International Journal of Computer Applications in Engineering Sciences
[VOL I, ISSUE IV, DECEMBER 2011] [ISSN: 2231-4946]

A Novel Approach for Intrusion Detection System in Distributed Networks Using Mobile Agents

A. Saravanan[#], M. S. Irfan Ahmed[*], S. Sathya Bama[#]

[#]*Sri Krishna College of Technology, Coimbatore.*
[*]*Hindusthan College of Engineering and Technology, Coimbatore.*

[1]a.saravanan21@gmail.com
[3]ssathya21@gmail.com
[2]msirfan@gmail.com

***Abstract*— The rise of the networked workplace has been the most remarkable change in the last three decades of information technology. As networks of computing resources have become common, the concept of distributing related processing among multiple resources has become increasingly important. We have seen an explosion in information availability on increasingly heterogeneous networks. Managing these diverse networks often requires the collection of large quantities of data from possibly dispersed parts of the network. This challenge provides a driving force to research the use of agents and in particular mobile agents to automate some network management tasks. New management paradigms are being proposed as an alternative to the centralized, client/server architecture.**
Agent mobility addresses some limitations faced by classic client/server architecture, namely, in minimizing bandwidth consumption, in supporting adaptive network load balancing and in solving problems caused by intermittent or unreliable network connections. This paper presents a distributed intrusion detection system (IDS), based on mobile agents, that detects intrusion in the network segment using similarity measures.

***Keywords*— Mobile Agents, Intrusion Detection, Distributed Systems.**

I. INTRODUCTION

As the use of computer systems increases, intrusions against them also increase proportionally. Intrusion is a set of actions which attempt to compromise the confidentiality, integrity or availability of a resource [1]. This is the reason behind the demands of effective and powerful intrusion detection system. These intrusions may come from different sources. But, the main threats come from people known as intruders, e.g. unauthorized users of computers or services on some computers. Intruders can be classified as masqueraders or external users, misfeasor or internal user and clandestine user can be either external or internal user [2]. However, Masquerading attack is a more serious threat to the security of computer systems and the computational infrastructure since an attacker pretends to be a legitimate user after gaining access to the legitimate user's account where he can get or understand all the information [3]. While by other kinds of attacks, an attacker can get only some segment of data or encrypted data, which is much more difficult to understand.

I. PROBLEM STATEMENT

With the growth of computer and network applications these security issues, such as network intrusion and virus infection, are becoming more and more severe [4]. In order to prevent information from malicious attackers, Intrusion Detection System (IDS) is used to detect various intrusions in network environment. The traditional IDS usually monitor the activities of a single host and then analyze the data which takes too much CPU time. And when all information is processed at a single location, the system will have limited scalability. The processing capacity of the analyzer limits the monitored network size and distributed data collection can lead to excessive data traffic over the network. To overcome the above limitations, a different and interesting approach is taken by systems which utilize mobile agents to perform distributed intrusion detection. We also take into consideration the features gained from agent technology, such as autonomous components, which offer considerable benefits.

II. RELATED WORK

Intrusion detection can be traced back to publication of a technical report in 1980 [5] and has become a well-established research area after the introduction of a model [6]. The intrusion detection has been improved over 3 decades and now here are two main classes of approaches for intrusion detection systems, namely, agent based and non-agent based methods. Non-agent based IDS usually monitors the activities of a single host or collects information of a special network with the deployment of a network IDS in a critical point of the network, and then and the data is analyzed by a single module using different techniques [7, 8].

In order to perform a good detection in the network, there has been a trend to build agent-based IDS for network applications in recent years. Agent can be used to

collect data from network or hosts by several data acquiring technology. For example, sniffing agent monitors in network [9]. SNMP agent reads event from MIB database [10]. Sensor agent directly reads from files [11].

