https://doi.org/10.1051/e3sconf/202344306016

Field monitoring application based on video surveillance: evaluation of system performance

N B. Usmanova[1*], *D* A. Mirzayev[2], *F* A. Ergashev[3,4], and *D* A. Yunusova[5]

[1]Tashkent university of information technologies named after Muhammad al-Khwarizmi, 108, Amir Temur Avenue, 100202, Tashkent, Uzbekistan
[2]Tashkent Institute of Finance, 100000, A. Temura 60A Street, Tashkent, Uzbekistan
[3]Tashkent State Technical University named after Islam Karimov, Universitetskaya 100095, Tashkent Uzbekistan
[4]Belarusian-Uzbek Intersectoral Institute of Applied Technical Qualifications in Tashkent, Karamurt-1 111208, Tashkent Uzbekistan
[5]Perfect University, 221a, Bogishamol street, 100164, Tashkent, Uzbekistan

Abstract. The article discusses the importance of a developed telecommunications infrastructure for the economic development of the state, as well as the role of IP video surveillance systems in integrated security systems. The issue raised is the integration of video surveillance with various technical systems, ensuring not only the notorious safety of agricultural production, but also helping to solve problems that are far from security. The authors paid attention to the characteristics of the IP camera traffic, examined the flow parameters, collected statistics and determined the average delay and packet transit time. Based on the data obtained, the authors developed a simulation model of an IP video surveillance system, which can be used to determine the optimal parameters of switching equipment for the system. This allows solving the problem of choosing network equipment at the design stage and reduces the likelihood of system failure at the implementation stage.

1 Introduction

One of the main factors for the economic development of any State was the existence of a developed telecommunications infrastructure. The telecommunications network was the basis for the development of informatization and the development of information resources, systems and services. Services are being integrated in various areas, including specialized systems such as security systems and various sectors of the economy [1,2].

In the domain of Smart Agriculture, it is essential to have special tools and system solutions in order to deploy the scalable monitoring system, wherein while related technologies being implemented actively, the surveillance system may be seen as a must, allowing to get control in production, improve the quality of products, protect property from evilpremeditation. The production facility, which has a large area, needs to be equipped with a video surveillance system and a security system. An important factor of any business is to

* Corresponding author: qwerty0409@mail.ru

preserve and control your property and materials. Moreover, this applies to agriculture, as it is very difficult to manage the consumption of raw materials, consumables, the use of agricultural machinery, and much more. Installing video surveillance on the farm in most cases, with the help of a video surveillance system helps to detect violation or illegal action at the initial stages, which allows to minimize the occurrence of accidents; or a quick fix.

After all, an expensive part of an imported tractor or combine harvester, delivered in scrap metal for a penny, may cost not one hundred thousand, and not only that, it can disrupt the crop or harvest. The CCTV system is awake, working around the clock, recording and transmitting data. High-quality digital video surveillance is a reliable aid and guarantee of successful farming.

In the context of wide distribution and use of security systems, implemented by technical means and included in the set of organizational security measures, the study of IP video surveillance systems coincides with the tasks of integration of new systems into existing networks, and the design of new systems requires the development of new methods for calculating network quality indicators that ensure the effective operation of security systems. Video surveillance systems are the industry's fastest growing security sector. A review of literary sources [3], shows that the search for effective network solutions for the field of video surveillance systems is poorly illuminated and largely achieved in an experimental way. Obtaining the calculation characteristics by studying the traffic created by IP camera video surveillance will help in the development of IP video surveillance systems.

2 Role of IP video surveillance for integrated security systems

Integrated security systems include a range of organizational and technical measures to protect facilities from any unauthorized entry into the facility, unauthorized collection of confidential information, theft, vandalism, or sabotage. They reduce commercial risks and increase the likelihood of business continuity. Integrated systems can and should be used in cases of occurrence of events of information security - use in court proceedings, corporate investigations, change of management of the information security system of the company.

