A Survey on Mobile Agent based Intrusion Detection System

Shiv Shakti Srivastava
Department of CSE
National Institute of Technology
Hamirpur, India

Nitin Gupta
Department of CSE
National Institute of Technology
Hamirpur, India

Saurabh Chaturvedi
School of CSE
Vellore Institute of Technology
Vellore, India

Saugata Ghosh
School of CSE
Vellore Institute of Technology
Vellore, India

ABSTRACT

Intrusion detection system (IDS) is the security mechanism that gathers and analyzes the information to detect unwanted attempts of accessing and manipulating the user and system activities and report it to the management station. A Mobile agent (MA) is a composition of computer software and data which is able to migrate (move) from one computer to another autonomously and continue its execution on the destination computer. Taking the recent development i.e. going to this field, mobile agent based intrusion detection system is an efficient way to the intrusion detection in the distributed environment. This paper is a review paper and currently summarizes the current state of the mobile agent based intrusion detection system. We discuss the performance gain that occur using mobile agent on intrusion detection system and review the existing mobile agent based intrusion detection system[MA-IDS] focusing on each of the categories of the classification, techniques used and the shortcomings of the current IDS design and implementations. Analyzing the existing [MA-IDS], we suggest some improvement that can be done in the existing system to avoid the malicious activities for the future security of the computer systems and the network.

1. INTRODUCTION

Today Computer System has evolved into a distributed computing machine, nothing is static now, not even the security threats and attacks. The security issues are of high concern today in the world of open system environment. The problem faced widely by the computer system and network is the network intrusion and virus infection. Intrusion is defined as "a set of actions which perform to minimize the confidentiality, integrity or availability of resources" [11].The key challenge is to provide the computer systems, a mechanism to overcome the security threats, attacks and anomalous activities that could affect the functioning of the system. Intrusion detection system (IDS) is the security mechanism that gathers and analyzes the information to detect unwanted attempts of accessing and manipulating the user and system activities.IDS can recognize the patterns of typical attacks, analyze the abnormal activity pattern and track the user's policy violation. So it often called as the "last line of defense" [2]. Basically IDS are being developed when the no of attacks on major network and sites increased. However, the initial design of IDS faced some shortcomings-

1. Centralized structure of IDS can be harmed in the case of high speed network.

2. There is a large number of false positives and IDS lacks in efficiency.

3. There is lack of communication in between the different IDSs.

4. The attacker can harm the hierarchical structure of IDS by cutting off the control branch and taking over the control network of the system. Here comes the mobile agent.

Mobile agent usefulness:

It is advisable to define, firstly, an agent. We refer to [4]:

An agent is a physical or logical entity characterized by the following attributes:

Autonomy: Agents operate independently and do not require any manual intervention.

Mobility: Agents suspend execution of code in one platform and move to another platform where they resume processing their code.

Rationality: Agents are capable of analyze and resolve a given problem rationally.

Reactivity: Agents analyze the changes that occur in a network and are able to take intuitive action accordingly.

Inferential capability: Agents use preprogrammed knowledge in order to execute general tasks.

Pro-activeness: Agents are able to take action according to the events occurring in the environment leading to the act of intrusion.

Social ability: Agents can meet and interact with other agent which may be dependent on an ontology in order to intuitive understand an environment.

The above attributes of mobile agents undoubtedly point to the fact that using a mobile agent virtually improves the functioning of the IDS. Mobile Agent-based Intrusion Detection System (MA-IDS) has their own limitations such as:

Code Size-IDSs consists of large volumes of code and thus it takes a lot of time to transfer the agent between the different hosts.

Lack of Prior Knowledge- Again if we try to make the mobile agents light weight, then we cannot preprogram them with system configuration.

Security-A major problem in a Mobile Agent Based Intrusion Detection System is to make it secure from intrusions. There are also factors like the time required to detect intrusion is quite high and other performance issues that undermine the working of MA-IDS adversely.

