Effective Intrusion Detection Approach in Mobile Ad Hoc Networks

SHEETAL M. YAWALKAR

Abstract—intuitively, intrusions in an information system are the activities that violate the security policy of the system, and intrusion detection is the process used to identify intrusions. It is based on the beliefs that an intruder's behavior will be noticeably different from that of a legitimate user and that many unauthorized actions will be detectable. Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. Intrusion Detection in MANET is one of the major concerns in peer to peer networking scenario where mobile / wireless nodes communicate with each other without any pre-defined infra-structural setup. This paper presents an overview of various intrusion detection models, identifying its issues, discusses on design and proposes an intrusion detection system shortly, This paper aims to pioneer and to assort current techniques of Intrusion Detection System (IDS) aware MANET. MANET is infrastructure-less, pervasive in nature with multi-hop routing, without any centralized authority. To support these ideas, discussions regarding attacks and researches achievement on MANET are presented inclusively.

Keywords:
Mobile ad hoc networks, Intrusion Detection System, distributed network, dos .

1. INTRODUCTION

The major task of intrusion detection system [1] is to discover the intruders from the network packet traffic data or system audit data. mobile ad hoc network (MANET) is a collection of wireless devices moving in seemingly random directions and communicating with one another without the aid of an established infrastructure In an ad hoc network, malicious nodes may enter or leave the immediate radio transmission range at random intervals or may collide with other malicious nodes to disrupt network activity or behave maliciously only intermittently, further complicating their Detection. A node that sends out false routing information could be a compromised node, or merely a node that has a temporarily stale routing table due to volatile physical conditions. Packets may be dropped due to network congestion or because a malicious node is not faithfully executing a routing algorithm. Since MANETs can be set up easily and inexpensively, they have a wide range of applications, especially in military operations and emergency and disaster relief efforts [2].

However, MANETs are more vulnerable to security attacks than conventional wired and wireless networks due to the open wireless medium used, dynamic topology, distributed and cooperative sharing of channels and other resources, and power and computation constraints [3].Intrusion detection systems (IDSs), which attempt to detect and Mitigate an attack after it is launched, are very important to MANET security. Several monitoring-based intrusion detection techniques (IDTs) have been proposed in literature [4] [5], [6], [7]. In a monitoring-based IDT, some or all nodes monitor transmission activities of other nodes and/or analyze packet contents to detect and mitigate active attackers MANET [8] is defined to be a collection of mobile / wireless nodes adopting a peer to peer communication with each other. Research efforts [9], [10], [11] work consistently to provide efficient / reliable and secured communication between nodes in a network Wireless networks are gaining popularity to its peak today, as the users need wireless connectivity irrespective of their geographic position. Mobile Ad Hoc Networks (MANETs) have become a stimulating and significant technology in recent years, because of the rapid proliferation of wireless devices. MANET must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researchers worked specifically on the security issues in MANET and many secure routing protocols and security measures within the networks were proposed. It is easily visionable as in a close future users will access Internet through wireless PDA, while roaming from a place to another. Mobile ad-hoc networks (MANET) are peer to peer wireless networks that do not trust on the presence of wired interconnections infrastructure. Attack prevention measures, such as authentication and encryption, can be used as the first line of defense for reducing the possibilities of attacks. However, these techniques have a limitation on the effects of prevention techniques in general and they are designed for a set of known attacks. They are unlikely to prevent newer attacks that are designed for circumventing the existing security

measures. For this reason, there is a need of second mechanism to detect these newer attacks and that is none other than intrusion detection.

