ANALYSIS OF VARIOUS SECURITY ATTACKS IN MOBILE ADHOC NETWORK

Aditi[1], Joy Karan Singh[2]

[1]*M.tech Student, Dept. of CSE,CT Institute of Technology & Research , Jalandhar,India*
[2]*Assistant Professor , Dept. of ECE,CT Institute of Technology & Research , Jalandhar,India*

ABSTRACT-*Security is a challenging issue in mobile ad-hoc network (MANET) due to its open nature, infrastructure less property and mobility of nodes. In modeling a new security mechanism for mobile ad hoc networks, one thing must consider the attacks contrast as well as the characteristics of the attacks that could be launched against the ad hoc networks and existing detection and mitigation schemes. A mobile ad hoc network (MANET) is basically a kind of network that contains autonomously nodes that can order themselves in different ways and run without any network administration. In lack of any infrastructure for security and continual changing topology of the network ensure the routing protocols vulnerable to variety of attacks. These attacks may seed either misdirection of data traffic or denial of services. This paper classifies several common attacks opposed to the ad hoc networks routing protocols based upon the procedure that could be used by attackers to take benefit from routing messages. In this paper, we investigate various attacks which can be implemented on various layers of MANETs.*

Keywords:- MANET, Security, Attack**,** Mobile, Wired

1. INTRODUCTION

MANET is a mobile Adhoc network. Nodes are casually connected with each other and creating arbitrary topology. The nodes can act as both routers and hosts. They have potential to self-configure makes this technology fit for provisioning communication. Nodes of an ad hoc network based on one another in onward transmission of a packet to its destination, due to the finite range of each single mobile host's wireless transmissions. Security in MANET is an expected component for necessary network intentions like packet forwarding and routing: network operation can be easily put in hazard if countermeasures are not interpolated into basic network functions at the primary state of their design. Unlike networks using devoted nodes to boost basic functions like packet routing, forwarding and network management, in ad hoc networks those functions are drawn up by all available nodes. This diversity is at centre of the security problems that are absolute to ad hoc networks. As opposed to devoted nodes of a ordinary network, the nodes of an ad hoc network cannot be depending for the accurate execution of serious network functions. However, analogous to other networks, MANET also vulnerable to many security attacks. MANET not only derives all the security threats jag in both wired and wireless networks, but it also familiarized security attacks unique to itself [1]. As people will be promoted to use a secured network, it is important to provide MANET with credible security mechanisms if we wish to see this exciting technology become widely applied in a next few years. Before the improvement of any security measure to secure mobile ad hoc networks, it is necessary to study the variety of attacks that might be concerned to such networks. The features of MANETs like: nodes mobility, varying topology, provides large number of degree of independence and self-organizing capability of that make it exactly different from other network. Due to the MANETs characteristics, to design and development of secure routing is daring task for researcher. The various attacks which can be featured on MANET is a major security flaw in MANET and is the reason of discussion in this paper[1][2][23].

2. CLASSIFICATION OF ATTACKS

Attacks are classified into different categories which are explained below.

2.1 Mobile vs. wired attackers

Mobile attackers have the same abilities as that of the another nodes of any particular ad hoc network. Having the same resource vanishing point, their abilities to damage the networks operations gets also finite. For instance, with the finite transmitting abilities and battery powers, mobile attackers could only hinder the wireless links within its vicinage. They are not capable to promote the network jamming attacks to upset the whole networks operations. On the other hand, wired attackers is a kind of attackers that are fit for gaining access to the outsider resources such as the electricity. Since the attackers have more resources, they could promote more severe attacks in the networks, such as jamming the whole networks or breaking precious cryptography algorithms [23]. Presence of the wired

attackers in the ad hoc networks (mainly in the environmental network) is consistently feasible as long as the wired attackers are able to establish themselves in the communication range and have approach to the wired infrastructures.

