International Journal of Cryptography and Security
ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, 2012, pp.-18-21.
Available online at http://www.bioinfo.in/contents.php?id=115

A REVIEW PAPER ON COMPARISON AND ANALYSIS OF DIFFERENT ATTACK AND INTRUSION DETECTION SYSTEM

KATHOLE A.B., PARDAKHE N.V., KUTE D.S. AND PATIL A.S.

J.D.I.E.T., Yavatmal, MS, India.
*Corresponding Author: Email- atul.kathole1910@gmail.com.

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- Wireless networks are gaining popularity to its peak today, as the user's wants wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Mobile Ad Hoc Network (MANET) has become an exciting and important technology in recent years, because of the rapid proliferation of wireless devices. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. Intrusion-Detection Systems aim at detecting attacks against computer systems and networks or in general, against information systems. IDS can be viewed as a guard system that automatically detects malicious activities within a host or network. In this paper we have studied about MANET, various characteristics and applications of MANET, also studied the black hole, wormhole and DOS attack, and analyzed Comparison between different Intrusion Detection Systems in MANET .
Keywords- Network, MANET, Attacks, Intrusion Detection System.

Citation: Kathole A.B. et al. (2012) A Review Paper on Comparison and Analysis of Different Attack and Intrusion Detection System. International Journal of Cryptography and Security, ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, pp.-18-21.

Introduction

Network- Any collection of devices/ computers connected with each other by means of communication channels that help the users to share resources and communicate with other users. There are two main types of network i.e. wired network and wireless network.

Wired Network- Wired network are those network in which computer devices attached with the help of wire.

Wireless Network- A network in which, computer devices communicates with each other without any wire.

Why Wireless Network- Wireless networks are getting popular due to their ease of use. Consumer/user is no more dependent on wires where he/she is, easy to move and enjoy being connected to the network. One of the great features of wireless network that makes it fascinating and distinguishable amongst the traditional wired networks is mobility. This feature gives user the ability to move freely, while being connected to the network. Wireless networks comparatively easy to install than wired network. There is nothing to worry about pulling the cables/wires in wall and ceilings. Wireless networks can be configured according to the need of the users. These can range from small number of users to large full infrastructure networks where the number of users is in thousands.

Mobile Ad hoc Networks

Mobile ad hoc network is an autonomous system, where nodes/ stations are connected with each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. Mobile ad hoc network topology is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. This property

of the nodes makes the mobile ad hoc networks unpredictable from the point of view of scalability and topology.

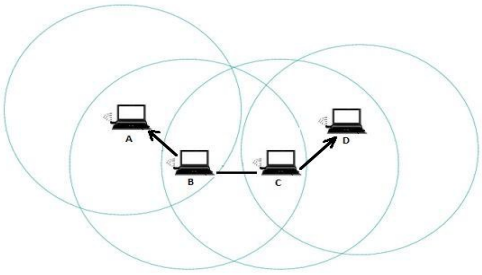

Fig. 1- Mobile Ad Hoc Network

Characteristics of MANETs

When a node wants to communicate with another node, the destination node must lies within the radio range of the source node that wants to initiate the communication. The intermediate nodes within the network aids in routing the packets for the source node to the destination node. These networks are fully self organized, having the capability to work anywhere without any infrastructure. Nodes are autonomous and play the role of router and host at the same time. MANET is self governing, where there is no centralized control and the communication is carried out with blind mutual trust amongst the nodes on each other. The network can be set up anywhere without any geographical restrictions. One of the limitations of the MANET is the limited energy resources of the nodes.

Applications of MANETs

The properties of MANET make it so much favorable that would bring so many benefits. There are so many research areas in MANET which is under studies now. The most important area is vehicle to vehicle communication. Where the vehicle would communicate with each other, keeping a safe distance between them as well as collision warnings to the drivers. MANET can be used for automated battlefield and war games. One of the most important areas where MANETs are applied is emergency services such as disaster recovery and relief activities, where traditional wired network is already destroyed. There are so many other application areas such as entertainment, education and commercial where MANETs are playing their role for connecting people.

A. Attacks

i. Blackhole 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 blackhole 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.

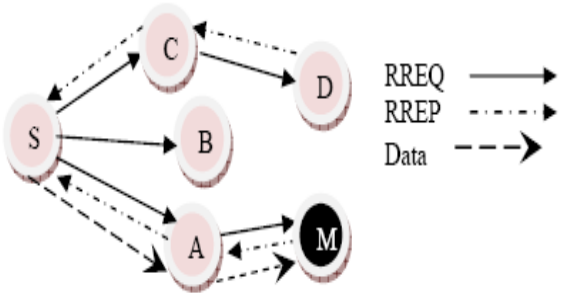

Fig. 2- Black hole attacks in MANETs

In figure 2, source node S wants to send data packets to a destination node D in the network. Node M is a malicious node which acts as a black hole. The attacker replies with false reply RREP having higher modified sequence number. So, data communication initiates from S towards M instead of D.

ii. Wormhole Attack

A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high-speed off-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.

