International Journal of Research in Engineering, Science and Management
Volume 4, Issue 2, February 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

Categorization of MANET Attacks

Suma Patra[1*], M. Sushma[2]
[1,2]*Department of Computer Science, Telangana Social Welfare Residential College for Women, Karimnagar, India*

***Abstract*: *Objectives:* Mobile Adhoc Networks (MANETs) are networks with wireless connectivity between mobile nodes. As these nodes are mobile in nature, the topology of the network will be ever changing. Unfixed network, no central monitoring system make the MANETs prone to several attacks and the detection of cause also becomes hard. The main objective of this paper is to explain all the attacks discovered till now.**

***Methods/Analysis:* In this paper, almost all the possible MANET attacks were defined and are grouped according to their nature. Nearly 50 different attacks are collected and defined. Using this content a beginner can be exposed to all the security issues of MANETs.**

***Findings:* MANET attacks are grouped as Misleading attacks, Group attacks, Denial of Service attacks, Identity related attacks, Routing table related attacks, Node Isolation Attacks, Packet related attacks, Confidential data retrieval or passive attack and Other attacks. A researcher need not to search for each attack in different contexts. Almost all the possible attacks and their functioning can be known using this single paper.**

***Applications/Improvement:* Till now, in several papers, only few attacks were explained and the solutions were proposed to a single attack. Complete idea on MANET attacks could not be achieved using them. This paper presents classification of a huge number of attacks. Understanding these attacks stated leads to the proposal of solutions and thus improves security in MANETS.**

***Keywords*: MANETs, Attacks, Categorization, Security, Malicious nodes.**

1. Introduction

In MANETs the devices are mobile and they don't have wires to get connected. Every node works as a router and there will be no central supervising system. The wireless nature, transportability of nodes and self-adjusting quality makes MANETs more preferable. These characteristics support the increasing use of MANETS. The vicinity in which there is a need for moving nodes wish to use these types of networks. While in transit many nodes are attached to the network and many are detached. This behaviour raises a variety of link attacks [1]. MANETs are much prone to various attacks in contrast to static networks that are in both wireless and wired networks.

This paper next discusses the advancement of MANET technology in section 2, Applications in Section 3, Drawbacks and challenges in Section 4, Classification of MANET attacks in Section 5, then the Conclusion and Future work in Section 6 followed by references in Section 7.

2. Advancement of MANET Technology

Earlier in 1970s, networks with radio communication were used. These are called Packet Radio Networks (PRNETs). In these networks, the message sent was accessible to all the persons at different nodes in the network.

Then in 1980s, improvements were made to PRNETs to result Survivable Adaptive Radio Networks (SURANs). These networks worked with the technique of Packet Switching. These are mostly used in battlefields with mobile nodes.

In 1990s Blue tooth technology evolved and is used in Commercial Adhoc Networks. Next was Ad-hoc sensor networks. Later wireless local area networks (WLANs) came into picture. Then the concept of Mobile Adhoc Networks (MANETs) arose and the research is still continuing in these networks.

3. Applications

- Military communications
- Policing
- Air crafts
- Battlefields
- Search and rescue operations
- Games
- Outdoor Internet accessibility
- Taxi cabs
- Sports stadiums
- Boats
- Fire fighting
- Recovery when disasters occur etc.

In all these aspects MANETs provide a noticeable support [2], [3].

4. Drawbacks and Challenges

The following are challenges and drawbacks of MANETS [4],

Deficiency of Central Monitoring System: To manage and mangle with communication system of MANETs, there will be no central management.

Detection of Malicious Node: Many devices join and many moves away from the network scope while in transit. So the detection of suspicious node is difficult

Adjustability: The network must be able to accept the

*Corresponding author: sumapatra@gmail.com

attachment of new nodes.

Cooperation between Nodes: The nodes in MANET need be more cooperative with all the other nodes in the network.

Ever Changing Topology: Due to the position change of nodes, reliance between the nodes gets reduced.