2. LITERATURE SURVEY

Zing and Lee [12] describe a distributed and collaborative anomaly detection-based IDS for ad hoc networks. Sergio Marti et al [13] describe an approach that involves the use of finite state machines for specifying correct AODV routing behavior and distributed network monitors for detecting run-time violation of the specifications. Yi and Nondrug [14] present a method for building confidence measures of route trustworthiness without a central trust authority. Papadimitratos [15] and Z. J. Haas [16] present various passive methods for establishing trust metrics and evaluating trust during run time. Michiardi and Molva [17] assign a value to the "reputation" of a node and use this information to identify misbehaving nodes and cooperate only with nodes with trusted reputations. E. Z. Ang [1] couple a trust based mechanism with a mobile agent based intrusion detection system, but do not discuss the security implications or overhead needed to secure the network and individual nodes from the mobile agents themselves. Sun, Wu and Pooch [18] introduce a geographic zone-based intrusion detection framework that uses location-aware zone gateway nodes to collect and aggregate alerts from intra-zone nodes. Gateway nodes in neighboring zones can then further collaborate to perform intrusion detection tasks in a wider area and to attempt to reduce false positive alarms. Sterne [19] proposed a generic architecture of IDS which tries to improve throughput in MANET in the presence of nodes that agree to forward packets but fail to do so. In MANET, cooperation is very important to support the basic functions of the network so the token based mechanism, the credit-based mechanism, and the reputation based mechanism were developed to enforce cooperation. Tseng [20] proposed "intrusion detection (ID) and response system" should follow both the natures. In this proposed architecture model, each node is responsible for detecting signs of intrusion locally and independently, but neighboring nodes can collaboratively investigate in a broader range.

3. MANET

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without any established infrastructure or centralized authority. In a MANET, the nodes are free to move about and organize themselves into a network. MANET does not require any fixed infrastructure such as base stations; therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously. The below figure shows a sample MANET

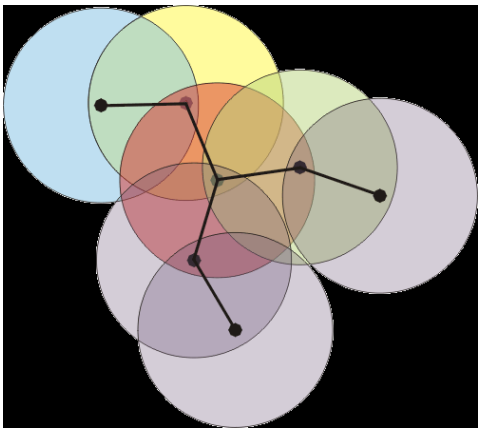


Fig. 1 Mobile Ad Hoc Networks

3.1 Characteristic of MANET [26]

•Autonomous terminal: Each node in MANET is autonomous and acts both, as router and host.

•Distributed: MANET is distributed in its operation and functionalities, such as routing, host
Configuration and security.

•Multi-hop routing: If the source and destination of a message is out of the range of one node, a multi
-hop routing is created.

•Dynamic network topology: Nodes are mobile and can join or leave the network at any time; therefore,
The topology is dynamic.

•Fluctuating link bandwidth: The stability, capacity and reliability of a wireless link are always inferior
to wired links.

• Thin terminal: The mobile nodes are often light weight, with less powerful CPU, memory and power.

•Spontaneous and mobile: Minimum intervention is needed in configuration of the network. The routing protocol should be an adapted one that allows users to communicate in the network. It should also support security. Some existing security technologies for wired network, such as encryption, can be utilized in MANET. However, because of the mobile and ad hoc nature of MANET, the applications of MANET are limited. Other technologies, such as firewall, do not apply to MANET, because of the lack of a centralized authority. Same as the wired network, MANET faces the security threat such as passive eavesdropping, spoofing, and denial of service. At the same time, because of its ad hoc nature, it suffers from more security threats. Threats to MANET can be classified into two groups:

•Vulnerabilities accentuated by the ad hoc nature: The topology of MANET is mainly determined by
Geographical locations and by radio range of the nodes. Therefore, it does not have a clearly defined physical boundary. In wired network, a centralized firewall can implement the access -control. However, in MANET,

access-control cannot be other attacks, such as denial of service (DOS) still threat MANET, even worse than for wired network, since the routing and auto configuration framework of MANET are more vulnerable to such attack.

