International Journal of 360 Management Review, Vol. 06, Issue 02, October 2018, ISSN: 2320-7132

Review on Different Detection and Prevention Techniques of Attacks in MANET

Monika Goyal[1], Dr. Sandeep Kumar Poonia[2], Dr. Deepak Goyal[3]

[1] *Research Scholar, Jagannath University, Jaipur, Rajasthan (India),*

[2]*Associate Professor, Jagannath University, Jaipur, Rajasthan (India),*

[3] *Associate Professor ,VCE, MDU,Rohtak, Haryana, India.*

ABSTRACT

A Mobile Ad hoc Network (MANET) is a set of machines and is self-governing having declaration during the anxious wireless connections. The machines in the network attach and link the network actively. Due to this type of environment machines are weak to different types of attacks. These machines are communicating without any permanent path or system. All machines in MANET are free to move and they can join and left the network any time without any information. So MANET has self-motivated topology [1]. MANET has incomplete announcement, self-motivated topology, shortened power, limited computation capacity, multi-hop routing. Due to its types of topology routing in MANET networks is hard. Machines in MANET are taking their routing choices so they are suffering from numerous of attacks and mainly of network troubles like jamming, packet lost, interruption etc. There are numerous threats in wireless Mobile Ad hoc Networks. MANETs suffers from disturbance in which a unbearable node may or may not contribute in route discovery method with an intension to corrupt the whole network performance. Interruption has serious collision on routing and delivery ratio of packets. Many researchers have conducted many methods to offer types of finding and avoidance schemes. Various attacks and a survey of the existing solutions are presented in this paper.

Keywords: Mobile Ad hoc Network, MANET, Security, Black hole attack, Byzantine attack, Gray hole attack, Jellyfish attack, Worm hole attack,

1. INTRODUCTION:

Mobile Ad-hoc Networks (MANET) is the network of mobile nodes attached wirelessly and not including any support of permanent connections. There are some characteristics of MANET, which are as follows:

- High user concentration and big rank of user mobility
- Nodes make contact directly if they are within broadcasting range
- Each machine perform as both host and router
- Less protected than wired network
- Distributed environment of process for safety, routing and host design.
- MANET is an independent organization of mobile node. It can function in separation or may have gateways to and interfaces with a fixed network.
- There are Bandwidth Constraints and power Constraints.
- Network topology is dynamic
- In this network no need of fixed path.

2. SECURITY CRITERIA OF MANET:

There are a number of security criteria of MANET which assurance the safety of network. Various are as follows [1]:

Authenticity: This criterion make ensures that the target nodes are authentic not imitate.

Availability: It refers to the possessions of the network to carry on give services.

Non Denial: This ensures that the sender and receiver cannot deny about sending and receiving the communication.

Integrity: This ensures that there should be no alteration in message when it reaches to destination node.

Authorization: By this property different contact privileges are given to different types of users.

Confidentiality: The message can't be showed in its original form by any illegal user.

3. MANET ROUTING PROTOCOL

Various routing protocols are in MANET. When a node wants to communicating with target node, it transmits its existing status to neighbors. Routing protocols can be classified into proactive, Reactive and Hybrid routing protocol.

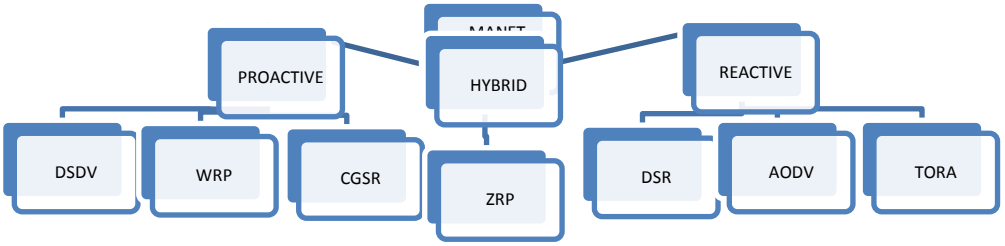

Fig 3.1

Proactive Routing Protocol: It also known as table-driven routing protocol. Every node keeps a routing table which contains record of neighboring nodes and available nodes and also the number of hops. As we increase the size of network, the overhead will also increase which results in turn down in performance. Destination sequenced distance vector (DSDV) and Optimized link state routing (OLSR) are examples of proactive protocol.

