AN EXTENSIVE ANALYSIS OF MANET ATTACKS USING SPECIAL CHARACTERISTICS

Gomathi K.

Research Scholar, Dept. of Computer Applications, Sathyabama University,
Chennai, Tamilnadu, India,
gomathikrishna@gmail.com

Dr. Parvathavarthini B.

Dean, St.Joseph's College of Engineering,
Chennai, Tamilnadu, India,
parvathavarthini@gmail.com

Abstract:

Wired or Wireless network, security is the most crucial part of any data transmission. Securing Mobile Ad hoc networks is an extremely tough issue because chances of having vulnerabilities are more when comparing to conventional wired networks. The MANET constructed by relying each node in the network. Due to the absence of central authority and dynamic topology MANET can accommodate misbehaving node as part of network. These misbehaving node or attacker fabricate different types of problems and that leads to total degradation of network performance. so understanding possible form of attacks are half way to reach the solution. In this survey paper we provide brief discussion of various types of attacks and issues associated with data transmission.

Keywords: MANET; Attacks; Misbehaving nodes.

1. Introduction

A Mobile Ad hoc Network(MANET) is an infrastructure less dynamic transitory network, each node act as both host and router. The participants of MANET, join and leave the network without any prior setup and with no control of centralized administration. The MANETs are mainly used where there is rapid communication is needed and there is no much more time for checking every participants for their reliability. One of the most critical issue in MANET is misbehaving nodes present inside and outside of the network and creates lots of problems in data transmission as well as draining valuable network resources. Automatically these leads to reduce the overall performance and lifetime also [Diwaker, Choudhary and Dabas (2013)]. To extend lifetime of MANET, various possibilities of attacks and some of their preventive measures are analyzed in this paper. However new variety of attacks may come in near future, so identifying and providing solution to these attacks is an ongoing research process and that makes MANET safe and sound network.

2. Attacks in MANET

The topology of MANET is a dynamic topology and any number of node can enter and leave over time. All these nodes cannot be reliable but network formed in this unfriendly environment. The teamwork of every node is assumed but that is not true in existent communication [Jayaraj Singh, Arunesh Singh and Raj shree(2015)]. There are an abundant range of misbehaving nodes present in the MANET that target to attack the secure data transmission. The attacks are classified based on many characteristics as follows.

2.1. On the basis of network operation

.2.1.1. Active attacks

The attacker disturbs normal network activity by alter or destroy the message being exchanged. The possible forms of active attacks are classified as follows [Navaneethan T and Lalli M (2014)]: .

- Fabrication Attacks: Attacker send fake messages to other legal nodes in network.
- Spoofing Attack: Attacker gives false information about authentic nodes IP address and MAC address.
- Impersonation: Attackers steal authentic nodes identity and interfere in communication.
- Modification: Attacker do some modification in part of the message.
- Dropping: Selfish nodes drop all packets without forwarding.

.2.1.2. Passive attacks

The attacker does not disturb the normal network activity. The attacker simply snoops the data being exchanged in the network. The confidential information's are disclosed by the attacker. Eg: Information disclosure or Eavesdropping attack, Traffic Analysis

2.2. On the basis of Existence

.2.2.1. Internal attacks

The node that belongs to network causes vulnerabilities by gaining unauthorized access and masquerade as an authentic node. The important information's are gathered by attackers.

.2.2.2. External attacks

The node from outside of the network mainly causes congestion by sending false routing messages. Due to these fake messages, the normal activity of the nodes in the actual network are affected and concluded with poor services.

2.3. On the basis of Mobility

2.3.1. Wired attackers

Wired attackers in MANET are more danger to network, since it has adequate resource for doing damage. The encrypted messages need additional time to break, wired nodes are provided with extensive resources for doing this.

2.3.2. Mobile attackers

Mobile attackers in MANET gives a lesser amount of damage to network, because its resources battery, bandwidth, coverage range and connectivity are very restricted like MANET node.

2.4. On the basis of Sight

2.4.1. Stealthy attacks

Some type of attackers are very silent, they do their damages in unexpected way and hidden from normal Intrusion detection System(IDS).

2.4.2. Non stealthy attacks

But some type attackers cannot hide their visibility, they can do their until its caught by detection mechanism.

2.5. On the basis of Traffic

Normally in network two types of data are transferred namely data traffic(actual message) and Control traffic(routing message).

