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

DOI: 10.25045/jpit.v07.i2.08

ANALYSING THE DEVELOPMENT TENDENCIES OF MONITORING METHODS OF THE COMPUTER NETWORKS

Today, the adoption of effective solutions for the management of computer networks (CN) is not possible without their monitoring. Monitoring of various parameters allows the CN to receive the necessary information about their condition. The paper deals with the development of methods for monitoring in the context of the development of the CN. The problems of the CN monitoring in various aspects, such as the construction of a distributed monitoring architecture, intellectualization of monitoring methods, collection, storage and analysis of large volumes of network data, network traffic classification and clustering, network monitoring visualization, QoS monitoring, Wi-Fi networks monitoring, and summarizing of the existing approaches to address these problems.

Keywords: *computer networks, monitoring, distributed monitoring architecture, intellectualization of monitoring techniques, network traffic classification and clustering, network monitoring visualization, QoS monitoring, Wi-Fi networks monitoring.*

Introduction

Today, computer networks have become an important factor in the efficient operation and development of almost all areas of the society. CN is a system in which a plurality of computers is connected together to share information and resources. CN and used applications can improve the performance of the work carried out by both public and private organizations. However, this dependence on CN emerges risks associated with the failure, the failure of networks or their low productivity, security breaches, etc. These risks may cause more damage, both material and moral (staff downtime, loss of reputation and customer dissatisfaction, etc). It is necessary to reduce these and other risks to constantly monitor the CN.

Monitoring is a very important element in the effective management of modern CN. The main purpose of the monitoring is to obtain the necessary information about the status of the CN, to take effective management decisions. Thus, monitoring generally involves measuring certain performance of the CN, and the aggregate function deducing from these measurements. These indicators describe the status and performance of the network in terms of resource use, overload, packet loss, and help administrators identify potential problems. However, by measuring and analyzing, the network traffic parameters can be maintained and ensure the security of users of the network from external and internal attacks [1].

When it comes to monitoring, the CN is composed of objects with various parameters that are characterized by the state of these objects and which are determined by the relevance and completeness. These objects include such CN elements as network equipment, network connections, network traffic, network services and users. At various stages of the CN's development, the various objects of the CN were monitored. Moreover, at various stages of the CN development, goals and objectives were determined and various methods were used.

The purpose of this article is to consider the issues of the CN monitoring methods in the context of the CN, because the development of the CN monitoring methods is inextricably linked with the development of the CN itself. At the same time, the article analyzes the existing concepts and methods for the CN monitoring, as well as existing problems in this area.

The evolution of computer networks

It is necessary to analyze the development of the CN itself before analyzing the development of the CN monitoring. Since the analysis of the development of the CN will allow us to understand the development of monitoring trends, and identify trends and development propects of this area.

Initially, the CN have been created as a network data switching or data, which included the results of the information and communication technologies development [2]. Nevertheless, today, CNs are a great repository of information that are constantly growing. At the same time, a great CN influence, exerted on other types of telecommunication networks, has led to their convergence, and digital voice transmission across the telephone network was one of the first stages of convergence. Since the late 1960's, voice in a digital format has become more common in telephone networks. Later, CN of such new services appeared as Voice over IP (Internet protocol), radio and television program. However, the network convergence process takes place today.

Creating a multi-terminal systems.

CN appeared in the late 1960s, and the first prototypes were multi-terminal system. In such systems, a central computer (mainframe) was used by multiple users. Each user of its own terminal can access to the central computer. Along with all of these, the time, which the central computer needed to respond to the users' request, was quite little. Therefore, it could serve multiple users simultaneously. It must be emphasized that such systems were generally operated in data centers. Later, the data centers' terminals have moved to workplaces at organizations. The calculations were carried out centrally, and input and output of data were put. Users were able to use the shared files and peripherals, as well as to run any program on a central computer at any time and get results almost instantly. It was a feeling that all the calculations were carried out at the terminals, and the emergence of such systems could be considered as the first steps in the local area networks' creation (LAN).

Creating global networks (WAN).