The interconnected elements of integrated security systems include: video surveillance systems, including hidden video distribution, remote video surveillance systems, wireless, distributed and centralized video surveillance systems; audio-control, including remote audio control; access control systems, remote control and access control systems, information on the location of employees on site; number recognition systems in parking lots; Technical protection of premises and facilities against unauthorized wiretapping, browsing and information gathering; listening protection equipment during external negotiations; Various comprehensive alarm and fire alarm systems; installation of barriers, turnstiles, lock chambers, etc.

Integrated security systems can be built on different remote sites with a common control center. There are many solutions of varying degrees of complexity that can bring several systems together and provide remote control and control, but most have the same structure.

It should be noted that the IP-based network platform allows the integration of previously separated systems such as video surveillance, fire and burglar alarm system, access control system and others, in a single system, allows you to control the system from anywhere on the planet via the Internet from a single device.

The development of modern, integrated security means is not possible without the growth and development of telecommunications, especially data transmission technologies. It was the development of the Internet that directed the manufacturers of security systems to develop integrated systems, with the support of network technologies. The development of digital technology has revolutionized the video surveillance industry, and this is where IP-based solutions exist [4].

In general, IP video surveillance technology is fully matched to the TCP/IP stack. Data networks are at the same time universal transport, providing for the exchange of different types of traffic, and at the same time have their own characteristics affecting the quality of transmission. The specificity of the IP-video surveillance network is that the network should provide minimal delay and have maximum protection against failures and overloads, because the IP-video surveillance system is primarily a security system. At the same time, in addition to the IP surveillance equipment itself, switching equipment plays a crucial role. The main traffic of the IP video surveillance system - streaming video, is the most complex type of traffic, for transmission through networks with packet switching. The key in the design and construction of a complex IP video surveillance system is the selection of the necessary switching equipment. Its choice often depends on the reliability and quality of the system [5].

3 Main components of IP video surveillance system and their parameters

To calculate the parameters of the switching and node devices of the network of the IP video surveillance system, it is necessary to study the flow parameters created by the IP camera during operation. Stream parameters can be determined by analyzing traffic generated by an IP camera.

This calculation for an IP-based security system can be made based on traffic parameters generated by the main sources in the system. Practice shows that the simple calculation of the network equipment start-up capacity, based on the determination of the bandwidth occupied and the sum-up of the seconds-short traffic, gives only approximate results. This leads to situations where switching equipment must be replaced at the start-up stage, and when it is found that the quality parameters of the system do not match the declared ones. The reason for this is specific traffic, in networks of integrated systems [5,6].

As already noted, most equipment manufacturers limit themselves to brief recommendations on the choice of network equipment, without going into the details of how this choice is made. The same applies to describing the characteristics of the operation of equipment in the network, manufacturers never disclose the protocols and mechanisms of the operation of their equipment at the link level. Traffic analysis allows to identify features and patterns that can be applied in the construction of simulation models of systems, for the design phase, and for the calculation of optimal parameters of network equipment.

The basic elements of the video surveillance system are: IP-camera; video surveillance server (network DVR - NVR); workstation (maybe several); data transmission network.

The IP camera is a digital video camera, the peculiarity of which is the transmission of digital video flow over the Ethernet and TokenRing networks, using the IP protocol.

Typically, before transmission, the matrix image is compressed using frame-by-frame (MJPG) or stream (MPEG-4, H.264) video compression methods. There are specialized IP cameras that transmit video in an uncompressed form. Protocols such as TCP, UDP, and other OSI transport layer protocols can be used in IP cameras. It is common to power IP cameras via PoE (Powerover Ethernet).

The simplest video surveillance system based on IP technology comprises an IP video camera or several, network switching equipment (network switch, hub), a cable or wireless network, and a recording and playback server. The system may also have workstations to view real-time records and videos, but these features may be focused on the server. Fig. 1 provides a schematic of such a system. The basis of the system in this case is a video surveillance server, on which the IP addresses of all cameras are stored, as well as the parameters of recording and quality of playing the picture in real time.

