Journal of KONBiN 2020
Volume 50, Issue 4
DOI 10.2478/jok-2020-0080

Piotr ŁUBKOWSKI, Dariusz LASKOWSKI
Military University of Technology (Wojskowa Akademia Techniczna)

THE QUALITY OF VIDEO COMMUNICATION IN ENCRYPTED TRAFFIC

Jakość komunikacji wideo w połączeniach szyfrowanych

Abstract: *The rapid development of network and computer technologies creates opportunities for offering advanced broadband multimedia services to a growing number of end users. Instant messaging and group communication services based on real-time video transmission based on global Internet resources are the most popular. The basic challenge related to the implementation of video transmission services is to ensure an appropriate level of quality and security (Quality & Security). The article presents a multi-criteria assessment of the impact of encryption protocols for multimedia video transmissions on the perceived quality of QoE (Quality of Experience) service implementation. The presented measurement method together with the proposed research methodology create the possibility of determining the likelihood of video service availability with accepted QoE in heterogeneous networks.*
Keywords: video communication, security, Quality of Experience

Streszczenie: *Gwałtowny rozwój technologii sieciowych i komputerowych stwarza możliwości oferowania zaawansowanych szerokopasmowych usług multimedialnych coraz szerszemu gronu użytkowników końcowych. Największą popularnością cieszą się usługi komunikacji natychmiastowej i grupowej bazujące na transmisji obrazu wideo w czasie rzeczywistym w oparciu o zasoby globalnego Internetu. Podstawowym wyzwaniem związanych z realizacją usług transmisji wideo jest zapewnienie odpowiedniego poziomu jakości i bezpieczeństwa (Quality&Security). W artykule zaprezentowano wielokryterialną ocenę wpływu protokołów szyfrowania multimedialnych transmisji wideo na postrzeganą jakość realizacji usługi QoE. Przedstawiona metoda pomiarowa wraz z zaproponowaną metodyką ba-dawczą stwarzają możliwość wyznaczenia prawdopodobieństwa dostępności usługi wideo o akceptowanej QoE w sieciach heterogenicznych.*
Słowa kluczowe: komunikacja wideo, bezpieczeństwo, jakość postrzegana

1. Introduction

Video over IP (VEoIP) technology has been growing in popularity for several years. Simple system architecture, the ability to reduce the costs of implementation and operation of the infrastructure mean that video communication services using VEoIP successfully displace traditional commutation solutions. However, the widespread introduction of VEoIP communication services requires meeting a number of criteria related to ensuring an appropriate quality level (*QoS – Quality of Service*) of video transmission and the appropriate level of security (*QoP – Quality of Protection*) of service delivery. The quality of the video connection is the basic factor determining the correctness of the VEoIP service implementation. Ensuring QoS is an important challenge as far as the value of parameters such as bandwidth, delay and packet loss are taken into account. Numerous disturbances occurring in ICT networks may negatively affect the quality of the VEoIP connection and in particular, the perceived quality of QoE video signal (*Quality of Experience*) [11]. However, QoE quality does not include only the subjective perception of video content, but also the effectiveness of the implementation of specific functions. It, therefore, requires a precise definition of quality indicators covering all possible interferences and at the same time considering the human factor. Maximizing the quality of video reception focuses on the optimization both the network and performance parameters. In the second group of parameters *Peak Signal-to-Noise Ratio (PSNR)*, *Structural SIMilarity (SSIM)* or qualitative indicators describing the quality of perceived *Mean Opinion Score (MOS)* are significant. The quality of video transmission is also affected by such indicators as *blur*, *blockiness*, *contrast* and *bitrate*.

The issues of video quality measurements are reflected in the recommendations and standards [5,6], they are also the subject of many scientific publications [2,3,8,13,14]. The problem which is discussed concerns mainly HTTP video streaming and covers the HLS and DASH implementations. As a result, we can observe the evaluation of such measures as Stall Detection, Average Representation Detection and Representation Quality Switch Detection are not fully reflected in the ITU recommendations. The mentioned publications also do not indicate the relationship between a specific encryption mechanism and the results obtained. However, they are an important set of information enabling the analysis of the problem of assessing the quality of encrypted video transmissions. Therefore, ensuring QoS quality with respect to the network layer and QoE with respect to the application layer is a major challenge for video systems.

