Distributed Intrusion Detection using Mobile Agent in Distributed System

Kuldeep Jachak
University of Pune,
P.R.E.C Loni,
Pune, India

Ashish Barua
University of Pune,
P.R.E.C Loni,
Delhi, India

ABSTRACT

Due to the rapid growth of the network application, new kinds of network attacks are emerging endlessly. So it is critical to protect the networks from attackers and the Intrusion detection technology becomes popular. There is tremendous rise in attacks on wired and wireless LAN. Therefore security of Distributed System (DS) is become serious challenge. One such serious challenge in DS security domain is detection of rogue points in network. Lot of work has been done in detection of intruders. But the solutions are not satisfactory. This paper gives the new idea for detecting rouge point using Mobile agent. Mobile agent technology is best suited for audit information retrieval which is useful for the detection of rogue points. Using Mobile agent we can find the intruder in DS as well as controller can take corrective action. This paper presents DIDS based on Mobile agents and band width consumed by the Mobile Agent for intrusion detection.

Keywords

Mobile Agent, Intrusion detection system, Distributed System, Rouge Point**.**

1. INTRODUCTION

The growing importance of network security is shifting security concerns towards the network itself rather than being host based. Security services must be evolving into network-based and distributed approaches to deal with heterogeneous open platform and support scalable solution [1]. The intrusion detection technology is the process of identifying network activity that can lead to a compromise of security policy. Intrusion Detection System (IDS) must analyze and correlate a large volume of data collected from different critical network access points. This task requires IDS to be able to characterize distributed patterns and to detect situations where a sequence of intrusion events occurs in multiple hosts [1]. Computer networks connected to Internet are always exposed to many kinds of cybercrimes. An Internet user with malicious intent can access, modify, or delete sensitive information present on other computers or make some of the computer services unavailable to other users. The infrastructure of current computer networks is so huge and complex that it is almost impossible to completely secure such networks. Therefore, an intrusion detection system (IDS) is needed to detect and respond effectively whenever the confidentiality, integrity, and availability of computer resources are under attack [2] Most of the current distributed IDSs use centralized Intrusion Detection (ID) models made of individual host and network monitors along with a centralized controller component. The individual monitors send intrusion data to the centralized controller component that performs analysis of the information it receives from each of the monitors. Some of the issues with the existing centralized ID models are:

- Additions of new hosts cause the load on the centralized controller to increase significantly. As a result, it makes the IDS non-scalable.
- Communication with the central component can overload parts of the network.

Some of these IDSs contain platform specific components.

2. RELATED WORK

The Distributed Intrusion Detection System (DIDS) is aimed at building distributed IDS that places monitors at every host and the network along with a centralized data analysis component (DIDS director) for data analysis. The DIDS architecture does not scale well for large networks since addition of any new component increases the load on the DIDS director component, and the data flow from monitors to DIDS director can consume high network bandwidth. DIDMA addresses these scalability problems by using mobile agents for decentralized data analysis [2]. Although fair amount of work has been done in investigating efficient methods of detecting rogue point in wireless and wired LAN, this area still offers plenty of opportunity for further investigation in this regards as most of the solutions available today are far from satisfactory. The brief information of related work has been mentioned below. Monitoring RF waves and IP traffic are two broad classes of approaches to detecting rogue APs. Most existing commercial products take the first approach they either manually scan the RF waves using sniffers e.g., Air Magnet, Nets tumbler or automate the process using sensors. Wireless clients are instrumented to collect information about nearby APs and send the information to a centralized server for rogue point detection. Wired and wireless connections can be separated by visually inspecting the timing in the packet traces of traffic generated by the clients. The Cooperating Security Managers (CSM) [3] is a distributed IDS that uses decentralized architecture consisting of security managers installed on every monitored host that coordinate with other managers to detect distributed attacks. On large networks, it requires coordination with higher number of managers to detect every attack, and hence scalability can be an issue. DIDMA performs decentralized data analysis using mobile agents that makes it more scalable. DIDMA uses platform independent components in contrary to platform specific security managers of CSM.

