International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 3, May - June 2013 pp-1850-1853 ISSN: 2249-6645

# Secure network monitoring system using mobile agents

Larkins Carvalho[1], Nielet D'mello[2]
[1](Department of Information Technology, Xaviers Institute of Engineering/Mumbai University, India)
[2](Department of Computer Engineering, Fr. Conceicao Rodrigues College of Engineering / Mumbai University, India)

***ABSTRACT:*** *There is a tremendous growth in computer network which demands efficient and secure network monitoring and network management. Mostly SNMP (Simple Network Management Protocol) based client server architecture is used for network management which uses SNMP as a protocol to provide Centralized approach of network management which is quite efficient in terms of performance. Foremost problems related to this architecture are heterogeneity in networks, limited amount of bandwidth, lack of resources, lack of fault tolerance capability and huge amount of traffic generated on central Server which can degrade the performance of network.*

*In this paper, we propose a system which follows distributed and decentralized approach for the purpose of network monitoring and management which reduces the traffic over the network. To facilitate distributed and decentralized monitoring, we proposed a secured multi-agent based architecture in which, we created different mobile agents for the purpose of getting network related information. Mobile agents retrieve network related information, which act as an Input for network administrator.It keeps an eye on an activity of each and every registered client using the mobile agent. The proposed application also focuses on reducing the network bandwidth used for monitoring the network by using agent per client architecture (mobile/roaming agent).*

***KEYWORDS:*** *controller agent, decentralized approach, mobile agents, snmp, secure network monitoring*

## I. INTRODUCTION

The advancements and globalization in the field of computer network have created many tribulations like security and network overhead [1][4]. To avoid these problems, network administrator has to monitor and manage network according to predefined security policy. Since last decade, network monitoring and its management have been the biggest challenges for any distributed network infrastructure. In recent years, mostly organizational network infrastructure used protocols like SNMP for network management and monitoring purpose. These protocols follow centralized approach of client server based architecture. In current communication infrastructure, many organizations follow centralized approach for network monitoring and network management that is all the work of all the clients is been handled through a single server and all the processing is done by server alone which creates extra burden on network and huge amount of traffic at the central server thereby reducing the performance of the network. So it created problems like limitation of bandwidth, high network latency, lack of fault tolerance capability, etc.

To reduce these type of problems we have implemented "SECURE NETWORK MONITORING". The main objective of this system is the implementation of separate monitoring system, implementation of mobile agent[2] at every client in the network. Here in this approach, user of each client machine will know that his machine is being monitored by network administrator or someone else. In order to achieve confidentiality and integrity, multi agent based architecture is developed which has various capabilities such as file monitoring[3], client activities monitoring etc.

This application has two modules, server and client. Server will receive data/reports/logs from client module and will perform the appropriate action. Client module will monitor each & every client pc for any activity like,

1. Internet usage
2. Storage usage
3. File system
4. Media activities
5. Performance related activities (e.g. which process is making excessive use of client processor, resulting in poor performance of client system)
6. Current running & executing processes
7. Information about open ports and target machines to which client is connected.

Based on the info received from client admin can perform various actions like killing the processes on client machine, shut it down, send the message to client etc. While sending data over the network there is possibility that it may get seen by malicious users, to avoid this data send by system is encrypted/decrypted using a basic algorithms.

## II. EXISTING SYSTEMS

Over the past few years extensive research work, on mobile agent implementation in network management has been done. Also, due to the increasing requirements in telecommunications, variety of transported flows in network must handle multimedia data traffic reliably with a high quality of service. There are several threads of research that have used mobile agents in a telecommunications network to manage connectivity and load balancing.

Rapid advancement of computer network requires efficient network monitoring and management for better utilization of resources. In current communication infrastructure, many organizations follow centralized approach for network monitoring and network management that is all the work of all the clients is been handled through a single server and all the processing is done by server alone which creates extra burden on network and huge amount of traffic at the central server thereby reducing the performance of the network. So it created problems like limitation of bandwidth, high

network latency, lack of fault tolerance capability, etc. Network monitoring and management followed centralized approach that is all the work of all the clients is been handled through a single server and all the processing was also done by server itself. It results in a huge amount of network traffic at the central server. Due to the huge network traffic performance of network degrades gradually.

The distinction between the existing systems and the proposed system can be enlisted as follows:

| **Existing System** | **Proposed System** |
|---|---|
| Centralized Approach | Decentralized approach |
| Most of the processing is done by server itself. | Each client performs his own processing & gives result to the server. |
| Load balancing problem occurs | Load balancing problem is resolved. |

## III. MOBILE AGENTS

Mobile agents[2] are programs being sent across the network from the client to the server or vice versa. An agent that can be executed after being transferred over the network will be called an agent host. A software agent is a common name and describes a software entity that computerizes some of the regular or difficult tasks on behalf of human or other agents. Mobile agents can travel in network following their itinerary and carrying logic and data to perform a set of management tasks at each of the visited nodes in order to meet their designed objectives.
Mobile agents allow the transformation of current networks into remotely programmable platforms. Mobile agents are a powerful software interaction model that let a program to be moved between hosts for remote execution. They are solutions for managing distributed networks.

