STUDYING AND CHARACTERIZATION OF THE DATA FLOWS IN AN IP-BASED NETWORK

Ivan Nedyalkov, Alexey Stefanov* and Gerogi Georgiev***

* South-West University "Neofit Rilski", ** Union of Electronics, Electrical Engineering and Telecommunications (CEEC)
e-mails: i.nedqlkov@gmail.com, astef@abv.bg, goshko.georgiev@gmail.com
Bulgaria

Abstract: The work proposes a method for evaluating the functioning of IP – based networks by using monitoring tools and mathematical distributions. The traffic flows in an IP-based corporate network have been studied. The protocols and packets that are exchanged in the network are monitored. A breakdown of their size and type has been made. The time delay of the packets is also monitored. Based on the data about the time delay of packets and their size, mathematical distributions are made. The distributions give additional information about the functioning of the network. The types of audio codecs used by the IP telephone exchanges are also observed.

Key words: IP – networks, IP-PBX, Monitoring, Mathematical distributions, Traffic characterization.

1. INTRODUCTION

Modern telecommunications networks are becoming more and more complex due to their technological heterogeneity, the functional complexity of the protocols used, and a wide variety of services and applications. The development of IP-based telecommunication networks involves a rapid increase in their capacity, the provision of a large number of broadband services and applications, guarantee of quality of service (QoS) and the security of the provided services. A number of authors indicate that it is necessary to develop new models and methods for the analysis of modern networks based on traffic measurements and monitoring [1, 2, 3].

Planning and managing these networks require accurate and effective measurements and monitoring [4, 5, 6, 10]. Applying the classic approaches to measuring, monitoring and planning modern IP-based networks is a challenging task. Measurements and monitoring of IP networks aim at evaluating and analyzing various aspects such as: topology and network connectivity; routing; security; attacks; quality of service; filtering, etc.

The purpose of the article is to study the data streams in a particular IP - based network to verify its functionality – are there large delays in packet exchange, what is the most commonly used protocol in the observed network, what is the traffic load and other.

For the monitoring of the network the classic passive monitoring method is used. The use of mathematical distributions for packet delays and packet size are proposed. These distributions are used for further assessment of the network.

2. TOPOLOGY OF THE MONITORED NETWORK

Figure 1 shows the topology of the studied network. As it can be seen, it is a corporate network consisting of two IP telephone exchanges: OpenScape Voice (OSV) and Asterisk. There are "N numbers" of IP phones, some of which are connected to OSV and the other part of them to the Asterisk. The purpose of the work is to study the traffic flows that are exchanged in the monitored network. The obtained results will show if the used IP network is properly designed for the type of information which is exchanged between the devices.

The tools used for the monitoring are installed on a dedicated workstation that "listens" to all the traffic that passes through the network. For this purpose, a mirror port is used on the switch, to which all traffic is forwarded. The tools used for the research are Capsa Colasoft and Wireshark.

Various types of mathematical distributions and approximations [7, 8, 9] will be used for the statistical analysis of the measurement results. The program with which the approximations and the distribution were made is EasyFit.

The use of mathematical distributions of the captured packets is used for further analysis of the obtained data. The mathematical distribution is done for two parameters - distributions of packet sizes and packet delay. The resulting distributions are used for further evaluating of the observed network.

3. RESULTS FROM THE MONITORING

Network monitoring is done within two days. The network observation time on these days is several hours. The measurements are conventionally divided into two types - day one when only audio traffic is monitored and day two when only video traffic is monitored. To monitor only one or the other traffic type reconfiguration of the mirroring port was performed:

- Firstly, only the traffic generated by the IP phones was monitored;
- Secondly the traffic generated by the workstations with installed applications for video conferencing was monitored.