The Autonomous Agents for Intrusion Detection (AAFID) project [4] makes use of multiple layers of agents organized in a hierarchical structure with each layer performing a set of intrusion detection tasks. AAFID uses only static agents and is deprived of some of the benefits mobile agents can offer. The Intrusion Detection Agent (IDA) system [5] consists of sensors running in every monitored host that report Marks Left by Suspected Intruder (MLSI) and a central manager responsible for dispatching tracing agents to the host whose sensor reports an MLSI. The tracing agents gather information related to intrusion from the sensors and send it to central manager for analysis. In DIDMA, there is no central manager, and mobile agents perform the aggregation and correlation function in a decentralized manner. Mobile agents are employed to apply human immune system model for intrusion detection in [6]. This IDS works on anomaly based detection principle where each mobile agent travels to every host in the network to detect any deviation from the normal behavior of that host. The intelligent agents for intrusion detection project [7], have developed IDS using distributed multiple layers of lightweight intelligent mobile agents that apply data mining techniques to detect intrusions.

One of the most recent work described in [8], uses components very similar to our IDS entities. Manager component of [8] dispatches mobile agents and analyzes the gathered data, whereas the MAD in DIDMA is involved with dispatching *attack specific* MAs and maintain the VHL to record the hosts on which suspicious activities are detected. The mobile agents in [8] are of two types: patrolling and fixed. While fixed agent is similar to our static agents used for host monitoring purpose, the patrolling agents are different from the MAs used in DIDMA. Patrolling agents just collect intrusion related data from the monitored hosts, while MAs used in our work gather data from the victim hosts, and also aggregate and correlate it with the data received from previous hosts. Therefore, MAs perform both the function of manager and patrolling agent and thus reduces load on the central component by decentralized data analysis. MAs are attack specific and are dispatched based upon the activities detected by the SAs. The mobile agents used in DIDMA use Voyager [9] mobile agent platform. Voyager offers secure socket for encrypted transmission of agents and JAVA sandbox type security, and hence, also run on secure platform similar to [8]. Object persistence is also provided in Voyager using object activation framework for loading objects on demand from the servers. Therefore, DIDMA does not require any extra effort for regeneration and recovery of agents like in [8] that uses GYPSY mobile agent platform. The IDS described in [10] is made of several layers of agents. Each layer sends information to the layer above it. The bottom layer is called surveillance agents that move to every hosts and collect intrusion related data in order to send the data to the upper layers for analysis and response. The IDS discusses how IDS with multiple smaller components are better than a single monolithic IDS module. The mobile agents of [10] *are not attack specific*, and do not perform any data analysis. Analysis of data is carried out by separate decision making agents.

3. DRAWBACKS OF EXISTING SYSEM

Manual RF scanning is very time consuming and detects rogue AP only when scanning is applied. This leaves ample scope for an attacker to launch attack and finish its work before he gets detected. This is severe loophole of this method.

- *Lack of Efficiency: H*ost-based IDSs often slow down a system and network-based IDSs drop network packets that they don't have time to process.
- *High Number of False Positives:* False alarms are high and attack recognition is not perfect.
- *Limited Flexibility:* Intrusion detection systems have typically been written for a specific environment
- *Limited Response Capability:* IDSs have traditionally focused on detecting attacks. While detection serves a useful purpose, often times a system administrator is not able to immediately analyze the reports from IDS and take appropriate action.
- *No Generic Building Methodology:* In general, the cost of building IDS from available components is considerable, due in large part to the absence of a structured methodology. No such structuring insights have emerged from the field itself.

4. REQUIRMENTS OF DIDS

Network-level monitoring and distribution pose some new requirements on intrusion detection systems:

- Networks produce a large amount of data (events). Therefore, a distributed intrusion detection system (DIDS) should provide mechanisms that allow the Network
- Security Officer (NSO) to customize event "collectors" so that they listen for only the relevant events.
- Relevant events are usually visible in only some parts of the network (especially in the case of large networks).Therefore, a DIDS should provide some means of determining where to look for events.
- A DIDS should generate a minimum amount of traffic over the network. Therefore, there should be some local processing of event data.
- A DIDS needs to be scalable. At a minimum, "local" should interoperate with other DIDSs (possibly in a hierarchical structure).

For maximum effectiveness, NIDSs should be able to interoperate with host-based IDSs so that misuse patterns include both network events and operating system events.

5. OUR APPROACH

5.1 Introduction of Mobile Agents

The Distributed Intrusion Detection System (DIDS) is a project representing an extension of the NSM, with the aim of adding two features missing from NSM. These are the ability to monitor the behavior of a user who is connected directly to the network using a dial-up line (and who therefore may not generate observable network traffic), and the ability to allow intrusion detection over encrypted data traffic. The DIDS project is sponsored by UC Davis, the Lawrence Livermore National Labs (LLNL), Haystack Laboratory and the US Air Force.

