INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY ISSN: 2456-6683 Volume - 4, Issue - 1, Jan – 2020
Monthly, Peer-Reviewed, Refereed, Indexed Journal Scientific Journal Impact Factor: 5.245
Received on : 30/12/2019 Accepted on : 10/01/2020 Publication Date: 31/01/2020

Passive Attacks in Mobile Ad-Hoc Networks

[1]Nidhi Malik, [2]Dr. R.B. Singh

[1]Researchscholar, [2]Professor,
[1]Department of Computer Science, [2] Department of Mathematics,
Monad University, N.H.9, Delhi Hapur Road, Kastla Kasmabad, Hapur, U.P., India
Email - nidhijaatt@gmail.com

Abstract: *This paper presents the impact of different types of passive attacks on mesh-based multicast in mobile ad hoc networks (MANETs). As per OSI model layers, the most common attacks are network layer, namely wormhole attack, black hole attack, byzantine attack, flooding attack, resource consumption attack and location disclosure attack. It is necessary to study how the number of attackers and their positions impinged the performance metrics of a multicast session such as packet delivery ratio, throughput, end-to-end delay, and delay jitter. I also examined attacker's success rates of invading into the routing mesh when the number of attackers and their positions vary. The results enable us to suggest measures to minimize the impacts of the above types of attacks on multicast in MANETs.*

Key Words: *encryption, packet collision, vulnerable, self-reticent, degradation, mitigation period.*

1. INTRODUCTION:

Mobile ad-hoc networks are collections of mobile nodes dynamically establishing short-lived networks in absence of fixed infrastructure. Each mobile node is equipped with a wireless transmitter and a receiver with an appropriate antenna. These mobile nodes are connected by wireless links and work as routers for all other mobile nodes. Nodes in mobile ad-hoc networks are free to move and organise themselves in an arbitrary fashion. These capable of MANETs enable to be deployed in disaster zones and all inaccessible hostile terraing very practical and easy to deploy in places where existing infrastructure is not capable enough to allow communication, just far instance , in disaster zones, or infeasible to deploy locations.

MANETs are the short term temporary spontaneously wireless networks of mobile nodes communicating with each other without the intervention of any fixed infrastructure or central control. Usually, it is an autonomous system of mobile nodes, mobile terminals, or mobile stations serving as routers interconnected by wireless links. Depending upon the locations, antenna coverage patterns, transmission power levels, and co-channel interference levels, a wireless connectivity exists among participating mobile nodes at a given time, either in the form of random multihop transmissions or ad-hoc network. Network communications and management tasks are usually performed in a distributed manner. Since the nodes move or adjust their transmission and reception parameters, MANET topology may vary from time to time.

An ad-hoc mobile wireless network is a network without any base stations, an infrastructure less network. Below fig:1 depicts the formation and working operation of a MANET. Data packets are transmitted in a "Store-and-Forward" method from the source node to the destination node in "Peer-to-Peer" multihop intermediate nodes acting as routers. The network may either operate as stand alone or as an extension of an infrastructure network with the help of few selected routers.

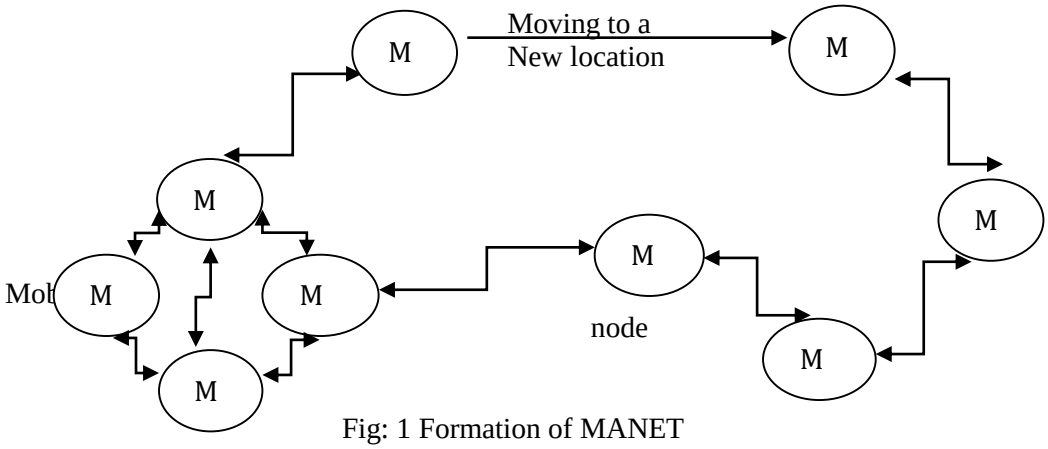


Fig: 1 Formation of MANET

2. SECURITY REQUIREMENTS:

a) Confidentiality

Confidentiality is the most important aspect of information security .We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentially of its information .Confidentiality not only applies to the storage of information, it also applies to the transmission of information. When we transmit a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer, we need a conceal it during transmission.