The next stage of development of the CN is the need to connect computers located at a great distance from each other, that is the creation of global networks. In this case, the main task was to provide access to the central computer of the terminals, which were located hundreds and sometimes thousands of kilometers from each other. At the same time, the connection was not only provided between the terminals and the central computer, but also between the central computers. As a result, computers were to communicate in an automatic mode, and the first farm, which was used to connect geographically remote computers based in different cities or countries. In such networks, the developers have implemented services such as file sharing, synchronization of databases, e-mail, etc. This GN development is mainly dependent on the development of telephone networks. However, it must be emphasized that exactly in the development of GN many fundamental implementations were introduced and elaborated on, which underlie the modern GN, such as: multilayered architecture of communication protocols (cooperation); packet switching technology; a packet routing technique in heterogeneous networks, etc.

Despite the fact that, the Global Networks inherited many features of the telephone network, and it was subsequently decided to abandon the use of channels commutation technology, which was successfully used in telephone networks for decades. Experiments and mathematical modeling, carried out by experts, showed that a network based on packet commutation can transmit packet traffic more efficiently. Although, due to the fact that the construction of high-quality communication lines connecting remote nodes was very expensive, the first GN used the existing communication lines that originally were intended for a variety of purposes. For instance, for a long time, GNs have been constructed on the base of telephone lines, therefore, the digital data transmission rate, which used such links was relatively low and amounted to hundreds of kilobits per second (Kbps). A set of services provided by these networks was limited to file transfer, which is mainly performed in the background and e-mail. In addition to the low data rate, such channels have another drawback - they significantly distort the transmitted signals. Thus, GN protocols that use low quality communication line were characterized by complicated control procedures and data recovery, as an example the protocol X.25 can be shown [3]. Usually, such low-speed networks of analog channels used to connect computers and switches.

Creating Internet.

In 1969, the US Department of Defense began research on computers connection to the network in the research centers. This network was called ARPANET (Advanced Research Project Agency Network) [4] and was the beginning of construction of the first and most well-known GN, known as the Internet nowadays. Various types of computers which used different operating systems and add-on modules were connected to the ARPANET for the implementation of communication protocols that were common to all computers. These operating systems could be considered as the first network operating systems that were different from the multi-terminal onces by not only distribution of network resources between users, but also allowance to distribute processing and organize data storage.

In 1990, the design of high-speed digital channels-based GN began, which greatly expanded the range of used services, some of which has been designed for the LAN. Due to the use of high speed channels, transmission of a great amount of multimedia information in real time, including image, video and voice became possible. World Wide Web (WWW) [5] - hypertext information service has become the premier information service on the Internet.

Creating a local area network (LAN)

The next stage of development of the CN is associated with the creation of a LAN. [6] In the early 1970s, large-scale integrated circuits that had low cost and high functionality have been developed, resulting in the creation of mini-computers. Mini-computers were able to solve problems much faster than central computers (mainframes). Even small organizations could have their own mini-computers, because of the relatively low cost. That was the beginning of distributed computing concept, in which computing resources distributed across the organization. Along with that, all of the mini-computers in the organizations functioned independently. As a result of the unification minicomputer of the organizations into a single network, first LANs were formed.

Then, personal computers (PCs) appeared, which have become an ideal element of a LAN, since they were powerful enough to support the networking software. However, it had the opportunity to combine their computing power to solve complex problems and to share expensive peripherals and disk space. Because of this, PC had been widely used in LAN, and played the role of not only customers, but also served as storage and processing centers. In this case, the standard technology, used in LANs, based on the same method of switching, which was used to carry traffic in the WAN, I.e, on the method for packet switching. Thus, we began to build a LAN using standard network technologies (e.g., standard network cables and adapters, as well as the Ethernet [7] technology and popular in those days, network Novell NetWare operating system [8]). Meanwhile, access to the shared network resources has became much easier, and, unlike the GE users did not need to remember complicated shared resource identifiers. In the next stages of development of CN difference between LAN and WAN began to decline, developers and networks began to combine separate LANs via WAN. As a result of this, the integration has been a significant interpenetration of the respective technologies. In addition, IP use also contributed to the integration of LAN and WAN.

Today, with the development of information technologies, CNs become very complex, diverse and distributed systems. This, in turn, leads to the emergence of new problems in their monitoring. CN monitoring problems can be considered in various aspects, such as the construction of distributed monitoring architecture, intellectualization methods of monitoring, collection, storage and analysis of large amounts of network data, classification and clustering, network traffic visualization network monitoring, QoS (Quality of Service) monitoring, monitoring Wi-Fi networks, etc.

