Leena Sahu *et al*, International Journal of Computer Science and Mobile Applications,
Vol.1 Issue. 1, July- 2013, pg. 24-30 **ISSN: 2321-8363**

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND MOBILE APPLICATIONS - IJCSMA

A Cooperative Approach for Understanding Behavior of Intrusion Detection System in Mobile Ad Hoc Networks

Leena Sahu[1], Chaitali Sinha[2]
[1]M.Tech Scholar
[2]Reader

leena1220@gmail.com[1], chaitali.choudhary@gmail.com[2]

Abstract

In recent years, the use of mobile ad hoc networks (MANETs) has been widespread in many applications and security has become one of the major concerns in MANETs. An Ad-hoc network is one that is an autonomous, self-configuring network made up of mobile nodes connected via wireless links. The mobile or portable devices are free to move at any rate/direction and are part of the network only when they are within range and due to these unique characteristics of MANETs, prevention methods alone are not sufficient to make them secure. Hence there is a strong need of Intrusion detection systems as a second line of defense for securing MANET. Most intrusion detection systems for mobile ad hoc networks are focusing on either routing protocols or its efficiency, but it fails to address the security issues. In this paper, we classify and discuss the various attacks, techniques used for intrusion detection are discussed and general issues that should be considered while implementing in intrusion detection system in Mobile Ad hoc Network (MANET) to provide high performance to the network.

Keywords*:* Intrusion Detection System (IDS); Mobile Agents; Mobile Ad-Hoc Network(MANET); Network Security

1. Introduction

Mobile Ad hoc Network are wireless networks or a collection of mobile hosts that communicate without fixed infrastructure based on the cooperation of independent mobile nodes. Each node in MANET can act as router as well as host. The proliferation of these networks and their use in critical scenarios (like battlefield communications or vehicular networks) require new security mechanisms and policies to guarantee the integrity, confidentiality and availability of the data transmitted.

Due to the nature of mobility for mobile networks needs additional mechanism for providing security. These vulnerabilities do not exist in a fixed wired network. Therefore, the traditional way of protecting networks with firewalls and encryption software is no longer sufficient. So there is a need to develop new architecture and mechanisms to protect the wire-less networks and mobile computing applications.

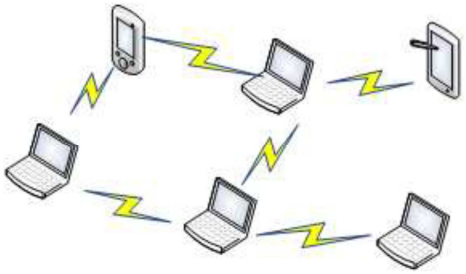

Fig. 1. Ad hoc architecture using IEEE 802.11 IBSS

1.1 Intrusion Detection System (IDS)

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system for the detection of such intrusions. Intrusion detection systems (IDS) are an important component of a network security infrastructure. It collects and analyzes audit data looking for anomalous or intrusive activities. As soon as suspicious event is detected an alarm is raised, so that the network administrator can react by applying suitable countermeasures.

There are three main components[1] of IDS: data collection, detection, and response.
In *Data collection* module collection and pre-processing of data are done i.e. transferring data to a common format, data storage and sending data to the detection module. Different data sources can be used as inputs in IDS: System logs, network packets, etc.. In the *detection component* data is analyzed to detect intrusion attempts and indications of detected intrusions are sent to the *response component*.
With respect to the source of data collected, IDSs are divided into host-based and network based. Host-based detector collect audit data from operating systems facilities, application logs, file information systems, etc., whereas network based detectors collect data from packets crossing a network segment.

