ABSTRACT

MANET which means Mobile Ad hoc Networks is popular because it requires no network infrastructure for the mobile nodes within the network to communicate. Any node can join or leave the network independently. The important features of MANET are dynamic topology, self-configuring, peer to peer architecture, use of wireless medium and so on. Due to the dynamic infrastructure, MANET provides high flexibility that attracts them to many application as well as prone to security threats. Many of the vulnerability in MANET are hard to detect. Even though the IDS was used as a security measure in wired network, researchers had explore the IDS as the security solution for the mobile ad hoc network In this paper, we study the different IDS techniques that can be applied on MANET. We will first describe briefly about the different types of security threats and then describe the IDS technique to counter the attacks.

Keywords: Attacks, Intrusion Detection Techniques, MANET, Security, Threats.

1. INTRODUCTION

Mobile nodes within the mobile network configure themselves and thus it doesn’t depend on any predefined network configuration [1]. It is cheaper as MANET is free from the use of physical medium. MANET provides high flexibility as a result of this dynamic topology and so is attracted towards many applications such as disaster recovery, rescue mission, tactical battlefield, mining operation, maritime communication, vehicle network, casual meeting, campus network, scene dispatch for emergency accident, wireless access system, co-operative mobile communication, military application and so on [2]. Setting up the traditional network configuration results in a high cost time consuming tasks, so we use ad hoc self-organization. Thus mobile ad hoc network is a wireless network that has attracted much concentration from the researchers. It provides temporary network topology which means that the mobile nodes have the freedom to join or leave the network independently.

Unlike the conventional wireless network, the MANET provides a reliable mode of communication among the nodes. In MANET, there exists both single-hop and multi-hop network. If the sender and receiver are within their radio range, then it is a single-hop network. On the other hand, multi-hop network are those in which mobile nodes are able to communicate via intermediate nodes, if they are not within their radio range [3]. This in contrast to the conventional wireless network, where communication between two nodes are possible only when they are in the transmission range [4]. Wireless network is formed by all the mobile nodes that have participated in communication in both single-hop and multi-hop, thus creating a mobile ad hoc network.
Due to the lack of fixed infrastructure, weak security authentication mechanism, dynamic topology, unreliability of wireless connection etc., MANET is vulnerable to several attacks. These attacks include eavesdropping, traffic analysis, black hole attacks, wormhole attacks, sink hole attacks, rushing attacks, Denial of Service attacks and so on. Therefore the security mechanisms have to be imposed on MANET. Security measures that were used on wired network cannot be fully accommodated into MANET because of the enhanced features of MANET. Thus MANET requires a robust security scheme to ensure the security.

Intrusion Detection is used as an efficient security mechanism. It is the firewall used in the network security. The activities that violate the security policy of system are called intrusion and the mechanism used to detect the intrusion is called Intrusion Detection Techniques. Basic assumption of intrusion detection is that the behaviors of normal and abnormal activities are different. IDS capture the data and with the evidence collected, it will determine whether any attack is presented or not. Response will be initiated to prevent or minimize the damage to the system, once an attack was detected. There is different intrusion detection techniques like specification based, anomaly based, agent based, and cluster based, promiscuous based and so on.

The rest of the paper is organized as follows. Section 2 describes the vulnerabilities and threats in MANET. Section 3 will give a brief idea about the variety of attacks. The different intrusion detection techniques will be taken on Section 4 and Section 5 will conclude the discussion.

2. VULNERABILITIES AND THREATS IN MANET

Threat is any event that if realized can cause damage to the system. Threats can create loss of confidentiality, availability or integrity. Weakness in a system that can be exploited by a threat is called vulnerability. Let us briefly describe the various vulnerabilities and threats in mobile ad hoc network.

Wireless Network: Nodes in the MANETs are connected using wireless links; thus MANET is susceptible to many of wireless attacks. Bandwidth available is typically low. Even though wireless network eliminates the cost involved in the installation of cables, there are chances of launching attacks like eavesdropping, jamming etc. Attacker for preventing the normal operation will consume network bandwidth.

