Mobile Agent for Monitoring Computer Networks

Roshan Kumara[1], Asoka S Karunananda[2]
[1]Center for computer studies, Sabaragamuwa University of Sri Lanka,
[2]Faculty of Information Technology, University of Moratuwa
Email:[1]rolanka@sab.ac.lk, [2]asoka@itfac.mrt.ac.lk

Abstract - **Network monitoring and maintenance have become crucial when a network comprises of several subnets with heterogeneous hardware and software environments. This paper presents the designing and development of a Mobile Agent based as a solution for monitoring the campus wide local area network in the Sabaragamuwa University of Sri Lanka. The System comprises of three Agents; Host Agent - located in a host, Mobile Agent - movable on the network, and an Agent running on a Mobile phone. The Mobile Agent consists of a stationary unit and a mobile unit. The stationary unit deals with scheduling and controlling while the movable unit travels to locations with faults and does repairing. The mobile agent has also been provided with basic toolkits such as newly updated virus guard, commonly used software, patches, etc. The Agent running on the mobile phone is responsible for sending messages to the administrator to attend to some critical faults. The system has been developed on JADE. JADE-LEAP implements the Agent on the mobile phone with limited resources. The system has been tested on several subnets to investigate the performance and accuracy in real cases.**

Keywords: **Mobile Agent, Computer Networks, Network Monitoring.**

1. Introduction

As networks grow larger, the network becomes more complex. Network monitoring becomes more crucial. In order to maintain and deliver high quality service to end users, network performance and usage must be monitored constantly and potential faults must be dealt with proactively. So the Network Administrators face the challenge of ensuring network efficiency, using of cost-effectively, and providing main services continuously. They need to monitor the whole network system with regard to connection failures and virus infection, if a problem is available, and then manage it while investigating the current status. Computer-based solutions for monitoring networks and communication with the Administrator have been a research challenge.

In recent years, Mobile Agent Technology (MAT) has emerged as a new paradigm for computer network management and monitoring its performance [1]. As a result, a number of research papers involved in MAT in computer network have been published. For instance, Network health care monitoring [2], network configuration management and fault diagnosis [3], Distributed Network Management [4] and Self-Configuring Network Monitor [14] can be cited as few examples. In order to review the technology for monitoring network, the latest trend is to deploy the Mobile Agent to monitor large scale heterogeneous networks. The Mobile Agent is a special object that is autonomous and has the ability to migrate from one node to another node, carrying logic and data, performing actions on behalf of the user. The Mobile Agent concept has many advantages likes autonomy, reactive, proactive, and adaptive capability and collaboration with other agents. After considering all the cases discussed above and current issues of the university network, MAT is more appropriate for monitoring the computer networks and its services. So this paper reports on the design and implementation of Mobile Agent based on network monitoring system (MobiNET).

Accordingly, the MobiNET contains three software agents; the first is Host Agent (HA) and the second which plays significant role in monitoring networks process, is Mobile Agent (MA). The third is in a mobile phone which is connected to the system. The MA has been designed with two main parts. One can live-in on any machine such as server, which is called Scheduling and Control Unit (SCU). It is responsible to manage all the functions of the Network Indicator (NI) and Work Schedule (WS). The other main part is Mobile Unit (MU); it has the ability to migrate to each subnet via LAN for repairing and maintenance of the network. Before its migration, threats from the virus and its possibility are investigated; next the migration process is completed for the maintenance on the host. When the system faces a critical situation, suddenly SCU identifies and subsequently sends the SMS and email which include descriptive information for the cause. The third agent, who lives in the mobile phone, is responsible for monitoring the paoosiblr failures of the MobiNET. If such a failure occurs then the Monitor Agent

sends SMSs to inform the Administrator. In this case, this system has been completely implemented by Java programming language, using JADE tool as an agent development environment.
The rest of the paper is organized as follows. The first section is a brief introduction of the paper. The second section describes related works in monitoring network. The Third section discusses the technology adopted to solve the problem and its appropriateness. The fourth section includes a discussion on the proposed approach to solve the problem. The fifth section reports on designing and implementation of the system. Next section points out the evaluation of the system, while the last section describes conclusion and further works.