•Vulnerabilities specific to the ad hoc nature: The routing and auto configuration mechanism of MANET introduces opportunity for more attack because in both mechanisms, all nodes have full trust between each other

3.2Challanges in MANET

Regardless of the variety of applications and the long history of mobile ad hoc network, there are still some issues and design Challenges that we have to overcome [21]. This is the reason MANET is one of the elementary research field. MANET is a wireless network of mobile nodes; it's a self organized network. Every device can communicate with every other device i.e. it is also multi hop network.

Following are the traditional problem and challenges faced in this field.

•The channel is unprotected from outside signal.

•The wireless media is unreliable as compared to the wired media.

•Hidden terminal and exposed terminal phenomenon may occur.

•The channel has time varying and asymmetric propagation properties.

•The scalability is required in MANET as it is used in military communications, because the network grows according to the need, so each mobile device must be capable to handle the intensification of network and to accomplish the task.

•MANET is infrastructure less network, there is no central administration. Each device can communicate with every other device, hence it becomes difficult to detect and manage the faults. In MANET, the mobile devices can move randomly. The use of this dynamic topology results in route changes, frequent network partitions and possibly packet losses.

•Each node in the network is autonomous; hence have the equipment for radio interface with different

Transmission/ receiving capabilities these results in asymmetric links. MANET uses no router in between.

•In network every node acts as a router and can forward packets of data to other nodes to provide

Information partaking among the mobile nodes. Difficult chore to implement ad hoc addressing scheme, the MAC address of the device is used in the stand alone ad hoc network. However every application is based on TCP/IP and UDP/IP.

4. IDS BACKGROUND

An intrusion -detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device—it is not a stand-alone protection measure. Depending on the detection techniques used, IDS can be classified into three main categories as follows:

1) Signature or misuse based IDS

2) Anomaly based IDS

3) Specification based IDS

• The signature -based IDS uses pre -known attack scenarios and compare them with incoming packets traffic. There are several approaches in the signature detection, which differ in representation and matching algorithm employed to detect the intrusion patterns. The detection approaches, such as expert system, pattern recognition, colored petri nets, and state transition analysis are grouped on the misuse.

• The anomaly - based IDS attempts to detect activities that differ from the normal expected system behavior. This detection has several techniques, i.e.: statistics, neural networks, and other techniques such as immunology, data mining, and Chi - square test utilization. Moreover, a good taxonomy of wired IDS"s w as presented by D ebar.

• The specification – based IDS

Are hybrid of both the signature and the anomaly based IDS. It monitors the current

Behavior of systems according to specifications that describe desired functionality for security

Critical entities [22]. A mismatch between current behavior and the specifications will be reported as an attack.

5 IDS IN MANET

Intrusion detection system serves as an alarm mechanism for a computer system. It detects the security compromises happened to a computer system and then issues an alarm message to an entity, such as a site security officer so that the entity can take some actions against the intrusion (Axelsson, 2000;Greg, 2004). An ID contains an audit data collection agent, which keep track of the activities within the system, a detector which analyzes the audit data and issues an output report to the site security officer (Axelsson, 2000).

In the discussion of IDS in MANET, two concepts need to be distinguished: intrusion detection techniques and intrusion detection architecture. Intrusion detection techniques refer to the concepts such as anomaly and misuse detection. They mainly solve the problems like, how an ID detects an intrusion with a certain algorithm, given some audit data as input data. The intrusion detection architecture deals with problems in a larger scope. Intrusion detection architecture needs to employ certain intrusion detection techniques as a module. But it also contains many other modules, such as a module on how the

nodes in a network can collaborate in decision making regarding intrusion detection. In wired network, a node can usually make intrusion detection decision based on the data collected locally. Therefore, an intrusion detection technique can meet the need for intrusion detection once it is deployed on a node. In wireless network, however, it is very difficult for a node to make decision just based on data collected locally. Nodes must collaborate or exchange data at least in making an intrusion detection decision. Therefore, an architecture to define the roles of different nodes and the way they communicate is extremely important in wireless IDS.

