Advances in Wireless and Mobile Communications.
ISSN 0973-6972 Volume 10, Number 5 (2017), pp. 1185-1195
© Research India Publications
http://www.ripublication.com

Attacks Finding and Prevention Techniques in MANET: A Survey

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 Haryana, India.

Abstract

A Mobile Ad hoc Network (MANET) is a group of mobile nodes and is autonomous having statement through the insecure wireless links. The nodes in the network add and join the network energetically. Due to this kind of nature nodes are weak to various kinds of attacks. There are many threats in wireless Mobile Ad hoc Networks. MANETs suffers from interruption in which a hateful node may or may not participate in route discovery mechanism with an intension to corrupt the overall network performance. Intrusion has serious impact on routing and delivery ratio of packets. Many researchers have conducted different techniques to propose different types of detection and prevention schemes. Here various attacks types and a survey of the existing solutions is presented.

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

1. INTRODUCTION:

Mobile Ad-hoc Networks (MANET) are the networks of mobile computing devices joined wirelessly without any support of fixed interactions. There are some characteristics of MANET, which are as follows:

- No need of fixed road and rail network.
- Topology of the network is dynamic.
- Two node be in contact directly if they are within radio range
- Less Secure than wired network
- 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.
- Distributed nature of operation for security, routing and host configuration.
- More scalable than Fixed Network.
- High user density and large level of user mobility
- Nodal connectivity is intermittent.
- Each node act as both host and router

2. ISSUES IN MANET:

2.1 Randomly Changing Topology

2.2 Limited Energy

2.3 No centralized control

2.4 Scalability

2.5 Threat from Compromised node inside network

3. SECURITY CRITERIA:

There are some security criteria of MANET which guarantee the safety of network. Some are as follows [1]:

3.1 Availability: It refers to the property of the network to continue provide services.

3.2 Integrity: There should be no modification in message when it reaches to destination node.

3.3 Confidentiality: The message can't be viewed in its original form by any unauthorized user.

3.4 Authenticity: This ensures that the destination nodes are genuine not impersonate.

3.5 Authorization: Using this property different access rights are assigned to different types of users.

3.6 Non Repudiation: This property ensures that the sender and receiver cannot disavow about sending and receiving the message.

3.7Anonymity: The information related to the identity of a node should be kept to preserve privacy.

4. ROUTING PROTOCOL:

There are many routing protocols in MANET. Whenever a node wants to communicate with target node, it broadcast its current status to neighbors. Routing protocols can be classified into proactive, Reactive and Hybrid routing protocol.

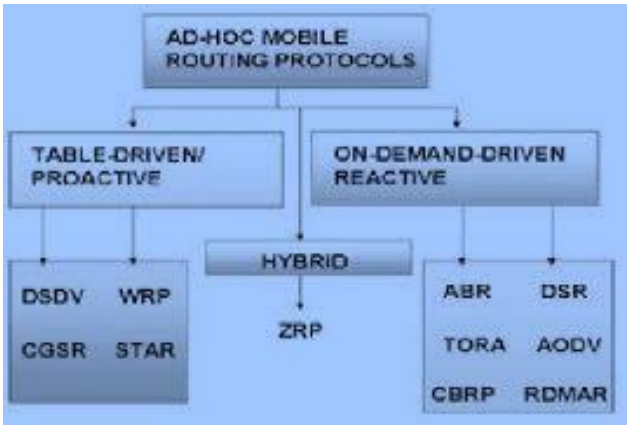

Fig 4.1

4.1 Proactive Routing Protocol: This is a table-driven routing protocol. Each node maintains a routing table which not only contains record of adjacent nodes and reachable nodes but also the number of hops. If the size of network increases, the overhead also increase which results in decline in performance. Destination sequenced distance vector (DSDV) and Optimized link state routing (OLSR) are proactive protocol.