The development of computer networks monitoring methods

Based on the analysis of the evolution of the CN, we can conclude that monitoring methods were also improved along with the development of CNs. Each stage of development of CN, somehow, defined goals, objectives, and monitoring problems. With the increasing complexity of the CS, increased complexity of their monitoring methods. For instance, at the initial stage of the era of information in order to ensure continuity of service and security of central computers automatic monitoring systemi needed, which would be monitored by their general use. Nonetheless, such systems were vulnerable to human errors that could lead to the destruction of the system information or user information, and retain control over the system after all necessary calculations had been ended [9].

By the end of the 60s, there was a hardware monitoring system for monitoring time-sharing [10], and software with a graphical interface [11, 12]. Such a monitoring system to perform periodic collection, storage and processing of certain network parameters. At the same time, there were problems with the selection of the most significant data and methods of displaying them.

With the development of information technology, the widespread use of the CN has begun. Though, there were problems with their service (administration). This was mainly due to the fact that there was no enough IT professionals and the cost of their services was very high. As a result, the cost of ownership of the CN was very high. Therefore, for the analysis of monitoring data of the CN began to develop a variety of expert systems [13, 14]. These systems are mainly used traffic characteristics and network information about the applications, and greatly facilitated the implementation of network administrators on CA management.

In 1995, the remote monitoring method was proposed, for the implementation of the Distributed Management CS IETF (Internet Engineering Task Force), which is called Remote MONitoring (RMON) [15]. The method was to use monitors - devices that monitored network traffic. Monitors could be implemented in the form of devices with embedded applications, and in the form of separate devices. Monitor tasks were to monitor network traffic network segments in which they were located, and the prevention of network administrators of anomalies in the form of alarms. At the same time, network administrators by determining the types and thresholds alarm values could regulate the amount of collected data, that was, to filter events and as a result facilitated the decision-making process, although the monitors themselves were able to perform some pre-processing of data before transmitting them to the network administrator. However, this monitoring approach CS, still the main burden on the adoption of management decisions of the CS, was on network administrators. Artificial intelligence has been used to solve this problem, namely the intelligent agents [16, 17] that could be successfully applied to monitor network traffic, fault diagnostics, congestion control, access, etc.

The increased use of the CS real-time applications such as audio and video, as well as the need to add Web functionality to network applications has led to the need for network management based on the Web. An essential element of this management is to monitor traffic. In [18], to monitor traffic flows in real time, the authors offer traffic monitoring system based on CORBA (Common Object Request Broker Architecture) [19]. This allows web applications to find the appropriate network management monitors traffic flow in real time and retrieve information from them about the traffic. This information can be displayed in graphical form, and used to obtain additional parameters associated with traffic flows in real time.

Distributed monitoring of CN

With the increasing scale of modern CN there is a need for efficient and scalable systems, distributed control. The basis of these systems is a distributed monitoring. In the literature you can find a description of the various approaches to distributed monitoring CN. For example, mobile agents [20] have been used for distributed and dynamic network monitoring. As agents, the authors used IBM Aglets system and showed that both the distributed application, of CN monitoring based,

Java can effectively carry out data collection and analysis and to adapt to changes in network performance. However, the effectiveness of distributed monitoring depends on the efficiency of CN scalable monitoring infrastructure. To reduce deployment costs of such a system, the optimal hierarchical monitoring architecture has been proposed [21], the essence of which was the optimal allocation of resource-intensive tasks over a network. One of these tasks is to survey the individual network nodes. The choice of the number of interviewers nodes has a significant impact on the value of the measurement infrastructure and network bandwidth. To solve this problem, the authors optimized scalable distributed poll system. Also, for optimum monitoring of the infrastructure elements of artificial intelligence were used, namely, the Hopfield network [22]. In addition, for efficient and scalable distributed monitoring of CN was needed for effective monitoring of distributed algorithms. In [23] two algorithms have been proposed by the author, which can reduce communication costs. The first of these was called DSM (Distributed Subnetwork Monitoring) algorithm, which assumes that the network consists of several subnets, and each has its own local management. The basic idea of the algorithm is that each local manager carries out the collection and processing of monitoring data on the same subnet. And when the amount of local variables exceeds the threshold value, the manager begins to gradually collect the data from the other subnets. At the same time, as the local manager is closer to the data on the same subnet, the connection between the nodes and the local manager is more effective.When exceeding, in some sites the mean values of the variables for the node result is smoothed other variables subnets, which reduces the need for a survey of all the nodes in large CN. Fully distributed monitoring) algorithm because this algorithm, no subnets and local managers.–The second algorithm has been called FDM (Fully Distributed Monitoring The network nodes interact with each other and perform the task of monitoring and when the node exceeds the limit, the search for other nodes with more available resources. Another approach to distributed network monitoring architecture proposed in [24], the essence of which is a decentralized collection and storage of network traffic data. In this approach, the network traffic is collected and stored directly on the respective devices over the network. When this data is processed in parallel on the respective local data and used for this Map-Reduce technology [25].