The intrusion detection technique is basically independent from the architecture or environment. In other words, anomaly and misuse detection can be utilized in wireless environment just as they are in wired network. The difference in implementation is mainly on what audit data to take as input to the algorithm. However, most IDS in MANET utilize anomaly detection because of the special nature of MANET. The most literature on IDS in MANET the author reviews focus on different architectures of IDS in MANET, rather than different detection techniques. Many Literatures do not describe the detection techniques used in detail. Some even just states that the architecture can utilize both anomaly and misuse detection techniques. The current paper, therefore, focuses on the different architectures of IDS, rather than the detection techniques that the architectures use. This section first discusses the attacks in MANET and the security task of IDS in MANET. Then, the requirements for IDS in MANET are identified. Finally, the possible architectures of IDS in MANET are analyzed.

6. ATTACKS IN MANET

Attacks in MANET can be classified in terms of consequence and techniques (Lee and Huang, 2003). Based on consequence, attacks can be grouped into:

•Black hole: all packets are routed to a specific node which will not forward them at all

•Routing loops: cause a loop in routing path.

•Network partition: the network is divided into sub networks where nodes cannot communicate each other even though path exists between them.

•Selfishness: A node will not serve as a router for other nodes.

• Sleep deprivation: A node is forced to use up its battery.

• Denial of Service: A node is prohibited from sending or receiving packets (Lee and Huang, 2003; Zhou and Haas, 1999). Based on the techniques of attack, they can be grouped into:

• Cache poisoning: information in routing tables is modified, deleted or contains false information.

• Fabricated Route Messages: route messages, such as route requests and replies with malicious information are inserted into the network. They can be done by:

A False source route: a wrong route is broadcasted in the network, such as setting the route cost to 1 no matter where the destination is.

b. Maximum sequence: alter the sequence field in control messages to the maximum possible value. This will Cause nodes to invalidate all legitimate messages with reasonable sequence filed value.

•Rushing: In several routing protocols of MANET, only the messages that arrive first Are accepted by the recipient. The attacker can block legitimate messages that arrive later by distributing a false control message.

•Wormhole: A path is created between two nodes that can be used to transmit packets secretly.

•Packet dropping: A node drops packets that are supposed to be routed.

• Spoofing: insert packet or control message with false or altered source address.

•Malicious flooding: Forward unusually large amount of packets to some targeted nodes (Lee and Huang, 2003).

7. SECURITY TASKS OF IDS IN MANET

Brutch and Ko (2003) presented two security tasks of IDS in MANET:

•Detect attacks against routing protocol: In MANET, an attacker may inject, replay, or distort routing information in order to partition the network or cause excessive load, while inside nodes may pass incorrect routing information (Sun and Wu, 2003; Lee, 2002; and Marti, 2000).

•Detect attacks against mobile nodes: This is just like in wired network; we need to protect individual workstation

8. REQUIREMENTS FOR IDS IN MANET

The difference between wireless and wired network as regard of IDS are as follows:

•IDS for MANET must work with localized and partial audit data. In MANET, the audit data is always localized and partial because MANET does not have a fixed infrastructure such as firewall or gateway that is used in wired network to collect complete and global audit data (Zhang and Lee, 2003).

•Network -based IDS does not work for wireless network.

•It is more difficult to IDS in MANET to distinguish between normal and intrusion traffic. In wireless network, There is often no clear line between normal/abnormal activities: In wireless network the connection is not stable and mobile nodes can join and leave the network at any time. For instance, a node which is temporarily out of Synchronization may send packets that could be considered packets of attack activities. (Zhang and Lee, 2003).