4.2 Reactive Routing Protocol: This protocol is also called on demand routing protocol. When a node want to transmit data packet the reactive protocol started. The advantage of this protocol is that wasted bandwidth induced from cyclically broadcast gets reduced. The main disadvantage of this protocol is that it leads to packet loss. Adhoc on-demand distance vector (AODV) and Dynamic Source Routing (DSR) are the example of reactive routing protocol. In AODV, each node records the information of next hop in its routing table. The route discovery process executed when the destination node can't be reached from source node. The source node broadcasts the route request (RREQ) packet to start route discovery process. All the node receive the RREQ packets sends the route reply (RREP) packet to the source node if the destination node information is occurred in their routing table. Route

Maintenance process is started when the network topology has changed or the connection has failed. The source node is informed by a route error (RRER) packet. In DSR nodes maintains their route cache from source to destination node. Performance of DSR decreases with the mobility of network increases, a lower packet delivery ration within the higher network

4.3 Hybrid Routing Protocol: This protocol contains the advantages of proactive and reactive protocol. Proactive protocol is used to gather the unfamiliar routing information, then reactive protocol is used to maintain the routing information when topology changes. Zone Routing Protocol (ZRP) and Temporally-ordered Routing Algorithm (TORA) are the example of hybrid protocol.

5. ATTACKS IN MANET

Attacks in MANET can be classified as Active and Passive attacks. An Active attack is one in which an attacker which is a certified node wipe out or alter the data that is being exchanged in the network. While a Passive attack attacker node which is an unauthorized node get the data without disrupting or damaging the network operation.

Another classification can be External and Internal attacks. In External attacks the attacker node is one which do not belong to that network while in Internal attacks the Attacker node belongs to that network. Internal attacks are more severe than External attacks since attacker knows all secret information and have privileged access rights.

Many security issues such as snooping attacks, wormhole attacks, black hole attacks [2], routing table overflow, poisoning attacks, packet replication, and denial of service (DoS) attacks, distributed DoS (DDoS) attacks [3] have been studied in the recent years. The misbehavior routing problem [4] is one of the popularized security threats such as Black hole attacks. Some researchers propose their secure routing ideas [5-7] to resolve this issue, but the security problem is still an issue.

Attacks can also be classified on layered basis. Each layer undergoes different kind of attacks. Table 1 shows common type of attacks on various layers.

Restricting on network layer in [8] [9] [10] various network layer attack types are considered. Here some of them are discussed

5.1 Gray Hole Attack

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 [8]. Another intention of such attackers is to conserve their energy by interpreting the message intended for them only and otherwise they do not cooperate with other nodes, which ultimately degrade the performance of the network.

Table 1. Type of attacks on layers

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

5.2 Black Hole Attack

In this kind of attack a hateful node participate in route discovery mechanism by sending RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination [11]. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. As soon as the data transmission starts, hateful node drops the data packets that are needed to be forwardedto destinations. Black hole attack is more destructive as compared to gray hole attack.

5.3 Byzantine Attack

This attack can be done by a single intermediate node or a group of intermediates nodes, behaving as hateful nodes they either create a routing loop or direct the data packets to non-optimal path or selectively drop the packets. Such attacks are difficult to identify.

5.4 Flooding Attack

In this attack hateful node floods the network with the unnecessary data packets. The

victim nodes are not able to receive or forward any data packet and thus any data packet forwarded to such nodes is discarded from the network.

5.5 Wormhole Attack

In this wormhole attack a hateful node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network [12]. Due to broadcast nature of the radio channel the attacker may create a wormhole for those packets also that does not belong to him.

5.6 Routing Attacks

These kinds of attacks affect the normal operation of the routing protocol used in the network. Routing attacks can be of several types as:

5.6.1 Packet Replication Attack

In this attack the hateful node replicate the stale packet and forward to the other node on order to use the battery power and consume bandwidth and create confusion in the routing process.

5.6.2 Routing Table Overflow

In this attacker node create routes for non relevant node with an intension that no new routes are created. This causes an overflow of routing tables.

5.6.3 Routing Table Poisoning

In this hateful node propagate untrue routing updates or modify route update packet sent to other nodes.