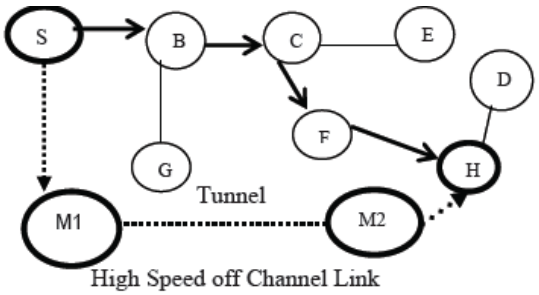

Fig. 3- MANET with a wormhole attack

iii. 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. Determining the source generating attack traffic is especially difficult when using stateless routing protocols (as in the Internet or geographic routing). Attackers routinely disguise their location using incorrect, or "spoofed", source address.

Classification of IDS Systems
Intrusion detection can be classified into three broad categories: Anomaly Detection, Signature or Misuse Detection, and Specification based Detection.

1. Anomaly Detection
In an anomaly detection system a baseline profile of normal system activity is created. Any system activity that is a deviation from the baseline is treated as a possible intrusion. The problems with strict anomaly detection are that

1. Anomalous activities that are not intrusive are flagged as intrusive.
2. Intrusive activities that are not anomalous result in false negatives.

One disadvantage of anomaly detection for mobile computing is that the normal profile must be periodically updated and the deviations from the normal profile must be computed. The periodic calculations can impose a heavy load on some resource constrained mobile devices and perhaps a light-weight approach that involves comparatively less compute might be better suited.

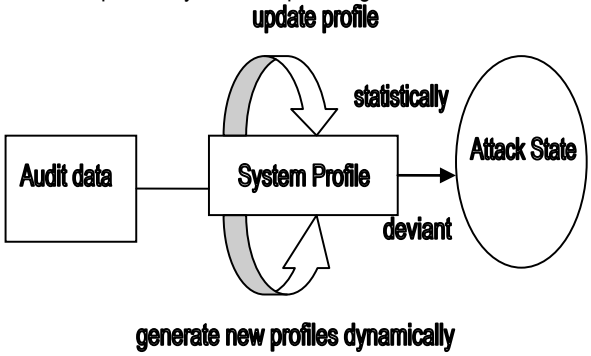

Fig. 4- Anamoly Detection System

2. Misuse Detection
In misuse detection, decisions are made on the basis of knowledge of a model of the intrusive process and what traces it ought to leave in the observed system. Legal or illegal behavior can be defined and observed behavior can be compared accordingly. Such a system tries to detect evidence of intrusive activity irrespective of any knowledge regarding the background traffic, i.e. the normal behavior of the system.

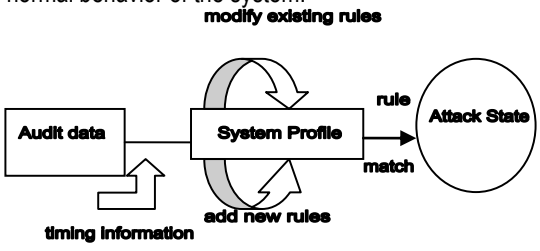

Fig. 5- Misuse Detection System

3. Specification Based Detection
Specification-based detection defines a set of constraints that describe the correct operation of a program or protocol, and monitors the execution of the program with respect to the defined constraints. This technique may provide the capability to detect previously unknown attacks, while exhibiting a low false positive rate.

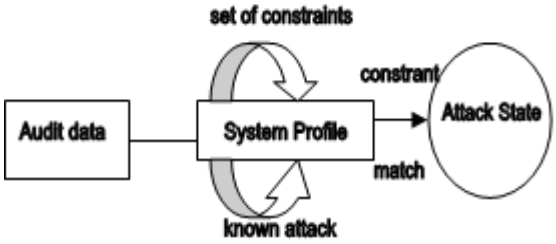

Fig. 6- Specification based detection

An offshoot to misuse and anomaly detection is compound detection which is basically a misuse inspired system that forms a compound decision in view of a model of both the normal behavior of the system and the intrusive behavior of the intruder. The detector operates by detecting the intrusion against the background of the normal traffic in the system. These detectors have a much better chance of correctly detecting truly interesting events in the supervised system, since they both know the patterns of intrusive behavior and can relate them to the normal behavior of the system.

Requirements
Some papers suggested IDS, which is one of the best solutions instead of intrusion protection against intruders on MANET. The traditional way (firewall and cryptography) are designed for known attacks and also each of these techniques comes with overhead and complexity. Unlike firewall that is the first line of defense and monitors border nodes to detect the external attacks, IDS appears just after an intrusion has happened and a node or network has been compromised. On the other hand intrusion detection monitors internal attacks as well as external attacks; that is why IDS is called as the second line of defense.

- IDS should not introduce any weakness and overhead in the MANET.
- IDS detection should have a proper response.
- IDS should itself be fault-tolerant and resistant to attacks, especially denial-of-service attacks.
- IDS should use as little system resources as possible to detect and prevent intrusions.
- High accuracy of the IDS.