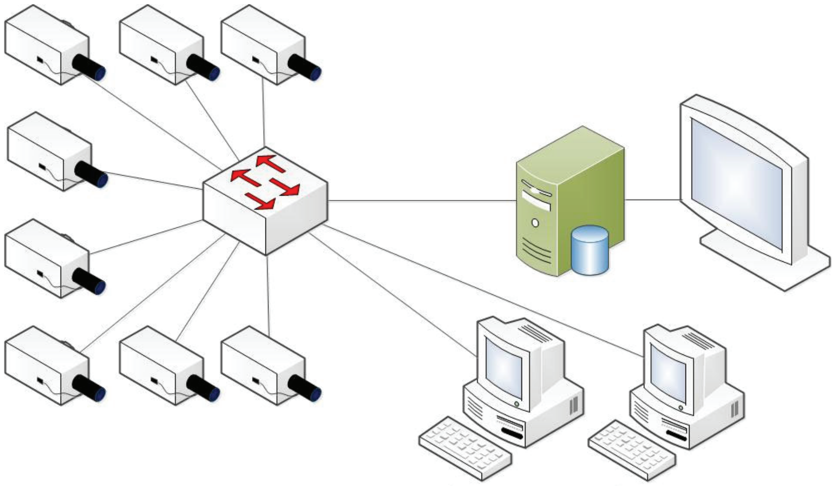

Fig. 1. Diagram of a simple IP video surveillance system.

The server initializes the transfer of video from the camera by sending the corresponding TCP packet. The package is small and contains a camera command to accept the previous package and ready to receive the next. Upon receiving the request, the camera sends a package carrying a piece of video information to the server. The server, having received the package from the first camera, requests the second, third, etc., until it successively polls everything, then goes back to the first.

4 Collection and processing of IP camera traffic

In view of the peculiarities of the information exchange processes between the IP camera and the CCTV server in different conditions, obtaining analytical expressions for them seems to be rather time-consuming task. The decision to develop a simulation model for one system design option that could be used to model other system options seems to be well founded. This approach will eventually allow to form a general method of building models of networks of IP-video surveillance systems.

An experiment made on the equipment of one manufacturer is considered. In this case, we will not consider delays and loss of packages that occur during processing on the server.

Collecting traffic involves capturing traffic from the camera to the server or from the server itself. To obtain reliable results and to avoid possible errors made by network elements, the option of capturing traffic on the server was chosen. The following equipment was used in the pilot network:

- 1.3 megapixel WDR HD IP camera - IPC-HF3300, DAHUA TECHNOLOGY;
- ACER ASPIRE 5749Z (CPU - Intel B960 @2.66GHz, RAM - 2Gb DDR3, system media - HDD).

The connection between the server and the camera is 100 Mbit/s (Fast Ethernet), 1.5m cross patch card. Features of IPC-HF3300P camera:

- sensor -1/3", resolution 2048 1536 (3 megapixels) CMOS matrix Sony Exmor, supported progressive scanning, sensitivity 0.1 Suite in color mode, 0.005 Suite in black and white (at F=1.2);
- compression - H.264/MJPEG, two threads are supported.

The camera supports a Maximum 20fps frame at 3M resolution (2048 1536) and 25/30fps at 720P resolution (1280 720), the width of the stream can lie within 32kbit/s. 8Mbit/s.

A limit of 8 Mbit/s is selected for the experiment, when the camera generates the maximum amount of traffic. To achieve this, the camera was set the maximum resolution of the picture, and the server - the maximum quality of recording was set.

CCTV server software - Pro Surveillance SystemV.4.06, DAHUA TECHNOLOGIES (included in the camera delivery). Minimum PSS System Requirements:

- operating system: Windows XP /2003/Vista/7 (also MacOS 10.6.5 and Linux USE)
- CPU: minimum P4 2.8 GHz or Dual Core 2.0 GHz and above.
- Graphics card: Support DirectX 9.0c and above.
- RAM: minimum 1GB and above.
- monitor: thread 1024 768 or higher.

The server is a computer that meets the performance requirements of PSS, ACERASPIRE 5749Z. The main parameters are:

- operating system - Microsoft Windows 7.
- Processor: Intel B960, 2.66 GHz.
- graphics card: Intel HD Graphics.
- RAM: 2Gb DDR3.
- monitor: resolution 1366 768.

