International Conference on Recent Innovations in Applied Science, Engineering & Technology
(IEI, Mumbai) The Institution of Engineers, Mumbai, India (AET-2018)
16th-17th June 2018 www.conferenceworld.in ISBN : 978-93-87793-30-2

A SURVEY ON SECURITY ISSUES IN MANETS

Pruthvi Patel[1], Pimal Khanpara[2] , Jitali Patel[3]

[1]*Computer Engineering Dept., Nirma University, (India)*
[2]*Computer Engineering Dept., Nirma University, (India)*
[3]*Computer Engineering Dept., Nirma University, (India)*

ABSTRACT

The characteristics of Mobile Ad-hoc Network(MANETs) such as infrastructure less,dynamic topology have found widespread applications in Military Tactical Operations,Search and Rescue Operations,Disaster Relief Operations,Law Enforcement and for Commercial use. A MANET is Vulnerable because of its characteristics such as lack of denoted centralized authority, bandwidth and battery power.

Keywords: MANET, Security, Attacks, Security Goals

I. INTRODUCTION

Mobile Ad-hoc Networks(MANETs) are perfectly suit-able for situation where setting infrastructure is either not feasible or is costly because it is infrastructure-less and also wireless. The most interesting feature of ad hoc network is that the functions of components that provide infrastructure like switches, routers, etc. are performed by nodes present in the network. MANETs have been utilized as a part of military applications for ensuring the timely flow of information and command in battle since the 1970s. [1] Due to fast and easy deployment it is also used to establish communication and provide rescue services after floods or earthquakes. MANETs are also used for on-the-fly collaborative computing outside an office environment. It is also used in communication dispatch systems for taxis to guide the route, inform about passengers pickups, personal networking like cell phones, PDAs, etc. Due to its characteristic such as open medium, mobility and dynamic topology,lack of central monitoring and management, cooperative algorithms and no clear defence mechanism, A MANET is highly vulnerable to attacks. The sender always wants to send data as quick as possible and securely to the receiver. Attackers exploit this and announce themselves to have shortest path and highest bandwidth available over the network.Limited battery of mobile nodes is also one of constrains in MANET of which attackers takes an advantage. They keep the node awake until it's exhausted and go into permanent sleep by wasting its power.

II. SECURITY ISSUES IN MANETS

MANETs are more susceptible to different security is-sues than the wired networks, Here, in this section we have described security goals and various security issues of MANETs, as shown in the Fig. 1.

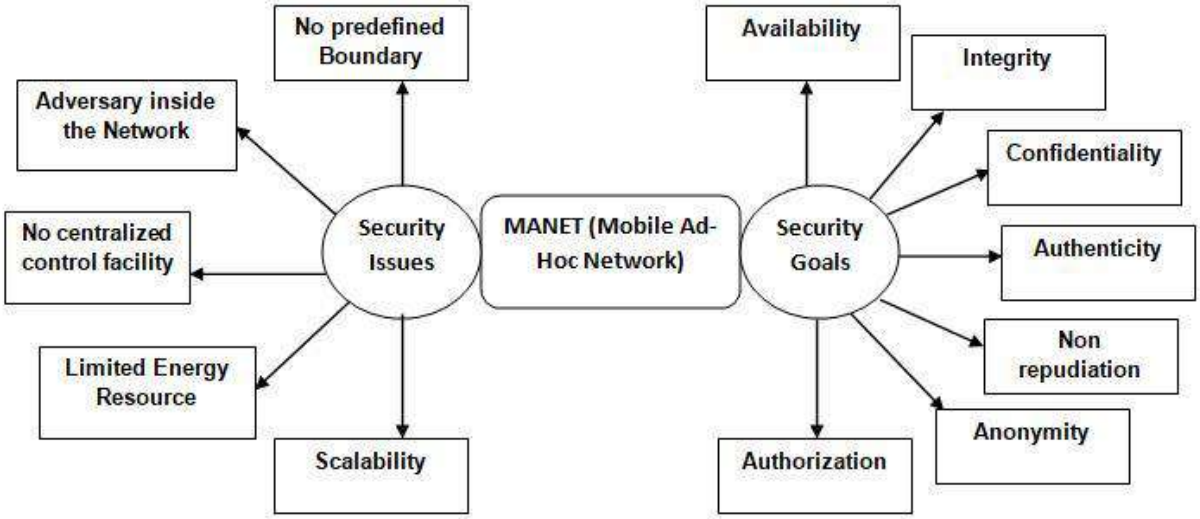

Figure 1. Security Issues and Security Goals in MANET

No predefined Boundary

In mobile as hoc networks we cannot precisely define a physical boundary of the network. Nodes in MANETs are allowed to join and leave the network at any time. As soon as an attacker comes in the range of a network it will be able to communicate with the nodes of network.