This may cause inaccessible of some part of network, sub-optimal routing or congestion in the network's portions. If the hateful node poison the routing table/cache in which information about routes is maintained then such attack is known as Route Cache Poisoning.

5.6.4 Rushing Attack

In this when attacker node receive any request packet for route discovery then it sends the packet in the whole network before any other node forward the request packet. Due to this if same request packet send by authorized node to already

received nodes then they consider packet as duplicate and discard it. In this way attacker will always be part of the route and it is extremely difficult to identify such hateful node.

5.6.5 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.

5.7 Jellyfish Attack

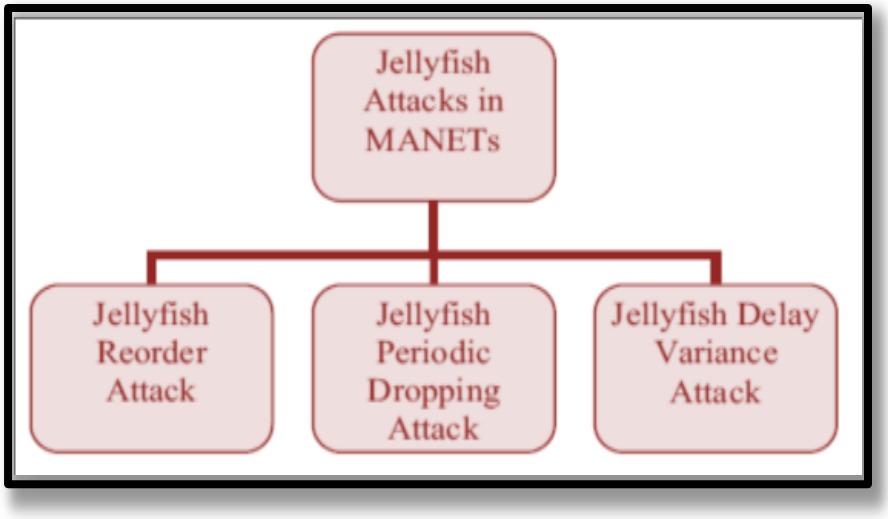

Fig 4.2

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.

Table 2. Comparison of Proposed Ids Methods and Drawbacks for Attacks in Multi hop

Name of attack	**Attack type(function)**	**Routing Protocol**	**Description of attack**	**Finding /Prevention mechanism**	**Description**	**Drawbacks**
Black hole attack	No forwarding of packets	AODV,DSR, SAR	Hateful node receives RREQ & send forged (fake) RREP with high sequence no(fresh route)	1. Black Hole Attack an Detection Method 2.Detection,Prevention and Reactive AODV 3.Defense mechanism	1. Analyze the Destination sequence number. 2.Stores the Destination sequence number of incoming	1. Additional delay due to pre-process 2. Does not consider other attacks 3.Less performance because it does not
Jellyfish attack	Delaying the data packet transmiss ion	Routing	It receives the packet but does not unexpectedly transmit the packets	1.Cluster and super cluster intrusion detection & prevention technique for reorder attack. 2. Packet reordering using hashing concept. 3.Enhancement in AODV protocol.	1. algorithm based on buffer comparison for detecting and preventing a Jellyfish Reorder Attack 2.inquired about congestion behavior of TCP and its variants under Packet reordering attack. The paper has also proposed a solution to packet reordering using hashing concept . 3. Increasing performance of AODV.	The main strength of this attack is that it is compliance with all the data plane and control plane protocols, so that the detection and diagnosis of the attack becomes difficult and time consuming.
Byzanti ne attack	Creates routing loop	Routing	Routing of packets on non best possible routes or forming the loop	1. Response and recovery engine 2. Attack Defence System In MANET Using Game Theory.	1.These engine employs a game- theoretic response strategy against adversaries modeled as opponents in a two-player Stackelberg stochastic game. 2. The first player i.e. compromised node will try to behave maliciously by making some moves like not to send data to next hop. The second player i.e. nodes equipped with Game Theory mechanism will make the move in order to defend himself from the consequences of move made by the compromised node.	Byzantine attack is difficult to detect in manet because of the forming loops.
Packet droppin g attack	Droppin g of packets	DSR,A ODV	Selfish nodes or compromised nodes drops all packets that they receive	PDA: Point Detection Algorithm	If the number of packet drop nodes increases then the data thrashing would also likely to be boost	Packet loss is higher in the ad-hoc network. If the number of packet drop Nodes is en larged then the data loss would also be likely to mount.
Neighbor	Disrupte	Route	Showing two	SAR: secure aware	SHA-1 algorithm is	This is become