IDSs can be further subdivided into further categories with respect to the implemented detection technique, namely Anomaly based intrusion detection system, Misuse or Signature based detection and Specification based detection IDS technique.

a) Anomaly Based Detection

Anomaly-Based IDS [10][5]examines ongoing traffic, activity, transactions and behavior in order to identify intrusions by detecting anomalies. It works on the notion that "attack behavior" differs enough from "normal user behavior" such that it can be detected by category and identifying the differences involved. This technique profiles the symptoms of normal behaviors of the system such as usage frequency of commands, CPU usage for programs, and the like. . Various techniques have been applied for anomaly detection, e.g. statistical approaches and artificial intelligence techniques like data mining and neural networks. The most difficult task is defining a normal behavior, as it can be change with time, so the system must be kept updated .Such techniques are capable of detecting previously unknown attacks and this is very important in an environment where new attacks and new vulnerabilities of systems are announced constantly but have high false positive alarms if database is not updated

b) Misuse or Signature Based Detection

It is generally preferred by commercial IDSs since it is efficient and has a low false positive rate. Signature-Based IDS [3][5]use a rule set to identify intrusions by watching for patterns of events specific to known and documented attacks. It is typically connected to a large database which houses attack signatures. It

compares the information it gathers against those attack signatures to detect a match. These types of systems are normally presumed to be able to detect only attacks "known" to its database. Thus, if the database is not updated with regularity, new attacks could slip through. It can, however, detect new attacks that share characteristics with old attacks. Also, signature based IDS's may affect performance in cases when intrusion patterns match several attack signatures. In cases such as these, there is a noticeable performance lag. Signature definitions stored in the database need to be specific so that variations on known attacks are not missed.

c) Specification Based Detection

In *specification-based intrusion detection*, a set of constraints on a program or a protocol are specified and intrusions are detected as runtime violations of these specifications. It combines the strengths of anomaly-based and misuse-based detection techniques, providing detection of known and unknown attacks with a lower false positive rate . It can detect new attacks that do not follow the system specifications. Moreover, it does not trigger false alarms when the program or protocol has unusual but legitimate behaviour, since it uses the legitimate specifications of the program or protocol . It has been applied to ARP (Address Resolution Protocol), DHCP (Dynamic Host Configuration Protocol) and many MANET routing protocols. Defining detailed specifications for each pro-gram/protocol can be a very time consuming job. New specifications are also needed for each new program/protocol and the approach cannot detect some kind of attacks such as DoS (Denial of Service) attacks since these do not violate pro-gram specifications directly.

On the basis of various intrusion detection techniques, when intrusion is detected, an appropriate response mechanism is triggered accordingly. Responses to detected intrusions can be passive or active. In passive responses an alarm raises and a notification is given to the proper authority. In active responses, it tries to mitigate effects of intrusions and are divided into two groups: those that seek control over the attacked system, and those that seek control over the attacking system. The former tries to restore the damaged system by killing processes, terminating network connections, and the like. The latter tries to prevent attacker's future attempts, which can be necessary for military applications.

Overall the observations made that any intrusion detection system should have some characteristics or constraints, they are:

- The systems generally cover restricted sets of attacks.
- The systems usually target a specific protocol.
- Some proposed IDS systems do not take into account mobility of the network.
- Inadequate acknowledgement is given to the resource constraints that many nodes are likely to be subject to, and to the likelihood of nodes with different capabilities.
- Several network architectures proposed do not sit well with the dynamic nature of MANETs.
- A more extensive evaluation of many of the systems would seem appropriate.

1.2 Architecture of IDS in MANET

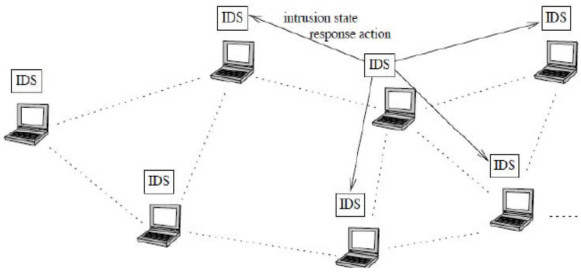

Fig 2: Architecture of IDS in MANET

Intrusion detection system can be configured based on the infrastructure of the network .Some architectures are discussed here

Standalone IDS: In this architecture, the IDS runs on every node in order to detect the intrusions independently. In the IDS running on the network they do not cooperate and no data is exchanged among them .When we have flat network infrastructure this architecture is more suitable to be used.