2.5.1. Data traffic attacks

The node aims to damage original data by simply drop or delay the forwarding. The important data may be lost in the communication, automatically this leads to overall performance degradation.

2.5.2. Control traffic attacks

The node aims to corrupt the route by accessing routing messages and forge the original route. The fake routes are initiated by the attackers to redirect the messages.

2.6. *On the basis of Partnership*

2.6.1. Direct collaboration attacks

The attackers directly have a partnership with node that exist in the network and give some troubles.

2.6.2. Indirect collaboration attacks

The attacker is no longer part of the network, it stays outside but causes congestion by sending excessive messages.

2.7. On the basis of Number of Attackers

2.7.1. Single or Independent attacker

Single attacker initiate very simple attacks due to their limited capacity like closed coverage range, limited battery etc,.

2.7.2. Multiple or colluding attackers

Several attackers are join together to launch attacks, definitely these type of attacks cause heavy damage to network and also results in poor performance or entire shutdown of the system. [Raghavendran C.H.V, G. Naga Satish and Suresh Varma P(2013)]. Fig. 1. represents these attacks clearly.

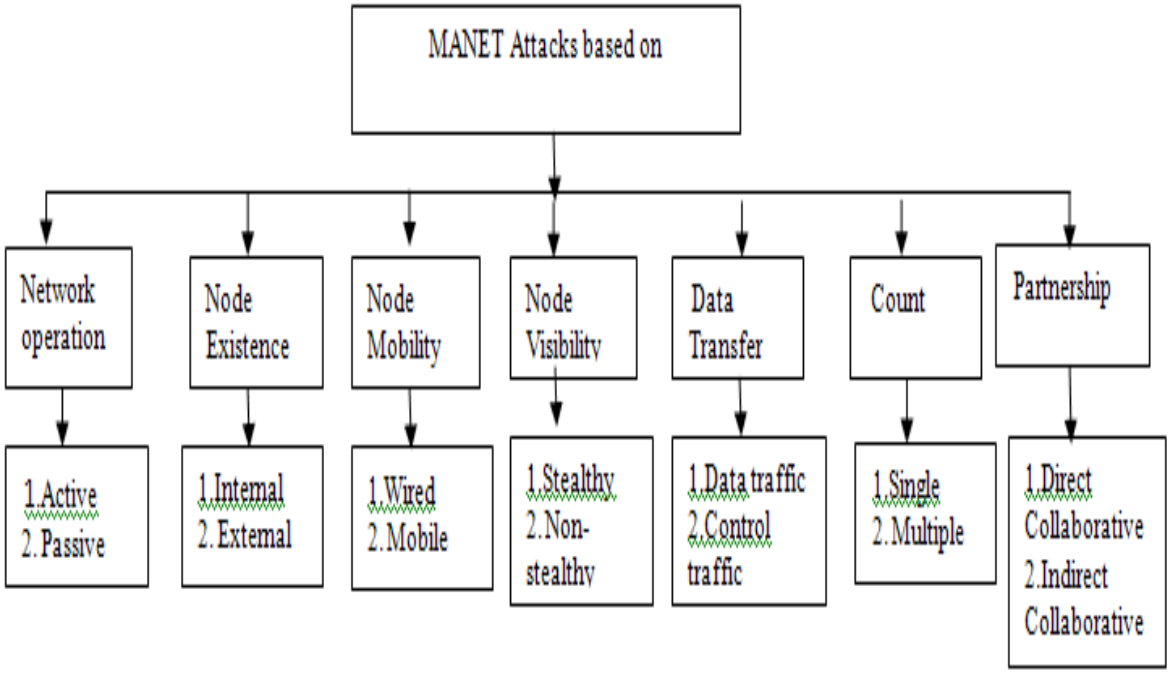

Fig. 1. MANET attacks classification based on different characteristics.

2.8. On the basis of layers in MANET

The attacks can also be classified according to MANET layers.[Punya Peethabram and Jayasudha ,(2014)]

2.8.1. Physical layer attacks:

Attacks in this layer primarily focus on communication channel.

- **Eaves dropping**: Unauthorized nodes tuning its frequency with legitimate nodes frequency and unknowingly access the information.
- **Jamming:** The receivers frequency range are known by malicious node and that actively prevent the actual reception of messages. This Denial of Service(DOS) due to receivers radio signal are destroyed by noises of illegitimate users.

