ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

A Survey on Intrusion Detection Systems in Mobile Ad Hoc Networks

Treesa Nice P. A.

Department of Computer Science and Engineering, Rajagiri School of Engineering and Technology, Ernakulam, India

Abstract: The mobile ad hoc networks (MANET) have been used in recent years, in many applications. They are more vulnerable to malicious attack. It is very tough to accomplish the complete security in the mobile ad hoc network. This is because of some of its unique characteristics. Besides the prevention methods, we need to detect and take necessary actions to provide the security to these types of networks. For this purpose we are using many intrusion detection systems (IDSs). In this paper, we have described the different characteristics of ad hoc networks and some of the attacks in ad hoc networks. Besides that, a comparative study about the existing IDSs is also presented.

Keywords: Ad hoc network, Anomaly detection, IDS Agent, Home Agent.

I. INTRODUCTION

A mobile ad hoc network is a collection of wireless mobile hosts forming a vibrant network infrastructure without any standard infrastructure or centralized administration.

Each node in its radio communication range can communicate with other nodes by using its wireless transmitter and receiver. In MANET, we can have multi-hop communication which means that in order for a node to forward a packet to a node that is out of its radio range, it has to cooperate with other nodes in the network. Therefore, each node must act as both a host and a router at the same time.

Intrusion means any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. Intrusion Prevention is the primary defense because the primary step is to make the systems safe from attacks by using passwords, biometrics etc. Even if intrusion prevention methods are used, the system may be subjected to some vulnerability. So we need a second wall of defense known as Intrusion Detection Systems (IDSs), to detect and produce responses if necessary.

Section 2 describes the different characteristics of mobile ad hoc networks. In section 3, the attacks in MANET are described. In section 4, the classification of IDSs is described. A comparison between existing IDSs is provided in section 5. Finally, conclusion is given in section 6.

II. CHARACTERISTICS OF AD HOC NETWORKS

The different characteristics of MANET includes lack of centralized administration, limited resources, dynamically changed network topology, wireless communication, limited power, limited bandwidth etc. Due to these features, mobile ad hoc networks are more vulnerable to attacks.

Dynamic Topology: Ad hoc networks require complicated routing protocols. Misbehaving node can generate wrong routing information which is very tough to discover. The devices' mobility also causes a problem.

Lack of Infrastructure: Ad hoc networks do not have any fixed infrastructure or centralized coordination. Therefore the traditional security mechanisms such as cryptography and certification are inapplicable.

Susceptibility of nodes: Physical protection of nodes is not possible. Hence they can be captured more easily and falls under the control of an attacker.

Susceptibility of channels: In wireless network, message eavesdropping and injection of fake messages into the network is easy without having physical access to network components. Denial of service is also possible here.

III. TYPES OF ATTACKS

Passive attacks and active attacks are possible in MANET. Passive attacks will not alter the data. It will just read the data and are destroy the confidentiality by eavesdropping. But in active attack, the data will be altered by attacker which includes modifying the data or injecting new malicious data. This involves overloading of network or preventing nodes from using the networks services effectively anymore.

Internal attack is the attack which comes from compromised node inside the network. External attack is the one in which unauthenticated attackers can replay old routing information

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

or inject false routing information to partition the network or increase the network load.

In unbalanced use of transmission channel one node tries to prevent other nodes in its neighbourhood from getting fair share of the transmission channel. Some of the possible methods for unfair use of the transmission channel are ignoring the MAC protocol, malicious flooding, overcrowding the transmission channel with garbage packets, ignoring the bandwidth reservation scheme, sleep deprivation (a node is forced to weaken its battery power) and network partition (a connected network is partitioned into sub-networks where nodes in different sub networks cannot communicate even through a route between them).

Anomalies in packet forwarding includes drop packets, delay packet transmission, Denial of Service, routing loop, fabricated route messages etc. Drop packets attack can be classified into two types: black hole attack in which a misbehaving node drops all types of packet and gray-hole attack in which an attacker selectively drops data packets. Wormhole attack is one in which a tunnel is created between two nodes that can be utilized to secretly transmit packets.

IV. CATEGORIZATION OF IDS

IDS can be categorized into two depending on the data collection mechanism and the detection techniques.