- *Host agent module*: An audit collection module operating as a background process on a monitored system. Its purpose is to collect data on security related events on the host and transmit these to the central manager.
- *LAN monitor agent module*: Operates in the same fashion as a host agent module except that it analyzes LAN traffic and reports the results to the central manager.
- *Central manager module*: Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion

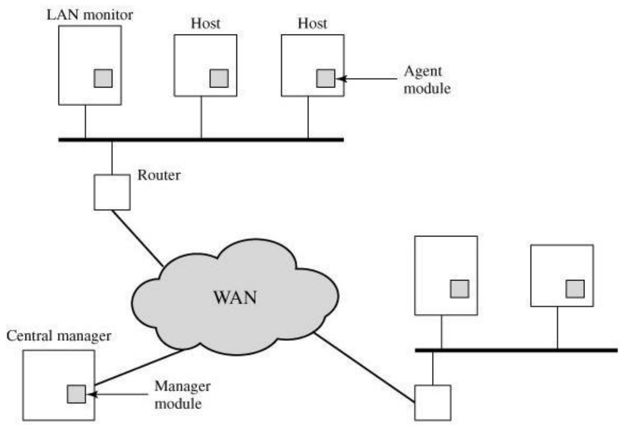

Fig 1: Architecture of DIDS

5.2 Why Mobile Agents?

After initial euphoria of mobile agent, now expectations of research community from mobile agent are more realistic. After decade of first introduction of mobile agents, it is now clear that mobile are best suited for remote information retrieval. Considering nature of mobile computing where computing hosts are away from each other and in such scenario if we want to know what is happening on remote host, use of mobile agent become unavoidable. Therefore detection of presence of rogue access point in wired, wireless or hybrid (wired as well as wireless mixed) type of network is a fit case for use of mobile agent for such detection.

5.3 Mobile Agent Architecture

The scheme is designed to be independent of any operating system or system auditing implementation. Fig. 2 shows the general approach that is taken. The agent captures each audit record produced by the native audit collection system. A filter is applied that retains only those records that are of security interest.

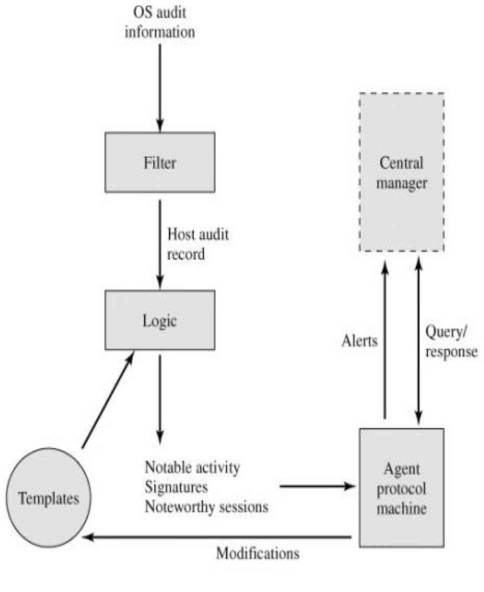

Fig 2: Architecture of Mobile Agent

These records are then reformatted into a standardized format referred to as the host audit record (HAR). Next, a template-driven logic module analyzes the records for suspicious activity. At the lowest level, the agent scans for notable events that are of interest independent of any past events. Examples include failed file accesses, accessing system files, and changing a file's access control. At the next higher level, the agent looks for sequences of events, such as known attack patterns (signatures). Finally, the agent looks for anomalous behavior of an individual user based on a historical profile of that user, such as number of programs executed, number of files accessed, and the like Here we propose architectures to detect rogue point using mobile agent. Below are the abbreviations used in this architecture:

SA- Server Application

CA- Client Application

MAS- Mobile Agent System

MA- Mobile Agent

5.4 Detection Methodology

As shown in Fig. 3, SA will start generating alpha-numeric strings after every 2 minutes. It will broadcast them over entire network. Computers which will be active at that time will record these strings and will acknowledge them. Mean time MA will start from central server. SA with itself will have file containing so far generated alpha numeric strings.MA will take this file from SA. MA will select any active computer from network randomly and will visit that computer.MA will ask to produce any past generated alpha-numeric string. This selection of past generated, to be asked, alpha-numeric key will be totally random in manner so that attacker will find it difficult in guessing the pattern of selection. As Client is an authorized computer, it will have that alpha-numeric key with it. He will produce it and will get authenticated. This process will repeat for another client by using random computer selection method. If client will not have MAS and CA deployed on it, MA will not get executed on it. As MA is not getting executed on one of computers of your network, this will be considered as serious offence and access point connected that computer will be declared as rogue point and client will be marked as intruder. In this way we managed to detect intruders and rogue point. After visiting all computers MA will return to central server and will take newly updated file of alpha-numeric strings from SA. After that it will again keep visiting computers in network in above mentioned manner. If the client has stolen the alphanumeric key from trusted client in this case MA will check the alphanumeric keys as well as attributes of files like date of creation etc. from these audit information server can take action against that client.

5.5 Bandwidth Consumed by Mobile Agent

The total bandwidth consumed in a centralized IDS model can be given by Eq.1.

$$H*C\text{…………………….} \ \mathbf{(1)}$$

C - The amount of raw data (greater than 20KB in normal cases) at a host.

H - Total number of monitored hosts in the network.