Changing scale

The scalability of the MANETs keeps changing constantly with respect of time. It is very difficult to know the number of nodes in network in future. The services and protocols of MANETs must be compatible to the scalability of network.

No centralized control facility

MANETS have not the facility of centralized control which may lead to many security problems. It becomes very difficult to detect any attack. Traffic cannot be monitored from a centralized point instead the control is distributed at every node.

Adversary inside the Network

The nodes of MANET can freely join and leave the network at any time. The nodes inside the network may also behave as an attacker.It is difficult to detect the behavior of the node is malicious or normal. Thus these type of attacks are more harmful than the external attack.

Limited Energy Resource

All the nodes in MANETs rely on battery power for their functions.The attacker can sent huge traffic to the target node. The target node may be busy in handling these packets; this will results in the battery power down.This will cause a denial of service (dos) attack because now the node will not be able to serve the network.

III. SECURITY GOALS

Availability. Availability means the network should provide the services continuously disregarding the network state.A denial of service attacks is exploits this property.

Integrity. Integrity means there should not be any kind of addition,deletion or modification to the message.This means the originality should be preserve.

Confidentiality. It assures that the message cannot be even viewed to any illegitimate person in its original form.

Authenticity. It is the method of proving the identity of an individual which ensures that the parties are not attacker and hence genuine.

Non repudiation. It is the property which states, the sender and receiver cannot deny about sending and receiving the message.

Authorization. Authorization means to assigning the different access rights to different level of users.

Anonymity. It means to all identity related information of a node should not be revealed.Privacy should be preserved.

IV. MANETs Attacks:Network Layer

There are various network layer attacks in MANET, which are explained below.

Flooding Attack

In Flooding attack, forged packets are inserted into the networks by malicious node in the network.These unnecessary flooded packets also known as ghost packets loop around into the network.The affected nodes will not be able to receive or forward any packet. These ghost packets will use network resources such as bandwidth, processing time and power along the way. That leads to the network damage [2].

Blackhole Attack.

In this attack, attacker node injects false routing information to the network nodes and announcing that it has the optimal path and hence other legitimate nodes will route the data packets over it and will discard all the packets [3].

Link Withholding Attack.

In this attack, the malicious node doesn't announce link data to specific nodes and avoid the need to announce the link of nodes and this ends up in losing the links between nodes [3].

Link Spoofing Attack.

In this attack an attacker node declare fake links with its non-neighboring nodes to damage the routing services inside the network. As shown in the figure 2, A is the attacker node and T is the Destination node. A and B are MPRs (Multi Point Relay nodes are the nodes which does the work of carry messages between the various nodes of networks) for the Destination node T Till the attack happens. During the attack, the malicious node A will declare a fake link with the two hop neighbor C of the Destination node T. Node A has a minimum distance to reach node Ts two hop neighbor C hence node T will select node A as a MPR for it. When this completes, Node A will modifies or may drop the data packets and damage the network [4].

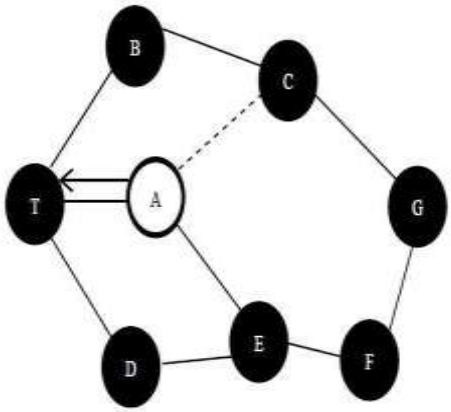

Figure 2. Link Spoofing Attack [5]

Replay Attack

Due to the MANETs mobility characteristic,Network topology frequently changes. So it is possible that current topology won't exist within the future. In a Reply attack repeatedly retransmission of the legitimate data to add network routing traffic that has been recorded earlier. This attack targets the freshness of routes. It maybe exploit to impersonate a selected node or to interrupt the routing functions of the network [6].

Colluding Misrelay Attack.