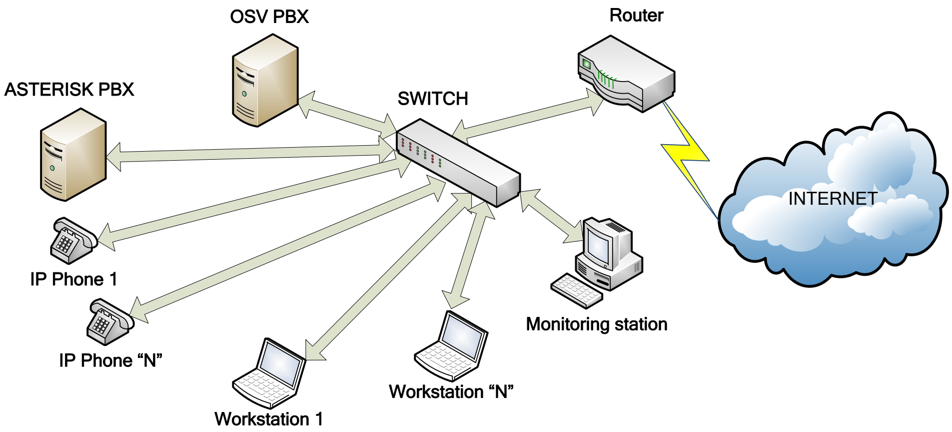

Fig. 1. Topology of the network

The captured packets for the time the network has been monitored have been processed using mathematical processing software and corresponding distributions are received that give a clear idea of the nature of the network traffic and the functioning of the monitored network.

3.1. Video traffic

Figure 2 shows the total generated video traffic in the monitored network. The source for the video traffic is only from video conferencing. The data capture interval is 5 minutes for summarization of the results. The average load is about 20 MB, so the generated video traffic does not cause a heavy network load, and therefore other data can be transmitted through the network. As it can be seen for the particular observed network the traffic is highly uneven and heterogeneous.

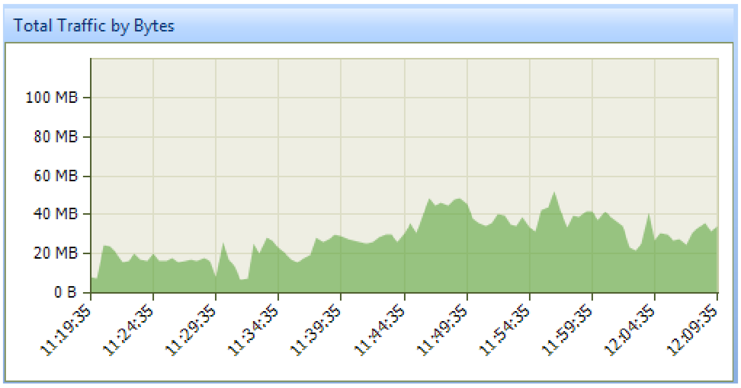

Fig. 2. Total generated video traffic

Figure 3 shows the broadcast and multicast packets. As it can be seen, the number of multicast packets is bigger than that of the broadcast packets. That is because of the source of the traffic – video conferencing. Because this is streaming media it uses specially reserved multicast addresses. Additional application of using multicast is for bandwidth savings. All of this proves that there are no anomalies and the performance of the video data transmission is normal.