2.2 Passive vs. active attacks

A passive attack observes unencrypted traffic and looks for clear-text passwords and delicate information that can be used in variant types of attacks. Passive attacks include traffic investigation, consideration of insecure communications, decrypting weakly encrypted traffic, and record authentication information like passwords[1][2]. Passive interception of network operations enables rivals to see upcoming actions. Passive attacks build in the disclosure of information or data files to an attacker without the approval or grasp of the user. In an active attack, the attacker attempts to bypass or fragment into secured systems. This can be completed along the stealth, viruses, worms, or Trojan horses. Active attacks involve attempts to circumvent or smash protection features, to launch malicious code, and to thieve or alter the information [3].

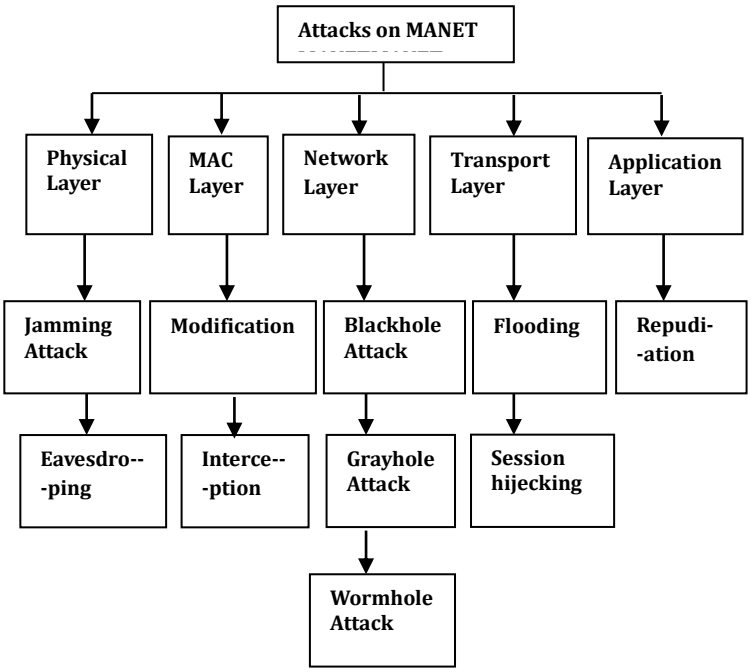

Figure 1: Classification of attacks according to layers

2.2 Inside vs. outside attacks

Insider attack is a kind of attack, in which an attacker compromised or detects a node, thus gaining authority for the encryption and authentication keys. The main method of detecting and reducing insider attacks is to scan the packet forwarding behavior between the nodes. In an outsider attack, attackers are assumed to have no awareness about the keys that are used to authenticate and encrypt. To prevent outside attackers from interfering with the data is polished by simply employing encryption and authentication methods [2].

3. DIFFERENT KINDS OF LAYERED ATTACKS

There are various types of attacks which can crumple the security of MANET. These attacks can be executed on different layers of the network. Some attacks can be executed on any of the layer of MANET and another's are for a specific layer. The layer-wise distribution of the attacks is mentioned in the Figure 1 below:

3.1 Jamming attack

A jammer is an operation whose main aim is to trying to get in the manner with the physical transmission and received wireless communications. A jammer continually emits RF signals to top up a wireless channel so that valid traffic will be fully blocked. The usual attributes for all the jamming attacks are that their communications are not manageable with MAC protocols [2]. The ratio of packets that are efficiently sent out by a valid traffic source contrast to the number of packets it plans to send out at the MAC layer. In jamming attack number of source are founded instead of single source which forward rough packets to the communication channels and jammed the channel. Due to this jamming, packet loss starts in the network. This reduces the regulation and reliability of the system. Due to this attack many difficulties are arise like channel becomes busy, transmission delay, new packet drops begin caused by full buffer space etc.

3.2 Eavesdropping

It is a kind of passive attack. The node simply detects the confidential information. The malicious node later used this information. The confidential information like location, public key, private key, password etc. can be collect by eavesdropper. The term eavesdrops means overhearing without expending any expending any extra endeavour. In this cut off and reading and conversation of message by unplanned receiver take place. In mobile ad-hoc network the mobile host shares a wireless medium[23]. Most of wireless communication use RF spectrum and broadcast by nature. Message transmitted can be eavesdropped and forgery message can be inserted into network.

