International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 12 Issue 2 –JANUARY 2015.

An Analysis of Defense Challenges and Attacks in Mobile Ad-hoc Networks

[*1]N.Geetha, [#2]Dr. P. Sivakumar and [*3]D.Bavya

[*]*P.G. Student, Dept of Computer Science and Engg, MIT, Pondicherry University, Puducherry*

[#]*Professor and HOD, Dept of IT, MIT, Pondicherry University, Puducherry*

[1]geethakodis12@gmail.com

[2]mvitithod@gmail.com

[3]d.bavya91@gmail.com

***Abstract*— A MANET is an infrastructure-less type of networks medium, which consists of numerous numbers of mobile nodes in the communication process and get interface with other mobile nodes present in the range. The nodes are present dynamically and establish connection paths with one another in the wireless network. The environment and configuration of such wireless networks makes it striking to different types of attackers. Defence from the attackers or attacks are a most important concern for protected message transmission between mobile nodes. MANET has no obvious procession of defence, so, it is reachable to both justifiable network users and malicious attackers. The presence of malicious or clone nodes in the network is one of the major dispute in MANET is to propose the robust security clarification that can defend MANET from various routing attacks or attackers intrusion. MANET can control in seclusion or in organization with a wired infrastructure networks, frequently through an opportunity node contributing in both networks for transfer or communication relay. This give, beside with their self-organizing facilities, is some of MANET's biggest potencies, as well as their biggest defence weaknesses.**

Keywords-MANET, mobile-node, malicious-attacker, gateway.

I. INTRODUCTION

A MANET [5] is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. Nodes in MANETs can join and leave the network dynamically [1]. There is no fixed set of infrastructure and centralized administration in this type of networks. Nodes are interconnected through wireless interface. The dynamic nature of such type networks makes it highly susceptible to various link attacks. The basic requirements for a secured networking are secure protocols which ensure the confidentiality, availability, authenticity, integrity of network. Many existing security solutions for wired networks are ineffective and inefficient for MANET environment. As the transmission takes place in open medium makes the MANETs more vulnerable to security attacks. In the presence of security protocol effect of various attacks can be reduced. The mobile hosts dynamically establish paths among one another in order to communicate. Therefore, the success of MANET communication highly relies on the collaboration of the involved mobile nodes.

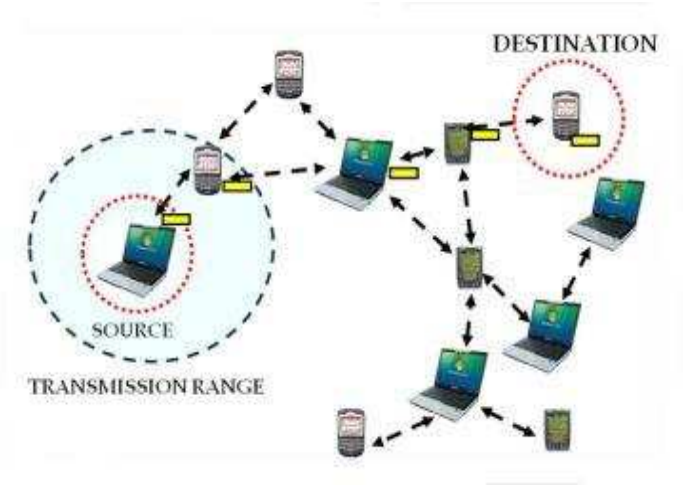

Figure 1: Structure of Mobile Ad-hoc Networks

Wireless ad-hoc networks [2] play a vital role in the communications fields. This is due to the strong signal transmission at the critical situation also in the battle fields. These type of wireless communication also used for the various purposes. Wireless mobile Ad-hoc network (MANET) and its various attacks and also discuss about the collision of the nodes in the networks. The MANET is attacked by different types of attacks but the collision of nodes occurs due to mobility of the mobile and deals with the flooding time of the networks, whereas the communication between the two or more devices by intermediate nodes itself without any centralized system so that attacks can be achieved easily in the network. The flooding time is very significant role in the mobile ad hoc networks.

