A Survey on Different Types of MANET Attacks in OSI Model

Mrs. Swetha M. S
Assistant Professor
Department of Information Science And Engineering
BMS Institute of Technology & Management, Yelahanka, Bangalore -560064, Karnataka

Dr. Thungamani M
Assistant Professor
Department of Computer Science & Engineering
COH UHS Campus GKVK BANGALORE 560065, Karnataka

Mr. Krishan Kumar
Student
Department of Information Science And Engineering
BMS Institute of Technology & Management, Yelahanka, Bangalore -560064, Karnataka

Abstract

A Mobile Ad-Hoc Network (MANET) is a compilation of mobile nodes (stations) communicating in a multi hop way without any lasting infrastructure such as access points or base stations. MANET has not well precise security method, so malevolent attacker can effortlessly access this type of network .In this paper we examine different type of attacks which happen at the diverse layer of MANET.

Keywords: Passive Attack, Security, Blackhole, MAC Layer

I. INTRODUCTION

A MANET contains movable nodes (stations) that can communicate with each other without the use of predefined infrastructure. There is no definite management for MANET. MANET is self-organized in nature so it has quickly deployable ability. MANET is very helpful to apply in dissimilar application such as battlefield communication, urgent situation relief picture etc. In MANET nodes are movable in environment, due to the mobility, topology changes with dynamism. Due to its fundamental Ad-Hoc environment, MANET attacks [1].

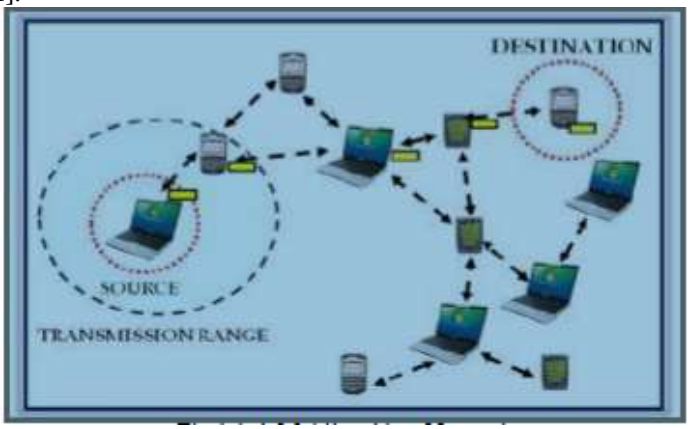

Fig. 1: MANET

II. TYPES OF SECURITY ATTACKS

A. *Passive Attacks*

In passive attack there is not any change in the message which is transmitted. There is an attacker (intermediated node) among sender & receiver which read the communication. This intermediary attacker node is also undertaking the duty of network monitoring to analyse which category of communication is going on.

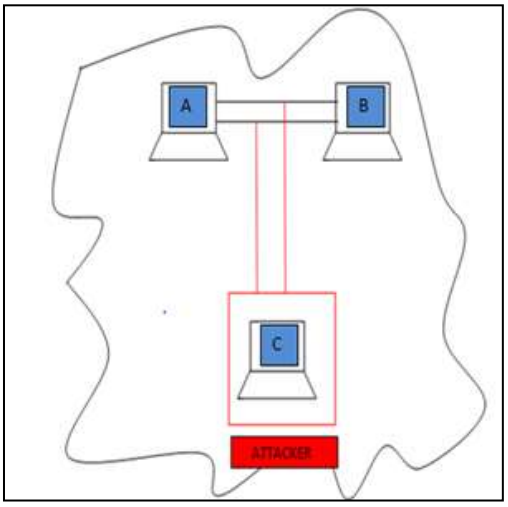

Fig. 2.1: Passive attack

B. Active Attacks

The information which is routing all the way through the nodes in MANET is distorted by an attacker node. Attacker node also streams some fake information in the network [1]. Attacker node also do the job of RREQ (re request) though it is not unsuitable node so the previous node rejecting its appeal due these RREQs the bandwidth is severe and network is stuck.