2. CLASSIFICATION OF INTRUSION DETECTION SYSTEM

Some of the classifications of the Intrusion Detection System are-

1. Traditional IDSs is classified into centralized and distributed approaches. In centralized system the data is gathered from different sites to a central site, central coordinator analyzes the data for checking the different intrusion while in distributed approach, mobile agents are used as an added benefit to analyze the data at the different sites locally, solving the problem of transferring the huge amount of data at one site.
2. According to the analyzed events IDSs are divided into two groups-Hosts Based Intrusion Detection System (HIDS) and Network Based Intrusion Detection System (NIDS). HIDS is designed for single computer system and focus upon what is happening in the system via the log files and internal auditing system whereas NIDS monitors the data exchange and intrusion for the whole network [6].
3. On the basis of analyzing network events, IDSs are classified into anomaly approach and misuse approach [6]. The anomaly approach is a way to detect the anomaly by comparing the current activity pattern of host and network with the predefined patterns while misuse approach relies on descriptions of attacks i.e. it detect those attacks that have been defined.
4. Passive and reactive system- Passive and reactive systems behave differently while detecting any intrusions in any network. In case of the former, the intrusion detection system (IDS) sensor identifies possible security breach, logs information about them, triggers alarms and sends reports to the security administrators. The latter, known as an intrusion prevention system (IPS), automatically takes action on detecting any potential security threat, either by resetting the connection or by reconfiguring the firewall to stop the network traffic from the potential source of attack [11].

3. CURRENT MOBILE AGENT BASED INTRUSION DETECTION SYSTEM (MA-IDSs)

In Intrusion detection system, a lot of research work is going on these days to improve the performance of system and the networks. The research work that has been done in the field of MA-IDSs focusing upon its architecture, technique, strength and weakness is discussed in this paper.

3.1 Wireless Ad-hoc Networks- Mobile ad-hoc network is collection of wireless mobile hosts forming a dynamic network infrastructure. The two approaches discussed are -first on the basis of access control and second on the basis of anomaly detection technique for mobile agents [7] and [10].

The first approach [7] discusses infrastructural problems of the current wireless Ad-hoc network which are characterized by the lack of infrastructure. This characteristic makes it difficult to apply generic administrative approaches to solve problems such as intrusion detection. The wireless Ad-hoc communication with Destination Sequenced Distance Vector Routing Protocol (DSDV) described in [8] based on Bellman-Ford routing algorithm. DSDV consists of a routing table for reachable destination, a table to next hop and neighbors' clusters to communicate network- wide. As the problem faced by the Ad-hoc network is access control here, so the two proposed authentication mechanism [7] are- RSA-1024 described in [9] and AES-128. Clustering is an alternative to the mobile agent, the head node responsibility in this mechanism are-load balancing, fault tolerance and security. It decrease network load, reduce overhead, increase packet delivery from source to destination, overcome network latency, make better use of resources through mobile agents. It is done by choosing some parameters for simulation and thus analyzing the behavior of routing protocols and comparing it with other proposed routing protocol for Ad-hoc network. Network bandwidth is utilized as DSDV performs well. There is low routing load and less overhead .The experiment is discussed in [7].

The second approach [10] focuses on the anomaly detection technique to ensure the security of mobile adhoc network. Cabrera Et al [12] provides the solution of intrusion detection system in adhoc network. The modern approach is described below –

Mobile agent approach: Mobile agent Monitoring the neighboring nodes and collect the information from neighboring home agent to determine the co relation among the observed anomalous pattern before it send the data. This approach provides security to current node, neighboring node and global network.

It consists of following parameters-

Home agent: Home agent is an important part of the network, which collects the information from other nodes. It works on application layer to network layer and monitors its own system continuously following the Bayesian classification approach and developing mobile computing application [13].

The technique followed is Bayesian classification approach; in this approach it is easy to find the behavior of pattern of the system. With help of this approach calculated:

1. Local Integration: Local integration modules concentrate on self system to detect the anomaly attacks.
2. Global Integration: Global integration module is used to find the intrusion result for entire network

The experimental result evolution considers some parameters-

Number of nodes in network, Terrain range of the network, Routing layer protocol and Mobility model and find out higher rate of anomaly detection, reducing the false alarm rate. It is discussed in [10].

The result is that it detects the high rate of anomaly and thus prevents the intrusion in the network. The false alarm rate problem is also reduced.