Scarcity of Resources: Resources like bandwidth, battery constraints, and virus tolerance levels will not be up to the mark.

Insecure Environment: Malicious nodes may enter the network as new nodes get added. This leads to data theft or stopping the services to nodes.

Varying Protocols: Each node in the network may have different protocols and all these nodes must be compatible with *each other*.

Inappropriate Boundary: The border of the network in all dimensions cannot be set accurately. Nodes can be added or deleted from the network.

5. Classification of MANET Attacks

A variety of attacks and their nature is stated in brief. References to handle with the attacks are also presented. This is used to make the research in the area of MANETs very easy and researchers evolve with many solutions for many attacks.

Basically MANET attacks are classified into Active and Passive attacks [5]. Where in active attacks the data packets while in transit may be changed, deleted, dropped or routed to different destinations. In Passive attacks the network activities are uninterrupted but unauthorized persons listen to the data messages.

In this paper these attacks are further classified based on their nature. They are,

A. Misleading attacks

This type of attacks misleads or misguides the network by providing false information. The following are few attacks which come under misleading attacks [3], [5].

Black Hole Attack: A malicious node suggests the sender that some route is the shortest route from source to destination. By this misleading information, the confidential data packets may be retrieved [6]-[8].

Bogus Registration: A node will get registered in the network using the details of authorized person and gets access to private information and there is a chance that the activities of the network get disturbed [9]. In this particular attack, persons misunderstand that the malicious person is authorized.

Eclipse Attack: This attack is not actually an attack but it supports to have other attacks in the network. Data packets are routed through different routes by misleading that there is traffic along the route.

Fabrication Attack: This attack is done by routing the packets through unoptimized routes [9], [10]. It exhibits that the next hop to be chosen is unavailable. Then the data chooses other route.

Link Withholding: This attack is also a type of routing table modification attack. In this attack the link between nodes are shown to be absent and thus communication through this route are stopped.

Link Spoofing Attack: This attack is also a routing table related attack. This affects both links and paths. The legitimate routes are changed and are shown as unoptimized. This leads to the selection of other routes.

Selective Forwarding Attack: This attack is also a packet related attack. In Selective forwarding attack, a node acts as a legitimate node and then drops the packets in random and sends some of them [9].

Sleep Deprivation Attack: In sleep deprivation attack, requests are continuously sent to the nodes which are not in the network [9], [11]. Wastage of Energy [12], band width is done in it.

Sybil Attack: In this attack, one node which is malicious acts as number of nodes using their unique legitimate identities [9].

Node Replication Attack: In this type of attack, many clones are made for a node in the network. This makes the detection of the actual node very difficult [13]. This can also be called as cloning attack.

Impersonation Attack: Internet Protocol (IP) address or Medium access control (MAC) address of other nodes are used as an identity or the malicious nodes [3]. With the same identity many nodes will be present in a same network. This causes a lot of confusion while transmitting data to a node.

B. Group attacks

These attacks are not caused by a single malicious node but a group of them by colluding with each other [9], [14].

Byzantine attack: It is a network layer attack. Few nodes in the network collude with each other and loops are formed between them. This leads, so that data is looped between few nodes or sent through unwanted paths.

Colluding Misrelay Attack: The malicious nodes collude with a few nodes in the network and create different attacks in data transmission by dropping, tampering the packets etc.

C. Denial of Service attack

In this type of attack the route to a particular target node is made busy by sending continuous messages [6], [11]. So there will be no chance for original messages to reach it. Energy of the node gets reduced and in turn this node will not be a part the network.

Distributed DOS Attack [15], Flooding Attack, Jamming, Resource Exhaustion Attack, and Selfish Behaviour of Nodes also lead to DOS attacks.

In Distributed DOS attack many nodes are targeted and made busy. In flooding attack repeated RREQ messages are sent to a node which is actually not in the network. Jamming is also a packet related attack where the data transfer frequency of nodes is computed and links are flooded with jam signals. This stops the services to that node. Resource Exhaustion Attack makes the resources of the network to exhaust by repeated sending of RRER and RREQ messages. Then Selfishness of nodes to conserve its resources also leads to denial of service attack.

