Comparison of different Mobile Agent Based Intrusion Detection Techniques

[1]Gurpreet Singh, [2]Dr. Jatinder Singh
[1]P.G. Department of Computer Science and IT., Khalsa College-Amritsar, Punjab, India
[2]Universal Institute of Engg. & Tech., Lalru-Chandigarh, Punjab, India

Abstract
The wireless ad hoc network is very common today, but the main issue is the security. There are many solutions provided by different researcher but still faces research challenges. The intrusion detection system is used for the security purpose but have some limitations for it. Mobile agent is the ideal behavior in the Intrusion Detection System. There are some various mobile agent techniques. In this paper we discuss the different techniques, comparisons of the techniques and tell more suitable for the intrusion detection.

Keywords
Intrusion Detection, Mobile Agents, Network Security, WLAN.

I. Introduction

The LAN network is very difficult to physically protect to the wireless network as in the case of wired network. The source of attacks from the opposition to a wireless network can be from the building, schools, colleges, office, several miles away, and the attack can come from anyplace. Some attacks are very harmful to the network when it is come into the network then it destroy the whole network or change the software coding. The risk is very high in wireless security then other case of security. Threats to wireless local area networks (WLANs) are various and potentially devastating. The Intrusion detection systems collect data and observe to recognize computer system and intrusions and mishandlings. In this paper we will discuss the various mobile agent intrusion detection techniques, comparisons of the techniques and tell more suitable for the intrusion detection.

1.1 Mobile Agents

A mobile agent is a software program that can be defined as autonomous executing programs to find the intrusion, move to another host, in a heterogeneous environment, without affected by the status of the originating node. A mobile agent execute the process and change from one node to another in a network and also change network to another network. This gives the agents the ability to communicate with one another, learn from their experience, and cooperate with each other.

1.2 Intrusions and Threats :

The dictionary defines an Intrusion as "The act of thrusting in, or of entering into a place or state without invitation , right or welcome." Or An intrusion is an active sequence of related events that deliberately try to cause harm, such as rendering system unusable, accessing unauthorized information, or manipulating information.[2] When someone stole, damage, misuse your data is called intrusion. Over the last several years, the definition, trends and styles of intrusions have been changing [7]. Intrusion profiles have enhanced from simple methods like tracing passwords, social engineering attacks [5], and exploiting simple software vulnerabilities to more sophisticated methods, like exploiting protocol flaws, defacing web servers, installing snifter programs, denial of service attacks or developing command and control networks using compromised computer to launch attacks. In addition to direct attacks and penetrations by humans (hackers or insiders), one of the additional rising problems in today's networks is the existence of malicious bots networks [10].

1.3 Intrusion & Intrusion Detection Systems

An intrusion-detection system (IDS) are software, tools, methods, and resources for detection, blocking and report unauthorized network activity.

1.3.1 Types of Intrusion Detection Systems

There are two primary types of IDS: host-based (HIDS) and network-based (NIDS).

1.3.2 Host-Based IDS

A HIDS resides on a particular host and looks for indications of attacks on that host. HIDS exists as a software process on a system. HIDS examines log entries for specific information. Periodically, the HIDS process looks for new log entries and matches them up to pre-configured rules. If a log entry matches a rule, the HIDS will alarm.

1.3.3 Network-Based IDS

A NIDS resides on a separate system that watches network traffic, looking for indications of attacks that traverse that portion of the network. NIDS exists as a software process on a dedicated hardware system. The NIDS places the network interface card on the system into promiscuous mode, the card passes all traffic on the network to the NIDS software. The traffic is then analyzed according to a set of rules and attack signatures to determine if it is traffic of interest. If it is, an event is generated [11].

1.4 A Wireless IDS

A Wireless IDS is like same as wired ids, distinctive features definite to WLAN intrusion and misuse detection when compared with standard, wired IDS.A wireless IDS assists to implement policy in addition to identifying attackers.
Wireless IDS are two types

1.4.1 Centralized wireless IDS

The former is generally a mixture of individual sensors collecting and forwarding all 802.11 data a central management system where the storing and processing of the wireless IDS data is performed, whereas, one or more devices that execute both the data gathering and processing/reporting functions of the IDS are typically comprised in the latter. The cost and management concerns restrict

1.4.2 Decentralized wireless IDS

The decentralized method has own storage device and the login users can handle all functions. It is used on the small WLANs.