In the recent years many intrusion detection systems making use of agents and mobile agents have been proposed. A novel mobile based distributed intrusion detection system [12], mobile agents for network intrusion resistance [13], design of a multi-agent based intelligent intrusion detection system [14], agent based network intrusion detection system [15], an adaptive intrusion detection and defense system based on mobile agents [16] and intelligent and mobile agent for intrusion detection system [17] are examples of systems which make use of mobile agents to perform distributed intrusion detection.

III. SOFTWARE AGENT TECHNOLOGIES

Software agents automate tasks that otherwise we would have to do ourselves. Both the ability to perform in distributed computing environments and the ability to supply some domain knowledge to automating tasks for users will distinguish software agents from other utility software programs.

A. Intelligent Agents

Intelligent agents are software entities that carry out some set of operations on behalf of a user or another program with some degree of independence or autonomy, and in so doing, employ some knowledge or representation of the user's goals or desires

B. Mobile Agents

Mobile agents are intelligent agents that can migrate among hosts. They can execute tasks autonomously in dynamic environments and reduces bandwidth requirements [18]. The difference between a non-agent Client Server Architecture and an agent based Client Server Architecture is explained below.

C. A Non-Agent Client Server Architecture

A client/server application consists of the client and the server, usually on separate machines communicating over the network. When the client needs data or access to resources that the server provides, the client sends a request to the server (which must be on-line). The server in turn sends a response to the client. This handshake occurs over and over again, each request and response requiring a complete round trip across the network, as shown in Fig.1.

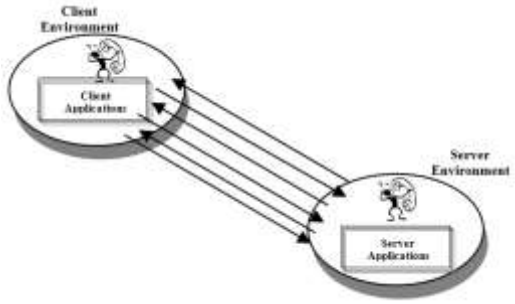

Fig. 1 Client Server Architecture

D. An Agent based Client Server Architecture

There are two areas where agents reside i.e. in the client and the server. The relationship between the client agent and server agent is shown in Fig.2. The fundamental difference in mobile agent architecture is that instead of the client talking to the server over the network, the client actually migrates to the server's machine. Once on the server's machine, the client makes its requests of the server directly.

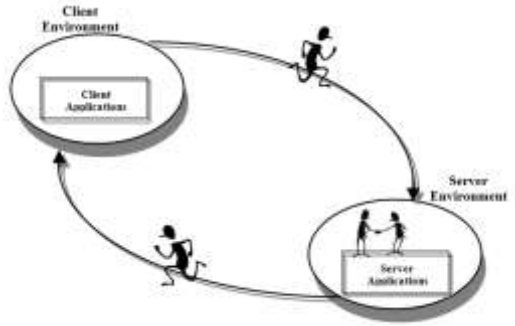

Fig. 2 Mobile Agent Architecture

IV. MOBILE AGENT BASED INTRUSION DETECTION SYSTEMS

Only a few research projects have already attempted to incorporate some ideas of mobile agent technology into intrusion detection systems. Although the architectural description is interesting no implementation has been provided so far. The following subsection briefly describes the various intrusion detection models based on mobile agents.

A. Agent Based Intrusion Detection

In this approach not only the workload will be divided between the individual processors, but also the IDS will be able to obtain an overall knowledge of the networks working condition. Having an overall view of the network will help the IDS to detect the intrusion more accurately and at the same time it can respond to the threats more effectively. In this approach, servers can communicate with one another and can alarm each other. In order to

respond to an attack, sometimes it can be sufficient enough to disconnect a subnet. In this type of system in order to contain a threat, the distributed IDS can order severs, routers or network switches to disconnect a host or a subnet. One of the concerns with this type of system is the extra workload that the IDS will en-force on the network infrastructure.