In this attack, various malicious nodes secretly works for modifying, dropping routing packets to disrupt the normal operations of a net-work.Detection is very difficult for this sort of attack. As shown in the figure 3 whenever target node T send any packets to the Malicious node 1 , it will forwards the packets to another malicious node 2 without performing any modification on it.Then the malicious node 2 will discards or modifies those packets.

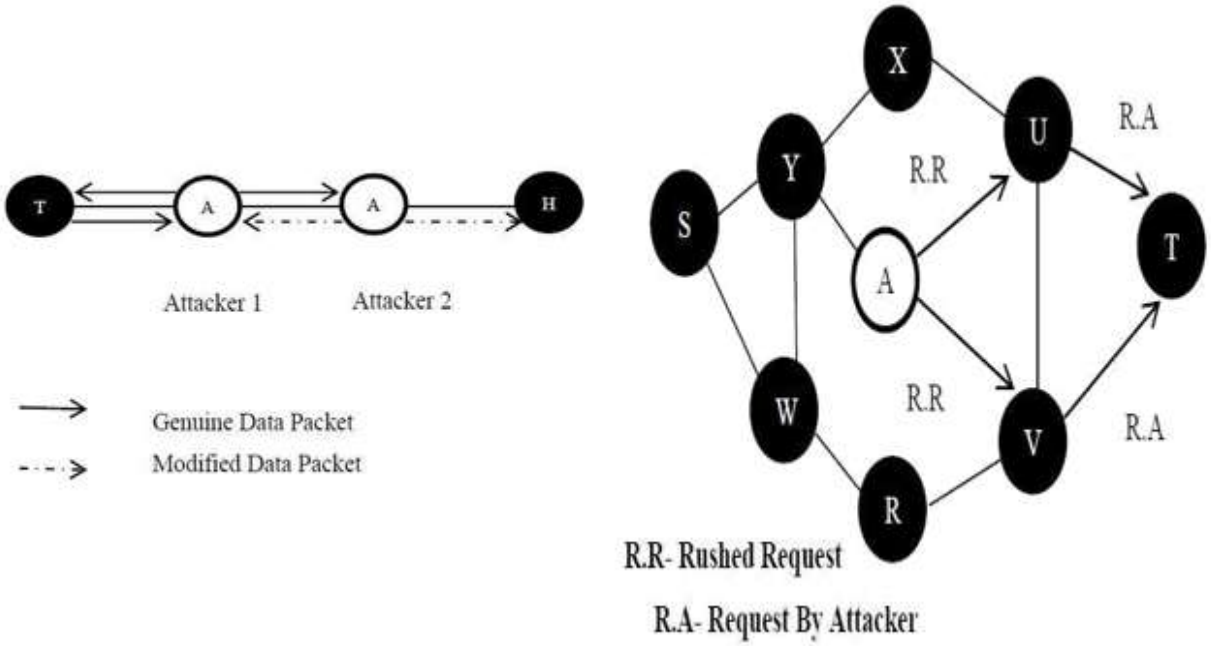

Figure 3. Rushing Attack [5]

Rushing Attack.

As shown in the figure 4 the source node (S), will initialize a route discovery request(RREQ) to send packets to the target or destination node (T).There is an attacker node(A) as shown in the figure, node A also forwards RREQ to target or destination node T, if the RREQ sent by A are the first one to reach the neighbors(U and V) of target node then the route for forwarding the packet from source S to T will be via Attacker node A. And when the original RREQ sent by the node S reaches the neighbors of the target node, they will be discarded. As a conclusion the Source node S will never be able to discover the correct route which does not include the attacker node [4].

Sinkhole Attack.

The attacker node tries to attract all nodes to it and broadcast false route in this case. In this a malicious node falsely introduces itself as the end to accept network traffic. Node tries to offer attractive link. It confuses the network by falling packets after alternation that affects the network functionalities [2].

Byzantine Attack.

This type of attack can be done by one or more intermediary nodes that are working with in network, behaving as malevolent nodes they carry out at-tacks for example creating routing loops or transfer the data packets through non-optimal path or selectively dropping the packets which result disturb the network. It degrades the routing efficiency within network. Such attacks are difficult to identify [2].

Location Disclosure.

Malicious node reveals information about the node locations or the network structure. It collect the location information of node such as a route map and then plans additional attack scenarios.Attacker try to discover the identities of nodes which is taking part in communication and analyze the traffic to learn traffic pattern of the network. The leakage of such information is harmful [5].

Wormhole Attack.

