames. Hence these communications are again transmitted and if the challenger maintains a suitable timing, it can avoid the end points from exchanging any helpful information. This will cause a significant drainage of power of legal nodes in network in an end-less synchronization-recovery protocol.

Overwhelm attack:

In this attack, an attacker might overcome network nodes, causing network to promote huge volumes of transfer to a support station. This attack use network bandwidth and drains node power.

Blackmail:

A black mail attack is related to routing protocols that uses methods for detection of malicious nodes and propagates messages that aim to blacklist the criminal.

Denial of service attack:

Denial of service attacks are meant at whole disorder of routing information and as a result the entire operation of ad-hoc network.

Man-in-the-middle attack:

An attacker sites among the sender node and receiver node and sniffs any information being transfer between two nodes. In some cases, attacker may imitate the sender to converse with receiver or imitate the receiver to respond to the sender.

SECURITY OF MANET ROUTING PROTOCOLS

To secure routing protocols from attacks many solutions are projected by researchers like AODV, DSDV, DSR, OLSR and FSR etc. [6]. As routing is a important mission for Ad-hoc network, thus this should be more secure. A protocol might be sufficient to satisfy security problems and working terms. Below are few solutions [7, 8, 9]:

1. SAR (Security Aware Ad-hoc Routing)
2 OLSR(Optimized link state routing)
3 SAODV (Secure Ad-hoc on Demand Distance Vector)
4 ARAN (Authenticated Routing for Ad-hoc Network)
5 ARIADNE
6 SRP (Secure Routing Protocol)
7 SEAD (Secure Efficient Ad-hoc Distance Vector)
8 SLSP (Secure Link State Routing Protocol)
9 DSDV (Destination-Sequenced Distance Vector Protocol)
10 DSR (Dynamic Secure Routing)
11 ZRP(Zone routing protocol)
12 TORA(Temporally- ordered routing algorithm)

SECURITY GOALS

Security involves a set of reserves that are sufficiently Funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self organizing manner. For these reasons, securing a mobile adhoc network is very difficult. The goals to estimate if mobile adhoc network is secure or not are as follows:

a. Availability:
Availability means the resources are available to certified parties at proper times. Availability applies both to data and to services. It ensures the survivability of network service regardless of rejection of service attack.

b. Integrity:
Integrity means that assets can be customized only by certified parties or only in approved way. alteration includes writing, changing status, deleting and creating. Integrity assures that a communication being transferred is never degraded.

c. Anonymity:
Anonymity means all information that can be used to recognize holder or present user of node should absence be reserved confidential and not be spread by node itself or the system software.

d. Authentication:
Authentication enables a node to make certain the uniqueness of peer node it is communicating with. Authentication is basically guaranteed that participants in communication are genuine. Authenticity is ensured because only the genuine sender can create a message that will decrypt correctly with the common key.

e. Confidentiality:
Confidentiality ensures that computer related resources are accessed only by certified parties. That is only those who should have access to something will really get that access. To keep privacy of some private information, we need to keep them top secret from all entities that do not contain license to access them. Confidentiality is sometimes called secrecy or privacy.[5]

f. Non repudiation:
Non repudiation ensures that sender node and receiver node of a communication cannot deny that they have yet sent or received such a message .This is cooperative when we need to distinguish if a node with some undesired function is compromised or not.

AODV Routing Protocol

There have been a lot of routing protocols projected to suit the different needs of MANETs. Unluckily most of these routing protocols do not reflect on security. One of the most popular of them is the Ad hoc On-Demand Vector (AODV) routing protocol. In this section we explain the process of AODV to recognize better the routing attacks explained consequently. We intend to demonstrate standards of attacks. Other protocols may be vulnerable to these or similar attacks, but may also be vulnerable to additional protocol exact attacks. Besides the consequences of attacks can have dissimilar impacts in diverse routing protocols.
AODV is a reactive routing protocol, find routes only when they are needed. It is claimed that AODV can hold low, sensible, and comparatively high portable rates, mutually with a range of data traffic loadings [26]. But, it makes no provision for safety. There are three main types of communication in AODV: route request (RREQ), route reply (RREP), and route error (RERR) communication. When a node wants to exchange data with a different node in the network and does not have a new path to this destination, it starts the path discovery process by spreading a RREQ message for the target node into the network. Middle nodes that accept this request either send a RREP to the source node if they have a new path to the target node and the "destination only" standard is not set, or forward the RREQ message to other nodes. A new path is a suitable path entry whose series number is equal to or greater than that controlled in

the RREQ message. If the request packet has been forwarded by this middle node before, it is mutely dropped. When the target node receives a RREQ for itself, it sends back a RREP message on the overturn path. The requesting node and the nodes getting RREP messages on the path change their routing tables with the new path[20,21,22].

A. Route Discovery

The procedure broadcasts a ROUTE REQUEST packet, which is swamped crossways the network. In accumulation to the source node address and target node address, the request packet contains path evidence, which report the order of hops taken by the request packet as it propagates during the network. RREQ packets use series numbers [13] to avoid repetition. Many distance vector routing protocols experience from a condition called Count to infinity [14]. This problem can be solved in AODV by using sequence numbering method which is resulting from DSDV. The source node looks for path by spreading a route request (RREQ).

B. Expanding Neighbors Search Technique

The source node broadcasts the RREQ packet to its neighbors which in revolve ahead the same to their neighbors. In particular in case of huge network, network wide broadcasts of RREQ organize are needed and to organize the same; the source node uses an increasing ring explore method. In this increasing ring explore method; the source node sets the Time to Live (TTL) value of the RREQ to a initial value. The next RREQ is broadcasted with a TTL value improved by an addition value if there is no reply within the detection period. Until a entrance Value is reached, after the RREQ is broadcasted the whole network the procedure of incrementing TTL value continues.

