Assessment of Security Vulnerabilities in MANET

Muskan Sharma[1], **Chander Prabha**[2]

M.E. Scholar, CSE, Swami Devi Dyal Institute of Engineering & Technology

Assistant Professor (CSE) & Head, IT department, Swami Devi Dyal Institute of Engineering & Technology

Abstract: ***As MANET is a mobile network, nodes are free to move, so it's more prone to attacks. Attacks might be active or passive. Passive attacks listen to message transmission and obtain the secret information where as active attacks are able to change the transmission data. Active attacks involve message replay, fraud counterfeiting, message tempering, and denial of service. Security is the main concern in MANET. Here we are discussing on the MANET attacks and how security needed in MANET. Security depends on availability, authenticity, integrity, authorization, confidentiality, scalability and non reputation.***

Keywords: MANET, MANET attacks, Security in MANET, Passive attacks in MANET, ACTIVE attacks in MANET

1. Introduction

MANET is a wireless, infrastructure less, self-configuring network. In Fig. 1 MANET, mobile work as nodes means data/packet transmission is done by mobile nodes and nodes can freely move and change their positions. So we need to focus on security of data. [1] MANET provides rapid connection between independent mobile users. We need an efficient self organizing mechanism which can detect a malicious behaving leader. [3]. The lack in any infrastructure makes the MANET network insecure leading to attacks such as blackhole and grayhole.

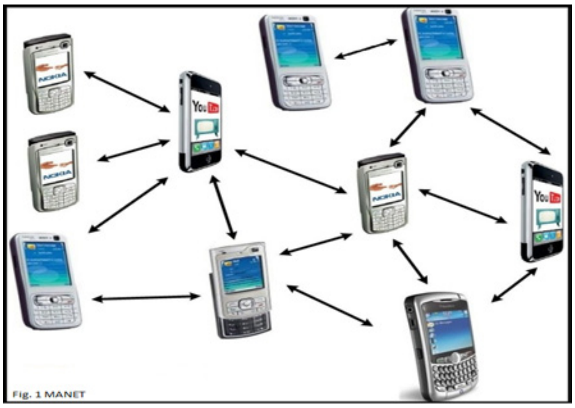


Fig. 1 MANET

2. Assessment of Vulnerability in MANET

MANET's being infrastructure-less networks are prone to vulnerabilities due to reasons mentioned below:

- **Absence of Physical Security:** Due to lack of physical security mobile nodes can be controlled or seized by an attacker. Its very hard to distinguish a trusted node from an untrusted node.
- **Dynamic Network Topology in MANET:** It is very difficult to predict the number of nodes in a network at some time in the future because any mobile node can join or leave the MANET network. It is hard to detect malicious behavior.
- **No way to centrally control the network:** Tasks like traffic monitoring and detection of attacks becomes very difficult in the absence of a centralized control facility.
- **Energy Resource Restriction:** Our network is assumed to be composed of nodes which operate on battery power with no alternate power source. Huge traffic may lead to more battery consumption as the target node may be continuously busy in handling other packets leading to denial of service attack. [5]