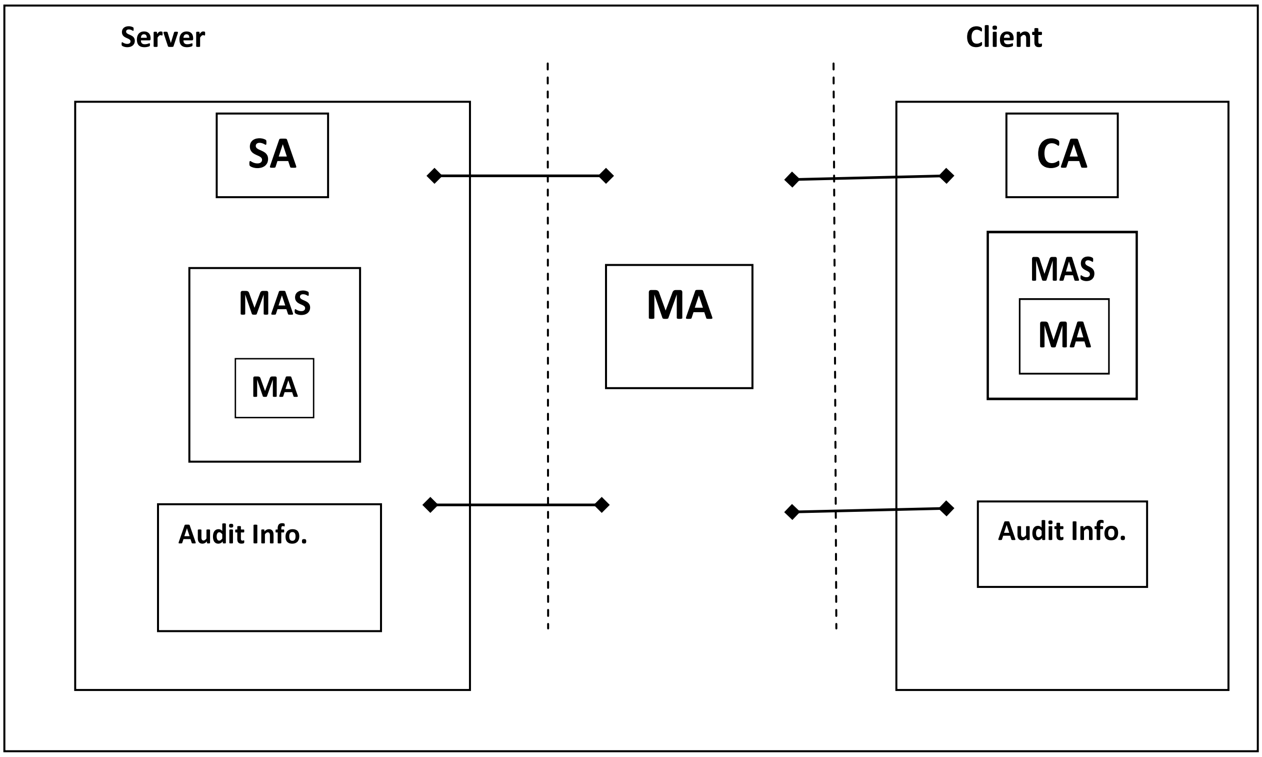

Fig 3: Mobile Agent based architecture for Intrusion Detection

In DIDMA, the total bandwidth consumed can be calculated by summing up the bandwidth consumed by an MA while moving from one host to another along with the gathered data. Assume that S_m is the initial size of an MA when it is dispatched from the MAD, S_0 is the initial size of the attack trace data gathered by an MA after visiting first host, and S_1 is the size of data carried by an MA after visiting the second host. After correlating the data received at the second host with the data gathered by an MA from the first host, the resulting increment in the size of initial attack trace data is $S1$-$S_0 = S_{inc}$ .For the sake of simplicity of analysis, we assume that the initial size S_0 is constantly incremented by S_{inc} due to each subsequent visit of the MA to any host. The total bandwidth consumed by DIDMA is given by Equation 2.

$$N*(2*(S_m+S_0) + (N-1)* S_{inc}) /2 \ldots\ldots\ldots\ldots 2$$

The above equation is derived by considering that (S_m + S_0) increases with an increment of S_{inc} at every host. N is the number of hosts added to the network out of total H monitored hosts, where N<<H. Experiments have been conducted to determine the size of an MA at the end of its itinerary along with the time period required for its travel from the MAD to the AA in some attack situations. The initial size S_m of an MA is very negligible since the MA object has still not gathered any data from the hosts. The MA size at the end of its itinerary depends on S_{inc}, while the S_{inc} depends on the extent to which the attack trace within the audit data gathered from any host can be aggregated with the data gathered from previously visited hosts.

S_{inc} can be negligible in the best case, where most of the data received from a visited host are aggregated with the data received from previously visited hosts. S_{inc} can be a small increment in average case, where some of the received data from a visited host get aggregated, and the rest of the data have to be carried as a separate record. S_{inc} can be considerable in the worst case, where none of the received data from a visited host are aggregated with the data already gathered by an MA from the previously visited hosts. Fig. 4. The variations in MA size with the number of hosts visited in the above discussed worst, average, and best case scenarios. We assume that N<<H since in most of the attacks, usually few hosts are compromised, and therefore, the number of hosts visited by an MA is also few.

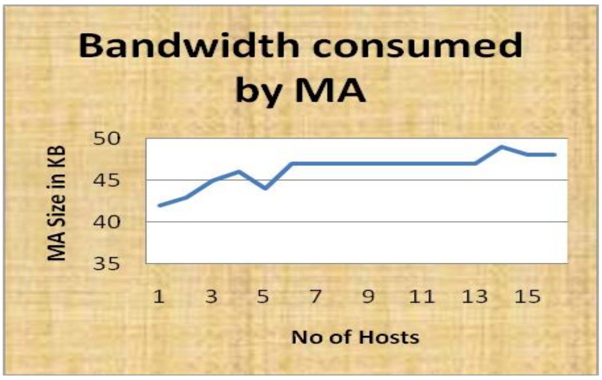

Fig 4: Architecture of Mobile Agent

6. ADVANTAGES OF MOBILE AGENT

Overcoming network latency in mobile agents can be dispatched to carry out operations directly at the remote point of interest, allowing them to respond in real time to changes in their environment.

- *Reducing Network Load:* Agents are small in size so they can travel through network and analyze the intruders in network. Instead of transferring the data across the network, mobile agents can be dispatched to the machine on which the data resides, essentially moving the computation to the data, instead of moving the data to the computation, thus reducing the network load.
- *Autonomous and Asynchronous Execution:* Mobile agents can exist and function independently from the creating platform, making them useful as IDS components.
- *Dynamic Adaptation:* The ability for mobile agent systems to sense their environment and react to changes is useful in intrusion detection. Agents may move elsewhere to gain better position or avoid danger, clone themselves for redundancy and parallelism, or marshal other agents for assistance.
- *Platform Independence:* Agent systems provide an abstract computing environment for agents, independent of the computer hardware and software on which it executes.
- *Protocol Encapsulation:* Mobile agents can incorporate the protocol directly and bring about an upgrade in the interface with the movement of an agent to another host.