3.2 Distributed Architecture

There are various approaches to the distributed architecture-

3.2.1 Intrusion Detection based on SNORT

The snort and sniffer is open application software both are used to detect the malicious activity on distributed intrusion detection system. This includes overcoming latency, reducing network load and adapting dynamic environments [24]. It consists of the following objective:

A new mechanism is developed for acquiring extra data about user action from client machine or control module in server applications. It reduces the congestion from the distributed intrusion detection system.

Intrusion detection system compares to sensor distributed network [25] and find out many resources problem .Mobile agent collect data and sends the data to the main station for analysis purpose.

The components are -

Data Flow Capture: It captures the data from the monitors and sends the data to the intrusion detecting system for detecting malicious activity.

Intrusion Detection Agent: It is an important part of the system, behaves like a central node and data pre-processing. It is used to check the system is normal or abnormal and is also used to inform the administrator, receive the data from the mobile environment and detect and pre-process the data using given set

of rules. If any error exists command is given to the mobile agent environment.
Mobile Agent Environment: In this paper mobile environment, create, interpret, execute, transfer and terminate agents.
Data Analysis: Data Analysis with a Function component is a SOM [26] training procedure .It is used to deliver the data to mobile agent and take useful information from them and send it for data analysis.
Sensors (Sniffing): It is used in network analysis and troubleshooting, performance analysis and monitoring for a decrypted text based password. It continuously sends the data to the network until any instruction is received to stop sniffing .It is discussed in [22].

3.2.2 Anomaly Approach-

To detect anomaly in the distributed network, there are two approaches-Anomaly approach and Misuse approach. The anomaly approach is a way to detect the anomaly by comparing the current activity pattern of host and network with the predefined patterns. Any deviation from the predefined patterns detect anomaly. Advantages- Anomaly approach is useful to detect even the unknown attacks. The current Intrusion Detection Problems in anomaly approach includes-
• Higher no of alarms that are caused by unusual but authorized activities.
• There are some attacks that are not detected which may occur over an extended period of time.
• All the abrupt changes in the network should not be considered as anomaly, and determining of the threshold above which anomaly is to be considered is intrusive.
A mobile agent based model for intrusion detection system called Mobile Agents for Intrusion Detection System (MAFIDS) described in detail in [6] is a four level approach that includes-the down level, the pretreatment level, the kernel and upper level. MAFIDS is a Distributed Agent Architecture approach. The four mobile agents are-Sniffer Agent, Filter Agent, Analyzer agent and Decision agent
Sniffer Agent-It offers a real-time look at the network conversation and protocols. The agent is cloned and distributed throughout the network.
Filter Agent-Intrusion can sweep in all levels of the distributed network, filter agent provide analysis of data by monitoring, aggregating, sorting and merging events from various sources.
Analyzer Agent-The analyzer agent analyzes the events gathered from the previous two agents. It actually works in detection period to find out the alarm condition in the network.
Decision Agent-Decision is transmitted to the administration level by the agent.
The techniques used are- Event Correlation engine and agents synergy [6].
The metrics that are used by the analyzer agent in its anomaly detection algorithm are-
1. Latency time of response (LTR)-It is the responsibility of analyzer agent to find out those agents who didn't respond to the messages.LTR is calculated by multiplying total latency time of response with the number of agents that didn't responds.
2. Number of cloned Agent (NCA)-Urgent message is sent by decision agent to the analyzer agent to notify the number of cloned agents. It occurs during the analysis of the normal traffic flow if decision agent detect that the number of actual cloned agent is greater than the maximum number of cloned agent..