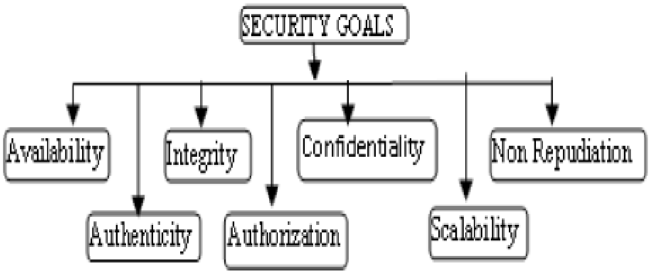
3. Attacks on MANET

- **Denial of Service Attack:** This attack is aimed at jamming the network with fake packets in order to bring down the path to the server to stop the service and deplete the resources of the nodes. [2]
- **Impersonation:** When a malicious node impersonates itself as a genuine node in order to monitor the network traffic or send fake packets.
- **Eavesdropping:** This is a passive attack meaning the intruder only performs monitoring on connections to get information about the traffic without injecting any fake information. In this attack, the intruder silently listens to communication by tapping the wireless link.
- **Sybil:** The intruder disguises itself as the identity of multiple nodes
- **Dropping packets:** The intruder drops packets destined for the target node which is harder to detect if selective dropping is performed.
- **Routing table overflow:** The intruder overflows the nodes' routing tables with fake routing information.
- **Detour:** The intruder creates virtual nodes on the optimal routes to make them appear longer than the other routes forcing the nodes to wrongly use the non-optimal route.
- **Rushing:** In order to make the nodes discard any other control packet in the network, the intruder broadcasts a route request and reply packets very quickly.
- **Hello flood:** The intruder broadcasts hello messages to all the network nodes in order to be wrongly considered as their neighbor by using strong enough power for these messages
- **Sink hole:** The intruder attracts the nodes to use its fake route making it easy to inject any of the above mentioned attacks.

4. Security Objectives of Mobile Adhoc Networks

Security is the major concern in MANET because it is wireless, infrastructure less network. In MANET, Fig. 2 Security is depends on Availability, Authenticity, Integrity, Authorization, Confidentiality, Scalability and Non Reputation things. [4]

- **Availability:** It refers to the property of the network to continue provide services regardless of the state of the network. A denial of service attacks is based to attack this property.



- **Integrity:** Integrity means no any modification, edition, addition, subtraction in data. Data will send safely from one node to another without any changes.
- **Confidentiality:** Confidentiality means only receiver can see the data which is sent by the sender, not any other person will able to see it.
- **Authenticity:** Parties can prove that they are authorized and they have permission to access the data with the help of this property.
- **Non repudiation:** It means the party who send and the other party who received the data cannot disavow about sending and receiving the message.
- **Authorization:** This property provides the access permission of that means that can edit, review, read, and write on data.
- **Anonymity:** The identity of a node should be kept private for privacy- preservation.

5. Conclusion & Future Scope

Here I discuss MANET Attacks and Security objectives. After using these points we can make our MANET secure. It is wireless and infrastructure less network and there is more need to concern about the security of the MANET network.

References

[1] Yanwei Wang, F. Richard Yu, *Senior Member, IEEE,* Helen Tang, *Senior Member, IEEE,*andMinyi Huang, *Member, IEEE.* **A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks**.

[2] Seyed Mohammad AsghariPari, Mohammad Noor mohammadpour, Mohammad JavadSalehi, BabakHosseinKhalaj, HamidrezaBagheri, Marcos Katz. **A Self-Organizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks.**

[3] Parkavi Murphy John (Research scholar, Computer science and Engineering, Anna University, Chennai-600025.), Dr.P.Vivekanandan (Professor, Department of Mathematics, Anna University, Chennai-600025). **A framework for Secure Routing in Mobile Ad hoc Networks.**

[4] Rashid Sheikh, Durgesh Kumar Mishra (Acropolis Institute of Technology and Research, Indore, India). Mahakal Singh Chandel (Arjun Institut: of Advaced Studies and Research Centre, Indore, India), **Security Issues in MANET: A Review.**

[5] Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng, College of Computer Science, Chongqing University, Chongqing, China. **Research on MANET Security Architecture Design.**

Author Profile

Muskan Sharma received the B.Tech. degree in Computer Science & Engineering from Indo Global College of Engineering in 2011 and pursuing M.Tech (2014) from Swami Devi Dyal Institute of Engineering & Technology. Now she is working on her Master's Thesis on MANET. She is exploring CBDS technique to detect the attacks.

Chander Prabha received the B.Tech. Degree in Computer Engineering from MMEC, Mullana in 2002 and M.E. from Punjab Engineering College (PU, Chd). Now she is working as an Assistant Professor (CSE) & Head of IT Deppartment in SDDIET, Barwala, Panchkula. Her field of interest in the area of wireless networks, Collaborative and distributive computing and network security.