A Wireshark network protocol analyzer (v. 1.8.5) [6] installed on the same personal computer as the CCTV server was used to capture the protocol traffic.

For the analysis selected traffic totaling 1 hour. In total, four files were selected and processed, each about 1 GB in size, and the log size corresponds to 15 minutes of traffic capture. The traffic obtained during the experiment was sorted by directions, the sorted traffic was sampled by package length, time accumulation and intervals between the nearest packets. Sorting by directions was done in the Wireshark program, a filter mapping by source was used. The segments that the camera originated from were exported from the Wireshark program to a CSV file and can be processed in MS Excel. Then the sample preparation was carried out. Table 1 shows the general format of displaying CSV files in MS Excel. The total sample length for each case is 2,633,549.

Table 1. IP camera traffic fragment. The process of confirming the connection and starting the exchange.

No.	Period	Source	Function	Report	Length
1	0.000000000	192.168.1.1	192.168.1.108	TCP	86
2	0.004328000	192.168.1.108	192.168.1.1	TCP	86
3	0.039984000	192.168.1.108	192.168.1.1	TCP	1514
4	0.039986000	192.168.1.108	192.168.1.1	TCP	1514
5	0.040066000	192.168.1.1	192.168.1.108	TCP	54
6	0.040142000	192.168.1.108	192.168.1.1	TCP	1514
7	0.040486000	192.168.1.108	192.168.1.1	TCP	1514
8	0.040520000	192.168.1.1	192.168.1.108	TCP	54
9	0.040686000	192.168.1.108	192.168.1.1	TCP	1514
10	0.040800000	192.168.1.108	192.168.1.1	TCP	1514
11	0.040826000	192.168.1.1	192.168.1.108	TCP	54

12	0.041012000	192.168.1.108	192.168.1.1	TCP	1514
13	0.041253000	192.168.1.108	192.168.1.1	TCP	1514
14	0.041255000	192.168.1.108	192.168.1.1	TCP	703
15	0.041310000	192.168.1.1	192.168.1.108	TCP	54
16	0.041377000	192.168.1.108	192.168.1.1	TCP	1514
17	0.041474000	192.168.1.108	192.168.1.1	TCP	1514
18	0.041499000	192.168.1.1	192.168.1.108	TCP	54
19	0.041717000	192.168.1.108	192.168.1.1	TCP	1514
20	0.041718000	192.168.1.108	192.168.1.1	TCP	1514

The server, when connecting to the camera, sends the TCP-packet "novation", to port 37777, the packet length 86 bytes. The camera responds to the request with the same type of 86-byte package. After 0.004 seconds, the camera starts sending video streams, packing them into 1,514 bytes. After receiving the fragment, the server processes it and sends a new request, 54 bytes in size. All subsequent traffic from server to camera is a sequence of such requests. The length of the request package is determined to 54 bytes. For each server query, the camera responds with several packages of 1514 bytes, usually 2 to 3, less often with longer sequences.

The resulting traffic is analyzed to determine its parameters, to build a simulation model of the IP video surveillance system. For samples obtained from the processing of IP camera traffic, the basic parameters were calculated, the results are summarized in table 2.

Sample processing was carried out in MATLAB 7.11.0, a mathematical calculation system with a built-in modelling environment.

Analysis of sample packet lengths found that 93.19% of all packets are packets with a length of 1514 bytes. This suggests that we are dealing with traffic close to deterministic traffic. Figure 2 presents a histogram for distributing packet lengths, and Fig. 3 presents a histogram for distributing packet intervals.

Table 2. Results of calculation of sample parameters obtained from IP camera traffic.