II. Previous Techniques for Prevention of Attacks in MANET

The migration [6] to wireless network form wired network has been a worldwide trend within the past few decades. Among all the up to date wireless networks, Mobile Ad hoc Network (MANET) is one amongst the foremost necessary and distinctive applications. On the contrary to ancient specification, MANET doesn't need a set of network infrastructure; each single node works as each a transmitter and a receiver and they trust their neighbors to relay messages. Nodes communication directly with one another once they are in range intervals constant communication varies. The self-configuring ability of nodes in MANET created it fashionable among vital mission applications like military use or emergency recovery. Unfortunately, the open medium and remote distribution of MANET create it at risk of numerous kinds of attacks. So, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. In this project, we define solid privacy requirements regarding malicious attackers in MANET. Then we propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

In recent [8] years mobile ad hoc networks (MANETs) have become a very popular research topic. By providing communications in the absence of a fixed infra-structure MANETs are an attractive technology for many applications such as res-cue operations, tactical operations, environmental monitoring, conferences, and the like. However, this flexibility introduces new security risks. Since prevention techniques are never enough, intrusion detection systems (IDSs), which monitor system activities and detect intrusions, are generally used to complement other security mechanisms. Intrusion detection for MANETs is a complex and difficult task mainly due to the dynamic nature of MANETs, their highly constrained nodes, and the lack of central monitoring points. Conventional IDSs are not easily applied to them. New approaches need to be developed or else existing approaches need to be adapted for MANETs. This chapter outlines issues of intrusion detection for MANETs and reviews the main solutions proposed in the literature.

Intrusion Detection Systems [11] (IDSs) for Mobile Ad hoc Networks (MANETs) are indispensable since traditional intrusion prevention based techniques are not strong enough to protect MANETs. However, the dynamic environment of MANETs makes the design and implementation of IDSs a very challenging task. In this paper, we present a non-overlapping Zone-Based Intrusion Detection System (ZBIDS) that fits the requirement of MANETs. On the local detection part, we present a general intrusion detection agent model and propose a Markov Chain based anomaly detection algorithm. We focus on the protection of MANET routing protocols and present the details regarding feature selection, data collection, data preprocess, Markov Chain construction, classifier construction and parameter tuning. We demonstrate that local detection alone cannot achieve desirable performance. Therefore, we further propose a collaboration mechanism among ZBIDS agents and an aggregation algorithm used by gateway nodes. With alert information from a wider area, gateway nodes' IDS can effectively suppress many falsified alerts and provide more diagnostic information about the occurring attacks. Security officers can have a general understanding about the attacks using the proposed MANET Intrusion Detection Message Exchange Format (MIDMEF). We carry out extensive simulation to evaluate the performance of ZBIDS at different mobility levels. Simulation results show that ZBIDS can achieve desirable performance and meet the security requirement of MANETs.

Flooding-based[10] route discover y is usually preferred in MANETs in order to set up the route with reliability between transmission pair. However, this approach may cause a serious contention in information transfer between adjacent nodes and a considerable amount of control packet s. The transfer of information between nodes is made secured by Intrusion detection system (IDS). The architecture of IDS is discussed in the manuscript to achieve the reliable and confidential transmission over MANET which follows some techniques such as Watch Dog, Confident, and CORE.

With recent [15] advances in network based technology and increased dependability of our everyday life on this technology, assuring reliable operation of network based systems is very important. During recent years, number of attacks on networks has dramatically increased and consequently interest in network intrusion detection has in-creased among the researchers. This paper provides a review on current trends in intrusion detection together with a study on technologies implemented by some re-searchers in this research area. Honey pots are effective detection tools to sense attacks such as port or email scanning activities in the network. Some features and applications of honey pots are explained in this paper.

III. Weakness in Manet's

Vulnerability is a weakness in security system [12]. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

Lack of centralized management

MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad -hoc network. Lack of centralized management will impede trust management for nodes.

Resource availability

Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

Scalability

Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

Cooperativeness

Routing algorithm for MANETs usually assume that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

Dynamic topology

Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

Limited power supply

The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

There are different types of attacker present in MANETs, which tries to reduce the performance of network. In this paper we study about various attackers and attacks in MANET.

IV. Different types of Attacks in Manet

Attacks on mobile ad hoc networks can be classified into different categories following:

Passive attack: in this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information [5]. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping:

Denial of service attack: Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network [2].

Traffic Analysis: In MANETs the data packets as well as traffic pattern both are important for adversaries [1]. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered. Traffic analysis in ad hoc networks may reveal following type of information.