2. The State of the Art for Monitoring Networks

An evolution of approaches for monitoring networks has been expanded by the growth in the network speed, bandwidth and technologies. The MA has taken a special place among them. The emergence of MA framework has led many researchers to examine their applicability for network management and monitoring. In this way, it would be interesting to discuss the appropriateness of the MA for monitoring the computer network.

Antonios [16] have developed the methodology for the Autonomous Network Monitoring System (ANMS). This system used traditional method for monitoring network congestion, anomalies, attacks and user define situation. Whenever it happens, the alarm issued by the system can then detect the system in a critical. Distributed Network Management System [4] has been used the MAT and addresses the scalability limitations of centralized network management. Their solution integrates with SNMP for gathering significant information, which is related to the network elements. Huawen Luo [5] has discussed the Agent related network management interaction with SNMP and using JADE as the agent development platform. Further, his discussion focuses on the inefficient problems when managing networks are large in scale, with additional features for programmability and customization of the system. Lee Yip [6] presents system prototype for small scale network management systems by using MAT. It provides the solution via the Internet environment and gives facility to the Administrator to manage and audit the hardware configuration remotely. That concept is more important to manage and update the network configurations remotely without the need of physical contact to the particular computer system. Hong van [7] presents the overall picture of the MA paradigm in computer network; how MAT has been applied in computer network and its applications, especially in fields of network management, resource management, routing and security. In addition to that, Peter Boon [8] has presented theoretical foundations for implementation of the MA system using java. According to the nature of the agent, it clearly indicates that requirement of the MA and its security requirements. Considering the above facts, agent design patterns are pointed out with its implementation using Java as the most suitable programming language.

After considering all these works, the author concluded that still no researcher is interested in producing a monitoring network system which has a dynamic on time communication with the Administrator and managing infections of the computer viruses.

3. Technology Adapted for Monitoring Networks

Agent is a powerful software interaction model that can act autonomously on behalf of its owner and other entities. Mobile Agent is also agent with ability to migrate freely between subnets across the heterogeneous networks. Therefore, MA is a combination of two distinct concepts: mobility and agent. It means, the main idea of mobility in MA is to move self-contained program and data near to a particular subnet. After this migration, MA will execute remotely relevant sets of management tasks, which have been defined according to the nature of the problem and its domain [7, 18]. At the end of these processes, the result will be handed over only to the particular agent. In this sense, this migration and execution results are useful to reduce traffic of the data transmission over the networks [7], that are solutions for the managing and monitoring distributed networks [19].

Features	Description
Mobility	Architecture provides the ability to the agent to move around from its origin location to the destination location to perform the task assigned.
Autonomy	Autonomy refers to the ability to operate without the direct intervention from humans and its own control over their actions and internal state.
Reactive	Reactive refers to the ability to perceive or sense the environment where it is living and to respond in a timely fashion.
Proactive	Proactive refers to the ability to determine the action and decision on behalf of the owners or users.
Adaptive (Learning)	Learning abilities give the agent the ability to adapt and learn from the environment, habits, preferences and working methods of its users.

Collaboration (Social)	Collaboration refers to the ability to collaborate with the other agents and the owners. Upon collaboration, an agent will consider the feasibility execution instruction before proceeding with further action.

Table 3.1: Special Features of the Mobile Agent

The MA has some special features; Table 3.1 describes agent features including mobility, autonomy, reactive, proactive, learning, and collaboration. Certainly, these features are used by the system to support monitoring in a productive manner. According to work in changing environments and react to unexpected events, a MA may need to adapt the current environment to execute the defined process correctly and efficiently.

In all respects, the most important concept of the MA is code migration. The main reason for code migration is to gain performance. For instance, a classic client/server model may consume some network bandwidth caused by all the request/response messages. Moving a process to another machine may reduce this, since only the process is transferred, and possibly, the results afterwards. This model also allows the client on which the agent will run to disconnect from the network after the agent was sent. Not only network bandwidth can be saved, but by sending multiple agents to different machines, parallelism can be achieved in a fairly simple way.