Another extremely important challenge for modern service providers is to ensure an appropriate level of security of the provided services. Since a significant part of the offered services requires or benefits from the widely used Internet, the aspect of service security has great importance. Currently, the use of network resources is associated with the risk of interception or modification of transmitted data and the use of such data in a manner inconsistent with its original purpose. The above threats apply to both corporate solutions and individual network users. Thus, ensuring the security of video communication by encrypting the transmission seems necessary and indispensable. Most cryptographic

protocols operate directly on user data, which can also affect the perceived quality of multimedia communication. Hence the need to monitor and evaluate encrypted video data sent over the IP network using various cryptographic mechanisms, and to use the collected information to increase the efficiency, effectiveness and reliability of the VEoIP service. The impact of the presented issues on the general characteristics of the quality of video communication is presented in fig. 1. The figure visualizes the impact of technical aspects related to the use of security and transmission quality mechanisms on the perceived quality of service delivery in the context of efficiency and reliability of video communication service.

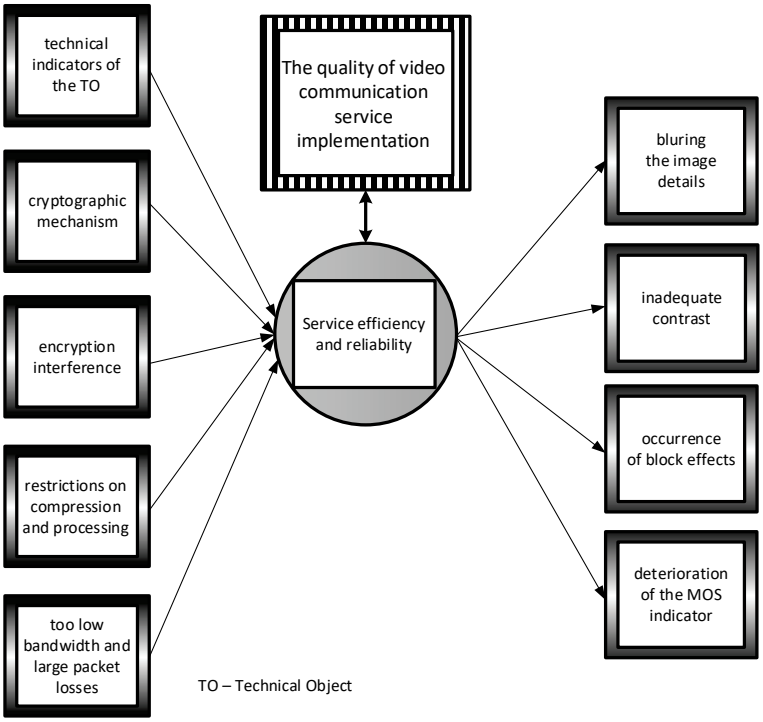

Fig. 1. Analysis of video communication quality problems in the aspect of external factors influence

The research methodology proposed later in the article uses the testing assumptions presented in the ITU-T standards [6] extended by the possibility of continuous monitoring of operational parameters of the research environment and verification of the configuration parameters of the tested video service. The use of a dedicated measurement application in the form of VQM (*Video Quality Monitor*) software enables the assessment of the quality of VEoIP communication in a wide range of video signal parameters. A reflection of the real working conditions of the extensive multimedia heterogeneous environment was

obtained thanks to the use of the IT platform for scientific research support launched at the Institute of Telecommunications of MUT.

The remaining part of this paper is structured as follows. The security requirements for video transmission are described in Section 2. Next, Section 3 presents methods of assessing the quality of video signal transmission, enabling consideration of a wide spectrum of assessment criteria. The analysis of determinants affecting the probability of video service availability with an acceptable level of perceived quality is presented in Section 4. Section 5 presents a description of the proposed methodology for estimating the impact of encryption on the quality of video transmission and the results of the selected experiments.

2. Security of video transmission

The security of video transmission depends on a number of factors, including physical and technical security as well as the impact of the human factor. Currently, the main threats to which multimedia communication users are exposed to using the resources of the ICT network include:

1. Irreversible loss of data,
2. Data corruption or modification,
3. The theft, deletion or loss of data,
4. Disclosure of data,
5. Lack of services availability.