•IDS should utilize minimum resources. The wireless network does not have stable connection and physical resource of network and devices, such as bandwidth and power, are limited. Disconnection can happen at any time (Zhang and Lee, 2003). In addition, the communication between nodes for IDS purpose should not take too much bandwidth resources.

•Encryption in communication is difficult to achieve. The communication between IDS on different nodes must
be secure to not allow attacks gain the access to such communication. However, encryption in Manet is a difficult task itself. In wired network, because of the requirement of physical connection for access, this problem is less obvious.

•IDS can not assume any node is secure. Unlike in a wired network, Manet nodes can be very likely
Compromised. Therefore, in cooperative algorithm, the IDS must not assume that
Any nodes can be fully trusted.

•IDS must address high false alarm rate problem. It is difficult to obtain enough audit data to make
An intrusion detection decision, because the bandwidth of Manet is much restricted compared with wired network. As a result, IDS in Manet can easily result in either having too much false alarm or missing many attacks (Kong and Lou, 2002).

There are three development issues need to be addresses:

i. Find an appropriate architecture of IDS that will fit the mobile and adhoc nature of the wireless network.
ii. Find a way to effectively use the audit data source in wireless network in anomaly detection. As mentioned earlier, the audit data in wireless network is often partial and local.
iii. Find a way to effectively distinguish attack traffic from normal traffic, especially that normal traffic that seems abnormal due to factors such as poor network connections. Otherwise, the IDS will have a high false alarm rate (Zhang and Lee, 2003).Levanter (2002) identified the requirements of IDS for MANET as follows:

a. Be truly distributed, which means IDS must detect intrusion on each node, but nodes can collaborate in making decision on whether to issue an alarm.

B.To deal with local and partial audit data, IDS may need to sense anomaly happened on other hops.

C.To deal with the problem that no clear line between normal/abnormal, IDS need to obtain high detection rate and low false alarm.

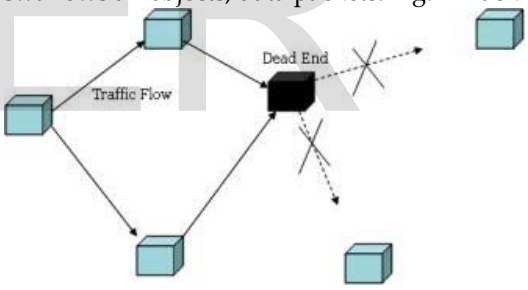
D.Given the resources constraints on wireless network, IDS should not consume too much resource, including power. Therefore, IDS should have run-time efficiency

9. WELL KNOWN INTRUSION DETECTION APPROACHES

A].Black hole Attacks

MANETs are vulnerable to various attacks. General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the ad hoc network.

Attacks in the network layer have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages; such as sequence number and hop count. A basic attack that an adversary can execute is to stop forwarding the data packets. As a result, when the adversary is selected as a route, it denies the communication to take place. In black hole attack, the malicious node waits for the Neighbors to initiate a RREQ (Route Request) packet. As the node receives the RREQ packet, it will immediately send a false RREP (Route Reply) packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a black hole as it swallows all objects; data packets. Fig. 2 Black hole attack

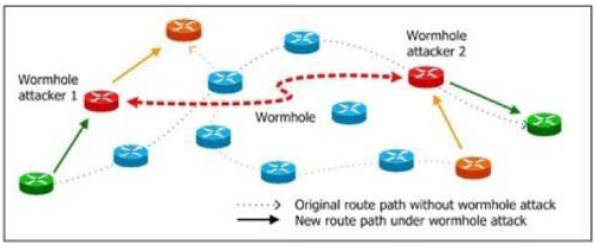


In figure 2,
Shows the black hole attack [23]
The attacker replies with false reply RREP having higher modified sequence number. So, data communication initiates from S towards M instead of D.