2.8.2. Data link layer attacks:

- **Traffic Analysis:** The adversaries monitor the entire network and communication happens in the network and gather information's about actual nodes location, topology used, present source and destination pair and when will be the optimum time for attacking the network.

2.8.3. Network layer attacks:

The optimum route decisions are taken in this layer for forwarding packets. So many attackers aims to collapse the path and misrouted the packets to illegitimate nodes [Athira and Jisha (2014)].

- **Black hole attack:** The malicious node announces itself having shortest route between source and destination and consume or drop the packets that are passing through it.
- **Worm hole attack:** The tunnels are created between attackers and the packets that are forwarded through this tunnel are overheard by multiple attackers.
- **Grey hole attack:** This type of attacks are special variation of black hole attack, where there is only selective packets are dropped not all the packets.
- **Sybil attack:** The fake identity nodes are created and they act like a legitimate node and consumes valuable resources.
- **Rushing attack:** The compromised node quickly responds for route request messages than the safe nodes, due to this safe routes are missed.
- **Flooding attack:** The attackers aims for wasting battery power and bandwidth by requesting path for non-existent node or by passing useless data.
- **Routing table Poisoning attack:** The attacker corrupts the routing table and false route entries are made in the routing table.

2.8.4. Transport layer attacks:

- **Session hijacking:** During the session setup, attacker take-off victim node's IP address and perform communication like legitimate node.

2.8.5. Application layer attacks:

- **Malicious code attacks:** The application software's and operating system both are vulnerable to worms, viruses and Trojan horses.
- **Repudiation attack:** The selfish node refusing to take part in the communication [Shikha Jain, (2014)]. Table 1. represents summary of these layered attacks and its consequences.

Table 1. Classification of MANET layer attacks

Manet Layers	Attack Name	Active attack	Passive attack	Consequence of attack
Physical Layer	Eavesdropping		yes	Confidential messages red by unauthorized users
	Jamming	yes		Packets not reach exact destination
Data link layer	Traffic Analysis		yes	Topology and node information gathered by unintended user.
Network layer	Black hole	yes		Malicious node drop packets
	Worm hole	yes		Packets forwarded in unsafe route instead of safe route.
	Rushing attack	yes		Safe routes lost by packets.
	Grey hole	yes		Malicious node drop specific node's packet but not all.
	Sybil attack	yes		Fake identity nodes consumes resources.
Transport Layer	Session hijacking	yes		Attacker take-off node's IP address.
Application layer	Malicious code attack	yes		Application may be affected by virus, worms
	Repudiation attack	yes		Refusing to take part in communication.

3. Conclusion and Future Directions

The uniqueness in MANET make more susceptible than wired network. In this study, try to categorize MANET attacks based on various characteristics as well as layer based attacks are analyzed. However different security mechanisms are employed to prevent these attacks ranging from Intrusion Detection System(IDS) to various cryptographic algorithms. Nevertheless still MANET susceptible to new kind of attacks. In near future we will try to come up with strong security mechanism that can gifted to fight against attacks.

References

[1] Athira V and Jisha G(2014): Network layer attacks and protection in MANET-A survey, International Journal on Computer science and Information Technologies, Vol5(3), pp 3437-3443.

[2] Diwaker C, Choudhary S and Dabas P (2013): Attacks on Mobile Ad-hoc Networks, International Journal of Software and Web Sciences, Vol4(1), pp 47-53.

[3] Jayaraj Singh, Arunesh Singh and Raj shree(2015): An Assessment of frequently adopted Security patterns in Mobile Ad hoc Network: Requirement and Security Management Perspective, Journal of Wireless Network and Microsystems, Vol 4, No. 1-2, pp 1-7.

[4] Navaneethan T and Lalli M (2014): Security attacks in Mobile Ad-hoc Networks- A Literature Survey, International Journal of Computer Science and Mobile Applications, vol. 2, Issue 4.,pp 1-7

[5] Punya Peethabram and Jayasudha J S,(2014): Survey of MANET Misbehaviour Detection Approaches, International Journal of Network Security & its Applications, Vol.6, No. 3, pp 19-29.

[6] Raghavendran C.H.V, G. Naga Satish and Suresh Varma P(2013): Security Challenges and Attacks in Mobile Ad hoc Network, International Journal Information Engineering and Electronic Business, Vol 3, pp 49-58.

[7] Shikha Jain, (2014): Security Threats in MANETs: A Review,International Journal on Information Theory(IJIT), Vol.3, No. 2,pp 37-50.