attack	d route	Discove ry	nodes are neighbors but actually those are not neighbor; from different networks	routing	applied in CA- AOMDV protocol to achieve secure routing in MANET. CA-AOMDV is used to generate stable link between source and destination.	more complex to differentiate between the neighboring node and the disrupted node.
DDOS attack	Authenti ctation	Securit y	Attacker try to prevent genuine & authorized user	1.Adaptive Intrusion Detection & Prevention method 2. Intrusion detection System	1. This method uses a combination of chi-square test & control chart to first detect intrusion and then identify an intruder. 2. This method first analyzes the main vulnerabilities in the mobile ad hoc networks.	1. Does not consider other related parameters to cover all routing attacks 2. Does not apply for large-scale networks

5.8 Rushing Attack

In AODV or related protocol, each node before transmitting its data, first establishes a valid route to destination. Sender node broadcasts a RREQ (route request) message in neighborhood and valid routes replies with RREP (route reply) with proper route information. Some of the protocols use duplicate suppression mechanism to limit the route request and reply chatter in the network. Rushing attack exploits this duplicate suppression mechanism. Rushing attacker quickly forwards with a hateful RREP on behalf of some other node skipping any proper processing. Due to duplicate suppression, 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 does send packets to proper node after its own filtering is done, so from outside the network behaves normally as if nothing happened. But it might increase the delay in packet delivering to destination node.

Table. Effects of attacks

Type of attack	**Technical skills used**	**Damage**	**Packet delivery ratio(PDR)**	**Throughput**	**Solving complexity**	**Probability of success**
Black hole attack	Lower	Lesser	More with DSR as compared to black hole without DSR	More with DSR as compared to black hole without DSR	Less than wormhole	Great Success
Worm hole attack	Higher	Maximum	Not evaluated	Not evaluated	Maximum	Great Success
Flooding attack	Lower	Lesser	Not evaluated	Not evaluated	Lesser	Lower then Others

Here we have discussed the issue of different attack and its effect on the DSR-based routing protocol. In contrast to the former investigations of single attack possibilities the presented analysis gives a detailed overview of each attack and allows the reader to directly compare and evaluate possible risks using defined criteria. The requirements necessary for a successful attack were analyzed as were the necessary effort, probability and skill levels. Damage resulting from a successful attack was also analyzed, completing a full picture of each attack which allowed comparison between the attacks. As a result of our work we had specificities the ad hoc mobile networks, the problems of security of routing protocols in these networks. Our preliminary results show that, if additional attacking nodes are present the impact of most types of attacks increases. However, particular type of attack (e.g. flooding) already achieve (more or less) their highest level of effectiveness when a single attacker is present. This systematic approach proves

that the greatest damage results from a successful wormhole attack or black-hole attack, which also requires the greatest effort. Conversely, flooding attacks have an average success of probability and are easy to perform but cause relatively low levels of damage The plan of work by comparing and analysing other routing attack viz , gray hole attack, selfish attack, rushing attack etc. was in process for some of the very popular on-demand and even secure routing protocols and compare them and also implementation and evaluation of our proposed solution mechanism for the same.

REFERENCES

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

[2] 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.

[3] 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.

[4] 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

[5] 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.

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

[7] 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

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

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

[11] 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.

[12] 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.