Conclusion
In this paper we studied the information about the network, concept of wired and wireless network, why use of wireless network. We also see the introduction about MANET and various characteristics and application of MANET. In this paper we have studied about the blackhole attack, wormhole and DOS attack, and analyzed different Intrusion Detection Systems in MANET. Intrusion-Detection Systems aim at detecting attacks against computer systems and networks, or, in general, against information systems .IDS can be viewed as a guard system that automatically detects malicious activities within a host or network. This paper also analyzes comparison between the different intrusion detection systems in the MANET. As security is big issue in MANET, this paper would be great help for the people who are conducting research for the problems in MANET.

References

[1] Rekha Pandit and Sanjeev Jain. *Analysis and Comparison of Different Intrusion Detection Systems in MANET*.

[2] Parsons M. and Ebinger P. *Performance Evaluation of the Impact of Attacks on mobile ad hoc networks*.

[3] Marti S., Giuli T.J., Lai K. and Baker M. (2000) 6*th Annual International Conference on Mobile Computing and Networking* (Mobicom), 275-283.

[4] Jani P.V. (2002) *Security within Ad Hoc Networks*, *Position Paper, PAMPAS Workshop*.

[5] Mishra A., Nadkarni K. and Patcha A. (2004) *IEEE Personal Communications*. 11, 48-60.

[6] Huang Y. and Lee W. (2004) *3th international conference on Distributed Computing systems*, 6, 1155-1168.

[7] Karygiannis A. and Antonakakis E. (2005) *IEEE International Conference in Pervasive Services*.

[8] Albers P., Camp O., Percher J., Bernard Ludovic and Puttini R. (2005) *1st Int'l. Wksp. Modeling, Evolution and Engineering, Massachusetts*.

[9] Rituparna Chaki and Nabendu Chaki (2005) 6*th International Conference on computer information and industrial mgmt application IEEE*.

[10] Buchegger S. and Le Boudee J.Y. (2005) *IEEE Communications Magazine*, 43(7), 101-107.

[11] Rebahi Y., Mujica-V V.E. and Sisalem D. (2005) 10*th IEEE Symposium on Computers and Communications*, 37-42.

[12] Aikaterini Mitrokosta and Nikos Komninos (2007) *IEEE Journal*.

[13] Bahareh Pahlevan zadeh and azman (2007) *International Conference on IEEE Telecommunication and Malaysia International Conference on Communication*.

[14] Roy D.B., Chaki R. and Chaki N. (2009) *International Journal of Network Security and Its Application*, 1(1).

[15] Raj P.N. and Swadas P.B. (2009) *IJCSI International Journal of Computer Science Issues*, 2.

C. Comparison Between IDS

Sr. No	Proposed System	Author	Methodology	Architecture	Highlights
1	Intrusion detection algorithm for manet	Rituparna Chaki Nabendu Chaki (2007)	The proposed IDSX offers an extended architecture and is compatible with heterogeneous IDS already deployed in the participating	Extended Architecture	The proposed solution virtually eliminates the problem of phantom intrusion detection to a great extent by aggregating the locally generated alerts to keep or discard a suspected intruder in a two step process. The anomaly based IDS solutions that are otherwise good in detecting both known and novel intrusions, but handicapped by high false alarm rates could be utilized in the lower level in the proposed two-step IDS approach.
2	A mechanism design-based multi -leader scheme for intrusion detection in MANET	Noman mohammed, Haldi atrok (2008)	The election of multiple leaders for intrusion detection in the presence of selfish nodes based on mechanism design theory.	The design of such incentives is based on the Vickrey, Clarke, and Groves (VCG) model by which truth-telling is the dominant strategy for each node	The following two advantages: First, collection of elected leaders is the optimal in the sense that the overall resource consumption will be balanced among all nodes in the network overtime Second, the scheme provides the leaders with incentives in the form of reputation so that nodes are encouraged to honestly participate in the election process. Simulation results show that our scheme can effectively prolong the overall lifetime of IDS in MANET and balance the resource consumptions among all the nodes
3	Intrusion detection with neural network & watermarking techniques for MANET	Aikaterini Mitrokosta (2007)	Neural network based combined with protection method which is based on water marking techniques	Self organizing map (SOM) Neural network	It exploits the advantages of the Lattice and the Block-Wise method in order to produce the most efficient and reliable results. The most sensitive part of the e SOM map that represents the existence of an attack in a node being the most sensitive part of the map is watermarked with the Block-Wise method and the rest of the map with the Lattice embedding method. The significant advantages of visual representation and watermarking, & advantages of eSOM and visual representation in order to achieve intrusion detection. Furthermore, For future work, the proposed intrusion detection engine can be employed to various routing protocols and used for the detection of various types of attacks as well as test it in real MANET applications.
4	Detecting Wormhole attacks in MANET through protocol breaking & packet timing analysis	Maria Gorlatora Peter C. Mason	Signal-processing detection method attack in an IPv6 802.1lb wireless Mobile Ad Hoc Network (MANET)	Test bed running a proactive routing protocol.	A certain percentage of the station's may drop traffic, or send the packets out issue of delays appearing in the message time series in heavy-load situations. Worm hole induce delay.