Snooping: Snooping is unauthorized access to another person's data [3]. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Active attack: In this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker's threat can be performed

Flooding attack: In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance [6]. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

Black hole Attack: Route discovery process in AODV is vulnerable to the black hole attack [8]. The mechanism, that is,

any intermediate node may respond to the RREQ message if it has a fresh enough routes, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

Rushing Attack: Rushing attacks are mainly against the on-demand routing protocols. These types of attacks subvert the route discovery process. On -demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack [1]. When compromised node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet can react.

Link spoofing attack: In a link spoofing attack, a malicious node advertises fake links with non -neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks.

Node Isolation Attack: The authors in this work have introduced an attack against the OLSR protocol . As implied by the name, the goal of this attack is to isolate a given node from communicating with other nodes in the network. The idea of this attack is that attacker(s) prevent link information of a specific node or a group of nodes from being spread to the whole network. Thus, other nodes who could not receive link information of these target nodes will not be able to build a route to these target nodes and hence will not be able to send data to these nodes.

Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point [2]. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole .In DSR, AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network.

Cloning Attack: Clone attack or node replication attack is a severe attack in WSNs [10]. In this attack, an adversary captures only a few of nodes, replicates them and then deploys arbitrary number of replicas throughout the network. It is very hard to distinguish between non compromised nodes a clone node since a clone has the same security and code information of original node. Hence cloned nodes can launch a variety of other attacks. The detection of cloning attacks in a wireless sensor network is therefore a fundamental problem. Many existing protocols expose the following limitations: high performance overheads, unreasonable assumptions, necessity of central control, and lack of smart attack detection etc. Few existing approaches like solved these problems. But here we present a security model to detect two more attacks along with cloning attack detection with the same communication cost and performance overhead. We used the benefit of mobile agent to reduce the communication cost. Also the proposed protocol considers Mobile Wireless Sensor Network environment.

Jamming: Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication [1]. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.

Active Interference: An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications. The effects of such attacks depend on their duration, and th e routing protocol in use. Attacker can change the order of messages or attempt to replay old messages. Old messages may be replayed to reintroduce out of date information.

Selfish Misbehavior of Nodes: Attacks under this category, are directly affects the self-performance of nodes and does not interfere with the operation of the network. It may include two important factors.

Conservation of battery power, and

Gaining unfair share of bandwidth

Malicious code attacks: malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.

Sybil attack: The Sybil attack especially aims at distributed system environments. The attacker tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from source to destination. A consequence of this is that attackers have a harder time to destroy the integrity of information.

Eavesdropping: The intruder silently listens to the communication by tapping the wireless link.

Man-in-the-middle attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

V. CONCLUSIONS

In this paper, we have analyzed the security threats an ad -hoc network faces and presented the security objective that need to be achieved. On one hand, the security -sensitive applications of an ad-hoc networks require high degree of security on the other hand, ad-hoc network are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. Therefore, a more ambitious goal for ad hoc network security is to develop a multi -fence security solution that is embedded into possibly every component in the network, resulting in depth protection that offer multiple line of defense against many both known and unknown security threats.

REFERENCES

[1] Gagandeep, Aashima, Pawan Kumar, Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review ,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[2] Priyanka Goyal,Sahil Batra , Ajit Singh, A Literature Review of Security Attack in Mobile Ad-hoc Networks, International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.

[3] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, Different Types of Attacks on Integrated MANET- Internet Communication , International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3).

[4] Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala,A Review of Current Routing Attacks in Mobile Ad Hoc Networks, International Journal of Computer Science and Security, volume (2) issue (3).

[5] Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail, Raed Alsaqour, Daud Israf, Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm, International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085).

[6] Rishabh Jain, Charul Dewan, Meenakshi, A Survey on Protocols & Attacks in MANET Routing, IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012 ISSN (Online): 2231 –5268

[7] Wazir Zada Khana, Yang Xiangb, Mohammed Y Aalsalema, Quratulain Arshada The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures, I.J. Wireless and Microwave Technologies, 2012, 2, 33-44 Published Online April 2012 in MECS.

[8] Pramod Kumar Singh, Govind Sharma, An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[9] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks, JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, JANUARY 2011, ISSN 2151-9617.

D Sheela , G. Mahadevan, Mollifying the Effect of Cloning, Sink Hole and Black Hole Attacks in Wireless Sensor Networks using Mobile Agents with Several Base Stations, International Journal of Computer Applications (0975 – 8887) Volume 55– No.9, October 2012.