Ramiz H. Shikhaliyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
ramiz@science.az

DOI: 10.25045/jpit.v06.i2.07

A MOBILE MULTI-AGENT-BASED CONCEPTUAL ARCHITECTURE FOR THE INTELLIGENT MONITORING OF COMPUTER NETWORKS

The article focusses on the development of a conceptual architecture for intelligent monitoring of computer networks (CN). Mobile multi-agents are used, each of which monitors the individual components of the CN such as network equipment, connections, traffic, services and users. This architecture can extend the coverage of the monitoring system and ensure the completeness of monitoring data. Also, the architecture is easily scalable if required to monitor the new components.

***Keywords**: computer networks, network monitoring, monitoring architecture, CN components, intelligent mobile multi-agents.*

Introduction

Today, along with the extensive use of network technologies, the complexity and scale of computer networks are increasing. More effective performance, the improvement of service quality, troubleshooting and network security have become very important tasks. Monitoring plays an important role in solving these problems and controlling CNs efficiently. For the effective management of CNs, it is important to analyse monitoring data, without which it is difficult to make reasonable decisions. At the same time, almost all the events occurring in the CN are important in decision making; accordingly, comprehensive monitoring of the CN need to be performed. Consequently, the effectiveness of CN control mainly depends upon the effectiveness of monitoring.

Analysis of existing monitoring systems shows that they have a number of shortcomings.

First, they are centralized that is, acquisition and processing of monitoring data is accomplished by one monitor in respect to a particular component of CN (for example, network traffic, network connections and network services, user behaviour, etc.). This complicates the acquisition, processing and analysis of the vast amount of data to be transmitted to the monitoring centre.

A second drawback is that intelligent methods are not used for the acquisition and processing of monitoring data, but if used, it is not known which methods have been considered.

A third disadvantage is that, if necessary, the monitoring function cannot be expanded.

Therefore, the use of intelligent technology can increase the efficiency of monitoring CNs because they are able to simplify and facilitate the monitoring of CNs. In addition, the use of intelligent technology minimises the role of humans in the monitoring of CNs, reduces the loss of valuable information, and minimises the impact of the monitoring system on the normal work of CNs [1].

This article focusses on the development of a conceptual architecture for monitoring the CN with the use of artificial intelligence elements. Namely, an intelligent mobile multi-agent-based conceptual architecture is offered for the intelligent monitoring of CNs because the existing architectures are not effective, as the characteristics of traffic and the topology of contemporary networks are so dynamic. Centralised monitoring architectures have problems with scalability, and static, hierarchically distributed monitoring architectures have problems with flexibility and productivity.

The paradigm of mobile agents (MA) has emerged in the area of distributed computing. They are separate programs that can shift across the network from one host to another, resume or restart their work, and act on behalf of users for tasks [2].

Thus, the mobile agents are autonomous, reactive and communicative subjects. Intelligence of the agents may include the ability to learn, adapt, analyse and make decisions, plan and perform complex tasks that include collaboration with other agents or users and the ability to move across the network and to perform tasks on each of the planned stopping point.

Review of works

The CN environment has changed substantially, in that it uses a variety of network services and hardware and software developed by different manufacturers, and the number of users has multiplied. These changes have led to an increase in the probability of various problems occurring in the network and have increased the complexity of CN monitoring.

The literature describes various approaches to the construction of a CN monitoring system. Available monitoring architecture cannot ensure the comprehensiveness of the monitoring data to identify and evaluate all possible problems that could occur in a CN because these architectures are intended to monitor certain aspects of CN performance (e.g., security, productivity, etc.) [3, 4] and a specific CN component (e.g., network equipment, network traffic, network services and users).

In [5] the authors offer Service Level Agreement (SLA) monitoring architecture to provide fault tolerance and security services for CNs (e.g., financial, commercial and other corporate services). Denial of the services specified in SLA can lead to significant losses, so their monitoring is necessary.

The proposed architecture allows the authors to determine the strategy for the control of network fault tolerance. In [6] the authors propose an “end to end” network monitoring architecture named gd2. The proposed architecture allows the dynamic monitoring of the grid environment and solves the scalability problem introduced by the grid environment, whereas available monitoring systems cannot implement monitoring of network performance in real time.