3.2.3 Multilevel Anomalies Detection approach-

In existing architecture, implementation of "Plug-in" used in anomalies detection system (ADS), so ADS need signatures' database and in computer system for movable nature ADS suffers a big outgoing flow. This centralized ADS architecture correlates in single level after taking incoming events. Due to the huge surcharge of the alerts, administrator machine may breakdown. Synchronous and Asynchronous detect are the two type of distributed multilevel approach. In distributed correlation levels the first step is to filter anomalies of all hosts which are the input for distributed detection for the architecture of the second level. The model use to minimize of false positive rate (FP) and network load for better network security. This architecture recognizes hidden anomalies with delayed period of synchronous and asynchronous detection by using mobile agent. Synchronous anomalies detections use a set of sensors in system. Sensor composed of a host ADS, a network ADS and an integrity checker. The anomalies detector result come in concentrator module which is divided in two parts collection of database of alert and normalization and after that all alerts will go correlate which is divided in two parts aggregation and synthesis for enhance anomalies detection. Asynchronous anomalies detection is of two types.
1. Local asynchronous anomalies detection
2. Distributed asynchronous anomalies detection.
On local asynchronous anomalies detection Static agent has been activated on each host by the administrator. Static agent (SA) collects the database of host that collects different events of alerts' log. The software agent use to enhance distributed asynchronous anomalies detection with the half of mobile agent. Mobile agent operates asynchronously on ADS if admin machine is not connected with network or sensor would harm. We refer to [19].
In multilevel ADS architecture the administrator supply a mobile agent (MA) to first host. The MA integrated by SA1 with doubtful detected results and sends to second host. Then it migrates by SA2 and passes to next host. So this process will repeat till it will return back to administrator.
In synchronous and asynchronous detection levels there will be three sensors and with the help of Denial of Service (DOS) attack for a host, then the distributed DOS attack on the whole network by propagation of this attack [20]. This technique is called SynFlooding [21].

3.2.4 Immune Mobile Agent-

It is based on dynamic clonal selection algorithm and collaborative signal mechanism. Mobile agent characteristic can shift to local host, so network load and improvement of real time capability can be reduced. Immune mobile agents roam on the network to monitor and detect any attack. Immune mobile agent architecture composed of central control agent(C-agent), detection agent (B-agent), memory agent (M-agent) and response agent (K-agent).B-agent and M-agent roam on the network and K-agent has activated if any attack has detected-agent mainly manage, coordinate on network and control roaming agent. M-agent is a set of memory detectors in the secondary response in immune system. M-agent activates if any antigen has detected in the system otherwise B-agent can detect all the time. The main job of collect agent is to collect data and it needs some extra property to improve the detection.
Intrusion detection system mainly used to protect from unwanted attempts at disabling, accessing and manipulating in the system of computer from suspected malicious source [16].The important aspect of IDS are false positive rate (FP) and false negative rate (FN).In this paper improved dynamic clone selection algorithm and collaborative signal mechanism are used to reduce false negative rate, improved real-time capability and network load. The strengths of the new distributed intrusion detection model based on immune mobile agent improve dynamic clone selection algorithm and collaborative signal

mechanism to reduce false negative rate and to increase detection rate.

3.2.5 Peer to Peer Intrusion Detection System

In peer to peer IDS, suspicious activities are checked by sending the detection request to other hosts of the system. It is used to avoid single point failure. The six types of agents discussed in this model are-Monitor Agent, Analysis Agent, Executive Agent and Manager Agent are static agents whereas Retrieval Agent and Result Agent are dynamic agents.

Monitor Agent-It collects and preprocesses the information of the system. Intrusion is detected and fixed at the host itself.

Analysis Agent-It integrates and analyzes the information from monitor agent. In the case of multi host attack, manager agents reply.

Executive Agent-Restoring corrupted files, preventing network connections and so on.

Each manager agent has a RAR.Retrieval Agent-Time to Life (TTL) is generated by initiator and tells about the number of rest nodes, the retrieval agent needs to visit.Working Process-Monitor agent analyses the network and any suspicious activity is reported back to the analysis agent. It is the responsibility of analysis agent to decide the nature of attack, whether it is attack or intrusion and accordingly executive agents are informed to take action against the intrusion or attacks.