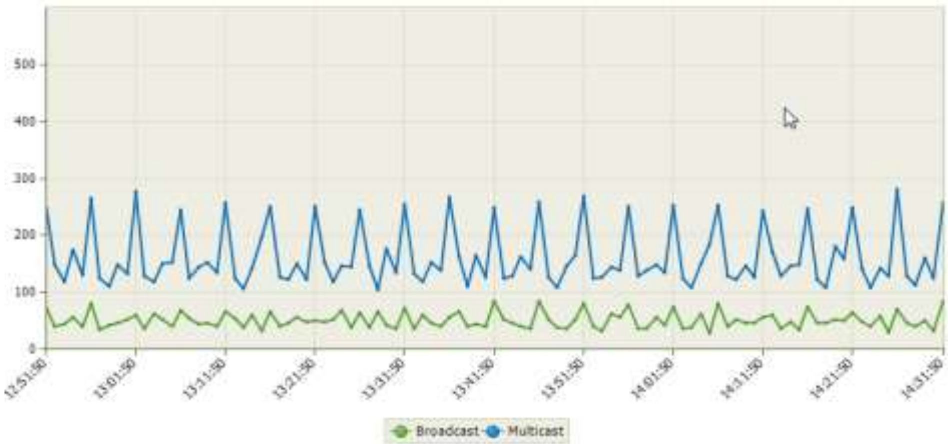

Fig. 3. Multicast and broadcast packets

Figure 4 shows that mainstream traffic sources on the network use UDP. This is completely normal, because the generated traffic is only video, and it is mainly transmitted via UDP. There are other traffic sources that use other protocols but they generate much less traffic, so they may not be taken into account.

Figure 5 shows the mathematical distribution and a Beta approximation of the packet delays for the video traffic. As it can be seen the packet delay is almost constant. This means that the network is properly designed, as a result of which packet delays are constant.

Figure 6 shows the distribution of the packets by size. Note that packets of up to 200 bytes size are much more than the rest. The Frechet approximation is used to show this. That is because of the Packetized Elementary Stream (PES). The video stream is torn down into packets with size of 188 bytes. The result is elementary stream of bits. For video traffic this is normal.

3.2. Audio traffic

Figure 7 shows the total audio traffic generated by the IP telephones for the monitored period. As it can be seen, it is much smaller than the video traffic, which is normal and dogmatic. As it can be seen from the results of the monitoring tool the traffic is even and homogeneous.

Name	Bytes	Packets	bps
Ethernet II	5.98 GB	11,391,992	4.942 Mbps
IP	5.98 GB	11,358,609	4.941 Mbps
UDP	5.89 GB	11,248,496	4.941 Mbps
BOOTP	743.92 KB	2,118	5.864 Kbps
DHCP	743.92 KB	2,118	5.864 Kbps
SSDP	549.31 KB	2,708	1.432 Kbps
SIP	483.16 KB	1,096	7.048 Kbps
DNS	449.31 KB	3,562	8.480 Kbps
DNS Response	254.80 KB	1,781	4.768 Kbps
DNS Query	194.52 KB	1,781	3.712 Kbps
LLMNR	56.34 KB	849	0.000 bps
NTP	28.88 KB	278	1.824 Kbps
CLDAP	27.79 KB	131	3.704 Kbps
MNDP	26.51 KB	174	1.248 Kbps
NBDGM	10.77 KB	44	1.976 Kbps
SMB	10.77 KB	44	1.976 Kbps
SMB_MAILSL...	10.77 KB	44	1.976 Kbps
MDNS	9.89 KB	64	696.000 bps
NBNS	8.67 KB	88	768.000 bps
TCP	93.63 MB	107,099	9.720 Kbps
HTTP	76.94 MB	57,139	63.504 Kbps
AMQP	10.42 MB	7,209	15.829 Mbps
SIP	1.07 MB	1,650	0.000 bps
LDAP	834.79 KB	1,283	108.008 Kbps
NBSSN	745.08 KB	2,442	28.936 Kbps