In [7] the authors propose a mobile agents-based architecture for distributed systems of active network monitoring. The distributed monitoring system of CN based on management protocols such as Simple Network Management Protocol (SNMP), or distributed object technologies such as Common Object Request Broker Architecture (CORBA) cannot solve the scalability problem. They are also not appropriate for the monitoring of large and dynamic systems like CNs. Despite the fact that the monitoring systems are distributed, the principle of their performance is predetermined.

The agents of the proposed monitoring system act as monitors of certain segments of the network and are not related to any specific network nodes; furthermore, they can move to achieve the most favourable location. Mobile agents are autonomous objects designed for the performance of specific tasks, and they can shift from one node to another.

In [8] and [9] the authors propose monitoring architecture for high-speed networks. In particular, in the first paper, the authors propose a High Speed Network Monitoring and Analysis (HISTORY) architecture, which is designed to monitor high-speed networks. This approach is based on high-speed monitoring, which can process up to one gigabit per second.

The monitoring architecture is based on standard protocols such as the Internet Protocol Flow Information Export (IPFIX) and Packet Sampling Protocol (PSAMP), which are used for monitoring the data transfer between the monitoring elements and for the subsequent analysis of the traffic. In the second paper, the authors propose an architecture called Next Generation Monitoring (NG-MON) to monitor the high-speed network (10 Gbps or higher). NG-MON uses a passive monitoring method in which serial and parallel processing of traffic packets are used, which reduces packet loss significantly. In addition, this approach uses a lower, fixed amount of capacity for each flow, as the amount of memory depends linearly on the rate.

Computer network monitoring methods

There are various methods for CNs monitoring in the literature, such as centralised and distributed monitoring [10]. In central monitoring, the one monitoring server directly monitors the entire system (Figure 1). At the same time, the server collects, aggregates and processes the network data. The centralised monitoring method is mostly used for the monitoring and control of relatively small networks where SNMP-protocol is used.

This monitoring method has some drawbacks such as low efficiency and accuracy and lack of scalability. The acquisition and processing of large amounts of network data can lead to an overload of the monitoring and network communication centre itself. As a result, the number of network elements is limited and the rate of data entries to the monitoring centre decreases as well.

Additionally, the SNMP-protocol uses polling constantly, which results in the generation of additional traffic, even if significant changes do not occur in the network.

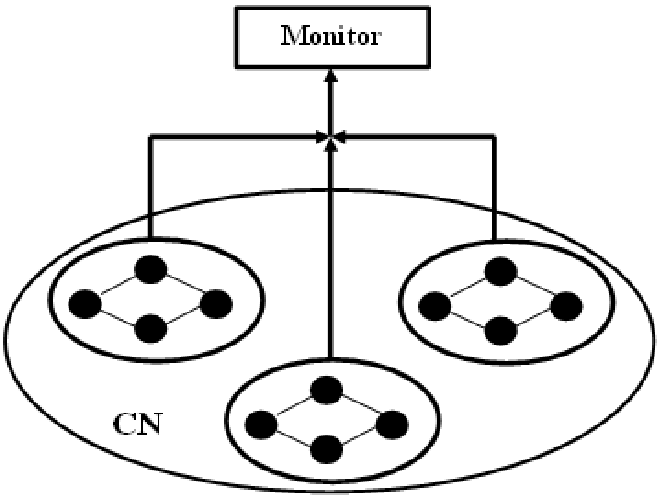

Fig.1. Centralised monitoring of computer networks

The distributed monitoring method allows the increasing performance and scalability of the monitoring system (Figure 2). This method is mainly used to monitor and control large networks. Distributed monitoring systems have a hierarchical architecture, which includes multiple monitors, one of which functions as the core, while others monitor separate segments of the network or subnets and collect monitoring data for the segments' elements. At the same time, monitoring functions are distributed between central and distributed monitors.