C. Setting up of Forward Path

When the target node or an middle node with a path to the target receives the RREQ, the RREP is produced and then it unicast the RREP towards the source node using the node from which it received the RREQ as the next hop. When RREP is received by an middle node and routed back along the overturn path, in its routing table it sets up a further path entry to target. If a path from source to the target has been recognized and then the source node can start the data broadcast.

D. Route Maintenance

When a out of order connection is detected, either by a MAC layer response or by not receiving HELLO messages, the upstream node sends Route Error (RERR) message to all antecedent nodes that use the wrecked link to arrive at their particular destinations. If the nodes have a path in their routing table with this connection, the path will be erased. Node S sends once more a path request to his neighbor nodes. Or a node on the way to the destination can attempt to discover a path to D. That method is called: Local Route Repair. A RERR message is sent to other nodes when dynamic path has out of order.

The benefits of AODV protocol are as under:

1. It does not place any extra burden on data packets as it does not build use of source routing.
2. The paths are established on order and destination order numbers are used to discover the newest path to the destination. The link setup interruption is lower.
3. It also responds very rapidly to the topological changes that affects the dynamic path.

The limitation of AODV protocol is:

1. Overhead on the bandwidth: Extra overhead on bandwidth will be occurred as compared to DSR.
2. This is susceptible to different kinds of AODV attacks as it based on the hypothesis that all nodes must collaborate and without their collaboration no path can be recognized.
3. Need on transmit medium: The algorithm requires that the nodes in the transmit medium can discover each other's broadcasts.

CONCLUSION

In this paper we survey on different Routing protocols and security attacks in MANET. We conclude that MANET (Mobile Ad-hoc network is one of temporary type of network which may affect by many types of security attacks. There are various features of attacks that should be reviewed before crafting any security plan for an Ad-hoc network. Black hole attack is type of in the mobile Ad hoc network which is to drop the message while the paths are being exposed. The malicious or black hole node will send a false path request reply to a false source which broadcasts a false request in the network. AODV is a reasonable option for ad hoc network establishment. This method also prevents and detects black hole node in the network.

References:

[1]. Rashid Sheikh, Mahakal Singh Chandel, Durgesh Kumar Mishra,"Security Issues in MANET: A Review",IEEE 2010.

[2] C.-C. Chiang, "Routing in Clustered multihop, mobile Wireless Networks with Fading Channel," Proc. /E€€ SICON '97, Apr. 1997, pp. 197-211

[3]. G. Indirani, Dr. K. Selvakumar, V. Sivagamasundari, "Intrusion Detection and Defense Mechanism for Packet Replication Attack over MANET Using Swarm Intelligence", (152-156) Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22, 978-1-4673-5845-3/13/2013 IEEE.

[4] Th. Clausen et al., "Optimized Link State Routing Protocol," IETF Internet draft, draft-ietfmanet-olsr-11.txt, July 2003.

[5] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007, page, 85-91

[6]. Umang S, Reddy BVR, Hoda MN, "Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption", IET Communications 4(17):2084–2094.2010.

[7]. Wu B, Chen J, Wu J, Cardei M, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks" In: Xiao Y,Shen X, Du D-Z (eds) Wireless Network Security. on Signals and Communication Technology.Springer, New York 2007.

[8]. Marti S, Giuli TJ, Lai K, Baker M, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks" 6th annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, August 2000. International Journal of Computer Applications (0975 –8887) Volume 80 – No 14, October 2013

[9] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[10] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," Proc. 2002 IEEE Int'l. Conf. Network Protocols, Nov. 2002.

[11] C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," 2nd IEEE Wksp. Mobile Comp. Sys.and Apps., 1999.

[12] P. Yi et al., "A New Routing Attack in Mobile Ad Hoc Networks," Int'l. J. Info. Tech., vol. 11, no. 2, 2005.

[13]. Tseng Y-C, Jiang J-R, Lee J-H, "Secure Bootstrapping and Routing in an IPv6-based Ad Hoc Network", Journal of Internet Technology 5(2):123–130, 2004.

[14]. Hu Y-C, Perrig A, Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy 2(3):28–39, IEEE2004.

[15]. Raja Mahmood RA, Khan AI, "A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks, International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, United Arab Emirates, November 2007

[16]. Mohammed Saeed Alkatheiri, Jianwei Liu, Abdur Rashid Sangi, " AODV Routing Protocol Under Several Routing Attacks in MANETs" ,2011 IEEE, 978-1-61284-307-0/11.

[17]. Htoo Maung Nyo, Piboonlit Viriyaphol, " Detecting and Eliminating Black Hole in AODV Routing", 2011 IEEE,978-1-4244-6252-0/11

[18]. Al-Shurman, M. Yoo, S. Park, "Black hole attack in Mobile Ad Hoc Networks", in Proc. ACM Southeast Regional Conference, pp. 96-97, 2004.

[19]. Roopal Lakhwani , Vikram Jain , Anand Motw ani , "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks", International Journal of Computer Applicaions (0975 – 8887) Volume 59– No.8, December 2012.

[20] Z. Karakehayov, "Using REWARD to Detect Team BlackHole Attacks in Wireless Sensor Networks," Wksp. RealWorld Wireless Sensor Networks, June 20–21, 2005.

[21] S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[22] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks," 2002 Int'l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.

[23] S. Kurosawa et al., "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," Proc. Int'l. J. Network Sec., 2006.

[24] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[25] Jyoti Raju and J.J. Garcia-Luna-Aceves, " A comparison of On-Demand and Table-Driven Routing for Ad Hoc Wireless etworks'," in Proceeding of IEEE ICC, June 2000.

[26] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[27] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conf. 2004.