A Proposed Agent System for Network Monitoring

Rana H. Majeed

Abstract:

The traditional centralized network management approach presents severe efficiency and scalability limitations in large scale networks. The process of data collection and analysis typically involves huge transfers of management data to the manager which cause considerable network throughput and bottlenecks at the manager side. All these problems processed using the Agent technology as a solution to distribute the management functionality over the network elements. The proposed system consists of the server agent that is working together with clients agents to monitor the logging (off, on) of the clients computers and which user is working on it. file system watcher mechanism is used to indicate any change in files. The results were presented in real time which is minimizing the cost that represents the important factor to successful management of networks that was achieved using agents.

Key words: Agent, Network Management, file system.

Introduction:

The need for data communication has evolved rapidly since the earliest days of computing. There has been a rise of computer networks in education, government and industry. However, faults and performance inefficiencies in these systems give rise to considerable business losses [1]. This makes the need for network management (including communication between network elements, systems and applications)

The term Network Management System (NMS) refers to the "sum of all procedures and products for planning, configuring, controlling, monitoring and of managing computer networks, as well as distributed systems and removing errors in all of these." [2]. the goal of NMS is to ensure that network users receive the information system technology services with the quality of services that they expect. To achieve this goal, the International Standard Organization (ISO) defined five network management applications: Performance Management, Fault Management, Security Management, Configuration Management and Accounting Management [3]. All of these management applications need to collect different management data from remote network elements, using what is called an information retrieval process.

Definition of an Agent:

There is no once-and-for-all definition to the term agent .However,one notation of agent that is broadly mentioned in many literatures is that an agent "is a software entity that can perceive and act in a proactive or reactive manner within a dynamic and uncertain environment where other agent exist and interact with each other based on shared knowledge of communication and representation"[4, 5]. To consider a software entity as an agent, it should have the ability to

*Al-Nahrain University, College of Information Engineering

interact (e.g. cooperate, coordinate and complete) with other agents and/or human as well as the ability to communicate and shared knowledge.

Agents and Management:

Eliot [6] believes that the place where agents are to achieve the biggest success is in the network arena, because of its complicated nature and its enabling infrastructure.

Also since cost is a critical factor in the network management, then agent must be the answer, for a number of reasons:

- Agents are persistent entities meaning they work all the time and for a long time.
- Agents are software entities and software doesn't ware out.[7]
- Software cost curve has a (bath tub) shape it starts high then drops to the low level that does not go up again unlike hardware [7].
- Agent support both modular and re- usability.
- They have high reliability.[7]
- They are automated entities and automation in the system can lower cost [8].
- Agents refine their performance.

For the past notes it is assumed that agents and agents based systems are good candidate to develop network management system.

Physical Implementation of the Proposed Agent System:

This section discusses agent design steps in of the system architecture**.** Agent design is divided in two parts **first**, network monitor **second**, File system watcher procedure. The network of the system is consisting of three computers one server and two clients.

1.System Architecture:

This section presents how the system put together to design a secure network using autonomous agents on the system work with **Client – Server.**

- **Server:** it is a SQL server which let its entire database available to all clients in the network that are connected to it.
- **Client:** it is a PC that are connected to server to send information to the server

So the proposed system will serve as:

- One PC applies as server, which has LAN card connected to hub as an out port.
- Second PC, implemented in the network as Client connected to the server through hub.
- Third PC, implemented in the network as Client connected to the server through hub. as shown in fig (1)
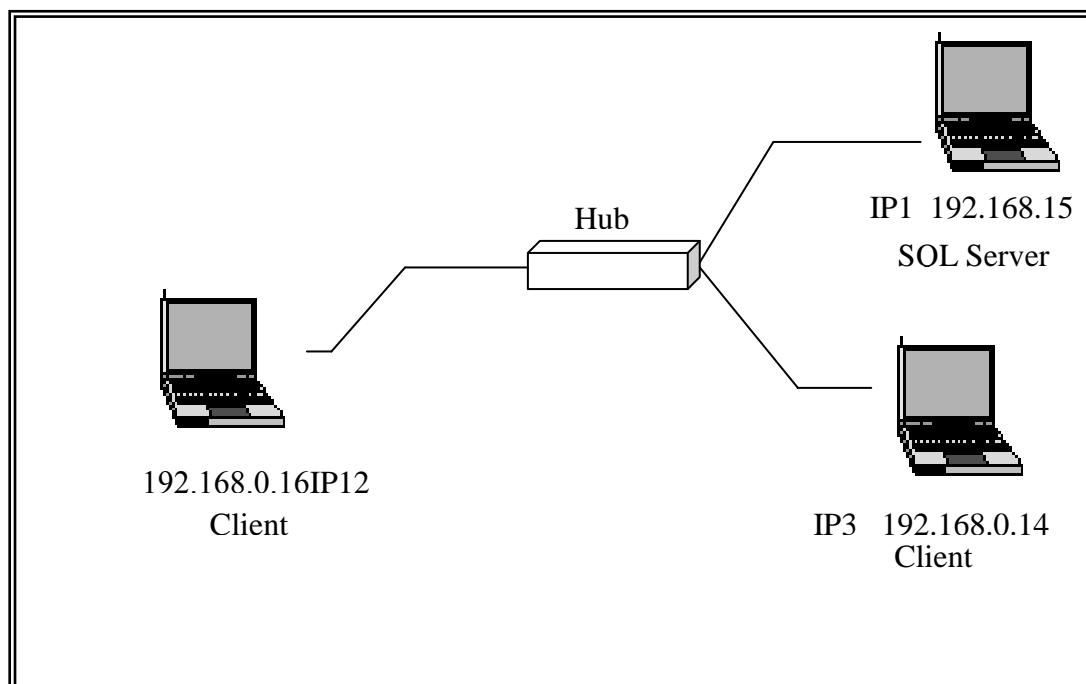
Fig (1) The Architecture of the Proposed System

Autonomous agent is a software agent that performs a certain security monitoring function at a server. The agent is called autonomous because it is independently running entities. The proposed model in Fig (1) shows a hypothelical distributed network management system using agent which consist of a network of client each client has a autonomous agent allocated to it.the system consists of the server agent located in server this agent is monitoring the whole system by communicating with other clients agents that located in clients.

2. Logical Design:

The proposed system consists of two parts (Clients agents and server agent). This can be explained by the following block diagram.
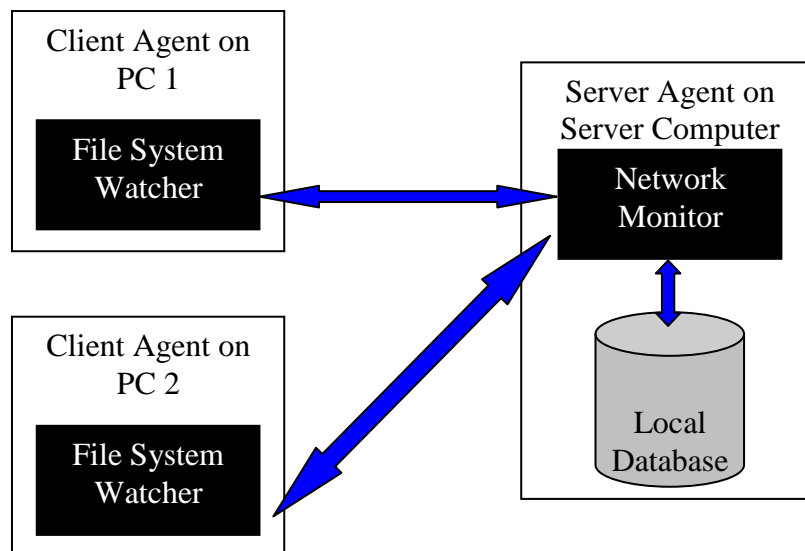
Fig (2) The Logical Design of The proposed System

2.1 Server Agent (Network Monitor)

The server agent is work autonomously in server computer and communicate with the client agent that work in client computer to retrieve information about the client computer and file system operations done in client computer. The sever agent an application to detect any changes in the file system directory this process is done automatically from the first moment of program running by communicating with clients if the connection is available and save any changes in the database of the server.