7. FUTURE SCOPE

The greatest potential for mobile agents lies with response to an intrusion rather than its detection. Because responses can be initiated from nearly anywhere in the network, mobile agents can deal with attacks in a more optimal fashion than in a conventional IDS. Mobile agents enhance an IDS's ability to trace an attacker through the attacked network, to respond at the target, respond at the source, to collect evidence from the host and network components about the attack, and to isolate the source and target. Following aspects are potential areas for exploration

- *Tracing an Attacker:* Attackers often log into a chain of many hosts before attacking a target and sometimes spoof their source address. To find the attacker the IDS must trace back along the chain and locate the actual host launching the packets.
- *Responding at the Target:* When an attack is detected, it is vital to automatically respond at the target host. A quick response can prevent the attacker from establishing a better foothold.
- *Responding at the Source:* Responding at the attacker's host gives IDS a much greater power to restrict the attacker's actions.
- *Evidence Gathering:* Mobile agents offer the ability to run anything, anywhere, at any time, making it conceivable that evidence may be gathered from different hardware platforms, different operating systems, and even different applications such as web servers. Mobile agents can also intelligently audit the network by dynamically reconfiguring the audit capabilities of relevant hosts to strongly audit suspicious or important network locations.

8. CONCLUSION

This paper addresses some of the disadvantages of the centralized distributed intrusion detection systems. DIDMA employs static agents as host monitors and mobile agents for data collection, aggregation and correlation, and to respond to any attack. DIDMA exploits the benefits of employing mobile agents such as reduced network bandwidth usage, increased scalability and flexibility, and ability to operate in heterogeneous environments. Some of the distinct features of this architecture are as follows:

Firstly, DIDMA offers a new technique for decentralized data analysis carried out by mobile agents at the site of audit data instead of sending the audit data to some central data analysis component;

Secondly DIDMA can be easily extended to detect new attacks by adding new MAs.

9. REFERENCES

[1] M. Eid. 2004. "A New Mobile Agent-Based Intrusion detection System Using distributed Sensors", In proceeding of FEASC.

[2] Mohammad Zulkernine. 2005. "DIDMA: A Distributed Intrusion Detection System Using Mobile Agents" proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks (SNPD/SAWN'05)

[3] White G, Fisch E, and Pooch U. 1994. "Cooperating security managers: A peer-based intrusion detection system," IEEE Network, 10(1): 20—23.

[4] J. Balasubramaniyan, J. O. G. Fernandez, D. Isacoff, E. H. Spafford, and D. Zamboni, "An Architecture for Intrusion detection is using Autonomous Agents," Technical report no. TR 98-05, Purdue University, USA, 1998.

[5] M. Asaka, S. Okazawa, A. Taguchi, and S. Goto. 1999. "A Method of Tracing Intruders by Use of Mobile Agents," INET '99, San Jose, USA, June 1999.

[6] N. Foukia, J. Hulaas, and J. Harms, "Intrusion Detection with Mobile Agents," Proceedings of the 11th Annual Internet Society Conference (INET 2001), Stockholm, Sweden, June 2001.

[7] G. Helmer, J. Wong, Y. Wang, V. Honavar, and Les Miller , "Lightweight Agents for Intrusion Detection," Journal of Systems and Software, Elsevier, vol. 67, pp. 109- 122, 2003.

[8] Shao-Chun Zhong, Qing-Feng Song, Xiao-Chun Cheng, and Yan Zhang, "A safe mobile agent system for distributed intrusion detection," Proc. of the International Conference on Machine Learning and Cybernetics, vol. 4, pp. 2009 – 2014, Nov. 2003.

[9] Recursion Software Inc, "Voyager ORB Developer's Guide," www.objectspace.com, http://www.ifi.unizh.ch/ddis/staff/vorburg/doc/Orb/index.htm

[10] Bernardes, M.C and dos Santos Moreira, E., "Implementation of an intrusion detection system based on mobile agents," Proc. of the International Symposium

on Software Engineering for Parallel and Distributed Systems, pp. 158-164 June 2000.

[11] W. Jansen, P. Mell, T. Karygiannis, D. Marks "Mobile Agents in Intrusion Detection and Response" National Institute for Standards and TechnologyGaithersburg, MD 20815

[12] A.V.Dhaygude, K.R. Patil, A.A.Sawant "Threats to Wireless Local Area Network (WLAN) And Countermeasures" ICONS'07, January 27-29, 2007, Erode,Tamilnadu,India.

[13] Wei Wei, Kyoungwon Suh,Bing Wang . "Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP ACK-Pairs",IMC'07, October 24-26, 2007, San Diego, California, USA.