Types of IDS depending on the data collection mechanism includes Network based IDS (NIDS) and host based IDS (HIDS). Network-based IDS runs on a gateway of a network or on a router and captures and examines the network traffic that flows through it. It will be useful to detect attack from outside. This is not suitable for MANETs since there is no central coordination. A host-based IDS captures local network traffic to the specific host. It is better for detecting attack from inside.

Types of IDS based on detection technique includes signature or misuse based IDS, anomaly based IDS and specification based IDS. In signature or misuse based IDS a priori knowledge on intrusions is used. It can be used only to detect the known attacks. Its disadvantage is new attacks cannot be detected.

In anomaly based IDS, system keeps only the normal behaviour. It checks for deviation from normal behaviour. Any deviation can be considered as anomaly. The advantage is that it can discover unknown attacks.

In specification based IDS the system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints.

V. EXISTING IDS

In this section we will compare the different IDS which are in use commonly.

The different types of intrusion detection systems considered in this paper include Distributed IDS using mobile agents, A cooperative intrusion detection system for ad hoc networks [4], Agent based efficient anomaly intrusion detection system [1] [7], Intrusion detection of packet dropping attacks in mobile ad hoc networks, Distributed intrusion detection (FSM based distributed) [3] etc.

In agent based cooperative and distributive model, the following modules are described [4].

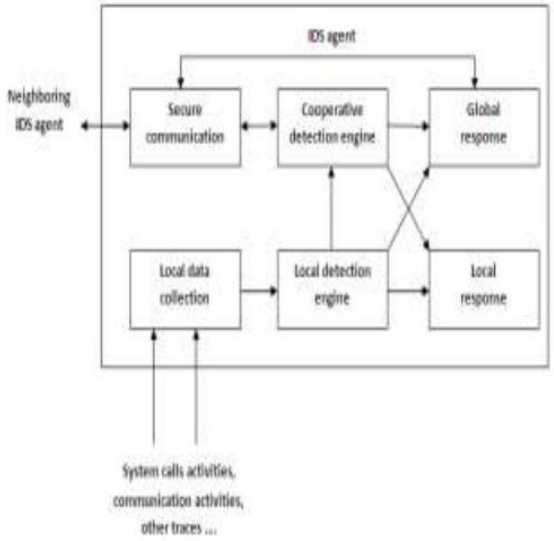

Fig. 1 Cooperative and Distributed Model

Home agent: Home agent is present in each system and it gathers information about its system from application layer to routing layer.

Current node: Home Agent is present in the system and it monitors its own system continuously. If an attacker sends any packet to gather information or broadcast through this system, it calls the classifier construction to find out the attacks. If an attack has been made, it will filter the respective system from the global networks.

Neighbouring node: Any system in the network transfer any information to some other system, it broadcast through intermediate system. Before it transfer the message, it send mobile agent to the neighbouring node and gather all the information and it return back to the system and it calls classifier rule to find out the attacks. If there is no suspicious activity, then it will forward the message to neighbouring node.

Data collection: Data collection module is included for each anomaly detection subsystem to collect the values of features for corresponding layer in a system. Normal profile is created using the data collected during the normal scenario. Attack data is collected during the attack scenario.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

Data pre-process: The audit data is collected in a file and it is smoothed so that it can be used for anomaly detection. Data pre-process is a technique to process the information with the test train data.

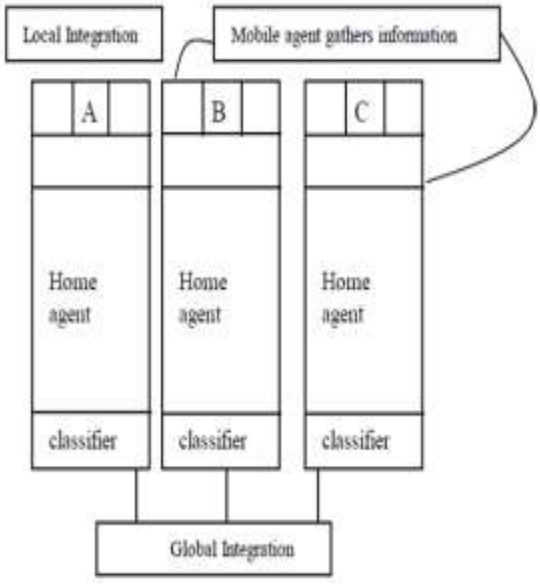

Fig. 2 Agent Based Cooperative and Distributed Model

Agent Based Cooperative and Distributive Model DIDS using multiple sensors by Kachirski and Guha in 2002 have given a distributed algorithm [11]. This multi-sensor intrusion detection system based on mobile agent technology is divided into three main modules. These mobile agents have some functionality such as monitoring, decision making or initiating a response. It divides functional tasks into categories and assigning each task to a different agent, the workload is distributed which is suitable for the characteristics of ad hoc networks. In the following figure, the distributed intrusion detection system (DIDS) using multiple sensors and the three different mobile agents such as action agent, decision making agent and monitoring agent are shown.