The MA is needed to install a Java Virtual Machine (JVM) as a support agent execution environment at each host the agent needs to visit. That is recommended to avoid moving agents unnecessarily, since this can increase network traffic [8]. Accordingly, there is no argument regarding the suitability of the MA for monitoring heterogeneous network.

4. Proposed Approach for Monitoring Networks

The MobiNET consists of three software agents; the Mobile Agent acts as the major of the system and the second is the stationary agent or the Host Agent which lives-in each connected subnet while the third is a Monitor Agent and it is on the mobile phone which is connected to the system. HA sends a request for the registration when the start-up process of the computer is activated. The MA has the ability to control the system and make it move to remote host for executions. Accordingly, the MA has been designed with two main parts. One can live-in on any machine such as servers, which is called SCU. It is responsible to manage the entire request, manage the NI, and control the WS of the MA. Other main part is MU; it has the ability to migrate to each host via the LAN and is responsible for the repairing and maintenance of the network. But, before each migration, threats from the viruses to the MU and the possibility of its migration are investigated by the SCU. After the migration, the MA can carry out its pre-assigned duties on the subnet. Sometimes MU will be unable to fix a particular problem. If it is a critical situation, then the MA sends an SMS to the Administrator. So it may be very useful to settle the problem immediately with the involvement of an authorized person. System failures of the MN are monitored by the Monitor Agent, and when a failure occurs; immediately the Monitor Agent identifies and sends the SMS message to the Administrator. In the view of proposed system, the MA must be able to carry out several concurrent processes in response to different external events. This implies that the behaviours of the MA must be scheduled cooperatively. The scheduler is implemented based on round-robin non-preemptive policy among all behaviours available in the ready queue.

User- The MobiNET is especially designed and developed for the usage of the Network Administrator by considering all the requirements.

Input- As the major input, data regarding the network status, network services and its failures are captured by the SCU communicating with SNMP agent. Furthermore, SCU sends ping message to each registered host of the MobiNET at fixed time intervals and gets the responses. That will be useful to detect the LAN connectivity and useful to carry on NI.

Process- in our approach, the university network is monitored by the system while maintenance process is continuing. Network monitoring functions investigate any system failures, virus updates and virus infections. The System is looking for any critical situation.

Output- The MobiNET provides the text based monitoring report for each computer and day reports regarding its service status and failures. This would be useful to carry on network maintenance to provide the qualitative and quantitative services to the end users. Additionally, when important subnets, servers, services or part of the network become a critical, the system immediately sends an SMS to the Admin. Concurrently, an email including reasons for the event is also sent to the Admin. Further, the SMS message is sent when system failures of the MobiNET occur. Then, necessary actions can be taken whenever and wherever the Admin is.

5. Design and Implementation of the MobiNET

As shown in Figure 5.1, the top level architecture of the system illustrates each module and its components and interaction with each other for the monitoring of the network process. The system

consists of three main modules: MobiNET (MN), Network Host (NH) and Mobile phone.

5.1 MobiNET (MN)
The MN is the main system and it contains the MA initially. The MA has been implemented with two units; SCU and MU. Always the SCU lives in the MN while MU is migrating for monitoring process.

5.2 Host Agent (HA)
The HA is a stationary agent and it lives-in each host of the network. As stated, the HA activates after the completion of the start-up process of the computer, and sends requests for host registration. In general, each HA is responsible to respond for the ping message from the MA and also sends an acknowledgement after the completion of the required process on the own host. In this sense, HA has limited behaviours to implement the defined tasks.

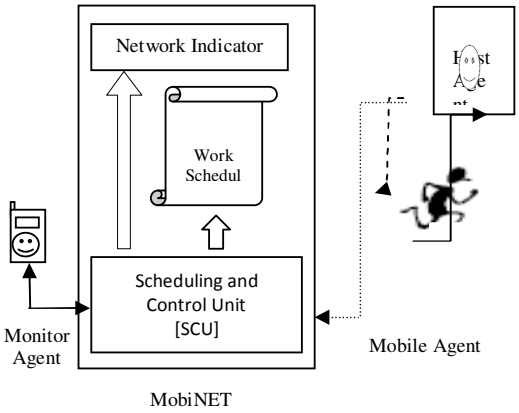

Figure 5.1: Top Level Architecture

5.3 Mobile Agent (MA)
The MA behaves as a system manager and it is the core part of the system, it is used to perform monitoring and controlling operation through its interaction with devices running agent processes. As stated, MA that runs on the MN server contains two modules: the static module is named as SCU and is located in a server, while the other module is MU and has the ability to migrate via network for remote execution, such as scanning for viruses, updating virus guard, removing virus infection, fixing problems.