Lack of fixed network infrastructure: MANET is designed in such a way that mobile nodes can join or leave the network independently. MANET has a dynamic topology. The nodes can behave normally or maliciously and it is difficult to distinguish among these behaviors. Once a node is compromised by the attacker, they can be used to launch many severe attacks on network.

Distributed Nature: Ad hoc network has a distributed nature instead of centralized management. It is hard to detect attacks especially when attacker change the attack pattern and target in different period of time. It is possible for a malicious node to become router agent in routing algorithm, thereby disrupting the network operation. It is difficult to distinguish among trusted and malicious node.

Limited Physical Security There is no clear line of defense in MANET. This is in contrast to wired network where the nodes get access only after passing through several line of defense. When the node enters the range of any other node in MANET, it becomes a part of MANET and thus can communicate with other nodes. There is no separate boundary between internal network and external world.

Resource Constraints: MANET is created using a number of different devices which can act as node in the network. One of the major resource problems that MANET faces is lower battery power. In wired network, nodes get power from the outlets which mean that they have infinite power supply. Nodes in the MANET may act selfish for saving their battery power.

3. ATTACKS ON MANET

Two types of attackers which are common in MANET are internal and external attacker. Internal attacker is those which are part of network, they are the trusted node with which information like routing information is shared. External attacker is not an authenticated node in the network, so they can be prevented easily compared to internal attackers. Attacks on MANETs can be passive or active.

3.1 Passive Attacks

Passive attacks do not cause any problem to data transfer. They silently watch the communication in order to get the information about the whole network. Confidentiality of data is affected as the adversary can use the monitored...
information for launching future damages to the network. Two types of passive attacks are eavesdropping and traffic analysis.

Eavesdropping is one of the passive attacks that unauthorizely intercepts the data communication. It is a direct threat towards the confidentiality of data that has to be kept secret during communication. Eavesdropper can fetch the critical information like location, password, public key, private key, pin etc. Security solutions like spread spectrum and frequency hopping can limit eavesdropping attacks.

In traffic analysis, the attacker examines the traffic (i.e. amount of data) involved in the communication. This attack is passive in the sense that attacker can only analyze the data; they can’t take part in the network. Attacker can get the existence and location of nodes, communication network topology, and sender and receiver node through traffic analysis attack. They seek to provoke the communication between nodes. Traffic analysis is the process of monitoring message for the purpose of deducing useful information, even if the message is encrypted.

3.2. Active Attacks

Unlike passive attack, attacker in the active attack can cause data alteration or unauthorized state change in the network. The attacker intentionally inserts, modifies or deletes the packet in the data communication. Examples of active attacks are black hole, sink hole, DoS attack, rushing, worm hole etc.

In sinkhole attack, attacker modifies the packet to disrupt the network. Here attacker compromise a node and make that node attractive to all other nodes in the network, thereby receiving the whole traffic. Sinkhole attack is usually targeted on routing protocols and it can be used as a basis for attacks like dropping and selective forwarding attacks.

Black hole attack like the sinkhole attracts the traffic to a compromised node. It prevents packets from reaching the destination by making the black hole node replying the route request message with a large sequence number and minimal hop count. It is much harder to detect if the black hole is a virtual node or node outside the network.

The purpose of denial of service attack is to steal the services of an ad hoc network or availability of certain node. This type of passive attack makes the node busy by frequently sending messages to other nodes. The receiver thus may not be able to receive the authorized message.

Wormhole attacks are also known as tunneling attacks. There will be two attackers on the network and the attacker at one point in the network receives the packet and tunnels it to other attacker on the network. These two attackers are connected via a high speed links. Users will be in the illusion that they have selected the shortest path. Packet leashes are the method introduced to prevent wormhole attacks.

Rushing attacks directly target the on demand routing protocols, thereby making the route discovery process difficult. On demand routing protocols broadcast a route request to every other node in the network in order to find a route. For reducing the message flooding overhead, each node will forward only the first route request that has arrived. If the attacker forwards route request and it reaches first at the destination, then route consisting of attacker node will be selected, any request from the non-attacker will be rejected.