In this attack, attacker node records all the packets at one point which is malicious node and tunnels them to another attacker node and then resend all packets into the network, as shown in figure 4.

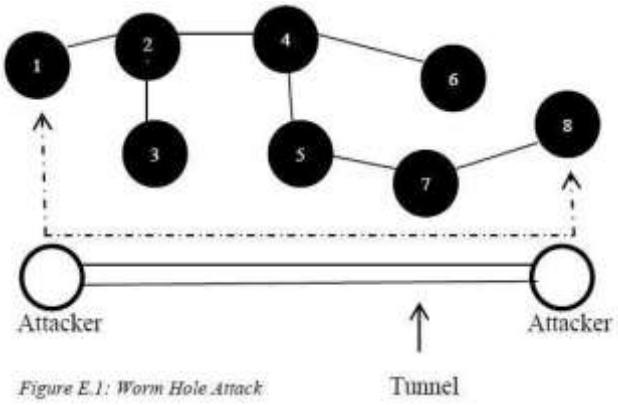

Figure – 4 Wormhole Attack

Attack	Effect
Blackhole	Discard all the packets that are routed through it because of false routing information that this is shortest path from source to destination.
Flooding Attack	Exhausts resources in the network like nodes battery power.
Gray Hole Attack	May or may not drop the data packets. At one point nodes may behave maliciously at another they may behave very much normal like other nodes in the network
Worm Hole Attack	Captures the packets at one node and replays them back into the network from the another node of the tunnel.
Rushing Attack	It will prohibits to the source node to RREQ to original target node and RREQ packets are discarded by target node.
Link Spoofing	Data Manipulation, Modification and dropping of Routing Traffic which results into Dos Attack
Colluding Misrelay Attack	Modifies and drops data packets surreptitiously

TABLE 1: Effects of Attacks

Layer	Attack	Security Issues
Physical	Jamming, Eavesdropping, Interception	Preventing Deniel of Services(DoS) and signal jamming attacks
Data link	Traffic Analysis,WEP Weakness, Monitoring, Disruption MAC(802.11),	Providing link-layer security support and Protecting the wireless MAC protocol
Network	Wormhole, Black hole, Flooding, Location Disclosures attack, Resource Consumption	Protecting the ad hoc routing and forwarding protocols
Transport	Session Hijacking, SYN Flooding	Securing and Authenticating end-to-end communications using data encryption
Application	Data Corruption, Repudiation	Identifying and inhibiting worms,viruses, application misues and malicious activity code in networks
Common attack on all layer	Replay attack, DoS attack, impersonation, man-in-middle	

TABLE 2: Different types of attack at different layer

Approach	Description	Limitations
Temporal Leashes [7]	Time stamp given for packet	All nodes require tightly Synchronized clocks
Statistical Analysis [8]	Finding the highest frequency link through analyzing relative frequency of each link appearing in obtained routes information	Works only with multipath on Demand protocols
LiteWorp [9]	Instead of one-hop, two-hop routing information is obtained by nodes; Because of this nodes know their neighbors neighbor	Works only when network is stationary
Localization [10]	Location Aware Guard Nodes (LAGNs) send hashed messages; if Wormhole is there in the network, a node detects discrepancies in the hash message	Not applicable to mobile networks

Network Visual-ization [11]	In a sensor network, each sensor senses distance of its neighbors and sends that information to cen-tralized controller from which it calculates topol-ogy; With no Wormhole, topology more or less re-mains flat	Mobility and terrains not studied for this solution
DELPHI [12]	In this method,itcal-culates the mean delay per hop for all possible routes.	will not work if the delay is because of some other reasons.
WARP [13]	Each node records the anomaly value of it's neighbour,If anamoly value is greater than threshold then it's affected by wormhole.	We need to set threshold carefully otherwise false detection will increase.
RTT-TC [14]	Two nodes suspect a wormhole tunnel between them if the RTT between them is more than 3 times of their current RTTavg. If there is a wormhole tunnel, those two nodes NodeID is inserted to their respective SUS lists	High message overhead

TABLE 3: Software/Protocol Based Approach

Approach	Description	Limitations
Geographical Leashes [7]	Ensuring that the re-ceiver must be within certain distance from the sender	Limitations of GPS technology
End-to-end Leashes [15]	Each intermediate node appends time and loca-tion information and Re-ceiver authenticates time and location information of a packet using sym-metric key	Limitations of GPS technology