Collection and classification of network traffic CN

The major part of the current research in the field of network traffic collection devoted to questions of gathering packages in high-speed networks with minimum data loss and data compression after the acquisition, i.e. reduce the volume. For example, in [26, 27], the authors discuss the data conversion issues for effective storage and processing and monitoring in the cloud, respectively. In [28, 29], the authors propose an approach to the development of data collection applications in high-speed networks based on standard hardware. Furthermore, in [30], for a full analysis of network traffic flows, authors propose a method of aggregation. An alternative to the centralized storage of data is the distributed data storage, but this approach is complicated by the storage process of data analysis, as well as administration and maintenance. Another type of distributed storage can be considered as a cloud storage [31, 32], which can also carry out data collection.

The usage of modern CS - greater number of network services and applications, hardware and software leads to the emergence of a wide variety of network traffic. Moreover, for an effective monitoring and management solution to the problem of the CS, an accurate identification and classification of traffic with respect to network services, applications and protocols is very important [33], because network traffic is one of the most important indicators of the actual work of the CS, i.e., the traffic is a carrier of information about the user behavior and the functioning of the CS.

The identification and classification of network traffic is particularly important for tasks such as the definition of priorities in shaping bandwidth for certain traffic, the establishment of rules

for network management, network security, diagnostic monitoring of the CS, etc. [34]. For instance, in order to ensure the normal operation of applications, which are important to the corporation, the network administrator must identify and limit (or block) P2P (peer-to-peer) traffic. In addition, an effective solution to most technical problems, such as the determination of the parameters and simulation workload communication channel, scheduling downloads of network equipment, initialization routes, etc., also depend on the accurate identification and classification of network traffic.

Nonetheless, the classification of network traffic in real-time is one of the major problems of modern monitoring of the CS. The classification identifies the application based on the use of specific "well-known" TCP or UDP port (usually port number information is available Titles TCP- or UDP-packets), but it is impossible to predict the port numbers used by most applications [35]. Thus, the need for more effective methods of network traffic classification that will determine the type of application on the basis of data, available in the main part of the TCP- or UDP-packets (or based on known behaviors protocols). The effectiveness of such methods of network traffic classification decreases because of the detail content inspection of packets. Therefore, most of researchers believe the methods of machine learning (ML), which is the part of the discipline of artificial intelligence, is more suitable for network traffic classification. In [36], an inspector of network traffic based on the ML methods, and is intended to minimize the call time in telecommunication networks from circuit-switched. This work is the beginning of the application of ML methods in the field of telecommunication networks. And, after that, ML was used for Internet traffic classification for the purpose of intrusion detection [37]. This work laid the foundation for the use of ML methods in classification of Internet traffic.

Visualization of the CS monitoring

Another problem associated with the monitoring of the CS, during a continuous and rapid receipt of data in the monitoring system there is a large amount of data accumulates, making it difficult to process and analyze numerically. Therefore, there is a need to use network data visualization techniques that allow network administrators to conduct network monitoring visually. The visualization of network data allows to introduce and display a large amount of network data in a graphical representation briefly, and an effective mechanism for monitoring network traffic characteristics. The visualization of network data is particularly important for the rapid assessment of the state of the network; it allows network administrators to quickly and easily interpret the results of the monitoring. The visualization also allows you to display the state of the network and identify bottlenecks, failures, misuse of network resources, etc dynamically. Meanwhile, imaging can be undertaken at various levels, such as: network load, bandwidth, packet types, etc. For the expression of the resulting images, visualizing different colors, which facilitate their interpretation are used, [38].