4. INTRUSION DETECTION TECHNIQUES

IDS generally detect unwanted manipulations to the system. It is an indispensible part of security system. By monitoring the system activities, the IDS are capable of detecting a violation to the security policy. IDS will generate a response to prevent or minimize the effects of an attack to the system. Let us briefly describe the different intrusion detection technique for MANET.

4.1. Agent Based Intrusion Detection

Zhang et al presented a general intrusion detection framework in MANET and the proposed architecture is as shown below. The proposed framework is distributed and meets the needs of MANET. The mobile ad hoc network is designed in such a way that an IDS agent is built in every node in the network and these nodes actively participate in the intrusion detection by detecting the signs of intrusion behavior locally and independently. The nodes are co-operative in the sense, even though a node has detected an anomaly without any strong evidence, it will pass the information to the neighboring nodes to figure out the possible traces of intruder. The conceptual model for IDS agent is figured by Zhang et al.
Local data acquisition is responsible for collecting data from nodes in the network. Local detection engine is responsible for detecting the anomaly in the data that was collected through local data gathering. Once an intrusion is confirmed with proper evidence, the response module will take actions like removing the compromised node, resetting communication channel, and so on. When an intrusion is detected without strong evidence, the co-operative detection engine will come into action. Node that has detected the anomaly will send the available information to all other nodes available in the communication range and then started working on it to find the evidence.

In order to get better performance on some attacks, the paper explores the idea of placing the intrusion detection technique in each layer on each node of mobile ad hoc network. By using this technique, it becomes easier to catch the attacks that are seemed to be legitimate at the lowest layer and easier to detect in the higher layer. As IDS agent runs on each node on the mobile ad hoc network, the battery power will get limited. Also overhead is more compared to single layer intrusion detection mechanism.

4.2. Cluster Based Intrusion Detection

As discussed by Zhang et al in his paper, an IDS agent is placed on every node which causes a dramatic amount of energy consumption in each node. Such a high demand for power can cause the situation that some node in the network began to behave selfish. This will affect the co-operative intrusion detection in that node in the greedy for saving their battery power may not act co-operatively. Huang et al\[13\] proposed a cluster based intrusion technique that solves such a problem.

Huang et al proposed a MANET which is created in such a way that by using proper clustering algorithm, network is divided into number of clusters. Every node is a member of at least one cluster. Cluster head (i.e., one node per cluster) is the responsible for the monitoring issue and instead of placing IDS agent on every node; here agent is placed on cluster head. All other nodes in the cluster should be within 1-hop vicinity when a node is selected as cluster head. Every node within the cluster has equal probability of being selected as cluster head. The clustering algorithm proposed by Yinan Li divide the network into cluster and selects the cluster head. Agent is activated on the cluster head and it will collect data and check for intrusion\[14\]. If the agent detects any anomaly, it will notify the nodes in the cluster after screening the compromised node via broadcasting. The nodes within the cluster after receiving the alarm will screen that node. Like the agent based intrusion detection, if agent can’t determine the occurrence of intrusion with available data, it will pass the information to the set of cluster head node and each cluster head will analyses the data. Agent will confirm intrusion when majority of cluster head notifies the existence of intrusion.

From the performance evaluation, we can conclude that this type of intrusion detection will help to save the battery power, CPU speed up is increased and little system resource occupied. However, the overhead of cluster head is more compared to the Agent based IDS, as it is the responsibility of cluster head to monitor data, detect anomaly and notify all other nodes within the cluster.

![Fig 1: conceptual model for an ids agent](image-url)
4.3. Specification Based Intrusion Detection

Tseng proposed the first IDS in MANET which uses network monitors. In specification based IDS, intrusions are detected by comparing the actual behavior of the node with the security specification. All nodes are assumed to be covered by network monitors. Network monitor consist of finite state machine and it is used especially for the route discovery process. The specification of AODV was stated on this FSM [15]. For each monitored node, the network monitor is responsible for maintaining a forwarding table.

In AODV, node uses route request and route reply message to find the path from source to destination. Each RREP and RREQ message in the range of network monitor (NM) is monitored in a request reply flow. NM employs FSM for each branch of request reply flow. The information such as route request packets are forwarded or not and route reply packets gets modified or not can be obtained through request reply flow. The paper also presented the situation of sharing information among the NMs when it needs information about previous message or other nodes that go out of the range.