3.3 Modification

In a message modification attack, rivals make some alteration to the routing messages, and thus imperil the nobility of the packets in the networks. Since the nodes are free to move and self-organize in the ad hoc networks, relationships between nodes at some times might involve the

malicious nodes[23]. These malicious nodes might utilize the sporadic relationships in the network to involve in the packet forwarding process, and later introduce the message modification attacks.

3.4 Interception

Attackers might introduce the interception attacks to get an unofficial access to the routing messages that are not deliberately sent to them[24]. This type of attack jeopardizes the probity of the packets because such packets might be refined before being delivered to the next hop. Besides, the interdict packets might also be examined before passed to the destination thus infringes the confidentiality.

3.5 Black hole attack

In "Black Hole Attack" a malicious node utilize the vulnerabilities of route discovery strategy of a reactive routing protocol. The malicious node as a transitional node on receipt of a RREQ message forward a RREP with the destination sequence number larger than is in the RREQ message specifying that it has a new route to the destination. This RREP from harmful node will reach origin node before the reply dispatch by destination/legitimate intermediate node. The source node will thus choose the route which goes through malicious node. By restating this for RREQs received from other sources[24]. The malicious node catches several routes enchanting the data traffic from all sources towards it thus producing a black hole in the network. The harmful/malicious node can then discard the traffic.

3.6 Gray hole attack

In this type of attack the attacker misguide the network by agreeing to send the packets in the network. As soon as it collect the packets from the neighbouring node, the attacker fall the packets. This is a kind of active attack. In the starting the attacker nodes treats normally and reply true RREP messages to the nodes that started RREQ messages. When it collects the packets it starts falling the packets and produce Denial of Service (DoS) attack. The dangerous behaviour of gray hole attack is different in many ways. It drops packets while sending them in the network. In some other gray hole attacks the attacker node acts maliciously for some moment until the packets are dropped and then shift to their normal behaviour[23]. Due to this behaviour it's very tough for the network to find out such kind of attack. Gray hole attack is also known as node misbehaving attack.

3.7 Wormhole attack

In this kind of attack, two remote region malicious nodes attached using high speed link. So, those two malicious nodes look to be neighbours. Whenever attacker collects a packet, he tunnels it into another malicious node in the network with the help high speed link. But users think like they getting the shortest path. It is also known as Tunnelling attack[24]. In this source node sends RREQ packets to all of the nodes, whenever malicious node X accepts RREQ packet it instantly forward that packet to another malicious node Y. So, a user believes this as a shortest path.

3.8 Flooding

Adversaries also might interrupt the normal operations in the packet forwarding procedure by flooding the aimed destination nodes with huge unnecessary packets. Nodes under the flooding attacks are unable to collect or forward any packet thus all the packets directed to them will be discarded from network [23] .

3.9 Session hijacking

Session hijacking takes benefit of the fact that most of communications are defends (by giving credentials) at session start-up, but not afterwards. In the TCP session catching attack, the attacker acquiring the victim's IP address, regulates the right sequence number that is look for by the target node, and then execute a Denial of service attack on the victim. That's why the attacker take place of the sufferer (victim) node and continues the session with the target[23].

3.10 Repudiation

On the network layer, firewalls can be established to filter the packet coming in and going out from the network. On the transport layer, whole connections can be fed to the port. But these results do not answer the problem of authentication or non-repudiation absolutely. Repudiation is a denial of involvement in all or part of the transmission processes. For example, a egoistic person could deny supervising an operation on a credit card purchase, or deny any on-line bank transaction, which is the archetypical repudiation attack on a commercial system[24].