Today, a variety of methods [39] for visualization of network data are offered. The common feature of these methods is to display a large volume of data in little space. Typically, methods of visualization of network data include simple line graphs and charts, that show changes in network traffic parameters. In this case, the metric used may vary from common measurements (for example, the use of network bandwidth) to more specific parameters.

Simple line graphs and charts are very effective for the display of the majority network metrics as it is easy to understand and interpret. Simple line graphs are one of the most common types of visualization and the most commonly used. This method is designed for visualization of the changes in network traffic parameters through time. At the same time, each parameter is assigned a unique color. For the analysis of network, simple line graphs provide an intuitive image, and depending on the nature of displaying of graphic line, network administrator can easily conduct traffic analysis and take appropriate decisions.

Simple graphics are used in many monitoring tools, for example, in the MRTG monitoring systems [40] and RRDTool [41]. MRTG used to visualize the current bandwidth usage over time.

In addition to these methods, more sophisticated methods were proposed, for example, in [42], the so-called radial traffic analyzer has been proposed to monitor network traffic, which uses concentric rings, and represents a hierarchical relationship between the different measurements. In general, this imaging method is intended for the quantitative analysis of hierarchically structured data, and is very well suited for the visual analysis of network data. Also, this method can be used for any set of data that has a hierarchical relationship.

Monitoring the quality of service of the CN

Nowadays, many different network protocols, applications, and multimedia services, which have different requirements on QoS (Quality of Service) are used in the CN, and particularly in the Internet. In such circumstances, providing for each network application, service, and media required level of QoS becomes a serious problem. Since QoS is complex, its quantification and guaranteed supply becomes a matter of difficult. Therefore, carrying out real-time continuous monitoring and management of QoS parameters CN becomes very important. However, QoS still remains one of the most ambiguous concepts defined by the CN. Depending on the tasks, to ensure the QoS of the network service can be defined in various ways and can include a plurality of different service requirements such as performance, availability, reliability, security, etc. All these requirements are very important aspects for integrated QoS support. Hence, to ensure the QoS of computer networks, it is required to provide a QoS structure that would include guidelines, specifications and QoS monitoring and control mechanisms [43].

Created by ITU (International Telecommunications Union), SLA (Service Level Agreements), which lies between the Internet service providers and subscribers, has allowed to define the QoS parameters of network services. Accordingly, the SLA is not based on the objective standards and may differ, depending on the client, the provider of Internet services and the services offered. [44] In this regard, the absence of a single QoS standard does not allow to define QoS network services properly .There are many studies and a variety of architecture, technology and QoS mechanisms have been developed over a decade [45-48]. A lot of research and development was performed IETF (Internet Engineering Task Force), for example, IETF RFC 1633 [49], IETF RFC 2430 [50], IETF RFC 2475 [51], etc. CAIDA (Cooperative Association for Internet Data Analysis) has created a network traffic-monitoring environment that is used to collect and analyze QoS data.

Through receiving the information, QoS monitoring can be divided into monitoring "point to point" [52] and the distributed monitoring [53]. During a "point to point" monitoring, QoS traffic monitoring between two points is held in real-time, i.e., between the sender and the recipient. And with the distributed QoS monitoring approach, along with the monitoring of "point to point" is also done QoS monitoring different network segments. The CS based QoS monitoring system model is based on the traditional model of network monitoring [54], which includes the following functional components: monitoring application, QoS monitoring, display and monitoring of objects [55].

Monitoring of Wi-Fi networks

The emergence of such wireless connection to the network technology as Wi-Fi (eg, IEEE 802.11), and cellular data network (for example, 3G / LTE) enabled final users to have easy access to the CS (eg, Internet). It is very widely used nowadays. Therefore, the issues of providing a good quality connection to the CC members and security becomes very important. However, the resolution of these issues, especially in large CS, becomes very difficult because of the lack of adequate monitoring schemes of Wi-Fi networks. Because, unlike conventional CS, which has developed a variety of monitoring methods and models in Wi-Fi networks, there are some

difficulties associated with monitoring. Firstly, wireless clients are mobile, making it difficult to collect, store and analyze the statistical data of each client. Secondly, the complexity of resource utilization accounting connection channels, for example in conventional CN channel bandwidth and transmission rate are fixed (i.e., represented as the bytes in seconds). The use of the channel resources may be expressed in bytes, but in the Wi-Fi networks bandwidth is represented as time (i.e., nano-second) and the transmission rate is changed dynamically. Thus, using a Wi-Fi network monitors the number of bytes and packets can not be used to determine the percentage of transmission channel resources in the current time. Third, the network resources are allocated among the various services and radio devices that generate interference that prevents the use of network resources completely.