Fig. 4. Used protocols by the traffic sources

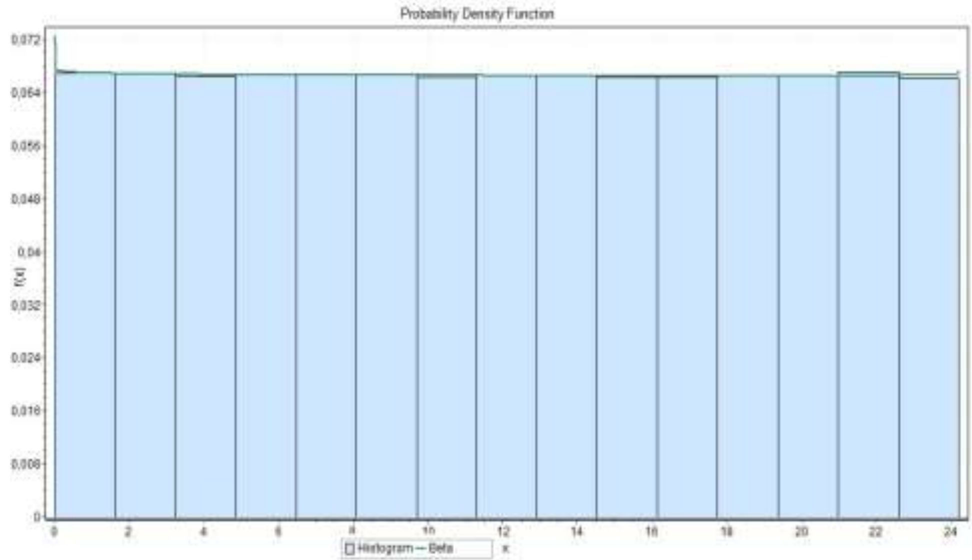

Fig. 5. Beta approximation of the time delay of the packets

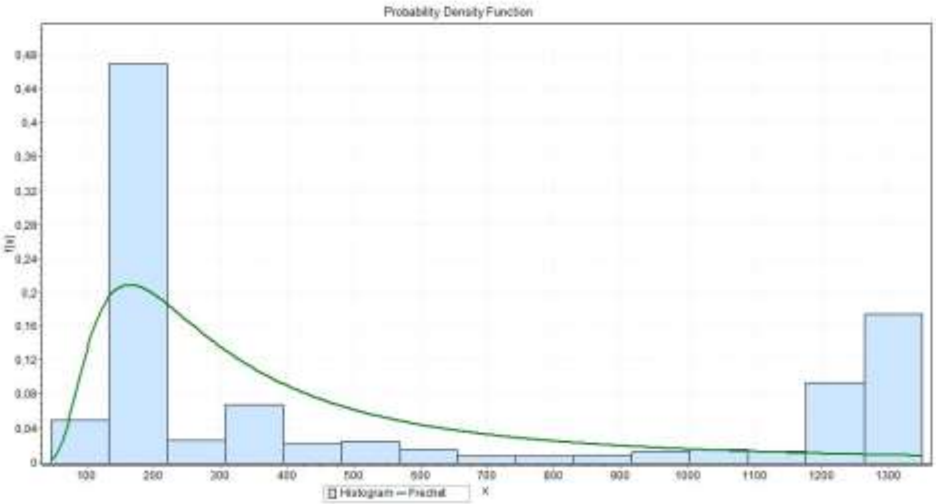

Fig. 6. Frechet approximation of the packet size

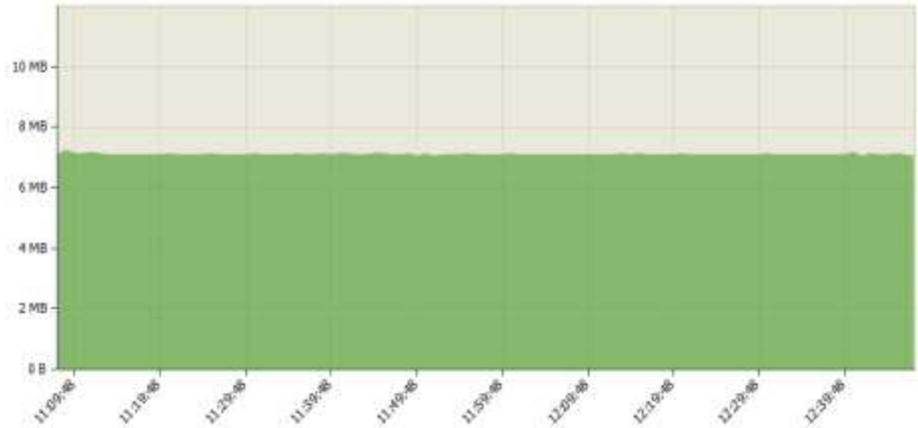

Fig. 7. Total generated video traffic

Figure 8 shows the protocols used by the traffic sources. Again, UDP is the most used protocol that characterizes audio data streams. Again, there are other traffic sources that are using different protocols, but the traffic generated by them is very small, almost insignificant and may not be taken into account in the surveyed network.

Name	Bytes	Packets	bps
Ethernet II	618.50 MB	2,605,345	2.105 Mbps
IP	617.85 MB	2,597,263	2.104 Mbps
UDP	510.88 MB	2,461,498	2.104 Mbps
SIP	376.86 KB	802	7.048 Kbps
BOOTP	147.49 KB	434	5.568 Kbps
DHCP	147.49 KB	434	5.568 Kbps
DNS	95.10 KB	800	1.536 Kbps
DNS Response	59.70 KB	397	896.000 bps
DNS Query	35.40 KB	403	640.000 bps
SSL	72.56 KB	116	0.000 bps
HTTPS	72.56 KB	116	0.000 bps
SSDP	65.68 KB	240	36.624 Kbps
MNDP	7.62 KB	50	1.248 Kbps
NTP	4.55 KB	47	752.000 bps