II. Drawbacks of Wireless IDS

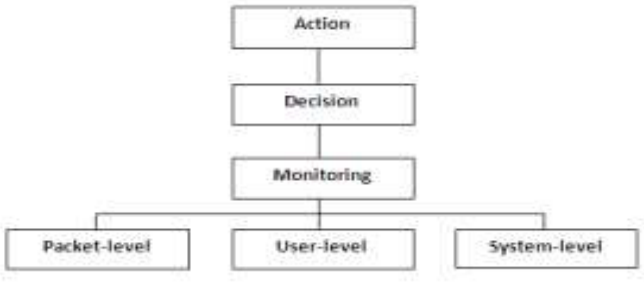
There are several drawbacks

1. Worse vulnerabilities which could potentially weaken the WLAN security. Wireless IDS technology is developing at a rapid pace though, and this caveat may not be a deterrent in the future.
2. A potential turn-off to a wireless IDS solution may be cost. Also, the cost of the wireless IDS solution will grow in conjunction with the size of the WLAN to be monitored, due to the requirement for a greater number of sensors. Therefore, the larger the WLAN, the more expensive the wireless IDS deployment will be.
3. Low performance : Because the intrusions are updated but when a ids make it is not work against the new intrusions. So it can not detect the intrusions.

III. Literature review

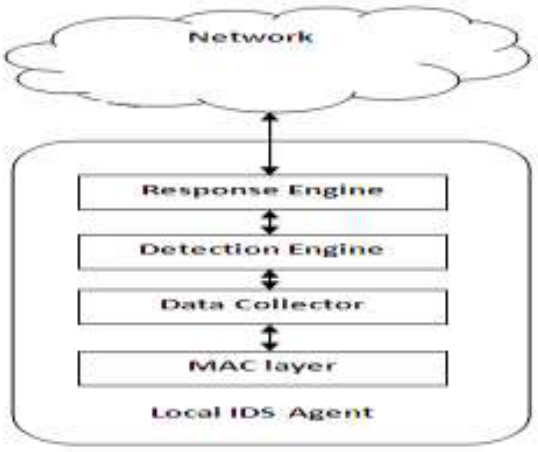
O.Kachirski [13] algorithm of distributed multi-sensor intrusion detection system based on mobile agent technology. In this algorithm the system has main three modules, each has there own work of mobile agent with some functions like : monitoring, decision making or initiating a response. These functional tasks divide into categories and assigning different agent. Monitoring agent: Network monitoring and Host monitoring are done by the agents of this class. 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 sensors 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 hosts 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 is run only on those nodes only which run network monitoring agents. These nodes collect all packets within its radio range and analyze
them to determine whether the network is under attack. Moreover, if the local detection agent not able to make a decision on its own due to unsatisfactory evidence, it reports to the decision agent for investigate further. This 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 clusterhead for each cluster. This cluster head will monitor the packets within the cluster
whose originators are in the same cluster are captured and investigated. This means that the network monitoring agent and the decision agent run on the clusterhead. In this mechanism, 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

According A. Mitrokotsa [10] proposed a distributed model. The proposed intrusion detection system is composed of multiple local IDSs agents. Each IDS agent is responsible for detecting possible intrusions locally. The collection of all the independent IDS agents forms the IDS system for the mobile wireless ad hoc network.

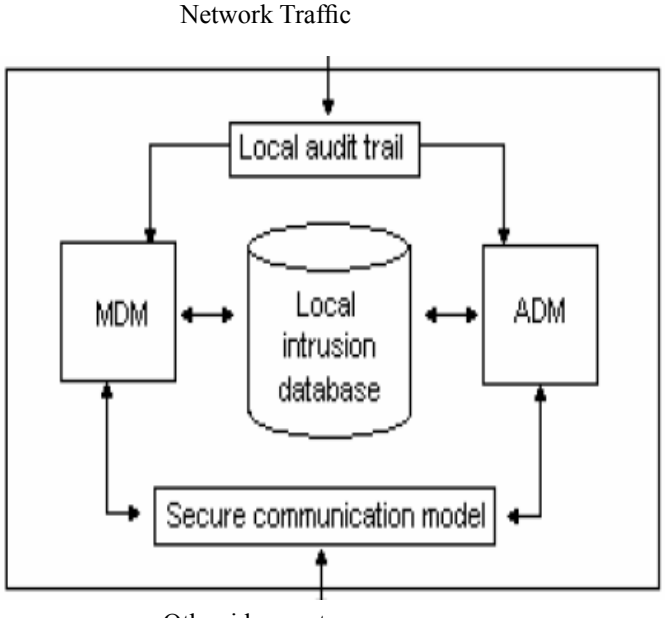


Each local IDS agent is composed of the following components:

Data Collector: Responsible for selecting local audit data and activity logs.
Detection Engine: Responsible for detecting local anomalies using local audit data. The local anomaly detection is performed using the eSOM classification algorithm. The procedure that is followed in the local detection engine is the one described below:
Select labeled audit data and perform the appropriate transformations. Compute the classifier using training data and the eSOM algorithm. Apply the classifier to test local audit data in order to classify it as Normal or Abnormal. Response Engine: If an intrusion is detected by the Detection Engine then the Response Engine is activated. The Response
Engine is responsible for sending a local and a global alarm in order to notify the nodes of the mobile ad hoc network about the incident of intrusion. Special attention should be paid on the function of the Response Engine in order to avoid possible flooding caused by the notification messages of intrusion. Thus, the broadcasted notification of intrusion is restricted to a few hops away from the node where the anomaly has been detected since the neighboring nodes run the greatest risk of possible intrusion. When the Response Engine is activated, the node fires a fake RTS (Ready to Send) message destined to the suspicious node. If the suspicious node replies to that packet then the node is classified as

malicious. Otherwise, the node fires an AODV ERROR message as the suspicious node is indicated as moved. After the discovery of the adversary the local IDS agent fires an ALERT message notifying its one hop neighbors. Alternatively, the local IDS agent could send ALERT messages to all potentially traffic generators that exist in its routing table, thus achieving a global response to all nodes that are directly influenced by the malicious node.

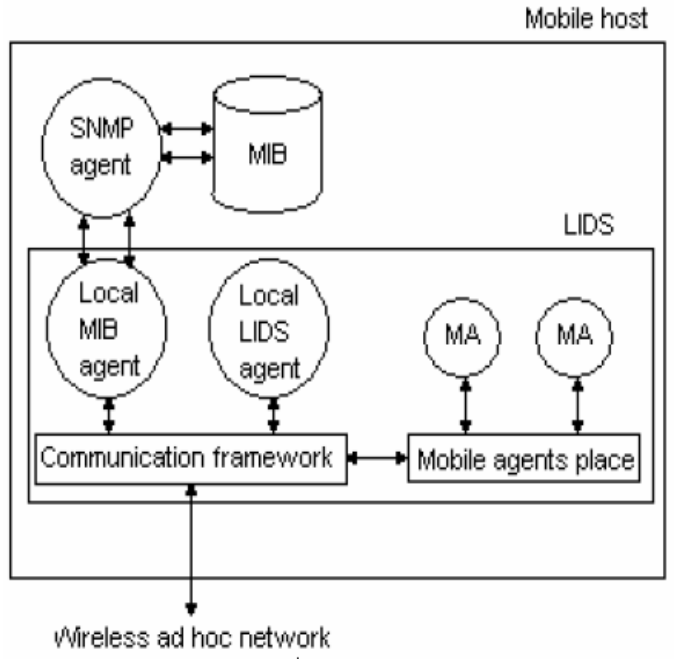
A.B. Smith [21] The architecture of this system has of two parts: mobile IDS agents which run on every node, and a stationary secure database that contains global signatures of known misuse attacks and stores patterns of each user's normal activity in a non-hostile environment. The IDS mobile agent's responsibility is to detect intrusions based on local audit data and participate in cooperative algorithms with other IDS agents to decide on attacks. Each agent consists of five parts: a local audit trail to collect audit data; local intrusion database to warehouse the necessary information for the IDS agent; secure communication module to enable different IDSs communication; anomaly detection modules to detect different types of anomaly; and misuse detection modules to detect different types of signatures. On the other hand, the stationary secure database acts as a secure trusted repository for the mobile nodes. Mobile nodes use this database to obtain information about the latest misuse signatures and find the latest patterns of normal user activity.



P. Albers [23] This system uses the collaborative work of mobile agents running on different nodes to make up for the complete intrusion picture. The architecture depends on the advantages offered by the Simple Network Management Protocol SNMP. Data used are those stored in the Management Information Base MIB of SNMP. Since SNMP uses UDP for communication, mobile agents are used to send requests to remote hosts to overcome the unreliability of UDP.
As the figure below shows several collecting agents work together in LIDS as follows:

• Local LIDS Agent: does local intrusion detection (misuse or anomaly) and response, and reacts to intrusion alerts by other nodes. As soon as a local LIDS detects an intrusion, it updates the other nodes of the network.