Protection against the above-mentioned threats requires conducting and maintaining specific security policy rules based on the security attributes specified in [7]. These include attributes such as content confidentiality, data integrity and authentication.

It is also worth mentioning such security attributes as non-repudiation and high availability. The confidentiality of the content guarantees that the information provided will not be disclosed to unauthorized persons, the data integrity is in turn associated with preventing intentional or accidental modification of the transmitted data in an unauthorized manner. The authentication process is to ensure that the identity of the person (or resource) having access to information is consistent with that declared in the security policy. Guarantees of access rights and the ability to use them are described in the availability attribute, while the unambiguousness of linking data exchange with the entity in this participating exchange determines non-repudiation.

The guarantee of maintaining security attributes is obtained through the use of security protocols responsible for encrypting data sent over the network. Basic encryption protocols include protocols such as IPSec, SSL, TLS and SSH, as well as the DTLS (*Datagram Transport Layer Security*) protocol. However, for multimedia applications offering video transmission, another group of solutions is used. This is due to the fact that multimedia traffic based on audio or video data is most often implemented in the form of streaming using the RTP (*Real Time Transfer Protocol*). Protocols such as SRTP (Secured RTP) and

ZRTP (*Zimmermann RTP*) apply to this application group. The presented group of protocols operates basically in different layers of the ISO/OSI reference model, offering various functionalities related to encryption not only of user data but also connection signaling. Internet Protocol Security (*IPSec*) provides IP-level encryption on both IPv4 and IPv6 versions. This protocol ensures that security attributes such as confidentiality, integrity and authentication are maintained. In addition, its use allows securing all communications from end to end. In turn, the SSL (*Secure Socket Layer*) protocol guarantees the integrity and confidentiality of transmitted data and is used at the transport layer level, so only information provided by the TCP layer is protected. It is most often used to ensure the security of application layer protocols, such as HTTP, FTP, Telnet and others. The SSL protocol is expanded with the TLS (*Transport Layer Security*) protocol. It ensures confidentiality and data integrity. Like SSL, it has some authentication mechanisms for the server and the client itself. The TLS protocol is most often used for signature e-mail's and authorization of web servers. The DTLS (*Datagram Transport Layer Security*) protocol is a protocol that provides secure data transmission in the form of datagrams. The DTLS protocol is based on the TLS protocol and provides a similar level of security guaranteeing confidentiality and integrity of data transmission. SSH (*Secure Shell*) protocol, also often called remote session protocol, is responsible for data encryption during connections between terminals and remote computers. SSH provides encryption of the entire data transmission and also creates the ability to recognize the user.

SRTP is an application layer protocol associated with the RTP protocol, which is responsible for the transmission of multimedia data in real time. It provides encryption, authentication and ensures the integrity of data streamed using the RTP protocol. The SRTP protocol, in turn, does not interfere with the signaling procedures, so the signaling phase is not cryptographically secured. ZRTP is also based on the RTP protocol. ZRTP is responsible for negotiating cryptographic keys between the two end points. ZRTP operates by generating a random key for each of the occurring connections. After the exchange of data between two users is completed, a randomly generated key is deleted, which prevents unauthorized reproduction of multimedia data.

The above-mentioned encryption protocols differ in the key length (56, 128 or 256) used, the integrity control mechanism and data authentication used, as well as the solutions used to increase the transmission resistance to packet loss or delay. Therefore, when analyzing the impact of data encryption mechanisms on the perceived quality of multimedia communication, a relatively wide spectrum of available solutions as well as a number of criteria reflecting both the characteristics of digital video information, multimedia streaming and user expectations should be assessed.

3. Methods of video quality assessment

The methods of video transmission quality assessment presented below are generally defined in two categories: objective methods and subjective methods. Objective methods

are characterized by the assessment of the video sequence in terms of its quality, using mathematical models that are used to determine the parameters describing the characteristics of the video signal, encoder or network characteristics. Depending on the availability of the reference video signal, these methods can be divided into [8]:

1. Full Reference – the method that gives the best results due to the comparison of the reference signal with the distorted signal. The results of the comparison are similar to those obtained using subjective methods.
2. Reduced Reference – a method in which only some parameters of the reference signal are used for comparative purposes.
3. No reference – the method does not have access to the reference signal, so the quality assessment is based on a distorted signal available at the receiving side. The advantage of this method is that it does not require sending a reference signal to the receiver.