Client Agent (File System Watcher) 2.2

The client agent is an autonomous application works on client computer this agent in system has a specific tasks (test network connection, client computer file system watcher and monitor and interactions with server agent by sending information to it).if the connection is available on the clients computer the agents client send the status of connection is on and the user name of the clients computer this information is saved on the server data base.

The clients agent is designed as a file system watcher which detect the exact action on the file system in a specific path or file system under control if any changes happened like (copy, deletion etc) the agents clients communicate with server agents and send the type of the change, the date and time and the server agent save this change in the server data base.

Results of the Proposed System

The interface of the server agent on the computer server before running consists of status of connection is off, computer name, user name , the last action on the file system view log .view log is a history of all actions and the date and time of those actions. Fig (3) shows the interface as the first moment of running a program or when two users on the clients computer log off.
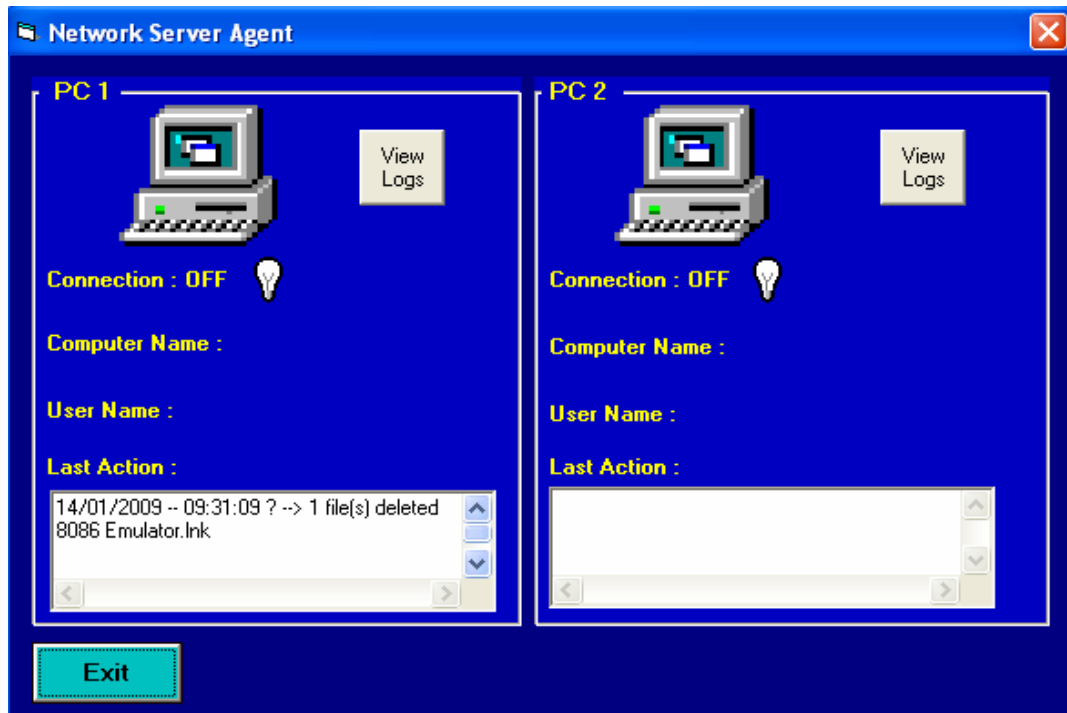
Fig (3) The server agent interface