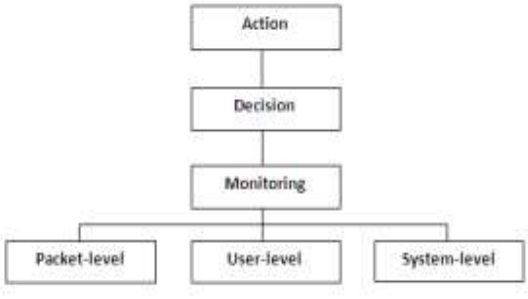

Fig. 3 DIDS Using Multiple Sensors

DIDS Using Multiple Sensors Monitoring agent: Functions of this agent is network monitoring and Host monitoring. A host- based monitor agent hosting system-level sensors and user-activity sensors is run on every node to monitor within the node. A monitor agent with a network monitoring sensor run only on some selected nodes to monitor at packet-level to capture packets going through the network within its radio ranges.

Action agent: Every node also has this action agent. Since every node hosts a host-based monitoring agent, it can determine if there is any suspicious or unusual activities on the host node based on anomaly detection. When there is strong evidence supporting the anomaly detected, this action agent can initiate a response, such as terminating the process or blocking a user from the network.

Decision agent: The decision agent run only on those nodes on which network monitoring agents are running. These nodes collect all packets within its radio range and analyse them to determine whether the network is under attack.
If the local detection agent not able to make a decision on its own due to unsatisfactory evidence, it reports to the decision agent. Further investigation is done by using packet-monitoring results that comes from the locally running network monitoring sensor. If the decision agent concludes that the node is malicious, the action module of the agent running on that node will carry out the response. The network is logically divided into clusters with a single cluster head for each cluster.

This cluster head will monitor the packets within the cluster whose originators are in the same cluster are captured and investigated. That is the network monitoring agent and the decision agent run on the cluster head. The decision agent performs the decision making based on its own collected information from its network-monitoring sensor; thus, other nodes have no influence on its decision. This way, spoofing attacks and false accusations can be prevented.

We will consider the algorithms used in each of these IDS, advantages and disadvantages.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

TABLE I
COMPARISON

Topic	Algorithm	Advantage	Disadvantage
Distributed IDS using mobile agents	Mobile agent based (independently & cooperatively)	Better n/w performance	
Agent Based Efficient Anomaly Intrusion Detection System	Agent based cooperative and distributive	Better performance compared to other algorithms, Low false alarm rate	No description about security of mobile agents
Local IDS	Mobile agent based distributed anomaly detection Independent decision making	Use SNMP data located in MIB to process data, transmit SNMP requests to remote hosts to overcome unreliability of UDP by using mobile agent, Cost of local information collection is negligible by running SNMP agent on each node	
A cooperative Intrusion Detection System for Ad Hoc Networks	Cluster based distributed detection scheme	Being cluster based, improves the efficiency of IDS in terms of memory usage and network overhead	Need to prevent a compromised node be elected as cluster head, Not mentioned about false alarm rate
Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Networks	Neural network based distributed detection	Identify the source of the packet dropping attack Able to identify new attack	Classes of the trained data have to be defined manually Continuously updating trained matrix
Distributed Intrusion Detection (FSM based distributed)	Cluster based distribute IDS	Good detection rate	FSM is created manually to detect behaviour of nodes
IDS based on a static stationary database (SSD)	Mobile agent anomaly, misuse and hybrid Independent decision making	Use of SSD limits communication with IDS agent Periodically up to date with non-mobile database	

VI. CONCLUSION

Ad hoc networks are an increasingly promising area of research with lots of practical applications. However, MANETs are vulnerable to attacks, due to their dynamically changing topology, absence of centralized infrastructures and open medium of communication. Due to this vulnerability, intrusion prevention methods such as authentication and encryption are not able to eliminate the attacks. Only reduces the attacks. Anomaly detection is more powerful among the various detection methods used. In this paper we have presented the characteristics of MANET, attacks in MANET and comparison of existing IDSs.