Multi hosts Attack-Analysis agent calls Manager agent when it analyses multi hosts attack. Now, manager agent acts as initiator and retrieval agent visits the hosts. The Result agents send the required information back to the manager agent (initiator), which take the decision to broadcast in the case of multi host attack.There are two Retrieval migration strategy-Retrieval Agent generation and Retrieval Agent Dispatch.Retrieval Agent Generation-In the multi hosts attack, the number of hosts the initiator should visits is taken into consideration. There are two cases; in the first case no. of neighbors are more than the no. of hosts of the retrieval agents to be travelled and less than in the second case.The model MADIDF is compared with the MASHD [28] model on the basis of detection precision, network latency and network load. The performance is measured upon four different network scales-ten hosts, twenty hosts, fifty hosts and hundred hosts. The experiment is executed hundred times in above four network scales. Some terms used are-

Detection Precision-It is the ratio of detected attack incidents to all attack incidents. It is the most important aspect of IDSs.Network Latency-The range from the time the attack happens to the time that all hosts take action.

Network Load- Overhead of total communication and agent migration during detection process.After comparing these two models, it is obtained that MADIDF is better than MASHD in detecting the precision for different work. Network latency and Network load of MADIDF is higher than MASHD because initiator spends more time and consume more network resources. It is discussed in [27].

So it provides efficient migration strategy,. The hosts of the MADIDF model are able to retrieve related information from other hosts and make more accurate decision.

3.2.6 Central coordinator approach

The architecture for IDS [30] on mobile agent detects the complex attack to the networks [31]. It imposes the light load on entire network and thus detects the suspicious activity. For suspicious activity of the host, distributed intrusion detection based on mobile agent(DIDMA) and design a per host entry , trigger is specific event that will be received by Victim Host List (VHL), based on the type of trigger event will be dispatched to visit all victim using the victim path, related data in each host and alarm distributed intrusion. Some shortcoming exists due to dependency on a central node model causing single point of failure [32].Network is configuring in various phases. In each phase there exist a manager and alternative manager, the basic component is setup on host manager in subnet and can be done automatically or manually. The coordinator association approach calculates the role coefficient for each machine. Role coefficient is measured on the basis of role factor, available memory and processing ability CPU and calculates the manager and alternative manager in the network.

Coordinator association architecture: Coordinator association proposed architecture is divided into three different sections. It is discussed in detail in [29]:

1. Central coordinator
2. Negotiator
3. Manager neighborhood

Central coordinator: Each section contains one manager [30], an alternative manager and some hosts. Manager component is setup on manager and alternative manager on each section. At one time one entity is active. it consists of following components:

1. Watchman: It finds out the predefined suspicious activity on own network. Watch manager is capable to detect the harmful activity and take action.
2. VHL: It is a list which is stored in mangers that receive the trigger event from victim host and stores the IP address and type of suspicious activity.
3. Dispatcher: This component receives event from the host on the subnet and dispatch a relevant surveyor to visit that host.
4. Surveyor: This component is responsible to investigate all the victim hosts, based on VHL and aggregate data in respect to suspicious activity. If surveyor identifies any distributed attack it will alarm the coordinator association on the section.

Negotiator: If any attack is found, the surveyor informs the coordinator association and negotiator component to warn other managers about the attack. Manager characteristic are:

Alarming: It works to alert the attack, if it receives the emergency alarm, all negotiators

Enforce the dispatcher to initiate and dispatch the specific surveyor.

Enquiry: If collected data is not enough to define as attack. The surveyor does not initiate an alarm and return back to manager. Negotiator send an enquiry message to other to check their VHL list, if none response than surveyor terminated.

Dispatch agent: If one or more negotiator respond to the enquiry message, the surveyor of the responding manager checks and find the existing attack.

Manager Neighborhood: It consists following characteristic:

1. Manager Watcher: Watchman is capable to detect the harmful activity and take action [33].
2. Affected manager: Using voting ballet approach node easily finds this manager.
3. Manager specification: it is used to store the data tables and information about other manager to the limited hosts.

The Central coordinator approach gives fewer loads on entire network and co-operation between managers allow detecting more complex distributed attacks [31].

result: In this work each phase of the association coordinator approach is explained by an example and shows that many types of attack is detected in distributed network on mobile agent.