Directional Antennas [16] [17]	Each pair of nodes determines the direction of received signals from neighbor; if directions match, relation is set	Not applicable to network without directional antennas
SECTOR	It uses distance bounding algorithm and calculates the distance between two neighbors by sending a one bit challenge and determines if the calculated distance is within maximum possible transmission range.	It needs specialized hardware to respond to one bit challenge

TABLE 4: Hardware/Middleware Based Approach

V. CONCLUSION

The distributed nature of MANETs and its dynamic topology makes it susceptible to various type of attacks accomplishing security a prime concern in the network. In this paper we have represented the various network layer attacks such as black hole,link spoofing attack,rushing attack, colluding misrelayattack,flooding attack,gray hole and worm hole.We have also reviewed a various existing solutions for the worm hole attack that have been previously proposed by different researchers. Main focused of this paper is on worm hole attacks where the malicious nodes breach the security and interrupt normal functionalities of the network. In addition to this the survey gives abreast information of all the works that are done in this field which is helpful to the researchers to find a rough idea of how they can carried their research in this field creating the network way more robust from these attacks.

REFERENCES

[1] A. Nadeem and M. Howarth, "A survey of manet intrusion detection and prevention approaches for network layer attacks," vol. 15, pp. 2027–2045, 03 2013.

[2] S. Kumar, M. Goyal, D. Goyal, and R. C. Poonia, "Routing protocols and security issues in manet," in 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dec 2017, pp. 818–824.

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Ja-malipour, "A survey of routing attacks in mobile ad hoc networks," IEEE Wireless Communications, vol. 14, no. 5, pp. 85–91, October 2007.

[4] R. K. Singh and P. Nand, "Literature review of routing attacks in manet," in 2016 International Conference on Computing, Communi-cation and Automation (ICCCA), April 2016, pp. 525–530.

[5] A. Vij and V. Sharma, "Security issues in mobile adhoc network: A survey paper," in 2016 International Conference on Computing, Communication and Automation (ICCCA), April 2016, pp. 561–566.

[6] G. Garg, S. Kaushal, and A. Sharma, "Comprehensive study on manets network layer attacks," in 2013 Fourth International Confer-ence on Computing, Communications and Networking Technologies (ICCCNT), July 2013, pp. 1–8.

[7] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wire-less networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370–380, Feb 2006.

[8] L. Qian, N. Song, and X. Li, "Detecting and locating wormhole at-tacks in wireless ad hoc networks through statistical analysis of multi-path," in IEEE Wireless Communications and Networking Conference, 2005, vol. 4, March 2005, pp. 2106–2111 Vol. 4.

[9] I. Khalil, S. Bagchi, and N. B. Shroff, "Liteworp: a lightweight countermeasure for the wormhole attack in multihop wireless networks," in 2005 International Conference on Dependable Systems and Networks (DSN'05), June 2005, pp. 612–621.

[10] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," in IEEE Wireless Communications and Networking Conference, 2005, vol. 2, March 2005, pp. 1193–1199 Vol. 2.

[11] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in Proceedings of the 3rd ACM Workshop on Wireless Security, ser. WiSe '04. New York, NY, USA: ACM, 2004, pp. 51– 60. [Online]. Available: http://doi.acm.org/10.1145/1023646.1023657

[12] H. S. Chiu and K.-S. Lui, "Delphi: wormhole detection mechanism for ad hoc wireless networks," p. 6 pp., 02 2006.

[13] M.-Y. Su, "Su, m.y.: Warp: A wormhole avoidance routing protocol by anomaly detection in mobile ad hoc networks. computers and security 29(2), 208-224," vol. 29, pp. 208–224, 03 2010.

[14] M. R. Alam and K. S. Chan, "Rtt-tc: A topological comparison based method to detect wormhole attacks in manet," in 2010 IEEE 12th International Conference on Communication Technology, Nov 2010, pp. 991–994.

[15] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks," Wireless Communications and Mobile Computing, vol. 6, no. 4, pp. 483–503, 2006. [Online]. Available: http://dx.doi.org/10.1002/wcm.292

[16] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks." 01 2004.

[17] L. Lazos and R. Poovendran, "Serloc: Secure range-independent localization for wireless sensor networks," in Proceedings of the 3rd ACM Workshop on Wireless Security, ser. WiSe '04. New York, NY, USA: ACM, 2004, pp. 21–30. [Online]. Available: http://doi.acm.org/10.1145/1023646.1023650