When one of the users in the client's computer log on the clients agent send information of the computer name and user name of the clients computer as shown in fig (4)
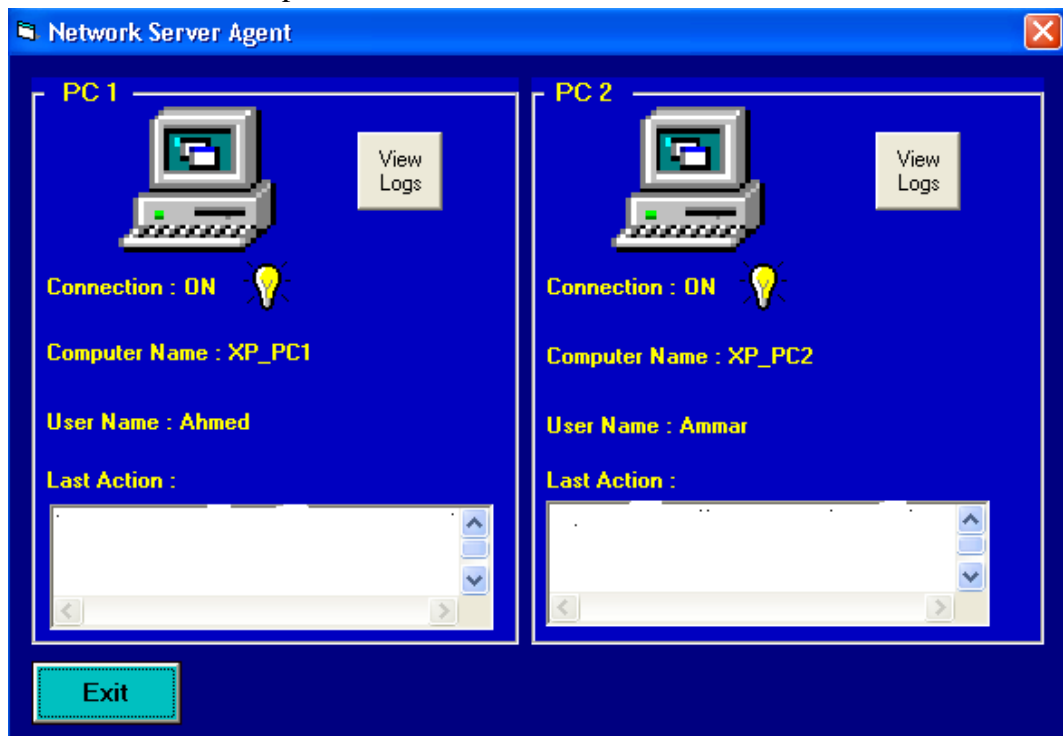

Fig (4) The log on of two users

When the file system watcher runs at the client computer the interface of this intelligent agent as shown in figure

When any change is done in the file system like (deletion, copy .. etc) the file system watcher in the client agent send the exacte action to the network

288

monitor agent for example when a code drag.txt file is deleted in the specific date and time and in a specific path and other actions on the rest files as shown in fig (5).
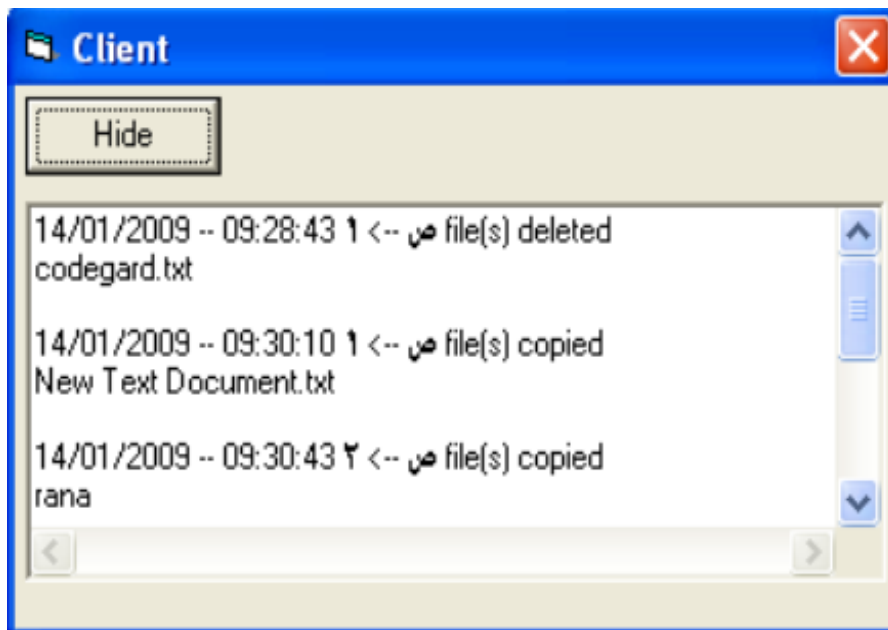