Table: Quick View of reviewed MA-IDSs

S/N	Architecture	Approach	Technique	Strength
1	AD-Hoc based	Destination Sequenced Distance Vector routing (DSDV).	Authentication Mechanism (RSA 1024, AES 128), Clustering of Mobile Agent.	Low routing, Less overhead.
2	AD-Hoc based	Anomaly detection using MA.	Bayesian classification.	High rate of anomaly, Reduce false alarm rate.
3	Distributed based	Anomaly detection	Event correlation engine, Agent synergy.	Reduced false alarm rate, ID is greater than SNORT.
4	Hybrid and Distributed based	Distributed multilevel (synchronous and distributed correlation) approach.	SynFlooding	Least result of false positive rate, false Negative rate, semantic detection.
5	Distributed	Immune based	Dynamic clonal selection algorithm and collaborative signal mechanism.	Reduce false positive rate, increase detection rate.
6	Distributed	SNORT based	Message exchange between server and SNORT.	SNORT performance is good.
7	Distributed	Peer to Peer IDS.	Retrieval agent generation, retrieval agent dispatch.	Efficient migration strategies, MADIDF is better than MASHD.
8	Distributed	Centralcoordination peer to peer ADS.	Agent based	Less load on entire network, detecting more complex distributed attack.

4. SUGGESTED CONSIDERATION FOR IMPROVED IDS

The IDS detects the suspicious, unwanted attempts, gathers and analyzes the information. We propose an architecture where the collective information of new intrusion, which is found from monitored network, is encapsulated and sent to other network to prevent it from unwanted activity using mobile agent as a precaution.

The intrusion detection systems usually operate on a passive reactive mode. However, with the aid of intelligence computation methods, Artificial Immune System (AIS) can be employed to build such intrusion detection systems. It is not enough to just detect and analyze intrusion in an environment; the source of attack has to be identified. If the attack is a known one, it would be blocked once the pattern is recognized as is the usual case; however, the IDS would block any new type of attack too.Basically, the intrusion information after being detected would be sent in an encapsulated form to the neighbor networks, so that the information does not require cloning. This ensures that the entire intrusion detection system would be less processor intensive and there would be reduced network overload.

Thus using mobile agents in immune system IDS's would be an improvement over static passive intrusion detection systems as explained here.The benefits of this architecture is that the intruder which is detected in one network may attack other network, so this type of information help other node of the network to alert and take recovery from the similar type of detected intrusion.

5. CONCLUSION AND FUTURE WORK

In this paper we have critically reviewed some existing mobile agent based intrusion detection system (MA-IDS) and proposed different types of existing MA-IDS architecture. The existing ways to detect the intrusion, the modes of data collection, the techniques of IDS used in the various scenarios and the security of the existing systems is also discussed. We focus upon the different type of intrusion detection system (IDS) approach like Anomaly detection, Misuse detection. We have mentioned different architecture of Hybrid, Network, Hierarchical and different structure like Centralized system and Distributed system. Immune mobile agent who is based upon Distributed ID System improves dynamic clonal section algorithm and collaborative signal mechanism to increase detection rate and reduce false positive rate. The aim of applying these types of

intrusions is to emphasize and mention other IDS [3]. We have included the strength and drawback of MA-IDS. In co-ordination association approach of IDS, dynamic load balancing technique can be used to resolve the problem of complexity in the network having large number of subnets in future [17]. The IDS approach can be enhanced by providing more security to mobile agents. In future work there is need to investigate the new concept of behavior to make this agent more intelligent to enhance the actual performance and track any new type of attack which is the main purpose to use the network IDS.

6. REFERENCES

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

[2] K. Boudaoud,"Détection d'intrusions : une nouvelle approach par systems multiagents", Thèse EPFL, 2000.

[3] F.A. Barika, N. El Kadhi,K. Ghedira,MA_IDS: Mobile Agents for Intrusion Detection System, Advance Computing Conference, 2009. IACC 2009. IEEE International, DOI: 10.1109/IADCC.2009.4809135

[4] Palmquis, Intelligent Agents in Computer and Network Management, http://www.gslis.utexas.edu/ palmquis/courses, 1998.