VI PROPOSED ARCHITECTURE

In this paper, agent based architecture is proposed to detect intrusions [14][16]. This approach proposes a fully distributed system made by set of nodes with two agents:

- Server Agent
- Client Agent
- Communication Agent

This collection of agents is used to determine any ongoing intrusion attempt. Each agent has an independent job to do so that any attempt to compromise the system can be quickly identified. The architecture with communication agent is shown in Fig. 3.

Client agents are installed on a client workstation, and responsible for collecting extra user information and then sending it to server agents with the help of communication agents.

Server agents are running in the server where masquerade intrusion is to be detected. They process the message sent from client agents. Moreover, the server agents can make a decision on whether the current user is a legal one or not.

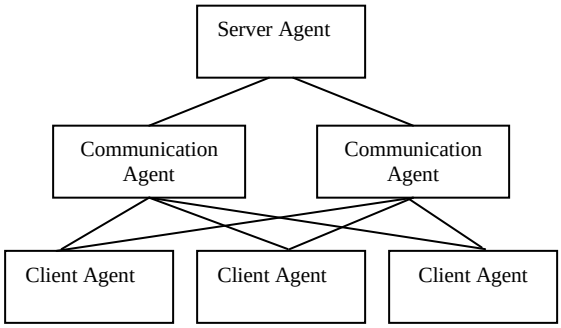

Fig. 3 Architecture with communication agent

Communication agent usually monitors the client agent's request. The received message is first parsed; then the useful message is forwarded to the server agents. And also it maintains the intrusion list.

A. Role of Client Agent

The main function of client agent is to collect extra user information, such as Operating System, network card, etc. which is used to improve the detection accuracy. The structure of client agent is shown in Fig.4. Layer 1 collects extra information by calling operating system API when the user login into the application. Layer 2 translates the message into a special format and Layer 3 simply sends the message to communication agent.

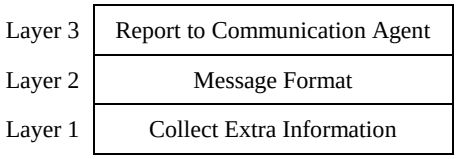

Fig. 4 Structure of Client Agent

Another important feature of the client agent is reliability in communication. Each client agent is connected to a default communication agent. However, when the communication agent is busy or fails to response, the client agent may select another communication agent from the local lists and then tries to connect to it.

B. Role of Server Agent

The structure of server agent is shown in Fig 5. It is split into two layers namely Description Layer and Detection/Decision Layer, distinguished by their functionality.

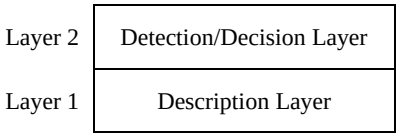

Fig. 5 Structure of Server Agent

1) Description Layer: Even though Intrusion can be detected on line or offline; this proposed method focuses on on-line detection, so we need a proper description of normal user. There are several alternative choices that can be used to describe the action of a normal user. Warrender represented a normal user by a database of user activities in short sequence [19], then, many kinds of intrusion can be detected by matching the user action sequence with the database. In the proposed system the normal user sequences are recorded in the database called user sequence database. However, we use an advance data mining algorithm to filter those events that may seems abnormal, because abnormal user sequence are not allow to be included in train set. So this data-mining algorithm should produce the sequence of normal user action event with high certainty, we use certainty factor to evaluate the similarity of patterns of sequence data. The detail of this algorithm is described in paper [20].After describing the normal user action the next step is to read the audit data generated by system by which we can construct an event sequence on line, which includes all events since last reading.