To overcome the serious issue of network traffic and to enhance the performance of network, a mobile agent is used. To control and manage network traffic, network infrastructure requires some intelligent system which should have the ability to give response dynamically and take right decision.
In order to reduce complexity and improve reliablility, we need to follow decentralized approach where mobile agents are the opinion. Mobile agents have the property of load balancing by which they distribute the overall load among different nodes.

Fig 1 shows the client server communication architecture. This architecture consists of one manager who generates no of mobile agents and sends it to the network of managed node. They travel from one node to another autonomously and asynchronously and perform monitoring and management task at each node and collect network related information. After completing monitoring and management task, mobile agents sent back to manager.

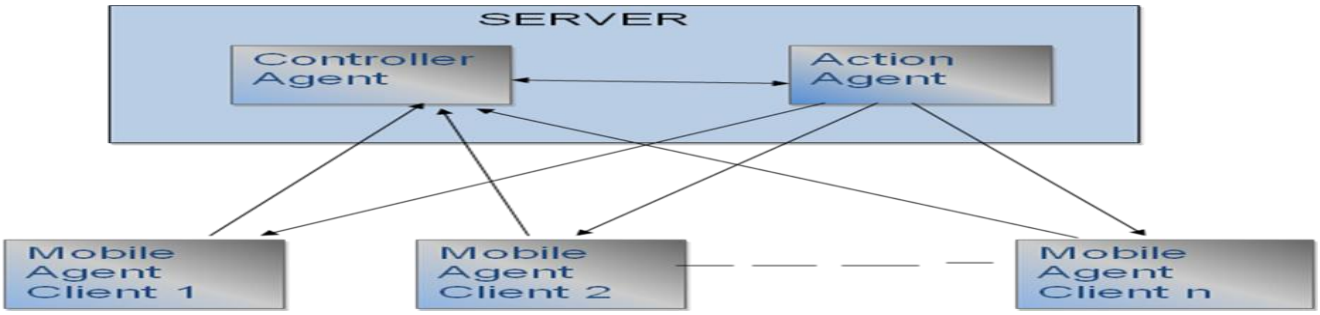


**Figure 1. Client server communication**

## IV. IMPLEMENTATION DETAILS

***IV.1 ALGORITHM***

**For Server:-**
**Step 1:** Start
**Step 2:** Run the Server.
**Step 3:** Wait for the Client for Connection.
**Step 4:** Check for any incoming Connection from Client, if Yes, Register the client and add it in the list of Connected Clients.
**Step 5:** Wait for the Information From Client.
**Step 6:** If any incoming information from Client then notifies Admin.
**Step 7:** Follow Steps 3 to 5 for more clients.
**For Client:-**
**Step 1:** Start.
**Step 2:** Check for the Server.
**Step 3:** If server is available then Connect and Go to Step 5.
**Step 4:** If not then Log Error and Go to Step 2.
**Step 5:** Monitor the client and send the information to server.
**Step 6:** If any action requested from server then execute that action.

**Step 7:** After executing the action notify server about it.
**Step 8:** Go to step 5.

### *IV.2 ARCHITECTURE*


**Figure 2. Architecture showing multiple agents**

In order to achieve confidentiality [6] and integrity in network monitoring, architecture based on multiple agents have been proposed. It is composed of different types of mobile and static agents which have the capability of resource monitoring, user activities monitoring. The fig 2 shows the architecture consisting of multiple agents[5]. In this architecture, we have one master controller agent (MCA) which is a main server and different Controller agent (CA). Each CA was dispatched from MCA and performed some specific task by dispatching monitor agent and action agent and then sent the response back to the MCA. Monitor Agent travels through a set of nodes and looks for the illegal and unauthorized activity against predefined rules set. After retrieving information regarding user activity and processes, mobile agent sends this information back to Controller agent.

In the same way, Action agent reaches to destination and performs action according to policy like System log off, unwanted process Killing, System shutdown.

### *IV.3 EXPERIMENTAL RESULTS*

The GUI of the system displays multiple client details after the admin logs into the system. Fig 3 shows a general view of multiple client activities that can be monitored by the admin. Fig 4 shows specific details that can be viewed and the actions that can be performed