	Packet length	**Packet spacing**
Minimum value	60	0.0002
Maximum value	1514	0.1705
Mathematical expectation	1463.80	0.0014
Dispersion	39507.00	0.00006211
Asymmetry in	-4.1384	7.7679
Excess	17.1578	69.6285

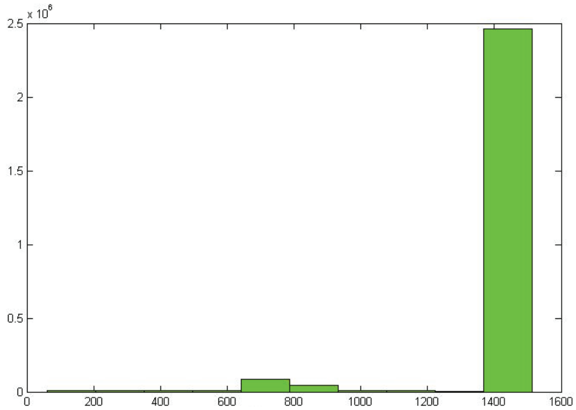

Fig. 2. Histogram showing the distribution of packages size.

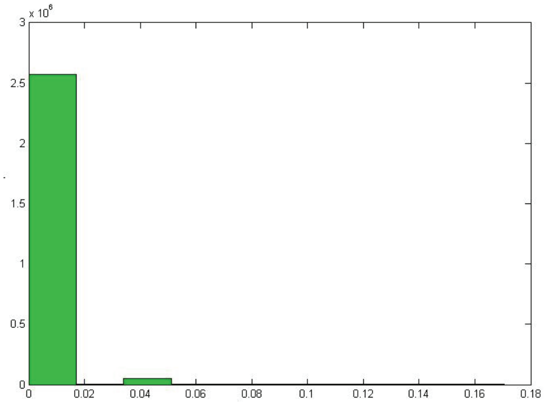

Fig. 3. Histogram showing the distribution of packet interval lengths.

To construct a simulation model, we assume that the IP camera creates a deterministic stream with a packet size of 1,514 bytes and a packet interval equal to the mathematical expectation of the interval. This will allow a fairly accurate description of the flow created by the IP camera in the network of the video surveillance system. Missing 7% of packets will not create a serious error, as we discard packets that have smaller size and larger intervals and therefore create a small load on the switch.

Five system scenarios were implemented, with different number of cameras, from 1 to 5 with increment 1. At each stage of the simulation, the performance of the switch from 5000 to 10000, with increment 1000. The simulation time of one stage is 5 minutes. In the simulation process the statistics on the passage of packets through the switch were collected:

- ethernet delay.
- TCP round trip time.

The samples from these values will provide the average packet delay through the switch. The delay value indicates the extent to which the switch's throughput meets system requirements. In addition, we can get the jitter delay value. The main for us is the delay statistics in the channel. Deviation of the TCP packet time depends on the delay in the channel but includes a delay in transferring the packet from source to server and forwarding the response from the server to the source. In this case, we use it to compare the results of the average delay time analysis.

The simulation data is exported from OPNET to MS Excel for further processing. The capabilities of MS Excel make it possible to calculate the values of average latency and pass times of packets, as well as to construct graphs of these values and find an approximate function for these graphs.

In the first scenario, the model involves one source. The flow rate processed by the switch is 720 pack/s. In the first step, the switch performance was selected to be 5,000 pack/s. For each further step, the output increased by 1,000. The delay values obtained because of the simulation are summarized in a table, their average value and the variance are calculated.

Table 3 presents the most appropriate approximation functions. Obviously, the delay value cannot reach zero, so the linear function is not applicable. The polynomial function has a maximum determination coefficient of R^2 but is a second-order curve and tends towards infinity, so is also not applicable in this situation. Of the remaining, the greatest determination coefficient is the power function.