b) Authentication

The authentication services are concerned with assuring that a communication is authentic. In case of a single message, such as a warning or alarm single, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the services assure that the two entities are authentic (that is, that each is the entity that it claims to be). Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission. Two specific authentication services are:

i. **Peer Entity Authentication:** Used in association with a logical connection to provide confidence in the identity of the entities connected.

ii. **Data – Origin Authentication:** In a connectionless transfer, if provides assurance that the source of received data is as claimed.

c) Availability

The third component of information security is availability .The information created and stored by an organization needs to be available to authorized entities .Information is useless, if it is not available in time . Information needs to be constantly changed, which means it must be accessible to authorized entities. The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity. Imagine what would happen to a bank if the customers could not access their accounts for transactions.

d) Integrity

Information needs to be changed continuously or as on requirement basis .In a bank when a customer deposits or withdraws money, the balance of his/her account needs to be changed . Integrity means that changes need to be done only by authorized entities and through authorized mechanisms. Integrity violation is may be due to the result of a malicious act; or an interruption in the system, such as a power surge, may also create unwanted changes in some information.

e) Non-repudiation

This refers to the provisions that guarantee that none of the parties involved can deny operations at a later date. The parties to the networked systems may use digital signatures and encryption to ensure non-repudiation and establish accountability of the transacting parties.

3. SECURITY CHALLENGES:

a) Dynamic topology-

In this, nodes are free to move in an arbitrary manner according to the user requirement and thus resulting in the dynamic network topology. The incorrect topology information considerably increase the end-to-end-delay, routing control overhead, increases the possibility of failure of nodes, and reduces the capacity . Hence, network topology management plays a vital role in maintaining dynamic configuration of the network and the performance of a routing protocol in MANETs.

b) Unpredictable Link Properties-

Signal propagation in wireless media is quite unpredictable due to problems that are caused by signal fading, interference and multipath cancellation. In addition, “Packet Collision” is intrinsic to wireless network.

c) Limited Bandwidth-

Using, wireless networks are constrained by availability of bandwidth.

i. **Limited Power** –Mobile devices and nodes are basically battery operated .This demands the use of extremely low-power components in the devices. The limited availability of battery power adversely affect transceiver input / output power, and CPU/signal processing.

ii. **Limited Security** –The Physical wireless medium of communication is inherently insecure and quite vulnerable to attack /interception. Without adequate security, unauthorised access and usage of ad-hoc networks violate QoS and networks performance.

d) OSI Model

The OSI reference model is a conceptual model composed of seven layers, each specifies particular network functions. It is now considered the primary architectural model for inter computer communication. The OSI model divides the task involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of task is then assigned to each of the seven OSI layers. Each layer is reasonably self reticent to enable it to execute / carry out assigned tasks independently. This permit / allows the solutions offered by one layer to be updated without adversely affecting the other layers. The OSI model defines internet working in term of vertical stacks of seven layers. The upper layers of the OSI model represent software that implements network services like encryption and connection management. The lower layer of the OSI model implement more primitive, hardware oriented functions like routing and addressing. The following list details the seven layers of the open system interconnection (OSI) reference model:-

Layers of OSI model

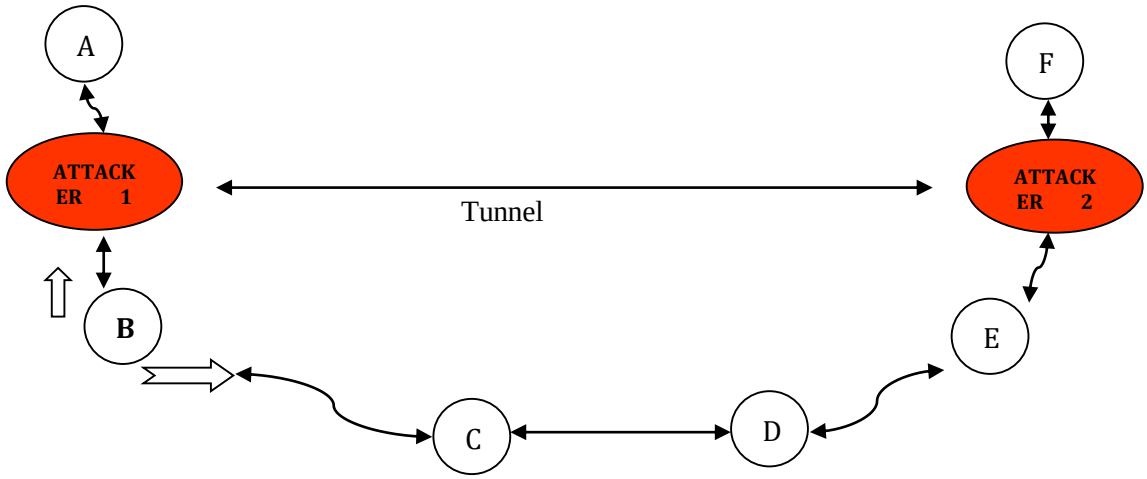
Layer 1 – Application
Layer 2 – Presentation
Layer 3 – Session
Layer 4 – Transport
Layer 5 – Network
Layer 6 – Data Link
Layer 7 – Physical

In the network design OSI model out of seven layers, I explain network layer (layer 5) attacks.