The main metrics used by objective methods include the PSNR (*Peak Signal-to-Noise Ratio*) metric and the MSE (*Mean Square Error*) metric.

The **PSNR** metric is a measure of the image noise and is expressed by the following formula:

$$PSNR = 10 \cdot log_{10} \frac{MaxErr^2 \cdot N \cdot M}{\sum_{i=0,j=0}^{N,M} (x_{i,j} - y_{i,j})^2} \tag{1}$$

where:
MaxErr – the value depends on the number of colors used (e.g. 256 for 8 bits),
N, M – image dimensions in pixels,
$x_{i,j}$ – value of the pixel with coordinates (i, j) of the original image,
$y_{i,j}$ – value of the pixel with the coordinates (i, j) of the received image.

The MSE metric represents the mean square error and allows for comparison of the quality with respect to subsequent pixels of the analyzed image, indicating a deviation from the average value. It is expressed by the formula:

$$MSE = \frac{1}{N \cdot M} \sum_{i=1,j=0}^{N,M} (x_{i,j} - y_{i,j})^2 \tag{2}$$

where:
N, M – image dimensions in pixels,
$x_{i,j}$ – value of the pixel with coordinates (i, j) of the original image,
$y_{i,j}$ – value of the pixel with the coordinates (i, j) of the received image.

In the case of objective evaluation, a number of artifacts can also be identified that affect the perceived quality of the video sequence. These include image flickering, mosquito noise, contrast, blur and block effects. They are the result of improper selection of coding parameters and compression of the digital image. For example, mosquito noise arises as a

result of quantization errors, and block effects are due to the wrong selection of bit representation for individual pixels of the image (fig. 2).

Fig. 2. Example of block effects (comparison of original and distorted image)

The advantage of objective assessment methods is above all the possibility of their use in relation to applications and services implemented in real time. It should be noted that the results obtained with objective methods are not always correlated with the results obtained using subjective methods.

Subjective video quality assessment methods allow you to evaluate the impact of compression, processing and data transmission techniques on user perceived quality expressed on a five-point MOS scale. User feelings can also be expressed on a scale of 0 to 100, which was introduced to take into account the broader spectrum of user feelings. The assessment criteria include concepts such as block effects, temporary image disappearance, motion discontinuity, image retention or the already mentioned snowing, blur, etc. The most popular assessment methods include the DCR (*Degradation Category Rating*) method, which compares image sequences in pairs. Test participants are presented alternately image sequences without any or with distortions. To eliminate accidental errors, multiple test repetitions under the same conditions are used, which allows for the distribution of quality deterioration results to be determined.

4. Availability of video communication service

The video communication service, like all multimedia services offered to the modern user, is a product of the $\boldsymbol{S}$ telecommunications system usually described by the mathematical model presented in the following form [9,10,12]:

$$S = \langle G, \{F_z\}, \{f_k\} \rangle \tag{3}$$

where:

$\{\boldsymbol{F_z}; z = \overline{1, Z1, Z \, 1, Z}\}$ – set of function F_z: T → R+,

$\{\boldsymbol{f_k}; k = \overline{1, K1, K \, 1, K}\}$ – set of function f_k: W → R+,

$\boldsymbol{G}$ – graph defined by:

$$G = \langle W, T, P \rangle \tag{4}$$

where:

W= $\{w_l: l = \overline{1, L1, L \, 1, L}\}$ – scalable set of graph vertices (network nodes),

T= $\{t_m: m = \overline{1, M1, M1, M \, 1, M}\}$ – scalable set of graph branches (telecommunications links),

$P \subset W \otimes T \otimes$ – W triple relationship such that for every $t_m \subset T$ there are $\boldsymbol{e}$ pairs of nodes $\langle w_i, w_j \rangle$ that $\langle w_i, t_m, w_j \rangle \in P$, where w_i is the start node and w_j is the end node. The network size is the sum of the nodes and connections:

$$|E| = |W| + |T| = L+M,$$

$$E = \{e_i: i = \overline{1, L+M}\} \tag{5}$$

Let's denote the operational state of the e_i component of x_i network and suppose it can take one of two values:

$$x(e_i) = x_i = \begin{cases} 1 & when \quad element \quad e_i \quad is \quad usable \\ 0 & when \quad element \quad e_i \quad is \quad unusable \end{cases} \tag{6}$$