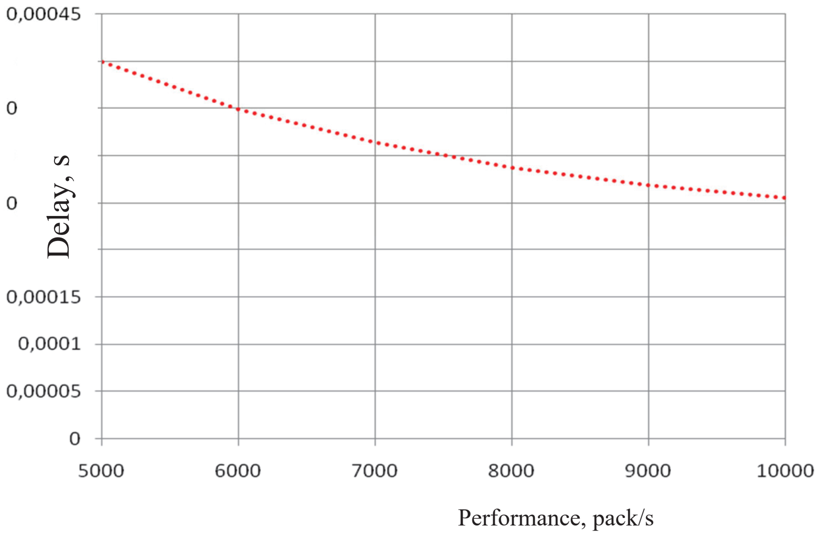

Fig. 4. Graph of average delay time on switch performance for first scenario.

Table 3. Approximation functions for the average delay time of the first scenario.

Function	Function expression	R^2
Polynomial	$y = 5 * 10^{-6} * x^2 - 6 * 10^{-5}$	0.999
Linear	$y = 3 * 10^{-5} + 0{,}0005$	0.947
Staid	$y = 0{,}00015 * x^{-0{,}25}$	0.990
Exponential	$y = 0{,}00011 * e^{-0{,}08x}$	0.971

Similar calculations have been made for scenarios 2, 3, 4 and 5. The average delay is shown in table 4. Also, the delay jitter values for all scenarios are calculated, and the values are shown in Table 5.

Table 4. Average delay values of modelling results.

Scenario	Switch capacity, pack/s					
	5000	**6000**	**7000**	**8000**	**9000**	**10000**
1 source	0.00040	0.0035	0.0041	0.0049	0.0061	0.00040
2 source	0.00035	0.0007	0.0035	0.0041	0.0051	0.00035
3 source	0.00031	0.0005	0.0035	0.0037	0.0044	0.00031
4 source	0.00029	0.0004	0.0035	0.0035	0.0039	0.00029
5 source	0.00027	0.0004	0.0005	0.0035	0.0037	0.00027

Table 5. Values of jitter delay based on model results.

Scenario	Switch capacity, pack/s					
	5000	**6000**	**7000**	**8000**	**9000**	**10000**
1 source	$1.80*10^{-8}$	$9.33*10^{-7}$	$2.51*10^{-6}$	$2.85*10^{-6}$	$6.07*10^{-6}$	$1.80*10^{-8}$
2 source	$1.68*10^{-8}$	$4.38*10^{-6}$	$7.01*10^{-6}$	$9.58*10^{-7}$	$3.23*10^{-6}$	$1.68*10^{-8}$
3 source	$1.84*10^{-8}$	$4.74*10^{-9}$	$1.44*10^{-6}$	$1.28*10^{-5}$	$1.99*10^{-6}$	$1.84*10^{-8}$
4 source	$1.54*10^{-8}$	$5.66*10^{-9}$	$7.20*10^{-6}$	$1.01*10^{-5}$	$1.12*10^{-6}$	$1.54*10^{-8}$
5 source	$1.78*10^{-8}$	$6.29*10^{-9}$	$2.87*10^{-7}$	$7.94*10^{-7}$	$8.43*10^{-6}$	$1.78*10^{-8}$

An approximation function is calculated for each scenario. All function expressions are given in table 6. Power function is selected as approximation, as it provides the greatest reliability when extrapolating range.

Table 6. Expressions of approximation functions for all scripts.

\	Function	Expression	R²
1 source	staid	$y = 0.00015 * x^{-0,25}$	0.990
2 source	staid	$y = 0.002 * x^{-1,21}$	0.867
3 source	staid	$y = 0.006 * x^{-1,14}$	0.553
4 source	staid	$y = 0.004 * x^{-0,19}$	0.926
5 source	staid	$y = 0.006 * x^{-0,31}$	0.990

On Figure 5 and 6 show graphs of approximating functions for the average time lag for scenarios 2 and 3. Similar graphs for scenarios 4 and 5 are given in Figure 5, 7 and 8.