Fig. 8. Used protocols by the traffic sources

Figure 9 shows the audio codecs used in the network. The used codecs are two because of the two IP PBXs – OSV and Asterisk. The used codecs are G.711 PCMU and G.711 PCMA, here it is interesting to note that each of the two IP PBXs uses a different codec.

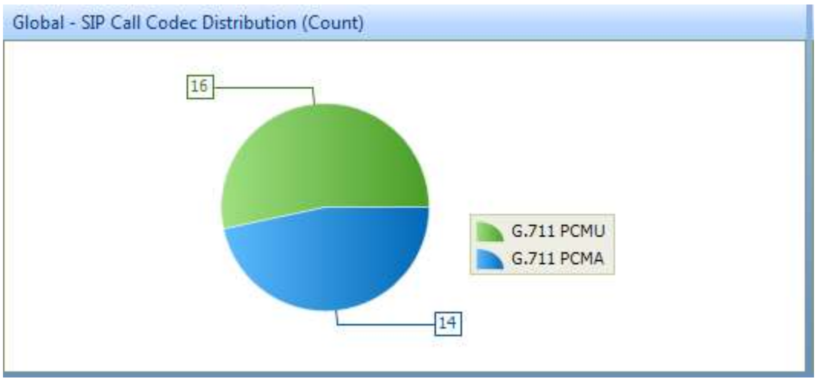

Fig. 9. Used audio codecs

Figure 10 shows the distribution of packet delays. The shown results are based on the use of the Gamma approximation. As it can be seen, the results are similar to those for video traffic - packet delay is almost constant. This means that the network is properly designed, as a result of which the packet delays are constant.

Figure 11 shows the packet size distribution by using Log-Logistic (3P) approximation. Note that packets of up to 240 bytes are much more than others - this is the useful information. Because of the used audio codec in the network – G.711, the voice packets are with size of 240 bytes (for 30ms voice payload size) and 160 bytes (for 20ms voice payload size). In the monitored network the voice payload size is between 25 and 30ms.