Distributed and collaborative IDS: In this type of architecture that every node in the MANET must participate in intrusion detection and respond by having an IDS agent running on them. The IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently.

Hierarchal IDS: In this architecture, the multi-layered network infrastructure is proposed where the network is divided into clusters, the cluster heads acts as a control points similar to switches ,routers or gateways in wired networks . The mobile agent for IDS architecture uses mobile agents to perform specific task on a node on behalf the agents. This architecture allows the distribution of the intrusion detection tasks. There are several advantages using mobile agents [7][8], for intrusion detection.

1.3 General Issues with Intrusion Detection System

Most of the Intrusion detection system suffers [3] from some common problem that may arise are:

First, the information that is used by the IDS is obtained from audit trails or from packets from a network. Data from origin to the IDS travels a long path and during that data may be potentially destroyed or modified by the attacker. Hence due to this, result may be misinterpreted by the IDS. This problem is referred to as ***fidelity problem***.

Second, Intrusion detection system continuously monitors the network even when there is no intrusion hence uses additional resources .This problem is ***resource usage problem.***

Third, the components of IDS are implemented as separate programs, they are susceptible to tampering. An intruder can potentially disable or modify the program ms running on a system, rendering the intrusion detection system useless or reliable. This is the ***reliability problem.***

As MANET has no centralized administration where the nodes communicate on the basis of mutual trust and this characteristic make it more vulnerable to be exploited by an attacker inside the network. Mobile nodes present within the range of wireless link can overhear and even participate in the network. In order to provide secure

communication and transmission, different types of attacks and their effects on the MANETs need to be understood first. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from.

2. Attack in Mobile Ad Hoc Networks

Based on consequences and techniques MANET can be classified as:

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, in black hole attack , a misbehaving node all type of packets(data and control packets both)
Routing loops: cause a loop in routing path.
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
Network partition: the network is divided into sub networks where nodes cannot communicate each other even though path exists between them.

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 is accepted by the recipient. The attacker can block legitimate messages that arrive later by distributing a false control message.
Wormhole: A tunnel (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).

3. Intrusion Detection using Agents

Intrusion detection can be done by various ways some using agent technology and others without using agents. In this paper the focus is on mobile agents[4], since the intrusion detection system without using agents has some limitations, some of them are central control, high false positive rate, configuration problem and non-scalable.

Some advantages of using mobile agents are that they can respond faster as they are directly dispatched from the central controller to the target host. By using mobile agents[17], the network load can be reduced as these mobile agents employ efficient search mechanisms there by reducing the necessity for data traffic among several hosts. As mobile nodes operate autonomously and asynchronously, they are not prone to failure even if the machine, which hosted them, fails. This provides added advantage of employing mobile agents in IDS. Mobile agents can be used in IDS with a flexible structure. Cloning, dispatching and sleeping of mobile agents can be done when the network configuration has to be changed. Also they can sense their execution environment and dynamically adapt to the situation. The mobile agents can be used on several different platforms without compatibility problems and even if one of the agents fails, the other agents in the IDS can take up the tasks of the failed agent and continue the

detection. Agents have the capability to clone and distribute themselves to the new machines when they are added to the network.

Drawbacks in using mobile agents are when a mobile agent[17] initiates a response it requires an administration rights. By granting a mobile agent all permissions to the host it is operating on, an intruder can easily induce any virus. Some hosts might also try to get the private information from the mobile agents, which contain client details. Observing the manner in which, the network attacks are increasing, it becomes necessary on IDS to detect attacks immediately and report them spontaneously. If mobile agents are used to accomplish this, the result is that it reduces the performance of the entire network.