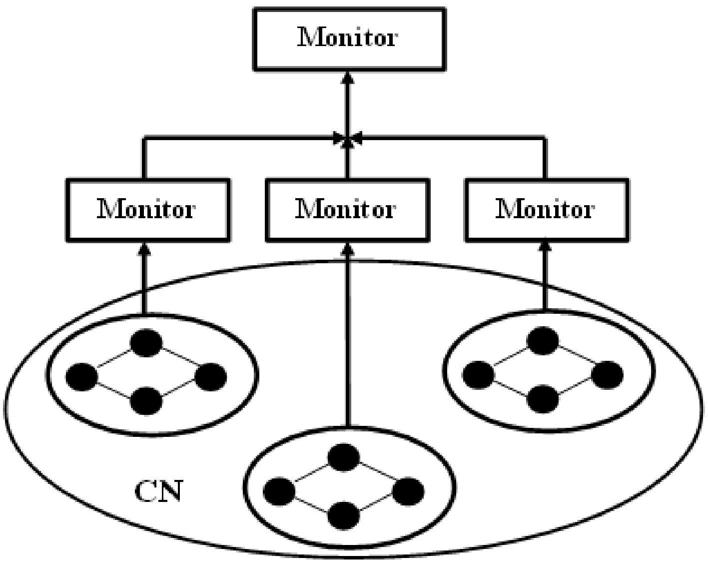

Fig.2. Distributed monitoring of computer networks

The main disadvantage of distributed monitoring is the fact that distributed monitors operate in specific network segments or subnets, and cannot adapt to changes in the CN. Thus, despite the fact that a distributed monitoring system can solve the problems of performance and scalability, they are not as effective in dynamic environments. Therefore, in this paper, we propose an architecture for monitoring a CN in which mobile multi-agents are used as distributed intelligent monitors, which we believe can help to solve the problem.

Multi-layer representation of the interaction of computer network components

To implement a comprehensive and effective monitoring of CN, it is necessary to develop a monitoring architecture that will allow the monitoring of key components such as network equipment, connections, traffic, services and users. Such architecture will allow the identification and assessment of all kinds of problems occurring in the CN. Before determining the architecture for CN monitoring, the interaction of the main CN components will be represented in the form of a pyramid, as shown in Figure 3.

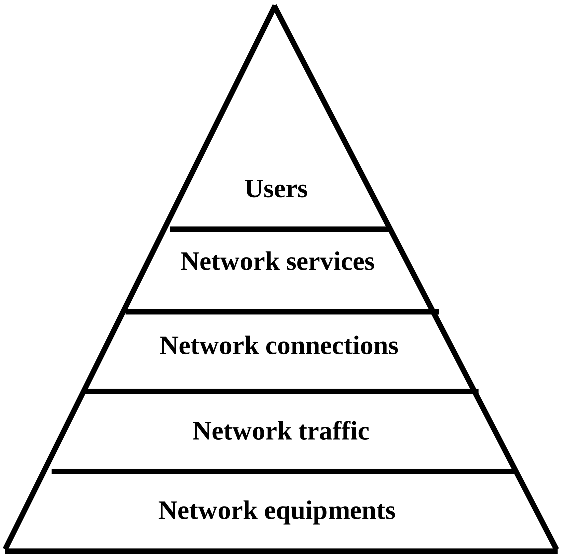

Figure 3. Multi-layer representation of the main components of computer networks

A layer of network equipment, which includes computers and network communication equipment, is at the base of the pyramid, shown in Figure 3. In this layer, data processing and storage and data package transfer between computers occurs. The next level includes a layer of network traffic, which consists of streams of data packages transmitted between computers and the Internet. The network traffic layer is followed by the layer of network connections that are available in network traffic. The next layer consists of network services that initiate the network connection and generate network traffic. Finally, the top level of the CN is a layer of users of the network services.

Conceptual architecture for computer network monitoring

In this section, a conceptual architecture for intelligent, mobile, multi-agent-based, comprehensive monitoring of a CN is proposed (Figure 4). The process of mobile agent functioning is presented in [1]. Initially, the mobile agent software module is created and stored on a separate computer, the home machine. The agent is sent to a remote computer, called the mobile agent host, for execution. The mobile agent host is also called the mobile agent server. Besides the agent, the mobile agent code and status data are sent to the host. The host provides the agent with a suitable environment for execution. At the same time, the mobile agent uses host resources (CPU, memory, etc.) to perform its task. After completing its task in the host, the mobile agent is transferred to another computer, and mobile agent migration continues as long as the mobile agent returns to the home machine after the completion of the task on the last machine in the route.