2) Detection/Decision Layer: In the network security domain, low trustfulness of the user means that the user is considered as an intruder. Trustfulness is determined in

the [0, 1] interval, where 0 corresponds to complete distrust and 1 to complete trust of the user. Here, each user action sequence is compared with the user sequence database. If the similarity of the two sequences is 1 then they are assumed to be identical which means that the sequence is not considered as an attack. Similarly if the similarity of the two sequences is 0 then they are assumed to be non-identical which means that the sequence is considered as an attack. Once the attack has been identified, then the copy will be sent to all the communication agents. Many algorithms for measuring similarity between the categorical sequences are available. In this paper, we have used an efficient method to measure the similarity [21] between two sequences S_1, S_2 is defined below:

$$\text{sim}(S_1,S_2) = \frac{|E_1 \cap E_2|}{\frac{|E_1| + |E_2|}{2}} \quad (1)$$

Here, E_1 be the collections of element pair of user sequence S_1 and E_2 be the collections of element pair of user sequence S_2. However, to avoid making wrong decision on the sudden action of normal users, an average similarity is computed on a sequence. Then, a decision can be made based on the similarity measure.

C. Role of Communication Agent

The main function of communication agent is to receive the message from client agent. The message contains extra user information. So the agent should extract the useful data and it then checks with the predefined intrusion list. If it matches with the list then the request will not be forwarded to the server agent by the communication agent. If the request is an intrusion, which is not identified by the communication agent then the server agent will identify it. Thus the communication agent minimizes the burden of the server agent. If the sever identifies the intrusion then the copy will be sent to the communication agent which adds the received intrusion in the intrusion list. However, in order to improve the scalability, all kinds of message are further encapsulated.

VII. Performance Analysis

In this section, the performance analysis has been done to check the effectiveness of the proposed system. First, the data is collected by monitoring audit data. Then the data set is parsed and encoded into sequence. Among the sample of 1000 users' data we randomly select some user as masquerader and the overall performance has been calculated, which includes hit rate and false alarm rate. In the experiment, the length of sequence has been from 30 to 100; the result is shown in Table 1 and performance graph is showed in the figure 6. As the length of the sequence increases, the performance of our detection algorithm is becoming better and better.

Table I. Performance of Proposed System

Instances	Detection Rate
Total Number of Instances	1000
Correctly Classified Instances	87.84%
Incorrectly Classified Instances	12.16%

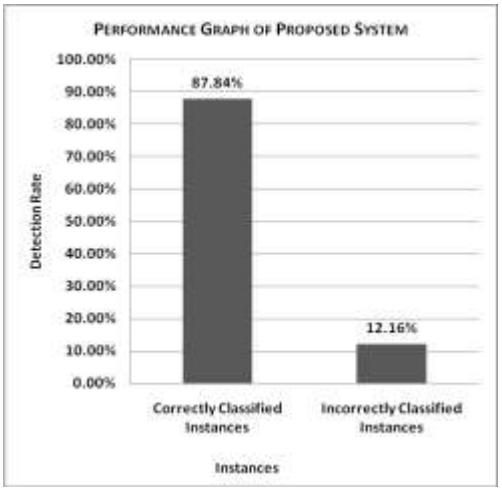

Fig. 6 Performance Graph of Proposed System

In the proposed system, the performance of the proposed detection algorithm can be better based on the length of sequence. Extra user information can effectively improve the performance of the detection algorithm.

VIII. Conclusion

In this paper an Intelligent Agent based distributed intrusion detection system architecture has been presented. The proposed system can detect simple and complex intrusions by monitoring various system tools installed on a network or a host. As demonstrated in examples the system is capable of not only detecting simple distributed attacks but also the attacks which are slow, distributed and multi event based attacks normally not detected by many existing IDS. Each agent used in the system performs a separate task and is independent. The system itself is robust and secure as each of its components is monitored by a different component, which makes it resist subversion. The system is both scalable and configurable as per the network requirements. For future work, the system presented is still being extended and implemented. Apart of the case of attack presented, they may be other several attack or abnormal situation in network system. So, during further steps of our work, we will reason about other scenario related to security events and enhance the addition proposal which correspond to the new scenarios.

REFERENCES

[1] J.P Anderson, Computer Security Threat Monitoring and Surveillance, tech, report, James P.Anderson Co, Fort Washington Pa., 1980

[2] William Stallings, Cryptography and Network Security, Third Edition

[3] R. A. Maxion and T. N. Townsend, \Masquerade detection augmented with error analysis," IEEE Transactions on Reliability, vol. 53, no. 1, pp. 124-147, 2004.