In [56], a test monitoring was conducted, and measurement technologies used in their large-scale Wi-Fi networks. For the solution of these problems, it is offered, in the MIB module (Management Information Base), to have some statistical counters that collect information related to the application of radio waves and interferences.

Some of the CN monitoring standards

Along with the CN monitoring methods in order to ensure the effectiveness of monitoring various standards were also established. These standards describe the property, state, methods and protocols of interaction between objects of the CN. Internet Control Message Protocol is used to determine the availability of nodes, analysis of various indicators, defined in RFC (Request For Comment) 792 [–As an example of the standards used in the monitoring of the CS, can lead standards such as: Internet Control Message Protocol (ICMP) 57]; to collect information protocol with nodes in different networks, defined in RFC869 [58];–Host Monitoring Protocol (HMP) Simple Network Management Protocol, is used to obtain information from the network nodes, originally defined in RFC 1067 [59] in 1988, and then as a standard in 1990 in RFC 1157 [60];–Simple Network Management Protocol (SNMP) Management Information Base, which contains information about the parameters controlled and managed network devices, defined in RFC1156 [61], etc.–Management Information Base (MIB). However, different applications have been developed to allow use of these protocols for receiving data from the CS network entities.

Conclusion

It is impossible to disagree with the fact that the Computer System is more and more integral part of our live, constantly evolving and becoming more extensive and complex with the development of information technology. At the same time, there are problems of management of the CS, and monitoring mechanisms are crucial for their effective management. Therefore, the issues of monitoring CS consideration in the context of the CS itself is relevant, since the development of the CS monitoring methods is inextricably linked with the development of the CS itself. In the light of these considerations, it is safe to say that monitoring is and will be one of the basic conditions conducive to the development of the CS. The results of the analysis of CS methods for monitoring development trends will identify the problems that exist in this area, and to develop more effective methods.

References

1. Vokorokos L., Adam N., Balarz A., Application of intrusion detection systems in distributed computer systems and dynamic networks // Computer Science and Technology Research Survey, 2008, pp. 19–24.
2. http://www3.nd.edu/~dwang5/courses/fall15/pdf/evolution.pdf
3. Poulton S., Packet Switching and x.25 networks, Taylor & Francis e-Library, 2003, 236 p.
4. http://en.wikipedia.org/wiki/ARPANET
5. http://en.wikipedia.org/wiki/World_Wide_Web