10. WORMHOLE ATTACK

A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a
High - speed of f-channel link, are strategically placed at different ends of a network. These attackers then record the wireless data they overhear, forward it to each other, and replay the packets at the other end of the network. Replaying valid network messages at improper places, wormhole attackers can make far apart nodes believe they are immediate neighbors, and force all communications between affected nodes to go through them.The below figure shows the worm whole attack [24]

.Fig. 3 Worm whole attack



11. DENIAL OF SERVICE

Denial -of-service (Dos) attacks consume the resources of a remote host or network, thereby denying or degrading service to legitimate users. Such attacks are among the most intricate security problems to address because they are
Easy to implement, difficult to prevent, and very difficult to trace. The most common DoS include attacks similar SYN Flood, Smurf, UDP Flood. Deter-mining the source generating attack traffic is especially difficult when using stateless routing protocols (as in the Internet or geo-graphic routing). Attackers routinely disguise their location using incorrect, or "spoofed", source address.

12. ANOMALY DETECTION VS.MISUSE DETECTION

: In order to detect an intrusion attack, one need to make use of a model of intrusion. That is, we need to know what an IDA should look out for. There are basically two types of models employed in current IDA: anomaly detection and misuse detection. The first model hypothesizes its detection upon the profile of a users (or a group of users") normal behavior [10]. It analyzes the user's current session and compares them to the profile representing the user's normal behavior. It then reports any significant deviations to a designated system administrator. As it catches sessions which are not normal, this model is referred to as an „anomaly" detection model.
Fig. 4 shows Anomaly detection system [25] and fig. 5 shows Misuse detection system [26]

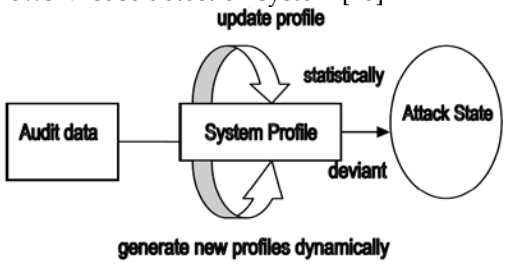


Fig. 4- Anamoly Detection System

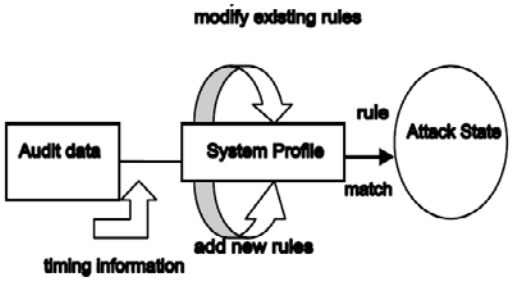


Fig. 5- Misuse Detection System

Anomaly detection bases its idea on statistical behavior modeling and anomaly detectors look for behavior that deviates from normal system use. A typical anomaly detection system takes in audit data for analysis. The audit data is transformed to a format statistically comparable to the profile of a user. The users profile is generated dynamically by the system (usually using a baseline rule laid by the system administrator) initially and subsequently updated based on the users usage. Thresholds are normally always associated to all the profiles. If any comparison between the audit data and the users profile resulted in deviation crossing a threshold set, an alarm of intrusion is declared. This type of detection system is well suited to detect unknown or previously not encountered attacks. The second type of model bases its detection upon a comparison of parameters of the user's session and the user's commands to a rule base of techniques used by attackers to penetrate a system. Known attack methods are what this model looks for in a user's behavior. Since this model looks for patterns known to cause security problems, it is called a „misuse detection model. Misuse detection bases its idea on precedence and rules, misuse detectors look for behavior that matches a known attack scenario. A typical misuse detection system takes in audit data for analysis and compares the data to large databases of attack signatures. The attack signatures are normally specified as rules with respect to timing inform action and are also referred to as known attack patterns. If any comparison between the audit data and the known attack patterns described resulted in a match, an alarm of intrusion is sounded. This type of detection systems is useful in networks with highly dynamic behavioral patterns but like a virus detection system, it is only as good as the database of attack signatures that it uses to compare with.