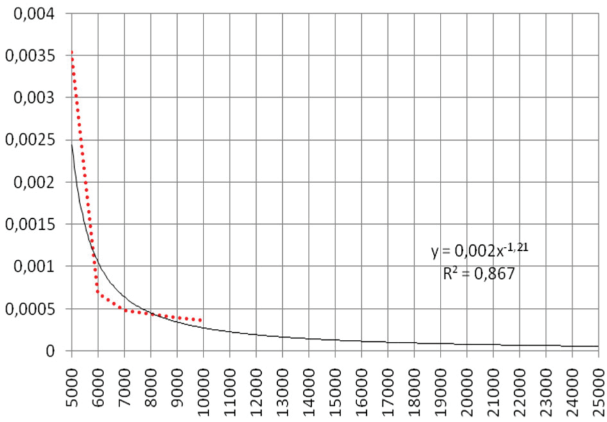

Fig. 5. Extrapolation of delay values for the second scenario.

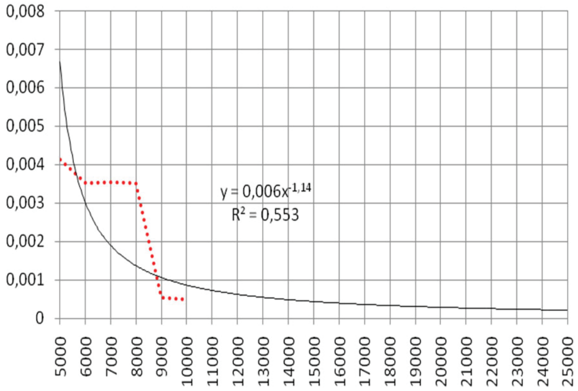

Fig. 6. Extrapolation of delay values for the third scenario.

According to the graphs for the second and third scenarios, it is possible to notice a sharp increase of delay by an order of magnitude, when the ratio of the flow rate to the capacity of some value is reached. This value is in the range from 0.25 to 0.28. If the flow rate does not exceed 0.25 of the switch's bandwidth, the delay is of order 0.0002... 0.0006, otherwise the value jumps to 0.002... 0.006. Therefore, there are sharp fractures in Scenarios 2 and 3 at points where the speed of traffic exceeds a quarter of the capacity of the switch. At other intervals where there is no change between the delay values, the graph manifests itself as an exponent (determination coefficient at least 0.9). This makes it possible to calculate that the delay-to-capacity method is not more than 10%.

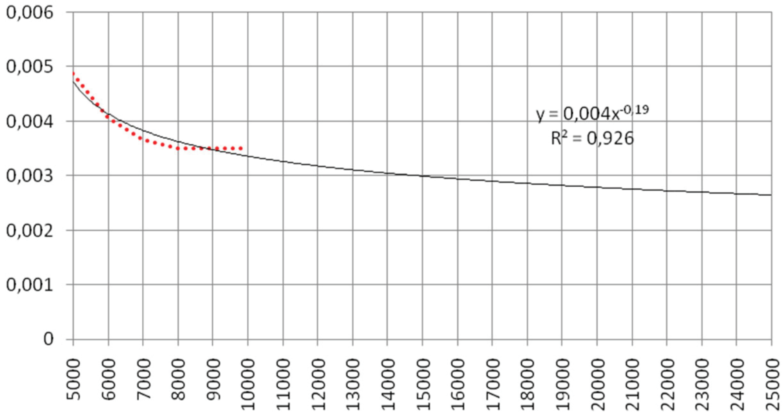

Fig. 7. Extrapolation of delay values for the fourth scenario.