Specification based intrusion detection introduces bandwidth overhead among the network monitors, especially when they share the information about the nodes that are out of range. Routing protocols that have clearly defined specification can use specification based intrusion detection to detect unknown and known attacks. This technique cannot be applied to detect the attacks that do not violate protocol specification directly.

4.4. Anomaly Based Intrusion Detection

In this type of anomaly detection technique, intrusions are treated as anomalies (deviations from common rules). Normal profiles are created offline or online during training phase and in the monitoring phase, set of activities are compared with the normal profile, mark the nodes as malicious when they deviate from normal profile [16]. This type of intrusion detection is useful in detecting unknown attacks. Black hole and dropping attacks can easily detected using anomaly based intrusion detection.

Huang proposed an anomaly based intrusion detection model that extracts the correlations among the monitored features. When an anomaly is detected, the rules which are created to determine the attack type and attacker were executed. The rules are based on the number of incoming and outgoing packets on the monitored node. For known attacks, these values are already computed. We can formulate the unconditional dropping of a packet m as follows [13]:

\[ FP_m(\text{forwarded percentage}) = \frac{\text{packets actually forwarded}}{\text{packets to be forwarded}} \]  

Node m is dropping all packets if \( FP_m \) is zero and packets to be forwarded are not zero. MANETs have strong feature correlation in normal behavior patterns.

Another type of anomaly based detection is Zone based IDS [17]. Based on geographic partitioning, the network is divided into a number of zones. The advantage of such architecture is that it will save the communication bandwidth and improves the detection performance as it collects data from many nodes. The nodes in a zone are called intrazone and interzone nodes are the nodes which work as bridges to other zones. Local detection is carried out by each node in the zone. It makes final decision by sending alerts to the interzone nodes. Zone based IDS causes detection and response latency even when there is enough evidence on local nodes [17].

4.5. Promiscuous Monitoring Based Intrusion Detection

Marti et al [18] specifies that if node A is within the range of node B, it can overhear communication to and from B even if those communications do not directly involve A. MANET rely on promiscuous mode monitoring which has the advantage of collecting data without additional overhead. Dropping and modification of packets can be detected using promiscuous monitoring, but it cannot detect misbehavior node in presence of ambiguous collision and receiver collision.

Watchdog and Path rater mechanism on DSR is used for detecting misbehavior nodes. The packets to be forwarded are copied to a buffer and watchdog detects the misbehavior by observing the behavior of neighboring nodes to these packets. Watchdog checks whether the neighboring node has forwarded the packet without making any modification or not. It will compare each overheard packet with the packet on the buffer and if there is a match, packet in the buffer is removed. If the packet stay in the buffer for a longer period of time, it increments the count for the node responsible for forwarding the packet [19]. The node is marked as misbehaving node, if the count exceeds certain threshold value and notification is sent to the source node. The information about the malicious node is given to the path rater. The path rater selects the reliable link instead of shortest path. Unreliable behavior is detected by line breaks and misbehavior is detected as packet mishandling/modification.

Reputation mechanism can be used to respond to the malicious node. Here misbehaving node is detected by monitoring the behavior of next hop neighbor and the misbehaving node is rated [20]. Parker et al [21] proposed a method to detect misbehavior in a wide variety of routing protocols by enabling a node to listen to all nodes in its transmission range, instead of node that forwards the packet. The information obtained from the promiscuous monitoring may be incomplete or misleading. As the packet is duplicated and transmitted, bandwidth required is more [16].
5. CONCLUSIONS

The goal of this study is to have a deep understanding of the different intrusion detection techniques. The basic security threats raised from the characteristics of MANET such as dynamic topology, resource constraints etc. The attacks coming from the internal nodes of the network are more dangerous and difficult to detect than those outside the network. The various vulnerabilities and threats in mobile ad hoc networks were analyzed. The paper studies about the various intrusion detection techniques and which all attacks can be there on the MANET.

REFERENCES