In this case, when the network elements can be represented using a vector $\vec{X} \, \vec{X} \, \vec{X} \, \overrightarrow{X}$ of *(L+M)* components which have values of 0 or 1:

$$\vec{\boldsymbol{X}} = [\underbrace{\boldsymbol{x_1}, \ldots, \boldsymbol{x_L}}_{\boldsymbol{L}}, \underbrace{\boldsymbol{x_{L+1}} \ldots, \boldsymbol{x_{L+M}}}_{\boldsymbol{M}}] \tag{7}$$

Let us also assume that the processes of faults and repairs of elements $\boldsymbol{e_i}$ are mutually independent and work properly together with the parameter $\boldsymbol{\lambda_i}$ (fault intensity) and repair time with the parameter $\boldsymbol{\mu_i}$ (repair intensity) and that they are exponential.

Similarly as in the case of network elements, it can be assumed that the sets of network operating states are composed of two elements. The criterion for classifying network states can be represented by the following relationship:

$$\Phi(STI) = \begin{cases} 1 & when \quad STI \quad network \quad is \quad usable \\ 0 & when \quad STI \quad network \quad is \quad unusable \end{cases} \tag{8}$$

The network is in usable state if and only if at all ***t*** moments all network elements are in a usable state. It also means that the service provided by such a defined network is usable, i.e. it reaches a certain level of quality from the point of view of network considerations.

At the level of technical analysis of factors affecting the degradation of the quality of the service provided, the impact of various types of elements (technical objects TO) occurring in the area of telecommunications services, i.e. terminals, servers, sensors, techniques and technologies and protocols used in data processing, and their preparation for transport through a telecommunications system.

In this environment, the implementation of the service is related to:

1. The implementation of threads and processes in terms of preparing digital data.
2. Functional possibilities of resources:
   - access and transport in terms of data transport,
   - control the traffic (routing commutating) in terms of flow control.

Considering the number and complexity of factors, it is proposed to group them into significant sets of determinants in the form of internal OT properties, operator properties and harmful environmental impact as components of the formula for the probability of the condition of usable state:

$$P_{SZ}\left(t, e_i\right) \cong f\left(P_{wWi},\ P_{pOpi}, P_{zOti}\right) \tag{9}$$

where:

P_{wWi} – probability of correct functioning of OT taking into account internal properties,

P_{pOpi} – probability of proper functioning of the OT operator, taking into account knowledge and experience in the time limits of project implementation (i.e. use or operation of the OT),

P_{zOti} – probability of OT being usable for the environment.

For further analysis, it was assumed that the defined $\boldsymbol{P_{sz}}$ value would be understood as the probability of providing the service with a defined quality level. In addition, due to the complexity and multifaceted conditions necessary to take into account, the following assumptions are proposed: independence of the usable condition, the stream of damage without memory, failure of one element does not change the usable status of the other elements, there are no functional or correlation relationships between the times of appearance of individual failure conditions elements, singularity and trouble-free (failure is the appearance of many defects suddenly) of the damaged stream.

5. Research methodology and results of VEoIP quality assessment

In order to assess the impact of selected aspects of encryption and heterogeneous network parameters on the quality of the VEoIP service, a research methodology has been developed based on the use of a measuring tool in the form of a dedicated VQM (*Video Quality Monitor*) software enabling the assessment of video quality based on the "no reference" method (fig. 3). The application performs quality assessment on MOS scale, and also provides the values of quality indicators such as ***blur***, blockiness (***block effects***), ***contrast*** and ***bitrate***. Acceptable values for the above quality indicators are as follows:

- for blur – ≤ 3,
- for block effects – ≤ 2,
- for contrast – $0 \div 0.15$.

These indicators, together with the overall rating expressed on the MOS scale, allow mapping the correlation of the feelings of the observer realizing the perception of the presented video sequence, i.e. QoE.