Other Techniques for Intrusion detection are the Watchdog/PathRater [18] which is a solution to the problem of selfish (or "misbehaving") nodes and to mitigate the effects of routing misbehaviour in MANET. The PathRater, respond to the intrusion by isolating the selfish node from the network operation and the watchdog detects the misbehaving nodes. Each node runs watchdog , whenever a node forwards a packet ,the watchdog module of that node verifies the node to which packet is send also forwarded that packet and this is done by listening in promiscuous mode to the next node's transmissions. If the next node did not forwarded the packet , the node is considered as misbehaving and by sending an alarm message to other nodes in friend list misbehaviour is reported . The Other nodes that receive alarm checks whether the alarm source is fully trusted and same node is accused by several partially trusted nodes and act accordingly. If the watchdog module detected misbehaviour is not source node for the packets, then a message to source is send identifying the misbehaving node .The PathRater module uses the information generated by watchdog to select a better route to deliver the packets, avoiding the selfish nodes.

4. Conclusion

This paper elaborates the foundations for the development of the intrusion detection system along with their operational architectures and also presents a classification based on the type of processing that is related to the "behavioural" model for the target system. This study also describes the main features of several IDS's systems/platforms that are currently available in a concise manner. The most significant open issues regarding Intrusion Detection systems are identified and the techniques that can be used to design the system. The presented information constitutes an important point to start for addressing Research & Development in the field of IDS. Countermeasures which are faster and more effective are needed to cope up with the attacks ever-growing. On the whole, this paper confirms a common trend in the experimental computer science.

References

[1] E. Lundin and E. Jonsson. Survey of intrusion detection research. Technical Report 02, Department of Computer Engineering, Chalmers University of Technology, 2002.

[2] Y. Zhang and W. Lee. Intrusion Detection in Wireless Ad-hoc Networks. In *Proceedings of the* 6*th International Conference on Mobile Computing and Networking*, Boston, MA, August 2000.

[3] B. DeCleene, *et al*. 2001. Secure group communications for wireless networks. IEEE Military Communications Conference.

[4]" Mobile agents-based intrusion detection system for Mobile ad hoc networks "2010 International Conference on Innovative Computing and Communication and 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering 2010 IEEE p-145

[5] Zhang Y, Lee W (2000), Intrusion Detection in Wireless Ad Hoc Networks. In Proc of the 6th Int Conf on Mobile Computer and Network (MobiCom): 275-283

[6] M. Esposito and C. Mazzariello, *et al*. 2005. Evaluating Pattern Recognition Techniques in Intrusion Detection Systems. The 7th International Workshop on Pattern Recognition in Information Systems. pp. 144-153.

[7] C. Krugel and T. Toth. 2001. Applying mobile agent technology to intrusion detection. In: ICSE Workshop on Software Engineering and Mobility.

[8]S. Marti, T.J. Giuli, K. Lai and M. Baker. 2000. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In: 6th International Conference on Mobile computing and Networking, OBICOM'00. pp. 255- 265, Aug.

[9]A.Mishra, K.Nadkarni and A.Patcha. "Intrusion Detection in Wireless ad hoc networks".IEEE Transaction on wireless Communications, vol. 11 no.1, pp48-60, FEB 2004.

[10]Shivarkar,Muzumdar,Dange "An improved approach for signature based and anomaly based Intrusion detection and prevention" International journal of computer and application,2010

[11] Abolfazl Esfandi "Efficient Anomaly Intrusion Detection System in Ad hoc Networks by Mobile Agents" 2010 IEEE proceedings.

[12]S.Hirnwal,**"**IntrusionDetection Technique in Mobile Ad hoc Network based on Quantitative Approach" International Journal of Computer Applications (0975 – 8887) Volume 37– No.8, January 2012

[13] T.Anantvalee ,J.Wu "A survey of Intrusion detection in MANET "wireless/Mobile network security, Springer, chapter 7, pp 170-196,2006

[14] [15]R.Nakkeeran, T. Aruldoss Albert and R.Ezumalai, "Agent Based Efficient Anomaly Intrusion Detection System in Ad-hoc networks" IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010

[16] Kruegel, C. and T. Toth. May 2001. Applying Mobile Agent technology to Intrusion Detection. In *ICSE Workshop on Software Engineering and Mobility*, Canada

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the ACM International Conference on Mobile Computing and Networking (MOBICOM)