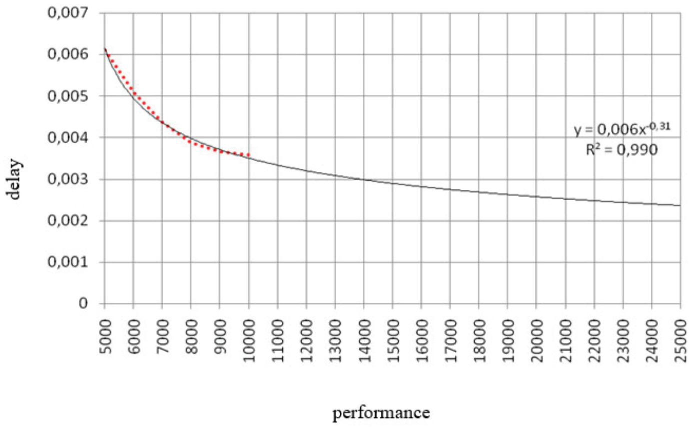

Fig. 8. Extrapolation of delay values for scenario 5.

Thus, having a known minimum packet pass-through tolerance for the system, as well as a known jitter delay tolerance, it is possible to search for the required network switch performance value, using approximate simulation results. To do this, it is necessary to build a model of the system, with the required number of traffic sources (cameras), to produce several cycles of model operation for different values of the switch performance. From the results, it will be possible to construct a curve to determine which performance values meet the system's latency requirements. To increase the accuracy of the model results, switches with a bandwidth known to be lower than the total flow rate of all sources should not be used in the model. This will eliminate the obviously unacceptable delays and packet losses.

5 Conclusion

Video surveillance systems are the most demanding element of integrated security systems in relation to data network parameters. IP-video surveillance systems maximally use network technologies in their work, construction of networks for IP-video surveillance systems imposes special requirements to the project and equipment. When designing IP video surveillance systems, it is necessary to make an economically justified choice of switching equipment, which will ensure quality operation of the system. Network optimization for IP video surveillance system consists in finding network equipment with optimal parameters for these system performance requirements. Often, the equipment recommended by the system manufacturer or system integrator has a knowingly excessive performance, and therefore is more expensive. As a result of the analysis of the traffic of the IP camera, it was possible to obtain the flow parameters sufficient for the construction of the camera model as a source. Using the camera model, it is possible to model the operation of the future system, and to select the parameters of network equipment, according to the system quality requirements. This solves the problem of selecting network equipment for the IP video surveillance system during the design phase and reduces the probability of system failure during the start-up phase. It also solves the problem of overpayment for network equipment, when selecting equipment with obviously excessive characteristics.

References

1. S. Muller-Schneiders, T. Jager, H.S. Loos, Wolfgang Niem, *Performance evaluation of a real time video surveillance system/ Visual Surveillance and Performance Evaluation*

of Tracking and Surveillance, 2005. 2nd Joint IEEE International Workshop (2005) https://www.doi.org/10.1109/VSPETS.2005.1570908

2. J.C. SanMiguel, Á. García-Martín, J.M. Martínez, *Performance Evaluation in Video-Surveillance Systems: The EventVideo Project Evaluation Protocols*. (In: Atrey, P., Kankanhalli, M., Cavallaro, A. (eds) Intelligent Multimedia Surveillance. (Springer, Berlin, Heidelberg 2013). https://www.doi.org/10.1007/978-3-642-41512-8_9
3. Youngboo Kim, Junho Jeong, A Simulation-Based Approach to Evaluate the Performance of Automated Surveillance Camera Systems for Smart Cities, in Appl. Sci. **13(19)**, 10682 (2023). https://www.doi.org/10.3390/app131910682
4. A.A. Igashev, F.A. Ergashev, *Screw conveyor with anti-friction polymer coating for cotton transportation* Annual International Scientific Conference on Agricultural Engineering and Green Infrastructure Solutions, AEGIS, 20-21 May, 2021, Tashkent, Uzbekistan (2021)
5. Sh. Gulyamov, A. Yusupbekov, D. Mirzaev, Z. Kuziev, E3S Web of Conferences **417**, 05011 (2023). https://www.doi.org/10.1051/e3sconf/202341705011
6. A.O. Ataullaev, O.X. Ataullaev, F.A. Ergashev, E3S Web of Conferences **417**, 05007 (2023). https://www.doi.org/10.1051/e3sconf/202341705007