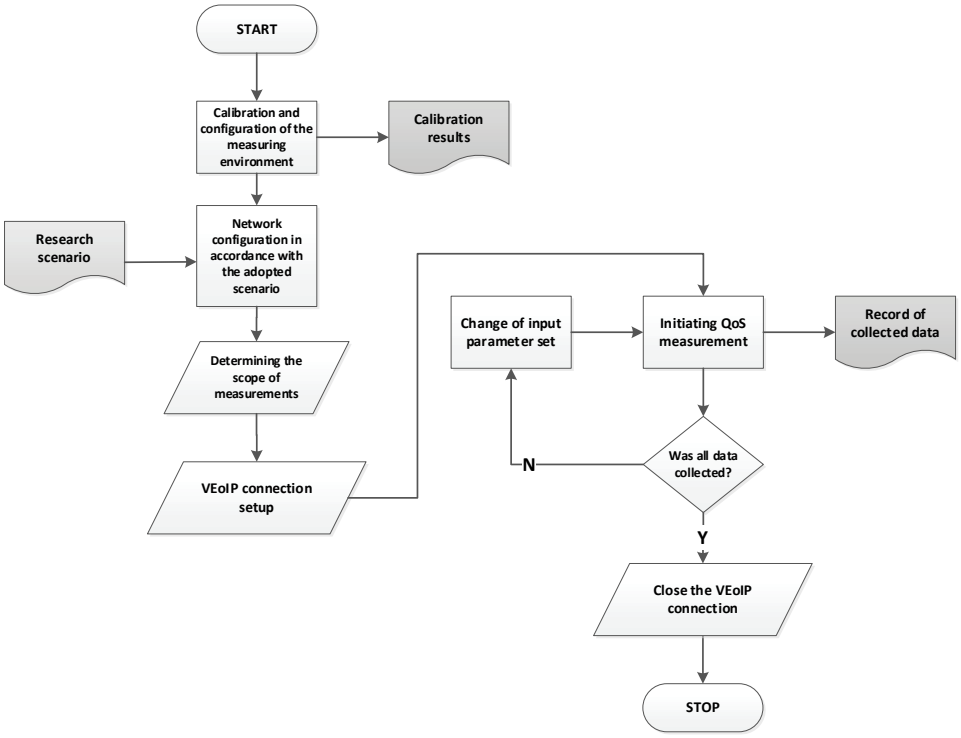

Fig. 3. Block diagram of the research methodology

The existing infrastructure of the IT platform supporting scientific research was used to carry out the research experiment (fig. 4). The research network consists of two local LAN subnets based on Ethernet technology, connected together by a backbone network, using for routing (routing) the iBGP and OSPF protocols. As part of the research, unused portion of this architecture was used. This ensured constant measurement conditions, and therefore no additional, uncontrolled network traffic. The LANforge interference emulator was used to introduce controlled changes in network properties. The interference emulator is a device that simulates network conditions. It allows us to introduce controlled interference into the tested network, such as bandwidth change, delay, jitter, packet losses, etc.

The conclusion about the correctness of the statement of network components in the field of data transmission, which is a reflection of information from the telecommunications system, is based on statistical estimation of the integrity of the hardware and software platform forming the service implementation chain. The research shows that this type of research environment can be considered as a source of reliable and repeatable output data adequately to the input data.

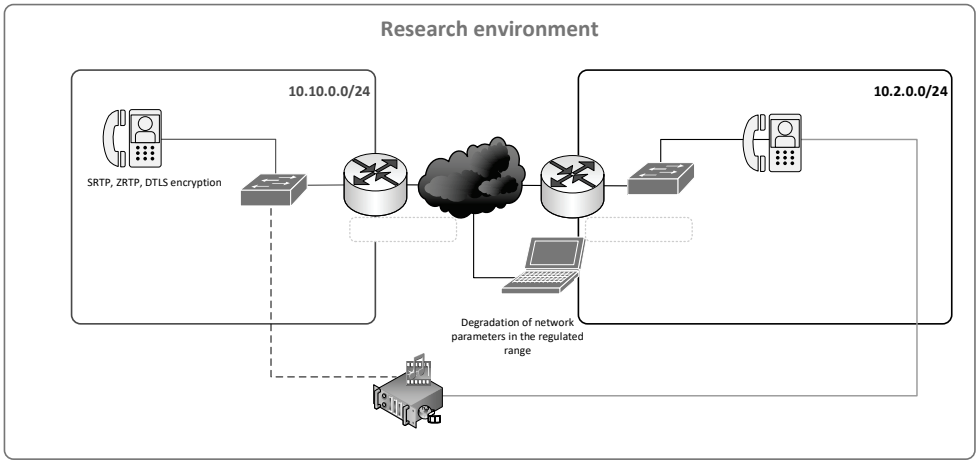

Fig. 4. Diagram of a research environment

In order to determine the impact of encryption on the quality of video communication service implementation, test scenarios were developed, and tests were carried out to determine:

- the impact of SRTP encryption;
- the impact of ZRTP encryption;
- the impact of DTLS encryption.