ACKNOWLEDGMENT

First of all I want to thank the God Almighty for showering blessings on me in preparing this paper. Then I thank my family members. I thank my teachers for guiding me. Last, but not least I thank my friends for giving me support for doing this work.

REFERENCES

[1] R. Nakkeeran, T. Aruldoss Albert. R. Ezumalai, "Agent Based Efficient Anomaly Intrusion Detection System in Ad hoc networks", IACSIT International Journal of Engineering and Technology Vol. 2, February, 2010
[2] Zougagh Hicham, Toumanari Ahmed, Latif Rachid Idboufker Noureddin, "Evaluating and Comparison of Intrusion in Mobile Ad Hoc Networks", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.2, March 2012
[3] Farhan Abdel-Fattah, Zulkhairi Md. Dahalin, Shaidah Jusoh, "Distributed and Cooperative Hierarchical Intrusion Detection on MANETs", International Journal of Computer Applications Volume 12, December 2010
[4] Yi-an Huang, Wenke Lee,"A Cooperative Intrusion Detection System for Ad Hoc Networks", Mobile Networks and Applications (2003)
[5] Amitabh Mishra, Ketan Nadkarni, Animesh Patcha, "Intrusion Detection in Wireless Ad Hoc Networks", IEEE Wireless Communic-ations, Feb 2004
[6] Xia Wang, "Intrusion Detection Techniques in Wireless Ad Hoc Networks", Proceedings of the 30th Annual International Computer Software and Application Conference 06

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

[7] Abolfazl Esfandi, "Efficient Anomaly Intrusion Detection System in Ad hoc Networks by Mobile Agents", IEEE 2010
[8] R.Saminathan, Dr.K.Selvakumar, "PROFIDES - Profile based Intrusion Detection Approach Using Traffic Behaviour over Mobile Ad Hoc Network", International Journal of Computer Application Vol.7, Oct 2010
[9] Yongguang Zhang, Wenke Lee, Yi-An Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", Mobile Networks and Application 2003
[10] Foong Heng Wai, Yin Nwe Aye, Ng Hian James, "Intrusion Detection in Wireless Ad-Hoc Networks", Introduction to Mobile Computing.
[11] O. Kachirski and R. Guha,"Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks" Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p. 57.1, January 2003.
[12] Levente Butty, Jean-Pierre Hubaux, "Report on a Working Session on Security in Wireless Ad Hoc Networks", Mobile Computing and Communications Review, Volume 6, No: 4
[13] Pin Nie,"Security in Ad hoc Network", 2006.
[14] Ioanna Stamouli,"Real-time Intrusion Detection for Ad hoc Networks", in 2003
[15] Ricardo Puttini, Jean-Marc Percher,"A Fully Distributed IDS for MANET", in 2007.
[16] Rajendra Prasad Mahapatra, Tanvir Ahmed Abbasi, "Real Time Intelligent Intrusion Identification in Wireless Ad hoc Networks", International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010
[17] Shengrong Bu, *F. Richard Yu*, Xiaoping P. Liu, *Helen Tang*, "Intrusion Detection in High Security Mobile Ad-Hoc Networks", IEEE Transactions on wireless communications, Vol. 10, No. 9, September 2011
[18] John Felix Charles Joseph, Bu-Sung Lee, Amitabha Das, Boon-Chong Seet, "Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks", IEEE Transactions on dependable and secure computing, Vol. 8, No. 2, March-April 2011
[19] Mohsenguizani, "Security in wireless mobile ad hoc and sensor networks", IEEE Wireless Communications, October 2007
[20] Farooq Anjum, Anup K. Ghosh, "Security in Wireless Ad Hoc Networks", IEEE Journal on selected areas in communications, Vol. 24, No. 2, February 2006
[21] Zhang, Lee, Yi-An Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", IEEE Transactions on wireless communications
[22] Y. Zhang and w. Lee, "Intrusion Detection in Wireless Ad Hoc Networks", 6th Int'l. Conference on Mobile Computing and Networking. Aug.2000