6. Clark D.D., Pogran K.T. and Reed D.P, An introduction to local area networks // Proceedings of the IEEE, 1978, vol. 66, no. 11, pp. 1497–1517.
7. Boggs D.R. and Metcalfe R.M., Ethernet: Distributed packet switching for local computer networks // Communications of the ACM, 1976, vol.19, no. 7, pp. 395–404.
8. http://en.wikipedia.org/wiki/NetWare
9. Swift C., Machine Features for a More Automatic Monitoring System on Digital Computers // ACM (JACM), 1957, vol. 4, no. 2, pp. 172–173.
10. Schulman F. Hardware measurement device for IBM system/360 time sharing evaluation / Proceedings of the 22nd national conference ACM Annual Conference/Annual Meeting, 1967, pp.103–109.
11. Grochow J., The graph display as an aid in the monitoring of a time shared computer system. Technical Report: TR-54, 1968.
12. Pikerton T., Performance monitoring in a time-sharing system // Communications of the ACM, November 1969, vol. 12, no. 11, pp. 608–610.
13. Barton B., Switlik J., A real-time expert system for computer network monitor and control / // ACM SIGMIS Database, 1988, vol.19, no. 2, pp. 35–38.
14. Hitson B., Knowledge-based monitoring and control: an approach to understanding behavior of TCP/IP network protocols // ACM SIGCOMM Computer Communication Review, 1988, vol. 18, no. 4, pp, 210–221.
15. Waldbusser S., Remote Network Monitoring Management Information Base. RFC 1757, Feb. 1995.
16. Cheikhrouhou M. M., Conti P., Labetoulle J., Intelligent Agents in Network Management: A State-of-the-art // Networking and Information Systems, 1998, vol. no.1, pp. 9–38.
17. Koch F.L., Westphall C.B., Decentralized Network Management Using Distributed Artificial Intelligence // Network and Systems Management, 2001, vol.9, no.4, pp. 375–388.
18. Yuming J., Chen-Khong T., Chi-Chung K., A Web-Based Real-Time Traffic Monitoring Scheme Using CORBA / Proceedings of the 2nd IFIP/IEEE International. Conference on Management of Multimedia Networks and Services, 1998, pp. 16–18.
19. http://www.ois.com/Products/what-is-corba.html
20. Kamangar F., Levine D., Záruba G. V., and Chitturi N., Distributed network monitoring using mobile agents paradigm / Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications, 2003, pp. 951–957.
21. Li L., Thottan M., Sanjoy B. Y. P., Distributed network monitoring with bounded link utilization in IP networks / Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. 2003, vol. 2, pp. 1189–1198.
22. Liu X., Yin J., Cai Z., Lu X., Chen S., Optimizing the distributed network monitoring model with bounded bandwidth and delay constraints by neural networks / Advances in Neural Networks – ISNN 2005, volume 3496 of the series Lecture Notes in Computer Science, pp. 805–810.
23. Du X., Toward efficient distributed network monitoring / IEEE International Conference on Performance, Computing, and Communications, 2004, pp. 87–94.
24. Elsen L., Kohn F., Decker C., Wattenhofer R., goProbe: a scalable distributed network monitoring solution / IEEE International Conference on Peer-to-Peer Computing, 2015, pp. 1–10.
25. Lee Y., Kang W., Son H., An Internet Traffic Analysis Method with MapReduce / Proceedings of the Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP, 2010, pp. 357–361.
26. Aceto G., Botta A., Pescape A., Westphal C., Efficient Storage and Processing of High-Volume Network Monitoring Data // IEEE Transactions on Network and Service Management, 2013, vol. 10, no. 2, pp. 162–175.
27. Aceto G., Botta A., de Donato W., Pescape A., Cloud Monitoring: A Survey // Computer Networks, 2013, vol. 57, no. 9, pp. 2093–2115.