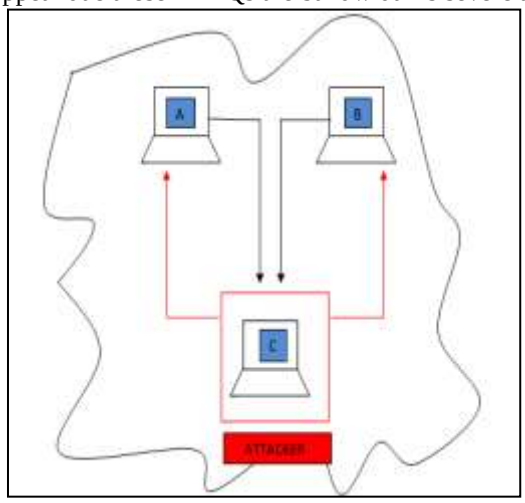

Fig. 2.2: Active attack

III. ATTACKS CORRESPONDING TO DIFFERENT LAYERS IN MANET:

Mainly there are five layers i.e. application layer, transport layer, network layer, Mac layer, & physical layer.

A. At Application Layer

Attack is done by virus, worms to contaminate the operating system or application software install in mobile devices.

B. At Transport Layer

1) TCP SYN attack (Denial of Service Attack)
TCP SYN attack is DOS in environment, so the genuine user does not get the facility of network when attack is occur. TCP SYN attack is performed to create a large number of arrest in opened TCP connection with and node.
2) TCP Session Hijacking
TCP session hijacking is done by the spoofing of IP address of a victim node after that attacker steals susceptible information which is being communicated. Thus the attacker captures the features of a prey node and continues the session with target.
3) Jelly Fish Attack
Analogous to the Blackhole attack, a jellyfish attacker opening needs to encroach into the forwarding group and then it delays data packets without cause for some amount of time prior to forwarding them. This result in considerably high end-to-end delay and hold-up jitter, and thus degrades the performance of real-time applications.

C. *Attacks at Network Layer*

1) Flooding Attack (Denial of Service Attack)

Attacker exhausts the network assets, i.e. bandwidth and also consumes a node's resources, i.e. battery power to interrupt the routing process to debase network performance. A malicious node can forward a huge no. of RREQ (re request) in petite period of time to a destination node that does not survive in the network. Because no one will rerun these RREQ so they will inundate the whole network. Due to flooding the battery power of all nodes as well as network bandwidth will be consumed and could guide to denial of service [7].

2) Route Tracking

This kind of attack is done to get receptive information which is routed through unlike transitional nodes [8].

3) Message Fabricate, Modification

In this variety of attack copied stream of messages is added into information which is communicated or some category of modify is done in information [13].

4) Blackhole Attack

In a Blackhole attack an attacker node sends bogus routing information in the network to claim that it has an best route and causes other high-quality nodes to route data packets throughout the malevolent one. For instance in an Ad-Hoc on demand distance vector routing (AODV), attacker can transmit forged RREQs including a fake target sequence number that is made-up to be equivalent or superior than the one be full of RREQ to source node, claiming that it has a enough fresh route to the end node. This causes the source node to choose the route that passes through the attacker node. So all the traffic will be routed in the course of the attacker and therefore, the attacker can abuse the information or sometime reject the traffic [8].

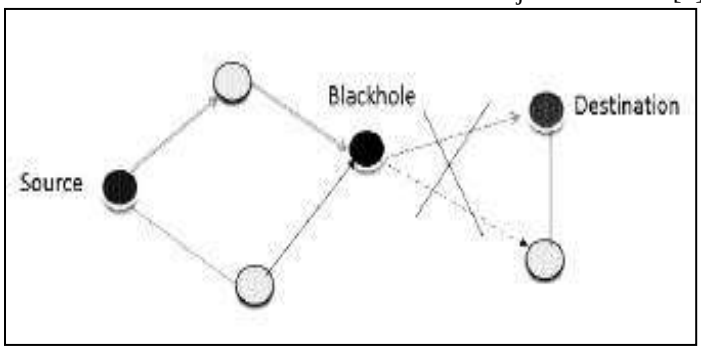

Fig. 3.3.4: BlackHole attack

5) Wormhole Attack

It is the unsafe one amongst the all attacks. In this attack, a couple of colluding attackers recodes packets at one position and replays them at an additional location using a private high speed network [5]. The significance of this attack is that it can be launched in every communication that provides validity privacy.