Active Interference: It is a physical layer attack. This type of interference is a DOS attack [15]. In it link between nodes are kept busy and stops communication between them. In it the data packets are sent in disorder or resent continuously [2], [9].

Session Hijacking: This attack also leads to the retrieval of

confidential data by hijacking a node This is done by stealing its IP address, unique identity, sequence number etc.

D. Identity related attacks

The intention of these attacks is to hide the details of nodes in the network. Because of this, messages cannot be sent to it and this node cannot be used as next hop. The following are few types of this attack [11], [13].

Information Disclosure Attack: Details of a node like its position etc. are disclosed by an attack. By knowing the personal information of a node many attacks can be made to it.

Invisible node attack: In this attack a node doesn't reveal its details related but actively work in the network.

Location Disclosure Attack: It is a part of information disclosure attack where the attacker discloses all the topology related information of a network. This gives scope to have many other attacks.

E. Routing table related attacks

These types of attacks are made by altering the actual details in the routing table. Few types of these attacks are [4], [16],

Source Route Modification Attack: It is a type of passive attack where confidential data is heard by malicious nodes. In it some node in the shortest path is collapsed by applying DOS attack [15]. Later a route where the malicious node is present is chosen.

Route sequence number modification attack, Routing table poisoning, Routing table overflow attack, Hop Count Modification Attack are related to the routing table.

RERR Generation Attack: False message regarding a route are sent continually by a malicious node. Due to this, link failures occur in a network.

Neighbour Sensing Protocol Attack shows that the link to the neighbouring nodes is absent. So, data transit is done through stale routes.

F. Node Isolation Attack

In this type of attacks, the target node is abandoned from the network [9].

Black Mail Attack is a type of node isolation attack where malicious node sends suspected messages to a node. Then that node is added to blacklist as it is treated as a malicious node too.

G. Packet related attacks

These attacks are related to the data packets that are sent through the network. Few types of it are discussed below [2], [6], [10].

Packet Replication: An attacker makes many replicas of a packet and they are sent to the destination. Single data packet will be received many times leading to confusion and the reduction of resources. Replay attack is a type of packet replication attack.

Data Packet Dropping Attack: The attacker node which is in the route of data transmission drops the packets and thus stops them in reaching the destination.

Gray Hole Attack: This attack is related to wrong routing and a type of misleading attack. Here, unoptimized routes are shown as an efficient one and the packets moving through this route are dropped 7.

H. Confidential data retrieval or passive attack

In these attacks, data in transit is not disturbed but a secret hearing of messages is done. Some attacks of this type are [11], [14].

Eaves Dropping: In a Mobile Adhoc Network, the data packets are transmitted from source to the destination by taking many hops. Any node in the route of transmission can retrieve the confidential data. The secret listening of sensitive or confidential data is called Eaves Dropping [2], [9].

Rushing Attack: In this type of attack, route requests are caught by an attacker and replies to the request very fast that the other nodes. So that particular node is selected for transmission of data. Then the data is tapped easily.

Man in the middle attack: A person at a node in between the source and destination can hear the messages between them.

Snooping: Snooping is observation of the actions of some node and reading the sensitive data like passwords while typing etc.

Wormhole Attack: A pair of nodes collides with each other and one node sends the data packets of attacked node to the other through a tunnel. This tunnel established between the malicious nodes is called a worm hole [9], [14]. Its detection is difficult.

Forged FA: A node itself shows that it is a forged foreign agent (FA). This degrades the network standards by retrieving the confidential data [9].

I. Other Attacks

Malicious Code Attack: Virus, worms, spywares and Trojan horses are sent to the target node. This code spoils the regular activities of it [6], [9], [11].

Overwhelm Attack: Many nodes in the network are overwhelmed. Due to this, the traffic at the base station raises, so energy consumption increases.