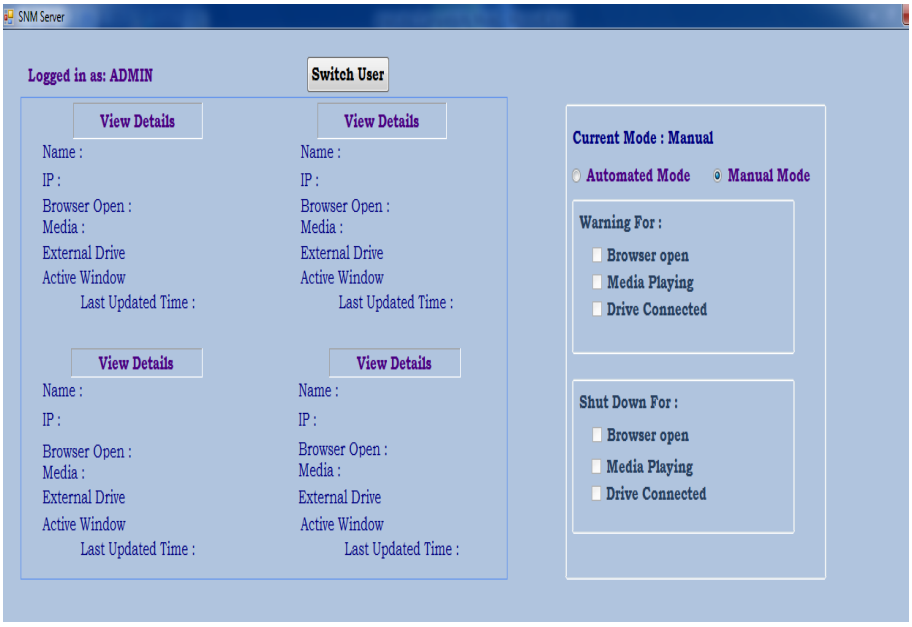


**Fig 3. Main screen to monitor multiple clients**

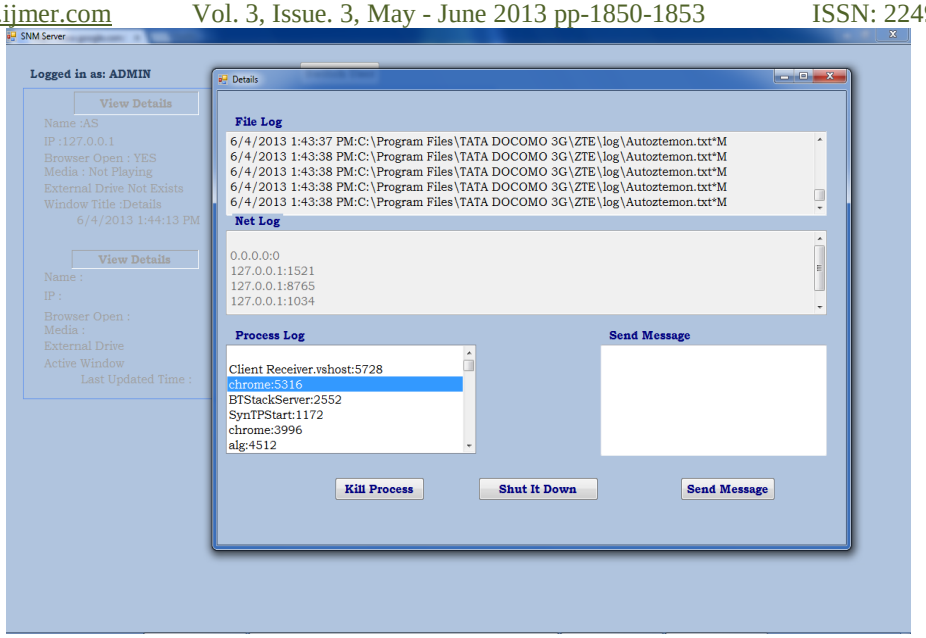


**Fig 4. GUI to view multiple logs and perform actions**

## V. CONCLUSION

In the process of making software application for Network Monitoring and Management using mobile agent which can be used for network monitoring, the various prospects which we have focused for network monitoring are Network Utilization, List processes currently being used, Network services and IP address verification. With this we have provided an authentication to the mobile agents by using simple cryptography algorithm which can stop any unauthorized agent to get executed in the network. With the help of Action agents we can take corrective action on client's suspicious activities.
Furthermore, mobile agent based network monitoring and management can overcome the shortcomings of SNMP and CMIP by decentralizing network monitoring and management.

## REFERENCES

**Journal Papers:**

[1]. *Network Traffic Analysis and Intrusion Detection Using Packet Sniffer*, Second International Conference on Communication Software and Networks, 2010

[2]. *Enhancing the Efficiency of Secure Network Monitoring Through Mobile Agents*, International Conference. on Computer & Communication Technology ICCCT, 2010

[3]. *Network Information Monitoring System in IPV6 Campus*, International Conference on System Science, Engineering Design and Manufacturing Information, 2011

[4]. *Network Sniffer Implement Network Monitoring*, International Conference on Computer Application and System Modeling (ICCASM), 2010

[5]. *A Secure Access Control Scheme Based On Group for Peer To Peer Network*, International Conference on Systems and Informatics (ICSAI), 2012

[6]. *Privacy Preserving and Ownership Authentication in Ubiquitous Computing Devices Using Secure Three Way Authentication*, International Conference on Innovations in Information Technology (IIT), 2012