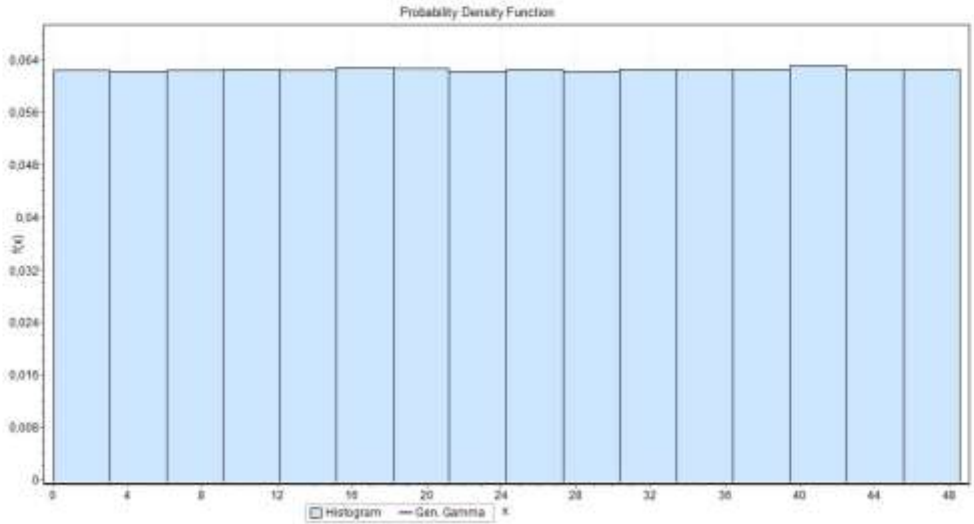

Fig. 10. Gamma approximation of the time delay of the packets

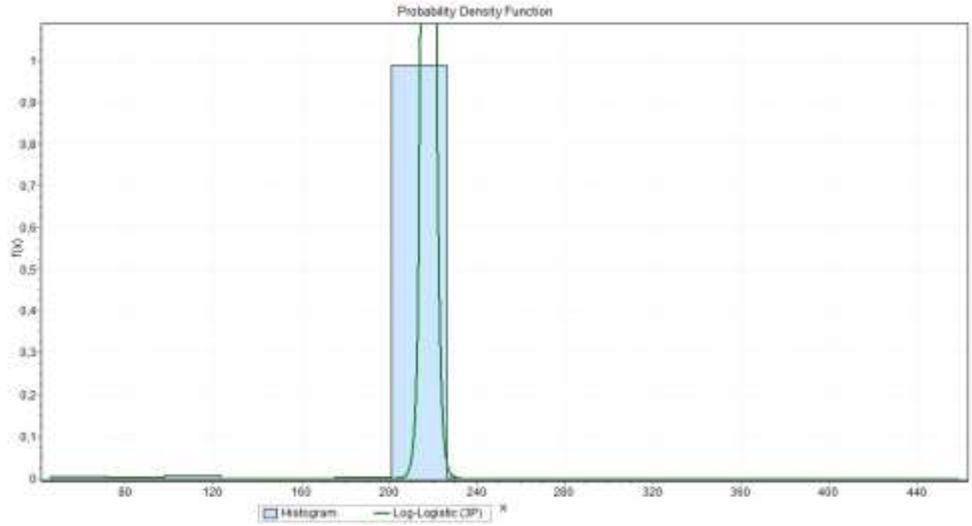

Fig. 11. Log – Logistic (3P) approximation of the packet size

4. CONCLUSION

The network load was measured over a period of time with different capture intervals. The change of the traffic in the network is also evaluated. A breakdown of application level protocols and breakdown of packet sizes has been made. The measured and monitored parameters are: types of protocols, size of the packets, packet delay, total generated traffic.

The use of mathematical distributions for further analysis of the results of the observation have been proposed. Mathematical distributions of packet sizes and time delay were made. From the obtained distributions for packet delay it was found that the delays between the packets are constant for voice and video streams, meaning that the network is correctly designed and there are no abnormalities in it.

From the mathematical distribution of the packet size the following results were found: it was established that during video streaming Packetized Elementary Stream (PES) has been used. That leads to optimal utilization of the network. If that is not used it will be detrimental to network performance because the video stream has the ability to increase the average real time packet size. Thus the network can be used to transmit other information during video calls.