5.3.1 Scheduling and Controlling Unit (SCU)
As mentioned, scheduling control unit is the stationary part of the MA and that is a new direction for the architecture of Mobile Agent system development. In this domain, after receiving a request message from the HA, it is accepted by the SCU. Then, the particular host will be registered. As a result, SCU updates the WS, & NI, and sends acknowledgment to the HA. Current status of the network is gathered via SNMP that is used to investigate the problems occurred. In the event that several problems occur in different subnets simultaneously, the SCU manages the work schedule concerning the matters such as priorities, its nature etc. Also, the SCU performs various tasks, especially investigation of network connection failures on each subnet and continuation of the NI, maintenance of WS and updating the system log file. After updating of the WS or NI, those events are stored into a database and serialized as the objects that can be used to store as an object when the system terminates due to unexpected errors. When the system starts, it can be de-serialized. In this case, object serialization is useful to store the object settings with java object output and input streams. SCU sends SMSs and an email to the Administrator when the network faces a critical situation. From the perspective of the system, the MA must be able to carry out several concurrent tasks in response to different external events. As stated in our approach, the SCU has been implemented based on round-robin non-preemptive scheduling among all behaviours.

5.3.1.1 Network Indicator (NI)
The NI is one of the components of the SCU, and it indicates an Internet and LAN connectivity of each host, especially web server, mail server, proxy server, DNS server and e-Learning management server. Further, that pays attention to indicate the virus infection and the state of the host. That will be important to continue network maintenance without any mistakes and enhancement of its services.

5.3.1.2 Work Schedule (WS)
The WS of the MA is controlled by the SCU and it is used to schedule the available works which require to be completed. When one is completed by the MA, that will be removed and list of schedule is shifted to upwards by one of them while log file is getting updated regarding the task completed. When urgent message is received, WS will be updated and made its priority also.

5.3.2 Mobile Unit (MU)
The special part of MA is called Movable Unit, and It executes the process required on the remote host according to available faults. If problems exist on to certain subnet, the MU is dispatched to the destination and it fixes the problem immediately. The MA should be protected from the computer viruses when it arrives and leaves the host and we recommend that MU should be scanned for viruses at each stage in the monitoring process. This unit

carries out its assigned duties on the subnet as entrusted by the stationary unit. For this purpose, the MU has been provided with basic toolkits such as newly updated virus guard, commonly used software, patches, etc. The MU performs certain tasks such as reading the WS for available works that need to be completed and then migrates by itself for repairing the connection failures, updating virus guards, scanning for virus infections and removing it without any interventions. After the completion of the required task on the certain subnet, MU reaches to its own server and updates the log file while removing the task which has already been completed, from the WS. The MA will be continuing these processes for monitoring networks. While MU is carrying on the respective jobs as defined, it sends the agent a message including process status to the MA. Then, the SCU understands that it is currently living in and continues defined jobs. Otherwise, as stated in the approach, New MU will be created and sent to the respective host to carry on its task. If MU is unable to reach the particular host, then, MU will be sent to the next host requested by the SCU to carry on the defined processes. After the completion of the task, the log file will be updated and the MU repeats the monitoring process for the next requested host.

5.4 Monitor Agent

The mobile phone has been connected to the system for communicating with the Administrator via sending SMS when the system requires. Failures of the MN are required to monitor for carrying out the monitoring process without any faults independently. Then, Monitor Agent is located on an external phone connected to the system, and responsible for monitoring system functionality. Further, the monitor agent is running in JADE-LEAP environment of the mobile phone. Once a failure in the main system occurs, the situation is identified by the Monitor Agent and an SMS is sent to the Administrator.