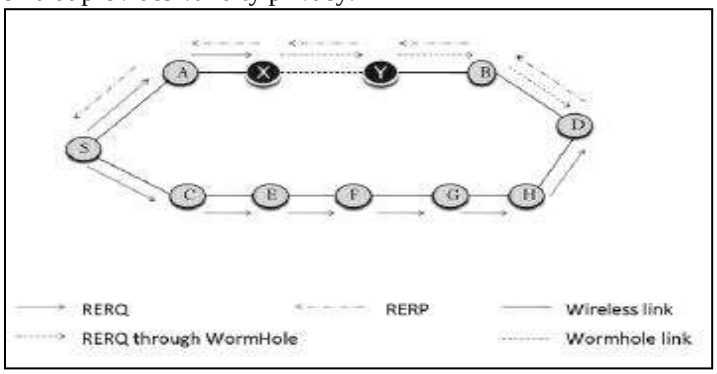

Fig. 3.3.5: Wormhole attack

6) Grayhole Attack

A variant of black hole attack is the Gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are

- Reducing all UDP packets while forwarding TCP packets
- Reducing 50% of the packets or dropping them with a probabilistic allocation. These are the attacks that seek to interrupt the network without being detected by the safety measures [8].

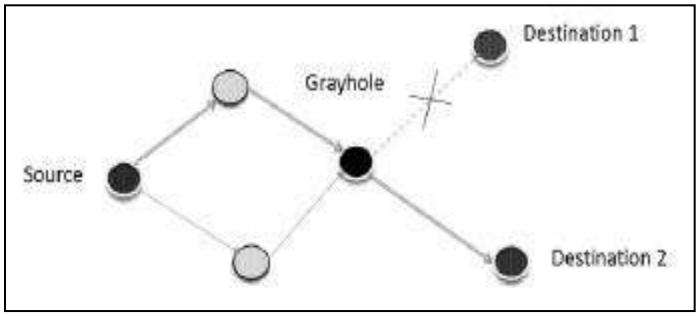

Fig. 3.3.6: Grayhole attack

7) Rushing Attack

Many demand-driven protocols such as ODMRP, MAODV, and ADMR, which use the carbon copy suppression mechanism in their operations, are susceptible to rushing attacks. When source nodes overflow the network with route finding packets in order to find routes to the destinations, each midway node processes only the first non-duplicate packet and rejects any replacement packets that arrive at a later time. Rushing attackers, by skipping a few of the routing processes, can rapidly forward these packets and be capable to gain access to the forwarding collection [4].

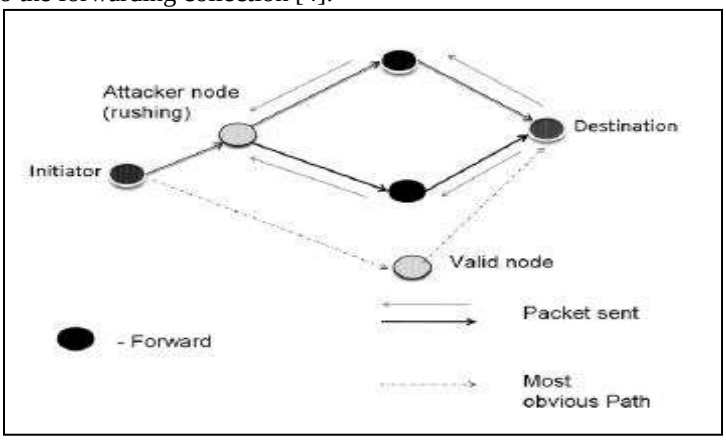

Fig. 3.3.7: Rushing attack

8) Link Spoofing Attack

In a link spoofing attack, a malevolent node advertises false links with non-neighbours to disturb routing operations. An attacker can present a false link with a target's two-hop neighbours. This causes the target node to select the malevolent node to be its multipoint spread node (MPR). As an MPR node, a malevolent node can then manoeuvre data or routing traffic, i.e. modifying or reducing the routing traffic. They can also perform various other types of DOS attacks [13].