The proposed conceptual monitoring architecture is multi-layered and covers the main components of a CN, such as network hardware, connections, traffic, services, and users. Separate intelligent agents including a network equipment monitoring agent, connections monitoring agent, traffic monitoring agent services monitoring agent and a user behaviour monitoring agent are used to monitor each element of the CN. In addition, each agent uses a different monitoring protocol. In this architecture, the agent-interface is the bridge between the administrator and the agents, which transmits the administrator requests to the agents and presents the results of monitoring to the administrator.

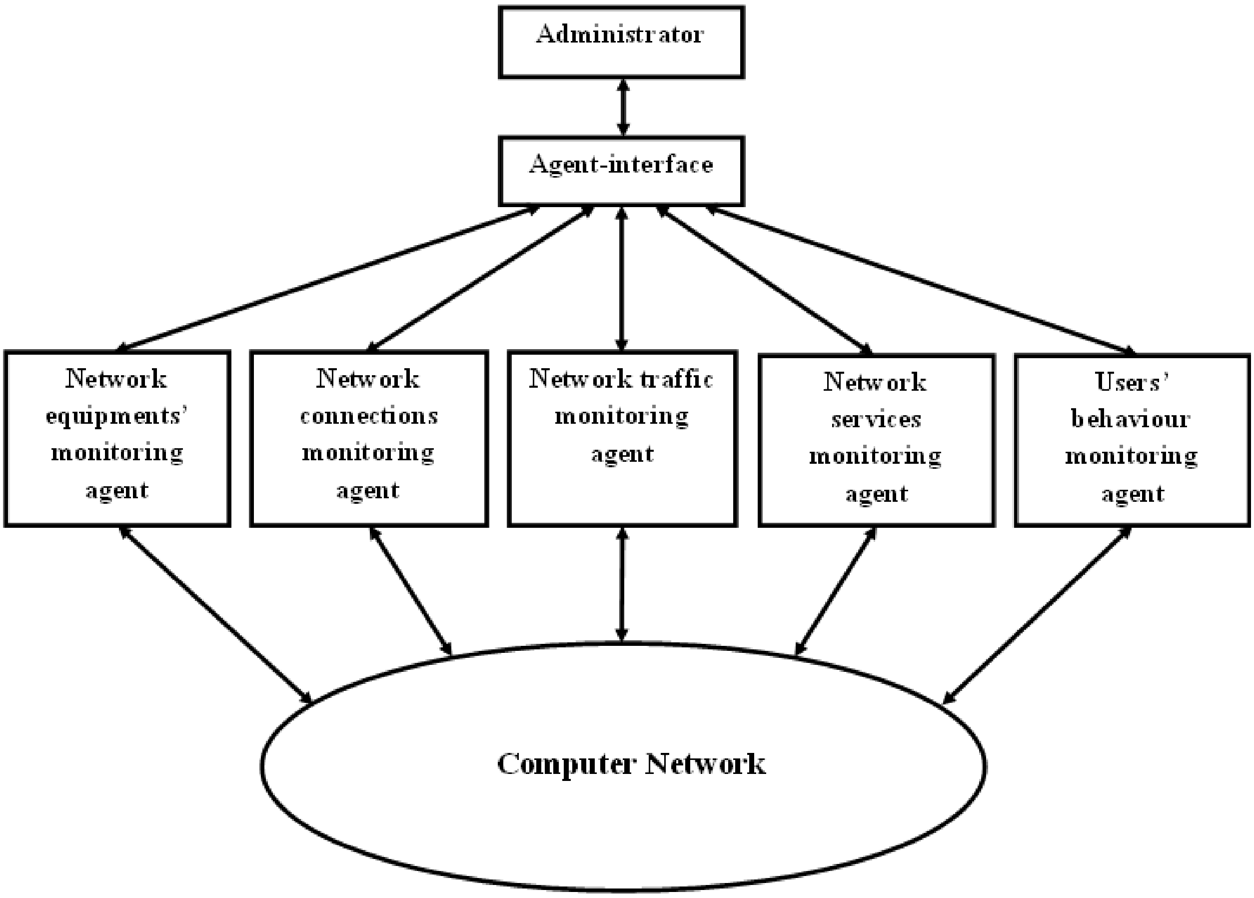

Figure 4. Conceptual architecture for intelligent monitoring of a CN

The advantage of the architecture is that the coverage of the monitoring system can be expanded, ensuring the completeness of the monitoring data of the CN. In addition, due to the intelligence and flexibility of the mobile agent, the rapid and effective solutions for network monitoring and control are possible. Furthermore, the system is easily scalable, since, if necessary, new intelligent agents can be introduced to monitor the new components. For example, to monitor CN safety, a security agent should be introduced [11].

Conclusion

In this paper we propose a mobile, multi-agent-based conceptual architecture for intelligent monitoring of a CN. The proposed architecture is multi-layered. Each level represents different components of a CN, such as network hardware, connections, traffic, services and users. The architectures of available monitoring systems are generally centralised, and the monitoring is performed for a particular component of a CN, for example, network traffic, connections or user behaviour. Such architectures for the monitoring of CNs are not effective in the circumstances of the ever-changing traffic and topology of contemporary networks. Moreover, they have problems with scalability. The proposed architecture can extend the coverage of the monitoring system of a CN, ensuring the completeness of monitoring data. In addition, the system is easily scalable, since, if necessary, new intelligent agents can be introduced. Due to the intelligence and flexibility of the mobile agents, rapid and effective solutions for network monitoring and control are possible.