[4] P. Loshin, Intrusion detection, Computerworld, http://www.computerworld.com/hardwaretopics/hardware/story/0, 10801,59611,00.html, 2001.

[5] J. P. Anderson. April 1980. Computer Security Threat Monitoring and Surveillance. Technical Report, James P. Anderson Co., Fort Washington, PA.

[6] D. E. Denning. Feb. 1987. A Intrusion-Detection Model. IEEE Transactions on software Engineering. Vol. 13, no. 2, pp. 222-232.

[7] L. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood, and D. Wolber, \A network security monitor," IEEE Symposium on Research in Security and Privacy, pp. 296-304, 1990.

[8] J. Hochberg, K. Jackson, C. Stallings, J. F. McClary, D. DuBois, and J. Ford, \NADIR: An automated system for detecting network intrusion and misuse," Computers and Security, vol. 12, no. 3, pp. 235-248, 1993.

[9] I. M. Hegazy, T. Al-Arif, Z. T. Fayed, and H. M.Faheem, \A multi-agent based system for intrusion detection," Potentials, IEEE, vol. 22 , no. 4, pp. 28- 31, 2003.

[10] L. P. Gaspary, E. Meneghetti, and L. R. Tarouco, \An SNMP agent for stateful intrusion detection inspection," Integrated Network Management, pp. 3-16, 2003.

[11] A. J. Rocke and R. F. DeMara, CONFIDANT: Collaborative object noti¯cation framework for insider defense using autonomous network transactions, Autonomous Agents and Multi-Agent Systems,http://netmoc.cpe.ucf.edu:8080/internal/conversion/2004/ CONFIDANT framework.pdf .2005.

[12] Amir Vahid Dastjerdi, Kamalrulnizam Abu Bakar. 2008. A Novel Mobile Agent Based Distributed Intrusion Detection System. World Acdemy of Scienec. Engineering and Technology 45 2008.

[13] H.Q. Wang, Z.Q.Wang, Q. Zhao, G.F. Wang, R.J. Zheng, D.X. Liu. 2006. Mobile Agents For Network Intrusion Resistance; Springer. LNCS. vol. 3842/2006, pp. 965-970.

[14] Xiaodong Zhu, Zhiqiu Huang, Hang Zhou. August 2006. Design of a Multi-Agent Based intelligent Intrusion Detection System. First International Symposium on Pervasive Computing and Applications, pp. 290-295.

[15] Cheung-Leung Lui, Tak-Chung Fu, Ting-Lee Cheung. July 2005. Agent-Based Network Intrusion Detection System, in Proc. of the Third International Conference on Information Technology and Applications. Vol.1, pp.131-136, Sydney.

[16] Mohamad Eid, Hassan Artail, Ayman Kayssi, Ali Chehab. October 2004. An Adaptive Intrusion Detection And Defense System Based On Mobile Agents, in Proceedings of the innovations in information technology. Dubai, UAE.

[17] A. F. Barika, N. El-Kadhi. November 2003. Intelligent and Mobile Agent For Intrusion Detection System. Proceedings of international conference of information and communication technology.

[18] Dominic Cooney, Paul Roe, Mobile Agents Make for Flexible Web Services, AusWeb 2003. The Ninth Australian World Wide Web Conference

[19] C. Warrender, S. Forrest, and B. Pearlmutter, Detecting intrusions using system calls: alternative data models," IEEE Symposium on Security and Privacy, pp. 133-145, 1999.

[20] J. P. Zeng and D. H. Guo, A new clustering algorithm for time series analysis, International Conference on Intelligent Computing (ICIC 2006), pp. 759-764, 2006.

[21] Seung-Joon Oh, Jae-Yearn Kim, “Clustering Categorical Sequences Using a K-Nearest-Neighbor Method” International Journal on Computer Applications, Vol 12 No.3,141-150,Sept 2005.