Fig (5) The change in the client agent interface

The last action done in the client computer is presented in the server agent interface as shown in fig (6) and if the administrator wants to see all the actions done in the clients computers the actions are saved in view log at the server agent interface as shown in fig (7).
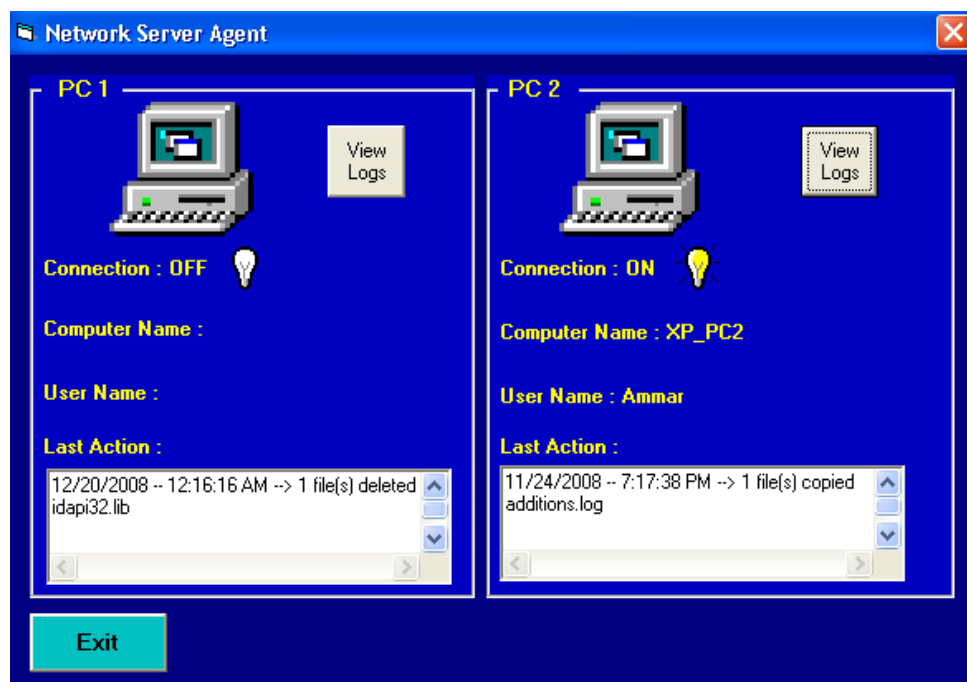