The MN has been implemented based on JAVA and JADE as an agent development environment. The eclipse tool is used as a programming code editor with Java (J2SE) and JADE. As stated above, the system has been modeled HA and MA. Agent ID is a unique name of the HA, that can be used to identify the specific agent and its host of the network. Each behaviour of the agent is completed with *jade.core.Behaviour* class. The instance of MA is identified by its code, state information and attributes. The Monitor Agent running on the mobile device was implemented using the LEAP add-on. The LEAF add-on, combined with JADE, provides a modified JADE-LEAF run-time environment for enabling FIPA agent to execute on mobile phone device running Java. It has been developed with consisting of only code excepting data. It especially affects to reduce the storage capacity and enhance the performance with managing available memory of the mobile device [26]. Assuming the communications for network monitoring scenario, MobiNet Ontology has been implemented in compliance with FIPA specification under *mobiNet.ontology* package and contains domain specific vocabulary. Further, defined *MobiNetOntology* gives syntax with different concepts, predicates and agent actions to make a meaningful message structure. SMSLib is a Java integrated API that provides required Java libraries to the system to send SMS text message. MA uses the GSM mobile phone connected via serial port or USB data port to send SMSs. At a critical situation, MA or Monitor Agent uses AT command to instruct the mobile phone to send relevant messages to the Administrator. As stated, the MA sends an email including the reason of the problem.

6. Evaluation

The prototypes developed in this project have been executed for monitoring the network status and identifying critical situations. As stated, a fair evaluation can only be achieved with careful selection of simulation parameters. In this sense, prototype of this system is applied on several subnets of a particular network including servers, in order to check for its reaction with reference to network failures and system accuracy in real life. During the testing period, we have also made some changes in certain subnets and inquire system responses by using system log details and NI.

Host No.	ACL Ping Messages	Disconnected by manually	Detected	Identifying critical	Message Sending
H48H83	192	12	10	8	7
H48H72	188	10	8	1	1
H49H05	192	10	11	2	1
H49H07	189	15	13	2	2
SN49H2	196	10	7	3	1

Table 6.1: Result of an identifying critical situation

Table 7.1 shows results of identifying a critical situation and sending Email and SMS messages. H48H83 is one of the servers and we made network disconnection manually. According to test results, System detects system failures and critical situations successfully and sends the email or SMS. The author defines specific limitations to identify the critical situation of the subnets.

7. Conclusions and Further works

Traditional network management and monitoring based on centralized architecture have been found with feasibility and inefficiency problems. In this sense, we proposed a Mobile Agent based solution. Applying the system, network failures have been evaluated by changing some state of the host and servers manually. Finally, the System records around 80% of system success with the identification of critical situations and sending messages. We discussed the overall system with three agents, one is Mobile Agent and others are Host Agent and Monitor Agent. Ontology of the monitoring network has been defined for agent communication in the system. We have already completed the first two agents and testing of the modules. Development of monitor agent is in progress. The MobiNET has been developed with the use of JADE and eclipse and the system runs on any platform which is connected to the LAN.

We have made some efforts to make the system more successful. Due to this extensive scope of the topic and problem domain, a complete software implementation of the system is beyond the scope of the paper. Implementation of the Monitor Agent and monitoring virus infection on the LAN could be considered as a future work.

7. Reference

[01]. Fabio Bellifemine, Giovanni Caire, Dominic Greenwood, "Developing Multi-Agent Systems with JADE", Telecom Italia, Italy, Whitestein Technologies AG, Switzerland,

[02]. Zapf M., Hermann K., and Geihs K. (1999 May), "Decentralized SNMP Management with Mobile Agents." In Proceedings of IM '99, Boston,

[03]. Ferudin M., Kasteleijn W, and Krause W., (1999) "Distributed Management with Mobile Components." In Proceedings of IM '99, the 6th IFIP/IEEE International Symposium on Integrated Network management, pp857-870, Boston.

[04]. Damianos Gavalas, Dominic Greenwood, Mohammed Ghanbari, Mike O'Mahony, (2000), "Advanced Network Monitoring Applications Based on Mobile/Intelligent Agent Technology", Computer Communications Journal, Vol. 23, No 8,

[05]. Huawen Luo, (2002), "Agent-based Network Management System", M.Sc. thesis, Faculty of Graduate Studies, University Of British Columbia.