Acknowledgements

This work was supported by the Science Development Fund under the President of the Republic of Azerbaijan – grant: No EIF-RITN-MQM-2/IKT-2-2013-7(13) -29/27/1

References

1. Shikhaliyev R.G. On the use of intelligent technologies to monitor computer networks // Artificial Intelligence, 2011, No1, pp. 124-132.
2. Gavalas D., Greenwood D., Ghanbari M.and O'Mahony M. Hierarchical network management: A scalable and dynamic mobile agent-based approach // Computer Networks, 2002, vol. 38, no. 6, pp. 693–711.
3. Ambika M., Nataraj R.V. Architecture for Real Time Monitoring and Modeling of Network Behavior for Enhanced Security // International Journal of Computer Applications, 2013, vol. 64, no.8, pp. 21–25.
4. Phipps A. Network performance monitoring architecture. Technical Report EGEE-JRA4-TEC-606702-NPM NMWG Model Design, JRA4 Design Team, September 2005.
5. Shirazi N.H., Schaeffer-Filho A., Hutchison D. Service Level Agreement Monitoring for Resilience in Computer Networks / 13th Annual Post Graduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting. Liverpool: Liverpool John Moores University, 2012.
6. Ciuffoletti, A., Marchetti, Y., Papadogiannakis A., and Polychronakis M. Prototype implementation of a demand driven network monitoring architecture / Grid Computing – Achievements and Prospects. Springer, 2008, pp. 85–97.
7. Liotta A., Pavlou G., Knight G. Exploiting Agent Mobility for Large Scale Network Monitoring // IEEE Network, Special Issue on Applicability of Mobile Agents to Telecommunications, 2002, vol. 16, no. 3, pp. 7–15.
8. Dressler F., Carle G. HISTORY – High Speed Network Monitoring and Analysis / Proceedings of 24th IEEE Conference on Computer Communications, Poster Session, Miami, FL, USA, Mar. 2005.
9. Han S-H., Kim M-S., Ju H-T., and James Won-Ki Hong. The Architecture of NG-MON: A Passive Network Monitoring System for High-Speed IP Networks, Lecture Notes in Computer Science 2002, vol. 2506, pp. 16–27.
10. Liotta A. and Pavlou G. Exploiting agent mobility for large-scale network monitoring // IEEE Network, 2002, vol. 16 no. 3, pp. 7–15.
11. Nguyen N. T. et al. A Multi-agent System for Computer Network Security Monitoring / Proceedings of the 2nd KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications, 2008, pp.842–849.