28. Deri L., Cardigliano A., Fusco F., 10 Gbit Line Rate Packet-to-Disk Using n2disk / Proceedings IEEE INFOCOM, 2013, pp. 3399–3404.
29. Banks D., Custom Full Packet Capture System, SANS, 2013.
30. Francois J., State R., Engel T., Aggregated Representations and Metrics for Scalable Flow Analysis / IEEE Conference on Communications and Network Security (CNS), 2013, pp. 478–482.
31. Sivashakthi T., Prabakaran N., A Survey on Storage Techniques in Cloud Computing // International Journal of Emerging Technology and Advanced Engineering, 2013, vol. 3, no. 12, pp. 125–128.
32. Spoorthy V., Mamatha M., Santhosh Kumar B., A Survey on Data Storage and Security in Cloud Computing // International Journal of Computer Science and Mobile Computing, 2014, vol.3, no.6, pp. 306–313.
33. Shikhaliyev R.G. About the application of intelligent technologies for computer networks monitoring // Artificial Intelligence, 2011, No 1, pp. 124-132.
34. Kim H., Fomenkov M., Barman D., Faloutsos M., and Lee K., Internet traffic classification demystified: myths, Caveats, and the Best Practices // Proceedings of the 4th Conference on Emerging Network Experiment and Technology, December 09 - 12, 2008, pp. 112–124.
35. Karagiannis T., Broido A., Brownlee N., and Claffy K., Is P2P dying or just hiding? / Proceedings of the 47th annual IEEE Global Telecommunications Conference, 2004, vol. 3, pp.1532–1538.
36. Silver B., Netman: A learning network traffic controller / Proceedings of the Third International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems, Association for Computing Machinery, 1990, vol. 2, pp. 923–931.
37. Frank J., Machine learning and intrusion detection: Current and future directions / Proceedings of the National 17th Computer Security Conference, 1994, pp. 22–33.
38. Shikhaliyev R.H., About Methods for Visualizing Network Monitoring / Proceedings of the 4th International Conference Problems of Cybernetics and Informatics, Baku, Azerbaijan, September 12-14, 2012, vol. 1. pp. 69–70.
39. D.A.Keim, Information Visualization and visual data mining // IEEE Transactions on visualization and computer graphics, 2002, vol. 7, no. 1, pp. 100–107.
40. T. Oetiker, and D. Rand, Multi Router Traffic Grapher. http://www.mrtg.org.
41. T.Oetiker, Round Robin Database Tool. http://www.rrdtool.org.
42. Keim D. A., Mansmann F., Schneidewind J., and Schreck T., Monitoring Network Traffic with Radial Traffic Analyzer / IEEE Symposium On Visual Analytics Science And Technology, 2006, pp. 123–128.
43. Shikhaliyev R.G. About the methods of monitoring and QoS management of computer networks // Problems of Information Technologies, 2013, No 1, pp. 15-23.
44. ITU-T, Support of IP-based services using IP transfer capabilities, Tech. Rep. Rec. Y.1241, 200.
45. Firoiu V. et al., Theories and Models for Internet Quality of Service // Proc. of IEEE, Special issue on Internet Technology, 2002, Vol. 90, Is. 9 pp. 1565–1591.
46. Soldatos J., Vayias E., Kormentzas G., On the Building Blocks of Quality of Service in Heterogeneous Ip Networks // IEEE Communications Surveys & Tutorials, 2005, vol. 7, No.1, pp.70–89.
47. Karam F., Jensen T., A Survey on QoS in Next Generation Networks // Advances in Information Sciences and Service Sciences, 2010, Vol. 2, No. 4, pp. 91–102.
48. Aurrecoechea C., Campbell A., and Hauw L., A Survey of QoS Architectures // Multimedia Systems Journal, 1998, Vol. 6, No. 3, pp. 138–151.
49. Braden R., Clark D., and Shenker S., Integrated Services in the Internet Architecture: an Overview, IETF RFC 1633, Tech. Rep., 1994. ftp://ftp.isi.edu/in-notes/rfc1633.txt

50. Li T. and Rekhter Y., A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE), IETF RFC 2430, Tech. Rep., 1998. ftp://ftp.isi.edu/in-notes/rfc2430.txt
51. Blake S., Black D., Carlson M., Davies E., Wang Z., and Weiss W., An Architecture for Differentiated Services, IETF RFC 2475, Tech. Rep., 1998. ftp://ftp.isi.edu/in-notes/rfc2475.txt
52. Jiang Y., Tham C.K., Ko C.C., A QoS distribution monitoring scheme for performance management of multimedia networks / Proc. of IEEE GLOBECOM'99, Brazil, Dec. 1999, Vol. 1A, pp. 64–68.
53. Foster I., Roy A., Sander V., and Winkler L., End-to-End Quality of Service for High-End Applications, Technical Report, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, 1999. www.mcs.anl.gov/qos/end to end.pdf
54. Stallings W., SNMP, SNMPv2 and RMON: Practical Network Management, 2nd edition, Addison-Wesley, 1996.
55. Jiang Y., Tham C.K., Ko C.C., Challenges and approaches in providing QoS monitoring. International Journal of Network Management, 2000, Vol. 10, No.6, pp. 323–334.
56. http://irtf.org/raim-2015-papers/raim-2015-paper42.pdf
57. Postel J., Internet control message protocol, RFC 792, 1981, http://www.ietf.org/rfc/rfc792.txt
58. Hinden R. M., A Host Monitoring Protocol, RFC 869, 1983, http://tools.ietf.org/html/rfc869
59. Case J., Fedor M., Schoffstall M., Davin J., A Simple Network Management Protocol, RFC 1067, 1988, http://tools.ietf.org/html/rfc1067
60. Case J., Fedor M., Schoffstall M., Davin J., A Simple Network Management Protocol, RFC 1157, 1990, http://www.ietf.org/rfc/rfc1157.txt
61. McCloghrie K., Rose M., Management Information Base for Network Management of TCP/IP-based internets, RFC 1156, 1990, http://www.ietf.org/rfc/rfc1156.txt