**International Journal of Engineering Research and Development**
*e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com*
*Volume 10, Issue 1 (February 2014), PP. 01-03*

# Mobile Agents for Sniffer Detection in Network Security Management

S. V. Patil, Dr[1]. S. D. Khamitkar[2]
[1]*Assistant Professor, Department of Computer Science & I.T., Rajarshi Shahu College, Latur (MS)*
[2]*Associate professor, School of Computational Sciences, SRTM University, Nanded (MS),*

**Abstract:-** In the network traffic sniffer is a type of program which steals the information in the network when data packets travel. In this paper we projected over the Mobile Agents for finding the sniffer program. The specially designed Mobile Agents and the Network Administrator plays very important role in detecting the sniffer program in the network security management. The Network Administrator sends the special Mobile Agents in the network and collects the information from different clients. After analyzing the information he easily identifies the sniffer program acting in the network.

**Keywords:-** Mobile Agent, Sniffer, Network Security**.**

## I. INTRODUCTION

According to different surveys it is proved that 85% threats are due to internal type threats from the employees inside. We can manage the external threats using firewall like options but it is very difficult to stay away from internal threats. Sniffers come under the internal threats. In this work we propose the Mobile Agents for detecting the sniffer program. In the Mobile agent, code and program execution state are present. Initially Mobile Agent present on home computer then it is dispatched on host computer at this time code and entire execution state transferred on host computer. The host platform provides the suitable environment for execution. Mobile Agent uses essential resources of the host computer. After completing its task Mobile Agent moves on another computer.

## II. REVIEW

In this section we are reviewing some literature related with Mobile agent and Network management and security. Once the mobile agent has migrated, the connection between the client and server is disconnected, later when mobile agent finishes its job at the server, then it will reconnect to the client or host. This clearly saves the network bandwidth especially in the wireless environment where disconnection is frequent and bandwidth play a major role [1]. 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. Mobile agents perform a task by migrating and executing on several hosts connected to the network. For the sniffer detection, the network administrator sends some special types of mobile agents in the network and collects information from different nodes. After analyzing this information the network administrator can identify the computer system running in promiscuous mode. [2]. We can categories network attacks into denial of services, unauthorized accesses from remote machine, unauthorized access from local super user (root) privileges and sniffing. Sniffers are programs that allow a host to capture any network packet illicitly. Detection of sniffer attacks is very difficult task to handle. Specially, if the sniffers are active because active sniffer can alter or block network traffic while passive sniffer can only monitor network traffic. [3]

## III. DISCUSSION ON MOBILE AGENTS

Mobile Agents are composition of computer software and data which migrates from one computer to another. While doing this, they continue their itinerary up to the home computer. Autonomy and mobility are main features of mobile agents, specifically mobile agent is a process where mobile agent moves from one environment to another environment, with remains data intact. Mobile agent itself decides when and where to move. When a mobile agent decides to move then they save their own state and this state transport to another host. Mobile agents are specific about mobile code and they are choosing the host and also active in respect of execution [1, 4].Mobile agents have special characteristics which can help intrusion detection in several ways. The use of mobile code and mobile agents computing paradigms have been proposed in several researches. The advantages include: overcoming network latency, reducing network load, executing asynchronously and autonomously, adapting dynamically, operating in heterogeneous environments, and having robust and fault-

tolerant behavior. Moreover implementation of mobile agents in languages such as JAVA provides mobile agents with system and platform independence and considerable security features [5].

## IV. DISCUSSION ON SNIFFER PROGRAM

A network sniffers monitor's data flowing over computer network links. It can be a self-contained software program or a hardware device with the appropriate software or firmware programming. Also sometimes called "network probes" or "snoops," sniffers examine network traffic, making a copy of the data but without redirecting or altering it. Some sniffers work only with TCP/IP packets, but the more sophisticated tools can work with many other protocols and at lower levels including Ethernet frames. Years ago, sniffers were tools used exclusively by professional network engineers. Nowadays, however, they are also popular with Internet hackers and people just curious about networking. Several sniffer software applications are available on the Web for download. [6]

## V. SYSTEM STRUCTURE AND DESIGN

The structure is made up of three components as Network Administrator, Mobile Agent Platform and Mobile Agent for detection. We are considering the Network Administrator also as a part of structure because he will create the mobile agent, monitor and analyze the information provided by the mobile agent for the security and management purpose. Mobile Agents are the main part of this architecture. They are specially designed to perform network analysis task. Whenever a mobile agent starts execution on a specified node, it monitors all the incoming and outgoing network traffic for that node. If it finds any irregular incoming traffic or any other malicious activity, it immediately sends an alarm message to the network administrator for necessary action. Following algorithm can be used for finding of sniffer program in the network.

1. Network administrator installs and configures Mobile Agent Platform on all the computers connected in the Network.
2. Whenever the whole system starts, the network administrator activates some specially designed mobile agents.
3. These mobile agents travel in the network and select any random node for execution.
4. Mobile Agent collects all the information about network activities including network traffic for that node.
5. As we know if any node runs a Sniffer, then it collects all the packets moving in the. So mobile agent sends an alarm message to the network administrator if it finds that the incoming network traffic is greater than a pre specified value.
6. Receiving this alarm message, network administrator can take necessary action.
7. If everything is normal then the mobile agent moves to another node and repeat the steps 4 and 5.
   So this whole process can detect the sniffer present in the network. So now using this algorithm we can detect sniffing activities in the network. [7]

## VI. CONCLUSION

Mobile agent provides a new way of network security. However, the security, infrastructure and standardizing issues still represent significant constraints. The main thing from our findings is that mobile agent has the potential in sniffer detection. Due to its nature of being an advanced way from the programming environment. Mobile agent selects any node at random and checks that node, if it trace too much incoming traffic on the network interface card then he report to the network administrator. So the sniffer can be detected. There are still many hurdles that need to be undertake, the most important is that mobile agents and mobile agents platform security. In future, some security procedures should be taken for the certain security.

## REFERENCES

[1]. S. V. Patil, Dr. S. D. Khamitkar & S. N. Lokhande, "Efficient use of Mobile Agents for Network Security & Management", Global Journal of Computer Science and Technology
[2]. Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013
[3]. Amit Mishra, "Mobile Agents: As a Solution for Sniffer Detection", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 4, August 2012
[4]. Abdul Nasir Khan, Kalim Qureshi, and Sumair Khan, "An Intelligent Approach of Sniffer Detection", the International Arab Journal of Information Technology, Vol. 9, No. 1, January 2012
[5]. Shiv Shakti Srivastava, Nitin Gupta, Saugata Ghosh, Saurabh Chaturvedi , "A Survey on Mobile Agent based Intrusion Detection System" International Symposium on Devices MEMS, Intelligent Systems & Communication (ISDMISC) 2011, Proceedings published by International Journal of Computer Applications® (IJCA).

[6]. Danny B. lange and Mitsuru Oshima "Seven Good Reason for Mobile Agents", (PP 88-89) Communications of the ACM, Vol 42.No.3, March 1999
[7]. http://compnetworking.about.com/od/networksecurityprivacy/g/bldef_sniffer.htm
[8]. A.R.M. Ravi Shankar, K. Mahesh, "Agent Based Network Sniffer Detection", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153