13. HOST-BASEDVS.NETWORK-BASED INTRUSION DETECTION

: Most IDA takes either a network-based or a host-based approach in recognizing and detecting attacks. Network -based approach (NIDA) listens to the network, and capture and examine individual packets flowing through a network

[25]. That is, they use raw network packets as the data source. They typically utilize a network adapter running in promiscuous mode to monitor and analyze all traffic in real time as it travels across the network. They are able to look at the payload within a packet, to see which particular host application is being accessed, and to raise alerts when attacker tries to exploit a bug in such code. NIDA are typically host-independent but can also be a software package installed on dedicated workstation. A side effect of NIDA is that its active scanning can slow down the network considerably [26]. Hence usage of it on an ad hoc network needs to be evaluated. Host-based approach (HIDA) is concerned with what is happening on each individual host. They are able to detect actions such as repeated failed access attempts or changes to critical system files, and normally operate by accessing log files or monitoring real-time system usage. In order for a HIDA to function, clients have to be installed on every host in the network. These clients reside on the hosts as processes and perform analysis on the audit data gathered locally, at the expense of the already limited resources of the hosts. Hence care has to be taken to ensure that the HIDA client running on a host in an ad hoc network does not drain resources more than necessary.

14. ONLINE DETECTION VS.OFFLINE DETECTION

: Intrusion detection systems can further be classified according to the timelines of the audit data being gathered and processed. Audit data can be gathered and processed while the host is online (connected to the network) or offline (disconnected from the network). When a system is performing intrusion detection in online mode, the audit data is processed in real-time. A host-based system will gather information about a host as long as the host is connected to the network. A network-based system will monitor the network traffic of the hosts throughout the time they are connected. Any intrusion detected is immediately notified to other hosts. By „real time" we mean that threat detection is done at the same rate that the network information is captured. By „online detection", we mean that the network information is captured and threat is detected when the nodes are connected to the network. When a system is performing intrusion detection in offline mode, the audit data is not processed in real-time but periodically. A host-based system will gather information about a host even if it is not connected to the network. Even if the host is connected, detection is done as scheduled by the system. A network-based system will monitor the network traffic of the hosts periodically as can be in the case of polling. Any intrusion detected is still immediately notified to other hosts but a delay is expected. A typical technique of an offline intrusion detection system is data mining.

15. CONCLUSION:

IDS can be viewed as a guard system that automatically detects malicious activities within a host or network .This paper summaries basics of MANET, challenges and attacks in MANET namely black hole attack, wormhole and DOS attack, and briefly describes different Intrusion Detection Systems in MANET and also provides comparison between them (Refer Appendix A). Intrusion-Detection Systems aims at detecting attacks against computer systems and networks, in general, attacks against information systems. History shows that intruders often find new ways to attack and cause damage to computer systems and networks. Therefore, we consider that enabling a protection mechanism to learn from experience and use the existing knowledge of attacks to infer and detect new intrusive activities (attacks) is an important and potentially fruitful area of future research. We also believe that the development and deployment of network security policies are vital in networks with a dynamic environment such as are found in MANETs; this is a further potential area of research. Finally, the attacker may try to
Attack an existing protection scheme; therefore the protections mechanisms need to be robust enough to protect themselves and not introduce new vulnerabilities into the system.

REFERENCES

[1] Ang, E. Z. "Node Misbehavior in Mobile Ad Hoc Networks," National University of Singapore, 2004

[2] I. Chlamtac, M. Conti, and J.J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," Ad Hoc Networks, vol. 1, no. 1,pp. 13-64, 2003

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE WirelessComm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[4] S. Marti, T.J. Guile, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom,pp. 255-265, Aug. 2000[7] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the Confidant Protocol: Cooperation of Nodes Fairness in Dynamic Ad-Hoc Networks," Proc. IEEE/ACM MobiHoc, 2002.