4. CONCLUSION

Security is an important service for wired and wireless network communications. The characteristics of MANET cause both challenges and occasions in acquiring the security goals, such as confidentiality, integrity, authentication, availability, non-repudiation, and access control. As described above there are many types of attacks which can be entertained on various layers and crumple the security of MANET. We know that each network device load and forward network packets if convenient space is present in the device buffer otherwise packet is discarded. In our study, we categories a variety of attacks associated to different layers. This separation of attacks on the basis of different layers makes simple to recognize a variety of security attacks in ad hoc networks.

REFERENCES

[1] Yi S., and Kravets R., "Key Management for Heterogeneous Ad Hoc Wireless Networks" , 10th IEEE International Conference on Network Protocols (ICNP'02) 1092-1648,2002 .

[2] Karthikeyan U., and Rajni ,"Security Issues Pertaining to Ad-Hoc Networks", 2004.

[3] Kyasanur P., "Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing, 2005.

[4] Hoebeke J., Moerman I., Dhoedt B., and Demeester P., "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", IJSER, *2005*

[5] Wu B., Chen J., Wu J., and Cardei M., "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" ,Springer ,2007.

[6] Chee V., and Yau W., "Security analysis of TORA routing protocol," Computational Science and Its Applications–ICCSA. Springer Berlin Heidelberg, pp. 975-986 , 2007.

[7] Tang C., and Oilver D., "An Efficient Mobile Authentication Scheme for Wireless Networks",IEEE, 2008.

[8] Hamieh A., and Othman J., "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution", IEEE, 2009.

[9] Lazos L., Liu S., and Krunz M., "Mitigating Control-Channel Jamming Attacks in Multi-channel Ad Hoc Networks" ACM, WiSec'09, March 16–18,Zurich, Switzerland, 2009.

[10] Dempsey T., Sahin G., and Morton Y., "Passive and Active Analysis in DSR-Based Ad Hoc Networks," Ad Hoc Networks. Springer Berlin Heidelberg , pp. 623-638 , 2010.

[11] Chen T., and Kuan W., "A Robust Mutual Authentication Protocol for Wireless Sensor Networks" ETRI Journal, Volume 32, Number 5, October 2010.

[12] Cicho J., Kapelko R., Lemiesz J., and Zawada M., "On Alarm Protocol in Wireless Sensor Networks",IEEE, 2010.

[13] Şen S., Clark J., and Tapiador j., "Security Threats in Mobile Ad Hoc Networks", IEEE, 2010.

[14] Defrawy K., and Tsudik G., "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE, Vol. 10, No. 9, September 2011.

[15] Donggang L., Raymer J., and Fox A., "Efficient and timely jamming detection in wireless sensor networks." Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on. IEEE, 2012.

[16] Rana S., and Kapil A., "Security-Aware Efficient Route Discovery for DSR in MANET," Information and Communication Technologies. Springer Berlin Heidelberg, pp.186-194, 2010.

[17] Joshi P., "Security issues in routing protocols in MANETs at network layer," Procedia Computer Science , pp. 954-960, 2011.

[18] Agrawal S., Jain S., and Sharma S., "A survey of routing attacks and security measures in mobile ad-hoc networks," pp.41-48, 2011.

[19] Sharma N., and Sharma A., "The Black-hole node attack in MANET,"Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on. IEEE, pp. 546-550, 2012.

[20] Rajakumar P., Prasanna T., and Pitchaikkannu A. "Security attacks and detection schemes in MANET," Electronics and Communication Systems (ICECS), 2014 International Conference on. IEEE, 2014.

[21] Davda, Maulik H., and Sheikh R. Javid. "A Review Paper on the Study of Attacks in MANET with Its Detection & Mitigation Schemes." International Journal 2, no. 4 (2014).

[22] Saini, S., & Kumar, R. (2013). Comparison of layerwise attacks in MANETs.2013.

[23] Kapur R., and Khatri S., "Analysis of attacks on routing protocols in MANETs," Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in. IEEE, pp. 791-798, 2015.

[24] Khan M., Jadoon Q., and Khan M., "A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks," Mobile and Wireless Technology 2015. Springer Berlin Heidelberg, pp.137-145, 2015.