[5] Farah Barika KTATA,Nabil KADHI,Khaled GHEDIRA,Distributed agent architecture for intrusion detection based on new metrics,NSS 09,The Third International Conference,doi:10.1109/NSS.2009.50

[6] Amira Hamdi Shabaan,Hesham ElZouka,Mohamed Abou ElNasr,Intrusion Detection System in Wireless Ad-hoc Networks Based on Mobile Agent Technology, Computer Engineering and Technology (ICCET), 2010 2nd International Conference.Doi: 10.1109/ICCET.2010.5486031

[7] J. Macker and S. Corson. Mobile ad-hoc networking (manet): Routing protocol performance issues and evaluation considerations. University of Maryland, Network Working Group Request for Comments:2501, Jan 1999.

[8] Wendi Rbiner Heinzelman, Anantha Chandrakasan, and Henri Balakrishnan,"Energy-E_cient Communication Protocol for Wireless Microsensor Networks", Published in The proceedings of the Hawaii International Conference on System Sciences, January 2000.

[9] Abolfazl Esfandi, Efficient anomaly intrusion detection system in adhoc networks by mobile agents, Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference,DOI: 10.1109/ICCSIT.2010.5563804

[10] Intrusion - Detection. http://en.wikipedia.org/wiki/intrusion detection,2010

[11] Jo1[o B. D. Cabrera, Carlos Gutierrez , Raman K. Mehra, "Ensemble methods for anomaly detection and distributed intrusion detection in Mobile Ad-Hoc Networks", Volume 9 , Issue I (January 2008) table of contents, Pages 96-119 , Elsevier Science Publishers, 2008.

[12] Abolfazl Esfandi, Ali Movaghar Rahimabadi, "Mobile Agent Security in Multi agent Environments Using a Multi agent-Multi key Approach", in Proc. 2nd IEEE International Conference on Computer Science and Information Technology, Vol. 4, August 2009, pp. 438-442.

[13] HPING, http://www.hping.org,2010

[14] Jing Xu, Yongzhong Li,A New Distributed Intrusion Detection Model Based on Immune Mobile Agent, Issued in APCIP2009,Doi: 10.1109/APCIP.2009.249.

[15] S. Axelsson, "Intrusion detection systems: a survey and taxonomy", Technical Report No 99-15, Chalmers University of Technology, Sweden

[16] S.A. Hofmeyr, S. Forrest, and A. Somayaji, "Intrusion detection using sequences of system calls", in Journal of Computer Security, Vol. 6,1998, pp. 151-180.

[17] J. Kim and P. Bentley. "Towards an artificial immune system for network intrusion detection: an investigation of dynamic clonal selection", in Proc. of the Congress on Evolutionary Computation, Honolulu,USA, 2002, pp. 1015-1020.

[18] Fakher Ben Ftima,Wiem Tounsi,Kamel Karoui,henda Ben Ghezala, Distributed Multilevel Anomalies Detection System Using the Mobile Agent Approach,Doi: 10.1109/GIIS.2009.5307046

[19] J.P.Gaulier, "Etude et definition des differentes attaques de scan et de deni de service", origamix, 2006.

[20] H. Wang, D. Zhang and K.G.Shin, "Detecting SYN Flooding Attacks", EECS Department, The University of Michigan, 2002.

[21] Mo Xiu-Liang,WANG Chun-Dong,WANG Huai-bin," A Distributed Intrusion Detection System Based on Mobile Agents", BMEI '09,DOI: 10.1109/BMEI.2009.5305477.

[22] Wayne Jansen, Peter Mell, Tom Karygiannis, Don Marks. "Applying Mobile Agents to Intrusion Detection and Response", NIST Interim Report (IR) - 6416. ACM October 1999.

[23] Stefan Fuenfrocken. "Integrating Java-based Mobile Agents into Web Servers under Security Concerns", Technical Report, Department of Computer Science, Darmstadt University of Technology, Alexanderstr. 6, 64283 Darmstadt, Germany.

[24] Stefan Fuenfrocken. "Integrating Java-based Mobile Agents into Web Servers under Security Concerns", Technical Report, Department of Computer Science, Darmstadt University of Technology, Alexanderstr. 6, 64283 Darmstadt, Germany.

[25] The main website of Win dump: www.tcpdump.org (Accessed in January 10, 2004).