Reactive Routing Protocol: It is also known as On-demand routing protocol. When a node desire to broadcast data packet the reactive protocol in progress. The benefit of this is that exhausted bandwidth induced from regularly broadcast gets reduced. But the disadvantage of this is that it leads to packet failure. Ad hoc on-demand distance vector (AODV) and Dynamic Source Routing (DSR) are the some examples of reactive routing protocol. In AODV, each node adds the details of next hop in its routing table. The route discovery procedure executed when the destination node can't be arrived from source node. The source node broadcasts the route request (RREQ) packet to establish route finding procedure. The entire node accepts the RREQ packets send the route reply (RREP) packet to the source node if the destination node details are occurred in their routing table. Route in DSR nodes keep their route details from source to destination node.

Hybrid Routing Protocol: This protocol is combination of advantages of proactive and reactive protocol. Proactive protocol is used to collect the different routing details, whereas reactive protocol is used to keep the routing details when topology changes. Zone Routing Protocol (ZRP) and Temporally-ordered Routing Algorithm (TORA) are the some examples of hybrid protocol.

4. SECURITY ATTACKS IN MANET

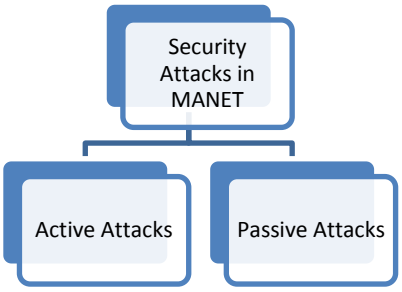

Figure 4.1

Security attacks in MANET can be divided as Active and Passive attacks.

ACTIVE ATTACKS:

In active attack an attacker is a specialized node wash out or change the data that is being exchanged in the network.

PASSIVE ATTACKS:

In passive attack attacker node is an illegal node gets the data without distracting or damaging the network operation.

Another categorization can be External and Internal attacks.

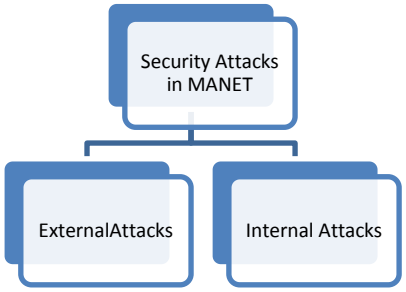

Figure 4.2

EXTERNAL ATTACK:

The attacker node in external attack is one which does not belong to that network.

INTERNAL ATTACK:

The Attacker node in internal attack is belongs to that network. Internal attacks are crueler as compared to external attacks since attacker knows all secret details and have advantage of access rights.

Many security attacks like wormhole attacks, black hole attacks [2], poisoning attacks, packet replication, and denial of service (DoS) attacks,[3] have been studied. The misconduct routing difficulty [4] is one of the security threats such as Black hole attacks.

Attacks can also be divided on layered basis. Each layer has many types of attacks. Table 1 shows some types of attacks on different layers.

Table 1. Attacks on layers basis

Layer	Attacks
Physical Layer	Jamming, , Eavesdropping, interceptions
Data Link Layer	Traffic analysis, monitoring
Network Layer	Wormhole, Flooding, Black hole, Gray hole, message tempering, Byzantine, resource consumption
Transport Layer	Session hijacking, SYN Flooding
Multiple Layer	Denial of Service (DoS), man-in-the-middle attack

Wormhole Attack

In this wormhole attack a unbearable node accept packets at one position in the network and tunnels them to another position in the network, where these packets are resent into the network [12]. Due to relay nature of the radio channel the attacker may generate a wormhole for those packets also that does not fit in to him.