9) Byzantine Attack

Byzantine attack can be launched by a single malevolent node or a set of nodes that work in collaboration. A compromised transitional node works without help or set of compromised intermediary nodes works in conspiracy to variety attacks. The compromised nodes can create routing loops, forwarding packets in extended route instead of best possible one, even may plunge packets. This attack degrades the routing concert and also disrupts the routing services [8].

10) Sybil Attack

A Sybil attack is a computer hacker attack on a peer-to-peer (P2P) network. It is named after the novel Sybil, which recounts the medical treatment of a woman with extreme dissociative identity disorder. The attack targets the reputation system of the P2P program and allows the hacker to have an unfair advantage in influencing the reputation and score of files stored on the P2P network. Several factors determine how bad a Sybil attack can be, such as whether all entities can equally affect the reputation system, how easy it is to make an entity, and whether the program accepts non-trusted entities and their input. Validating accounts is the best way for administrators to prevent these attacks, but this sacrifices the anonymity of users [10].

D. Attacks at MAC layer

1) MAC Denial of Service Attack (DOS)

At the MAC layer DOS can be attempted as:

There is a single channel which is used frequently, keeping the channel busy around a particular node leads to a denial of service attack at that node. An attacker node continuously sends spurious packets to a particular network node this leads to drain the battery power of the node, which further leads to a denial of service attack.

2) *Traffic Monitoring & Analysis*

Traffic analysis is a passive type of attack in nature this kind of analysis is done by attacker to find out which type of communication is going on. 4.4.3 Bandwidth Stealth In this kind of attack the attacker node illegally stealth the large fraction of bandwidth due to this congestion is happened in the network.

3) *MAC Targeted Attack*

MAC layer plays an important role in every piece of data that is exchanged through several nodes, ensuring that data is collected efficiently to its intended recipient. The MAC targeted attacks disrupt the whole MAC procedure [13].

4) *WEP Targeted Attacks*

The wired equal privacy (WEP) is designed to improve the security in wireless communication that is isolation and permission. However it is well known that WEP has number of weakness and is subject to attacks. a few of them are:-

1) WEP protocol does not indicate key organization.
2) The initialization vector (IV) is a 24 bit field which is the element of the RC4 encryption key. The recycle of IV and fault of RC4 help to create analytic attacks.
3) The mutual cure of non-cryptographic truthfulness algorithm, CRC32, with the stream cipher has a safety risk [11].

E. Attacks at Physical Layer

1) *Jamming Attack (Denial of Service Attack)*

DOS attack is also happened at physical level. Due to DOS there is denial of services accessed by a genuine network user. Example is jamming attack. Due to jamming &intrusion of radio signals messages can be misplaced or corrupt. Signals generated by a powerful transmitter are strong enough to overwhelm the target signals and can disturb communication. Pulse and random noise are most common type of signal jamming [3].

2) *Stolen or Compromised Attack*

These kinds of attacks are happened from a compromised entities or stolen mechanism like physical capturing of a node in MANET.

3) *Malicious Message Injecting*

Attacker inject bogus streams into the real message streams which is routing throughout the transitional nods, due to malevolent message injecting the functionality of network is disrupted by the attacker.

4) *Eavesdropping Attack*

Eavesdropping is the understanding of messages and exchange by unintended receivers. The nodes in MANET contribute to a wireless standard and the wireless communication use RF spectrum and transmit by nature which can simply intercepted with receivers tuned to appropriate frequency. As a result transmitted messages can be overheard as well as false messages can be injected into the network [3].