• Mobile Agents: transport SNMP requests to remote hosts to overcome the unreliability of SNMP message transfer over UDP. An LIDS can hand over a specific task to a mobile agent that it will achieve in an autonomous manner without any help from its LIDS. This comes in favor of MAHNs in which connections are not always reliable.



LIDS Architecture

IV. Comparison of different Intrusion Detection Techniques:

There are a lot of advantages and disadvantages of different mobile agent intrusion detection techniques. Differet techniques and there reference is shown in table 1 and comparison of these techniques is shown in table 2.

Table 1: References of different intrusion detection techniques.

Topic	Author name	Reference of the techniques
Distributed Intrusion detection system using mobile agent	Kachirski and Guha	MA 1
Intrusion detection system based on static stationary database	A.B. Smith	MA 2
Intrusion detection of packet dropping Attacks in Mobile Adhoc Network	A Mitrokotsa, R movropodi & C. Douligens	MA 3
Local Intrusion Detection System	P. Albers	MA 4

Table 2: Comparison Table of different mobile agent based Intrusion Detection Techniques.

Reference of the Techniques	Algorithm	Merits	Demerits	Based on	ID Method
MA 1	Mobile agent based cooperative and independently	1.Better performance in network	1. Only using the anomaly based detection method	Distributed Based	Anomaly
MA 2	Local audit data and participate in cooperative	1.Get information about latest misuse signature 2.Secure Network	1.No flexibility on MANET 2.Heavy computation on every node	layered Based	Signature
MA 3	Neural network based distributed mobile agent based detection	1.Ability to detect the new attack 2.To identify the packet dropping attack form the source point.	1. regular updating matrix. 2. The classes of the trained data have to write manually	Hybrid Based	Anomaly
MA 4	Simple Network Management Protocol	1.Suitable for MANET 2.Reduce communication overheads 3.Speed up Performance	1. it is not more suitable on WSN	Hybrid Based	Signature

V. Conclusion and Future Work

This paper is shown the comparison of four different mobile intrusion detection techniques. The analysis conducted in this paper over WAHNs IDS requirements and security challenges and the the mobile agents and their features show an exceptional promising match. Many of the features offered by mobile agents are just exact requirements of ideal WAHNs IDS. The only major disadvantage of mobile agents is their architectural inherited security vulnerabilities and performance. In spite of the novel ideas presented in the four mobile-agent based IDSs for WAHNs papers there still are other features that have not been fully utilized. In fact, fulfilling the ideal WAHNs IDS requirements could have been better achieved through superior deployment and incorporation of mobile agents. The next step of our research project is to sketch and implement new mobile-agent-based intrusion detection architecture that guarantees to suite WAHNs and at the same time enhance the performance of the mobile agent technique and achieves most of the advantages offered by other mobile agent and intrusion detection designs.

Reference

[1] Qiming Li, Ee-Chien Chang, Mun Choon Chan, " On the Effectiveness of DDoS Attacks on Statiscal Filtering", in proc. Of 24th Annual Joint Conference of IEEE Computer and communications societies, Vol. 2, pp: 1373-1383, 13-17 March2005, Doi: 10.1109/INFCOM.2005.1498362.

[2] pcmag.com-encyclopedia.

[3] H. Deng, W. Li, Dharma P. Agrawal, "Routing Security in Ad Hoc Networks," IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, October 2002.

[4] Y. Zhang, W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," Proceedings of the 6th International Conference on Mobile Computing and Networking, MobiCom 2000, pp.275-283, August 2000.

[5] Bishop Matt Malicious Logic [Book Section] // Introduction to Computer Security. - [s.l.] : Addison Wesley, 2005. - 0-321-24744-2.

[6] Mazda Salmanian, Julie H. Lefebvre, Steve Leonard, Scott Knight "Intrusion Detection in 802.11 Wireless Local Area Networks" Defense R&D Canada-Ottawa TECHNICAL MEMORANDUM DRDC Ottawa TM 2004-120, July 2004.

[7] CERT/CC Statistics 1988-2007 [Online] Available : // CERT Coordination Center. - 2007. - May 2008. - http://www.cert.org/stats/.

[8] H.BELLAAJ, REKTATA, A.HSINI, " Fuzzy approach for 802.11 wireless intrusion detection", in proc. of 4th international Conference: Science of Electronic, Technologies of Information and Telecommunications, March 25-29, Tunisia,2007.