4. NETWORK LAYER ATTACKS:

a) Worm hole attack

In worm hole attack, Attacker receiver packets at one location in the network and tunnels them to another location in the network, where the packets are resent into the network. It is a tunnel between two colliding attackers and this tunnels which is made between the nodes are known as Wormhole attacks. It affects in delay in packet delivery and failure to find valid routers. A Simple example is shown in below fig.



b) Black hole attack

A black hole attack is another attack possible in MANET, it is defined for on-demand routing protocol. The aim of this attack is malicious node falsely advertises good paths to the destination node during the path – finding processes. Due to this claiming it attracts all the packets and absorbed them without forwarding to destination node. Once it entered in the network, it drops forwarding data packet by making a black hole there. This node is called black hole node or black node. In black hole attack it first responds to route request discovery instead first checking its routing table. It increases the congestion and traffic in the network, and therefore attacker can misuse the traffic.

c) Byzantine attack

Compromised node /nodes works in collusion and carries out attacks such as creating routing loops ,packets on non-optimal paths, and selectively dropping packets, which results in disruption or degradation of the routing services.

d) Flooding attack

Attackers exhaust the networks resources i.e. . Bandwidth and also consume a node's resource, i.e. battery power to disrupt the routing operation to degrade network performance.

e) Resource consumption

Resource consumption attack is malicious node tries to consume / waste away resources of other nodes .It is the one of DOS attack, in which attacker exploits the route discovery process when the source node send the RREQ packet ,then attacker nod kept this packet with a different ID,in order to modify the processing ID of each node continuously and consume its limited energy of resource , memory and bandwidth . The main purpose of RCA is to consume the energy of legitimate nodes and to find the available link throughout.

f) Location disclosure attack

Attacker leak confidential information regarding the location of nodes or the structure of the network to unauthorized .It gathers the node location information, such as a route map, and then plans further attack scenarios. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern the traffic pattern.

5. CONCLUSION:

The gravest problem with computer security is that one cannot create a fully secure system. There are some issues about network and computer security which change over time, sometimes very rapidly over a very short period of time. We have tried to categorize the different types of ad hoc security attacks solely based on their characteristics to considerably reduce the mitigation period. By bringing the attacks under these two broad categories the complexity of naming also reduces. We have also kept a close look on the existing algorithms needed to mitigate the attacks and have tried to bind the attacks into categories according to that. Some attacks have characteristics, which make them unsuitable to be categorized into these categories, so they have been kept away from this topic of discussion for the time being. Further study is in progress to find out more common characteristics of the attacks to bind them more strongly into these categories and to ably design more powerful algorithm in mitigating DATA and CONTROL traffic attacks.

REFERENCES:

Books:

1. Schwartz, Mischa. (2009). Mobile Wireless Communication. Cambridge University Press. New Delhi. P. 307-308.
2. Dhunna, Mukesh and Verma, Deepak. (2009) Computer networks and Internet. Vayu Education of India. New Delhi. P. 169-170.
3. Kohar, Kuldeep Singh. (2009). Network Security. Vayu Education of India. New Delhi. P. 02-03.
4. Sharma, Sanjay. (2011) Data Communication Networks. 5th Edition. S.K. Kataria & Sons. New Delhi. P. 35-37.
5. Forouzan, Behrouz A. (2013) Data Communication and Networking. 5th Edition. Tata Mc Graw Hill Education Pvt. Ltd. New Delhi. P. 1078-1080.
6. Schiller, Jochen. (2013) Mobile Communication. 2nd Edition. Pearson. New Delhi. P. 330-332.
7. Rappaport, Theodore S. (2014). Wireless Communication. 12th Edition. Pearson. New Delhi. P. 493.
8. Forouzan, Behrouz A. and Mosharraf, Firouz. (2014) Computer Networks: A Top-Down Approach. Tata Mc Graw Hill Education Pvt. Ltd. New Delhi. P. 732-734.
9. Sharma, Sanjay. (2015) Mobile and Wireless Communication. 4th rep. Edition. S.K. Kataria & Sons. New Delhi. P. 325-326.
10. Stallings, William. (2015) Cryptography and Network Security. 6th Edition. Pearson. New Delhi. P. 529-530.