[06]. Lee Yip Fei (2003),"Study and implementation of mobile intelligent agent for network monitoring and management", INTI Journal VOL. 1, NO. 3, Pp 193-196.

[07]. Nguyen Hong Van (2004), "Mobile Agent Paradigm in Computer Network", CUC 6th CARnet Users Conference.

[08]. Peter Boon (2005), "Mobile agent systems implemented with Java"

[09]. E.F. de Araújo Lima, P. D. de Lima Machado, J.C.A. de Figueiredo, F.R. Sampaio, (2004), "Implementing Mobile Agent Design Patterns in the JADE framework",

[10]. CERT® Coordination Center, (2002), "A Brief Tour of the Simple Network Management Protocol" ,

[11]. Magid Nikraz1a, Giovanni Caireb, and Parisa A. Bahria (2006), "A Methodology for the Analysis and Design of Multi-Agent Systems using JADE", International Journal of Computer Systems Science and Engineering. pp1-6

[12]. Emmanuel Reuter, Fran¸coise Baude (2002), "A mobile-agent and SNMP based management platform built with the Java ProActive library", http://citeseer.ist.psu.edu/old/reuter02mobileagent.html,

[13]. "Java SNMP Package Introduction" (2008 May), www.gicl.cs.drexel.edu/people/sevy/snmp/snmp_package.html,

[14]. Brian L. Tierney, Deborah Agarwal, Vern Paxson, (2001-2004), "Self-Configuring Network Monitor", A High Performance Network Engineering Proposal: Network Measurement and Analysis For the period June 1, 2001 – May 31, 2004.,(2), pp 3-4.

[15]. Manoj Kumar Kona and Cheng-Zhong Xu, (2007), "A Framework for Network Management using Mobile Agents", IEEE International Conference on Communications 2007**,**

[16]. Antonios Danalis , Constantinos Dovrolis, (2004), "An Autonomous Network Monitoring System", International Journal of Computer Systems Science and Engineering. Pp2-3

[17]. Supranamaya Ranjan , (2006) "Adaptive Mobile Agents: Modeling and a Case Study", International Workshop in Distributed Computing (IWDC 2000), Calcutta,India

[18]. Damir Horvat, Dragana Cvetkovic, (2000), "Mobile Agents and Java Mobile Agents Toolkits", Proceedings of the 33rd Hawaii International Conference on System Sciences

[19]. Shamila Makki, Subbarao V. Wunnava , (2006) , "Application of Mobile Agents in Managing the Traffic in the Network and Improving the Reliability and Quality of Service", IAENG International Journal

of Computer Science, 32:4, IJCS_32_4_16

[20]. Danny B. Lange , Mitsuru Oshima, (2004), "Mobile Agents with Java: The Aglet API", Proceedings of the 33rd Hawaii International Conference on System Sciences

[21]. Joan Ametller, Sergi Robles, and Joan Borrell, (2006), "Agent Migration over FIPA ACL Messages", IEEE International Conference on Communications 2007

[22]. Weiqin Chen and Riichiro Mizoguchi , (1990), "Communication Content Ontology for Learner Model Agent in Multi-agent Architecture", publications from mizoguchi lab http://www.ei.sanken.osaka-u.ac.jp/pub/, Pp 3-7

[23]. Fabio Bellifemine, Giovanni Caire, Dominic Greenwood, (2004), "Developing Multi-Agent Systems with JADE", Telecom Italia, Italy, Whitestein Technologies AG, Switzerland, pp77.

[24]. Asha Nagesh, (2006) "Distributed Network Forensics using JADE Mobile Agent Framework", Student Trade Show and Project Reports, Arizona State University, pp 5-6

[25]. Fabio Bellifemine, Giovanni Caire, Dominic Greenwood, "Developing Multi-Agent Systems with JADE", Telecom Italia, Italy, Whitestein Technologies AG, Switzerland, pp-145-151

[26]. Alf Inge Wang, Carl-Fredrik Sørensen, "A Mobile Agent Architecture for Heterogeneous Devices", Dept. of Computer and Information Science, Norwegian University of Science and Technology, Norway. pp-1-3