IV. CONCLUSIONS

In this paper, we try to examine the security attacks at diverse layers of MANET, which produces lots of difficulty in the MANET operations. Due to the vibrant environment of MANET it is more prone to such class of attacks. In MANET the solutions are considered equivalent to specific attacks they work well in the existence of these attacks but they fail under unlike attack scenario.

REFERENCES

[1] Mrs. Swetha M S, Dr.Thungamani M, "Enhanced Anonymity in Hierarchical Routing Protocol for MANETs". International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC) at Priyadarshini Engineering College, Chettiyappanur, Vaniyambadi - 635751, Vellore District, Tamil Nadu, India .978-1-5386-4304-4/18/$31.00 ©2018 IEEE
[2] Sharma, R., Shrivastava, R. 2014. Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network.IJCSNS International Journal of Computer Science and Network Security
[3] Swetha M.S, Dr. Thungamani M, Pooja Reddy, Richa Singh, "A Survey on Privacy-Preserving and Authenticated Routing in Mistrustful Mobile Ad-Hoc Networks." In the proceedings of International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 4, April 2016
[4] Swetha M S, Chandana B N, Deepika M," A Survey on Homomorphic Data Concealment and Reliability in Multi Cloud Computing". In the proceedings of International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 2, February 2017.
[5] Boora, S. et. al (2011). A Survey on Security Issues in Mobile Ad-Hoc Networks, International Journal of Computer Science & Management Studies, Vol. 11, Issue.
[6] Kayalvizhi, K., Senthilkumar, N., Arul Kumaran, G. 2014. Detecting Sybil Attack by Using Received Signal Strength in Manets. International Journal of Innovative Research in Science & Engineering.
[7] Jenniefer, A. and Jose, J. 2014. Techniques for Identifying Denial of Service Attack in Wireless Sensor Network: a Survey. International Journal of Advanced Research in Computer and Communication Engineering, ISSN: 2319-5940, Vol. 3.
[8] Swetha M Dr.Thungamani M,Ankita Mishra, "Enhancement of Performance Analysis in Anonymity MANET through Trust-Aware Routing Protocol." In the proceedings of International Journal of Advance Research in Computer Science and Management Studies,Volume 5, Issue 5, May 2017
[9] Kumar, J., Kulkarni, M., Gupta, D. 2013. Effect of Black Hole Attack on MANET Routing Protocols, I. J. Computer Network and Information Security.
[10] Khemariya, N., Khuntetha, A. 2013. An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs. International Journal of Computer Applications (0975 – 8887).
[11] Mr. Muneshwara M.S, Mrs. Swetha M.S, Dr. Thungamani M and Dr. Anil G.N, Digital Genomics to Build a Smart Franchise in Real Time Applications. In proceedings of 2017 International Conference on circuits Power and Computing Technologies [ICCPCT]

[12] Boora, S. et. al (2011). A Survey on Security Issues in Mobile Ad-Hoc Networks, International Journal of Computer Science & Management Studies, Vol. 11, Issue
[13] Wazid, M. et. al (2011). A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques, International Conference on Computer Communication and Networks CSI-COMNET.
[14] Pandey, A. et. al (2010). A Survey on Wireless Sensor Networks Security, International Journal of Computer Applications, Vol. 3, No. 2.
[15] Rai, P. et. al (2010). A Review of MANETs Security Aspects and Challenges, IJCA Special Issue on "Mobile Ad-hoc Networks"
[16] Mamatha, G. S. et. al (2010). Network Layer Attacks and Defense Mechanisms in MANETS- A Survey, International Journal of Computer Applications, Vol. 9, No. 9.
[17] Khokhar, R. et. al (2008). A review of current routing attacks in Mobile Ad-Hoc Networks, International Journal of Computer Science & Security, Vol. 2, Issue 3.
[18] Gua, Y. (2008). a dissertation on Defending MANET against flooding attacks by detective measures, Institute of Telecommunication Research, The University of South Australia
[19] Biswas, K. et. al (2007). Security threats in Mobile Adhoc Network, Master theses, Department of Interaction & System Design, Blekinge Institute of Technology, Sweden.