[5] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the Confidant Protocol: Cooperation of Nodes Fairness in Dynamic Ad-Hoc Networks," Proc. IEEE/ACM MobiHoc, 2002.

[6] R. Molva and P. Michiardi, "Core: A Collaborative ReputationMechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," Proc. IFIP Comm. and Multimedia Security Conf., 2002.

[7] S. Banal and M. Baker, "Observation-Based Cooperation Enforcement in Ad Hoc Networks," Research Report cs. NI/0307012, Standford Univ., 2003.

[8] Perkins C.E, E.M. Royer, S.R. Das, "Ad hoc On-Demand Distance Vector Routing" draftietf-manet-aodv-08.txt, IETF MANET Working Group, June 1st, 2001.

[9] Gionis, Afrati, H. Mannila. Approximating a collection of frequent sets. In Proc. of 2004 ACM Int. Conf. on Knowledge Discovery in Databases (KDD"04), pg 12 – 19, 2004.
[10] Michiardi.P and R. Molva, "CORE: A Collaborative Reputation mechanism to Enforce node cooperation in mobile ad hoc networks," Communication and Multimedia Security Conference (CMS'02), September 2002.
[11] NS2 network simulator. http://www.isi.edu/nsnam/ns
[12] Zhang.Y, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks," Wireless Networks Journal (ACM WINET), vol. 9, no. 5, pp. 545-556, September
[13] Sergio Marti, T.J. Guile, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks",Proc. 6th annual International Conference on Mobile computing and Networking, U.S.A, 2006.
[14] Yi.S, P. Nadler and R. Kravets, Security-Aware Ad-Hoc Routing for Wireless Networks, UIUCDCS-R-2001-2241 Technical Report, 2001
[15] Papadimitratos, Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks", In Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January. 2002.
[16] Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, Nov./Dec. 1999[3] Michiardi.P and R. Molva, "CORE: A Collaborative Reputation mechanism to enforce node cooperation in mobile ad hoc networks," Communication and Multimedia Security Conference (CMS'02), September 2002.
[17] Michiardi.P and R. Molva, "CORE: A Collaborative Reputation mechanism to Enforce node cooperation in mobile ad hoc networks," Communication and Multimedia Security Conference (CMS'02), September 2002.
[18] Sun.B, Wu, U.W. Pooch, "Zone-based intrusion detection for mobile ad hoc", International Journal of Ad Hoc & Sensor Wireless Networks, September 2004[8] Sterne's, P. Balasubramanyam, et al. "A General Cooperative Intrusion Detection Architecture for MANETs", Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57-70, 2005
[19] Tseng, P et al, A specification based intrusion detection system for AODV, Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 125–134. ACM Press, 2003
[20] Sterne.D, P. Balasubramanyam, et al. "A General Cooperative Intrusion Detection Architecture for MANETs", Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57-70, 2005
[21] Imrich Chalmtac, Marco Conti, Jennifer J.-N. Liu "Mobile ad hoc networking: imperatives and challenges
[22] Chandrasekhar Ramachandran, Sudip Misra and Mohammad S, Obaidat "FORK: A novel two-pronged strategy for an agent-based intrusion detection scheme in ad-hoc networks" Computer Communications Volume 21, Issue 16, 25th October 2008, Elsevier.
[23] Jen SM, Laih CS, Kuo WC - Sensors (Basel) (2009), "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET".
[24] B. Mukherjee, L. Heberlein, and K. Levitt, "Network intrusion detection," IEEE Network, vol. 8, no. 3, pp. 26-41, May 1994.
[25] Sathish Kumar Alampalayam P. "Intrusion Detection and Response Model For Mobile Ad Hoc Networks".
[26] International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013

Author:-
S.M .Yawalkar, research scholar, SGBAU India
Working at Bhartiya mahavidhyalaya, Amravati
E-mail: sheetalyawalkar@gmail.com