Repudiation Attack: A node sends data packets and later he disagrees that he has sent the data. And also a person can deny, saying that he has not received some data even after getting it [14]. So, necessary measures have to be taken to stop someone from doing so.

Snaring Attack: This attack is made by taking a person into control and then operate a malicious node in his identity. The device of a soldier who is caught by his enemy can be used to attack.

Traffic Analysis: When the traffic in a MANET is analyzed, information regarding the active nodes can be known. Using this information, many attacks can be made to reduce the performance of the network.

6. Conclusion and Future Scope

Though MANETs result in many attacks, they are widely used due to wireless nature and mobility of nodes. Many security attacks were discovered and few solutions were also proposed. Many are still to be known. This paper serves for a researcher in beginning to know the basic information of

different attacks of MANETs.

So far limited research is done in the area of MANETs. There is a need for networks with mobile nodes and many attacks have to be resolved with some solutions. These type of networks are used for communication in military services, disaster management etc. So there is a high scope for MANETs to be used further.

References

[1] D. Maheshwari, R. Nedunchezhian. An Optimized Approach on Link Stability with Load Balancing in MANE using Balanced Reliable Shortest Route AOMDV (BRSR_AOMDV). Indian Journal of Science and Technology, 9(4), Jan. 2016.

[2] Jose Marinho, Jorge Granjal, Edmundo Monteiro. A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. EURASIP Journal on Information Security, March 2015.

[3] Priyanka Goyal, Vinti Parmar and Rahul Rishi. A Literature Review of Security Attack in Mobile Ad-hoc Networks. International Journal of Computer Applications, 9(12), November 2010.

[4] Saleh Ali K.Al-Omari, Putra Sumari. An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Applications. International journal on applications of graph theory in wireless ad hoc networks and sensor networks, 2(1), March 2010.

[5] Priyanka Goyal, Sahil Batra, Ajit Singh. A Literature Review of Security Attack in Mobile Ad-hoc Networks. International Journal of Computer Applications, 9(12), 2013.

[6] H. Yang, H. Luo, et al. Security in mobile ad hoc networks: challenges and solutions. In proc. IEEE Wireless Communication, UCLA, Los Angeles, CA, USA,11(1), 2013.

[7] K. Hizbullah, U. Arif Iqbal, Insafullah. A Khattak Approach for Detection and Removal of Black and Gray Hole Attacks in Manet. Indian Journal of Science and Technology, 9(4), Jan. 2016.

[8] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao. A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(4), 2011.

[9] Zaiba Ishrat. Security issues, challenges & solution in MANET. International Journal of Computer Science & Technology (IJCST), 2(4), 2011.

[10] Ch. V. Raghavendran, G. Naga Satish, P. Suresh Varma, Security Challenges and Attacks in Mobile Ad Hoc Networks, International Journal of Information Engineering and Electronic Business (IJIEEB), 5(3), April 2013.

[11] Nadeem. A, Michael P. Howarth. A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks. IEEE Communications Surveys & Tutorials, 15(4), 2013.

[12] K. Vinoth Kumar, S. Bhavani. An Efficient Secured Localization based Optimized Energy Routing for MANET. Indian Journal of Science and Technology, 8(35), Dec. 2015.

[13] Sachin Lalar. Security in MANET: Vulnerabilities, Attacks & Solutions. International Journal of Multidisciplinary and Current Research (IJMCR), 62-68, Jan./Feb. 2014.

[14] S. Marti, T. J. Giuli, K. Lai, M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (Mo-biCom'00), 2000,

[15] Tariq Ahamad, Abdullah Aljumah. Detection and Defense Mechanism against DDoS in MANET. Indian Journal of Science and Technology, 8(33), Dec. 2015.

[16] K. Abdelaziz, M. Nafaa, G. Salim. Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks. Computer Modelling and Simulation (UKSim), UKSim 15th International Conference, 2013.