Flooding Attack

In this attack unbearable node floods the network with the redundant data packets. The Nodes are not capable to receive or forward any data packet so any data packet forwarded to such nodes is useless in the network.

Gray Hole Attack

In this attack a unbearable node does not take part in route finding method that is initiated by other nodes and is then not a element of active route. Such unbearable nodes would increase the route detection collapse and damage the overall network performance [8]. Such attackers are preserve their power by interpreting the message planned for them and otherwise they do not assist with other nodes, which eventually corrupt the performance of the network.

Black Hole Attack

In this attack a unbearable node take part in route detection method by sending RREP message that includes the highest sequence number and this message is apparent as if it is upcoming from the destination or from a node which has a fresh adequate route to the destination [11]. The source then begins to launch out its data packets to the black hole trusting that these packets will accomplish the destination. As soon as the data communication begins, unbearable node drops the data packets that are wanted to be forwarded to destinations. Black hole attack is more critical as compared to gray- hole attack.

Jellyfish Attack

Jellyfish attack is different from Black- Hole & Gray-Hole attack. As this attack blindly sinking the data packets, it delays them before lastly delivering them. It may even mess up the order of packets in which they are received and sends it in arbitrary order. This change the normal flow control method used by nodes for consistent communication. Jellyfish attack can effect in important end to end delay and thereby corrupting QoS.

Packet Replication Attack

In this attack the attacker node repeat the stale packet and forward to the other node on order to use the sequence authority and consume bandwidth and generate misunderstanding in the routing procedure

Selfish Behavior

The attacker node selfish take part in route detection method and become a part of an active route. As the attacker nodes would begin dropping data packets that are not associated to him with an intension to keep energy which is necessary to forward data packets that belongs to other nodes.

Rushing Attack

In AODV or associated protocol, every node before communicating its data, first establishes a applicable route to destination. Sender node broadcasts a RREQ (route request) message in area and valid routes replies with RREP (route reply) with proper route details. Rushing attack disturb this replacement control method. Rushing attacker rapidly forwards with a intolerable RREP on behalf of some other node skipping any appropriate processing. Due to replacement control, actual valid RREP message from valid node will be discarded and therefore the attacking node becomes part of the route. In rushing attack, attacker node does send packets to appropriate node after its own filtering, so from external the network behaves normally as if nothing happened. But it might increase the interruption in packet delivering to destination node.

Table 2 . Effects of attacks

Type of attack	**Damage**	**Probability of success**	**Technical skills used**	**Throughput**	**Packet delivery ratio(PDR)**	**Solving complexity**
Flooding attack	Lesser	Lower then Others	Lower	Not evaluated	Not evaluated	Lesser
Worm hole attack	Maximum	Great Success	Higher	Not evaluated	Not evaluated	Maximum

Black hole attack	Lesser	Great Success	Lower	More with DSR as compared to black hole without DSR	More with DSR as compared to black hole without DSR	Less than wormhole

Conclusion:

Here we have discussed the issue of different attack and its effect. The necessities for a successful attack were analyzed as were the essential effort, probability and skill levels. Damage resulting from a successful attack was also analyzed, finishing a full picture of each attack which allowed contrast between the attacks. As a effect of our work we had specificities the ad hoc mobile networks, the troubles of security of routing protocols in these networks. Though, particular type of attack like flooding already recognizes their maximum level of efficiency when a single attacker is there. This methodical approach proves that the maximum damage results from a successful wormhole attack or black-hole attack, which also requires the greatest attempt. The plan of work by comparing and analyzing other routing attack like gray hole attack, selfish attack, rushing attack etc. was in procedure for some of the very accepted on-demand and even secure routing protocols and evaluate them and also execution and valuation of our proposed solution mechanism for the same.

REFERENCES

[1] 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

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

[3] Hu Y-C, Perrig A, Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy 2(3):28–39, IEEE 2004.

[4] 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

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

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

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