During audio transmission the voice payload size is between 25 and 30ms for G.711. The payloads for the G.711 codec are 160 bytes for 20ms payload and 240 bytes for 30ms payload. The obtained difference in the voice payload is due to the different used IP telephone exchanges (Asterisk and OSV).

The monitoring shows that the two IP PBXs use different audio codecs to transmit information.

The obtained results show the need of measurement and monitoring of the traffic in IP-based networks for optimization and evaluation. The proposed traffic monitoring and characterization method together with the use of the mathematical distributions can be used to make recommendations for improving network performance, evaluation and troubleshooting.

REFERENCES

[1] Mirtchev, S., R. Goleva, D. Atamian, I. Ganchev. Investigation of priority queue with peaked traffic flows, *Proceedings of the ACM Symposium on Applied Computing*, 2018, pp.1017-1019, doi:10.1145/3167132.3167407

[2] Ibrahim, L. T., R. Hassan, K. Ahmad, A. N. Asat. A study on improvement of internet traffic measurement and analysis using Hadoop system, *2015 International Conference on Electrical Engineering and Informatics (ICEEI)*, Denpasar, 2015, pp. 462-466, doi: 10.1109/ICEEI.2015.7352545

[3] Lena I., R. Hassan, K. Ahmad, A. N. Asat, H. Omar. Online Traffic Measurement and Analysis in Big Data: Comparative Research Review, *American Journal of Applied Sciences*, **4** (vol. 13), 2016, pp. 420 – 431. doi: 10.3844/ajassp.2016.420.431

[4] Mingbo, L., S. Wenjie, Z. Qianhong, T. Zhaoping. Design and implementation of IP network traffic monitoring system, *15th International Conference on Optical Communications and Networks (ICOCN)*, Hangzhou, 2016, pp. 1-3. doi: 10.1109/ICOCN.2016.7875854

[5] Iversen, V. B. *Teletraffic engineering and network planning*. DTU Fotonik, 2015.

[6] Madsen, O. B., M. T. Riaz. *Planning broadband infrastructure - a reference model. European Broadband Portal*, 2008

[7] Cruz-Pérez, F. A. et al. Approximating log-normally distributed secondary service time by hyper-exponential distribution for the analytical performance evaluation of cognitive radio networks, *20th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Bali, 2017, pp. 642-646. doi: 10.1109/WPMC.2017.8301891

[8] Xu, H., G. Fan, K. Li. Improved Statistical Analysis Method Based on Big Data Technology, *International Conference on Computer Network, Electronic and Automation (ICCNEA)*, Xi'an, 2017, pp. 175-179. doi: 10.1109/ICCNEA.2017.46

[9] Alani, M. M. Mathematical Approximation of Delay in Voice over IP. *International Journal of Computer and Information Technology* (ISSN: 2279 – 0764), **1** (vol. 3), January 2014, pp. 78- 82.

[10] Yang, S., F. A. Kuipers, Traffic uncertainty models in network planning, *IEEE Communications Magazine*, **2** (vol. 52), pp. 172-177, February 2014. doi: 10.1109/MCOM.2014.6736759

Information about the authors:

Ivan Nedyalkov – I have a PhD degree. I am working at the South - West University "Neofit Rilski" as a senior assistant. My field of research covers: monitoring of IP - based networks, characterization of the traffic flows in IP networks

Alexey Stefanov – Assoc. Prof. PhD in the South - West University "Neofit Rislki". The subjects of scientific researchers are: Mobile radio communication systems, Impacts of the digital music over the human perception, development of digital PMR systems.

Georgi Georgiev – He completed a PhD degree in Technical University - Sofia. Member of the Union of Electronics, Electrical Engineering and Telecommunications (CEEC). The subjects of scientific researchers are: IP network planning, monitoring of IP networks, cloud computing.

Manuscript received on 2 November 2018