[9] B. Schölkopf, J. Platt, J. Shawe-Taylor, A. Smola, "Estimating the support of a high-dimensional distribution," Neural Computation, v 13, no 7, pp. 1443-1472, 2001.

[10] Security Department of Homeland Cyber Security Research and Development [Report]. - [s.l.] : Department of Homeland Security, Science and Technologies Division, 2007.

[11] Jatinder Singh, Dr. Lakhwinder Kaur, Dr. Savita Gupta, "Analysis of Intrusion Detection Tools for Wireless Local Area", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7, July 2009.

[12] E. Eskin, A. Arnold, M. Prerau, "A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data," Data Mining for Security Applications, 2002.

[13] O. Kachirski, 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.

[14] K. Fall, Varadhanm, The ns Manual (formely ns Notes and Documentation), 2000.

[15] Stefan Schmidt, Holger Krahn, Stefan Fischer, Dietmar Watjen, " A Security Architecture for Mobile Wireless Sensor Network", in Proceeding of the First European Workshop on Security in Ad-Hoc and Sensor Networks, August 2004.

[16] S. Marti, T. Giuli, K. Lai, M. Baker, "Mitigating Routing Misbehavior in Mobile AdHoc Networks," Proceedings of the 6th International Conference on Mobile Computing and Networking (MOBICOM'00), pp.255-265, August 2000.

[17] Jelena Mirkovic, Max Robinson, Peter Reiher, George Oikonomou, " Distributed Defense Against DDoS Attacks", Technical Report CIS-TR-2005-02,CIS Department, University of Delaware,2005.

[18] Y. Zhang, W. Lee, Y. A. Huang, 'Intrusion Detection Techniques for Mobile Wireless Networks', ACM J. Wireless Net., vol. 9, no. 5, Sept. 2003, pp.545-56.

[19] AikateriniMitrokotsa, Rosa Mavropodi, Christos Douligeris,"Intrusion Detection of Packet Dropping Attacks inMobile Ad Hoc Network" TAyia Napa, Cyprus, July 6-7, 2006.

[20] Amitabh Mishra, Ketan Nadkarni, Animesh Patcha,Virginia Tech 'Intrusion Detection in Wireless Ad Hoc Networks', IEEE Wireless Communications, February 2004,pp. 48-60.

[21] A. B. Smith, "An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks," 5th Nat'l. Colloq. for Info. Sys. Sec. Edu, May 2001.

[22] Y. Huang, W. Fan, W. Lee, P. S. Yu, 'Cross-Feature Analysis

for Detecting Ad-Hoc Routing Anomalies',Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems, 2003, pp. 478-487.

[23] P. Albers et al., "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," 1st Int'l. Wksp. Wireless Info. Sys., Ciudad Real, Spain, Apr. 3–6, 2002.

[24] Krügel Christopher, Toth Thomas: A Survey on Intrusion Detection Systems. TU Vienna , Austria (2000) 7, 22–33

[25] Krügel Christopher, Toth Thomas: A Survey on Intrusion Detection Systems. TU Vienna , Austria (2000) 7, 22–33.

[26] L. Zhou, Z. J. Haas. Securing ah hoc networks. IEEE Network, 13(6):24{30, Nov/Dec 1999.

[27] Madge, (2005). Wireless intrusion detection systems (ids) evolve to 3rd generation proactiveprotection systems. Retrieved Apr. 06, 2006, [Online] Available : http://www.telecomweb.com/readingroom/Wi

[28] Jonathan P. Ellch Civilian, Federal Cyber Corps B.S., Purdue University, 2004 "FINGERPRINTING 802.11 DEVICES"ieeexplore.ieee.org/iel5/10599/33505/01592979.pdf?arnumber=1592979

[29] reless_Intrusion_Detection.pdf

[30] Martin Roesch, "SNORT-Lightweight intrusion detection for networks", Proceedings of LISA '99: 13th Systems Administration Conference Seattle, Washington, USA, November 7–12, 1999.

[31] Mike Chapple, "Snort The poor man's intrusion-detection system", [Online] Available : http://searchsecurity.techtarget.com.

[32] P. G. Neumann and P. A. Porras, "Experience with EMERALD to date," in Proc. Workshop Intrusion Detection Network Monitoring, Santa Clara, CA, Apr. 1999, pp.73–80