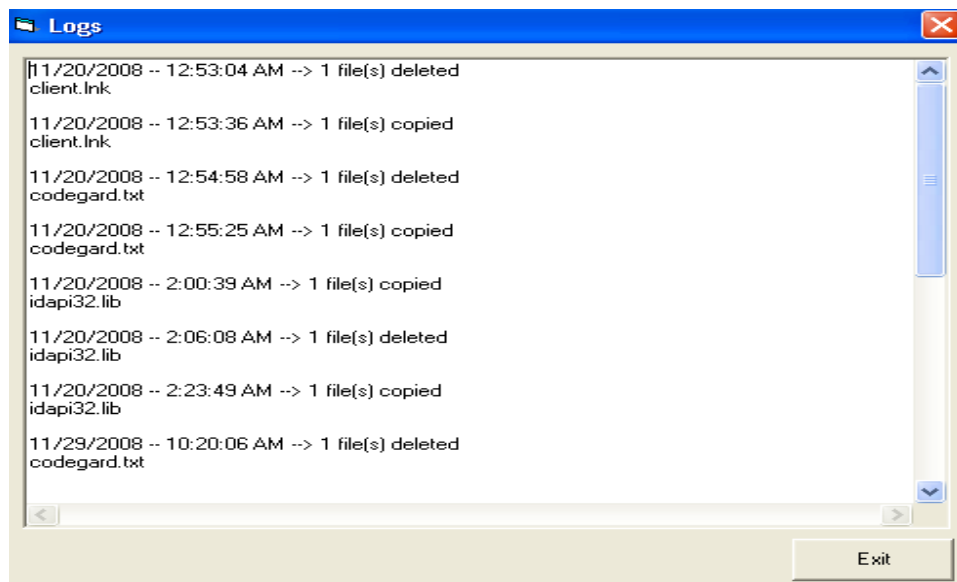**Fig (6) presenting last action on the server agent**

Fig (7) The View Log of All Actions

8. Conclusions

1. The proposed agent system is an autonomous program that can be work without any supervision.

2. The proposed system is used for getting information about client computer and to detect any changes in files or directory under control.

3. The agent is very important for monitoring because it works behind all application that works on desktop.

4. The agent was remained running until the user close his computer and record all the previous actions on sever database.

5. When two clients log on or log off at the same moment this process will presented at the same time on server computer.

References:

[1] D.Gavalas, "Mobile Software Agents for Network Monitoring and Performance Management", Ph.D. Thesis, University of Essex, UK, July 2001.

[2] G.Hegering, and S. Abeck," Integrated Network and System Management", Addison-Wesley, 1994.

[3] M. Subramanian, "Network Management Principals and Practice", Addison Wesley, 2000.

[4] N.R Jennings,and M. Wooldridge.,"IntelligentAgents:Theory and Practise",page 4-5,2000.

[5] Y.Shoham, "An Overview on Agent-Oriented Programming", In:Software Agent,J.M. Bradshaw (ED),Menlo Park ,Calif.,AAAI press 1997.

[6] M.Knapik,J.Johnson,*"Developing Intelligent Agents for Distributed Systems"*, McGraw-Hill Companies, Inc.,1998.

[7] S.Pressman, *"Software Engineering a Practitioner's Approach"*, 4th Edition, McGraw-Hill Companies, Inc., 1997.

[8] T.Rybezyniski, "Net Value The New Economic for Networking*"*, Nortel Networks, 2004.

نظام وكيل مقترح لأدراة الشبكة

رنا حميد مجيد

*وزارة العلوم والتكنولوجيا

الخلاصه:

ان الطريقه التقليديه المركزيه لادارة الشبكه تقدم تحديدات شديدة على كفاءة وتسلقية النظام الواسع للشبكة. ان عملية جمع المعلومات والتحليل النموذجي يتضمن تحويلات ضخمه في نقل المعلومات الى المدير والتي تؤدي الى سرعة وصول المعلومات واختناقات في الشبكة من طرف المدير. ان كل هذه المشاكل يمكن تجاوزها باستعمال نظام (تكنولوجية الوكيل) كحل للتوزيع والادراة الوظيفيه للشبكة. ان النظام المقترح يتالف من الخادم او الوكيل المستخدم والذي يعمل سوية مع زبائن الوكلاء لمراقبة دخول وخروج حاسبات الزبائن والتي يعمل عليها المستخدم.لقد تم استعمال نظام الفايل المراقب للاشارة الى اي تغيير في الفايلات.النتائج تقدم بالوقت الحقيقي او الاني وذلك يقلل الكلفة التي تمثل العامل المهم لنجاح ادارة الشبكه وذلك باستخدام وكلاء.