The rest of the article presents the results of individual studies assuming that the network bandwidth should be not less than 1500 kb/s, which will ensure specific video transmission conditions and make the results independent from the impact of network

parameters. The statistical sample size for estimating the value of the random variable was determined assuming a confidence level (1-α) = 0,95 and the required accuracy of determining the average value at the level of 25% of the standard deviation, so the overall number of the test performed was 396.

First of all, the quality assessment using the MOS indicator was tested. The results of these tests are presented in aggregate form in the next drawing (fig. 5). As you can see, encryption affects the perceived quality of the video service. The greatest impact was recorded for two protocols, i.e. for the ZRTP and DTLS protocols. This is due to the use of a different approach in the way of implementing secure multimedia communication, which in the case of these two protocols focuses on minimizing indicators associated with transmission delay, and less on the perceived quality of video image. In turn, the use of SRTP protocol using the AES-128 encryption algorithm allowed us to obtain much better results of the MOS indicator. Interestingly, these results turned out to be even better than in the case of unencrypted transmission. It was also noticed and explained in [1]. This is the result of designing the SRTP protocol to ensure that no changes are made to the quality of the transmitted video data. It is also worth emphasizing that in the case of unencrypted transmission, compared to other connections, the perceived video quality is similar for the entire duration of the connection. This is important because it is definitely less comfortable to watch audiovisual material whose perceived image quality changes continuously over a wide range of time values.

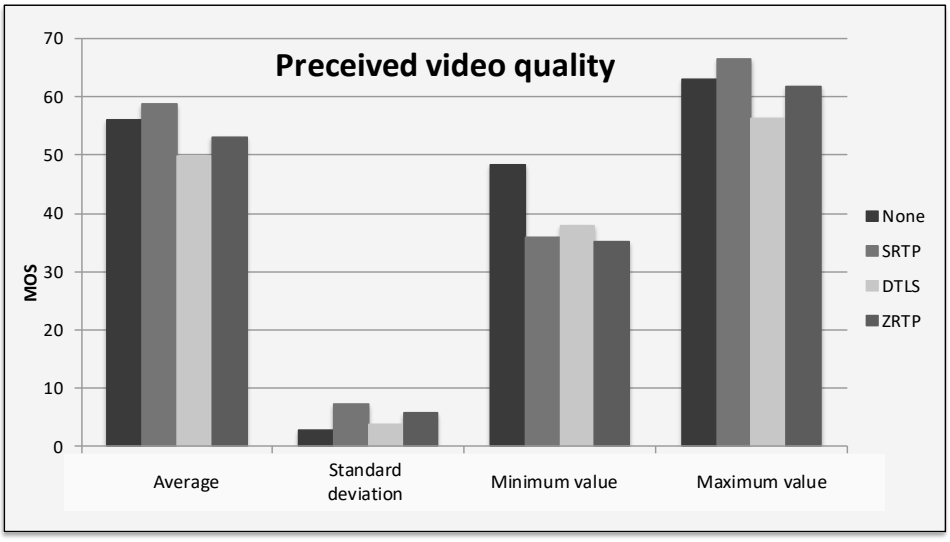

Fig. 5. Characteristic measurement values obtained for the perceived quality of the video service

The results of the impact of encrypted transmission protocols on the occurrence of block effects are shown in fig. 6. When analyzing the results of the measurements, it can be seen that the obtained values of the blockiness for each connection that was made, meet the

adopted criterion (the values did not exceed level 3). This does not mean, however, that this effect did not occur. It was only very little visible and therefore did not affect the viewing comfort. Moreover, the values obtained for unencrypted and encrypted transmission using the SRTP, DTLS and ZRTP protocols were at a similar level, and most of them were in the range from 0.35 to 0.4, and thus significantly below the allowable standard.

Figure 7, in turn, shows the results illustrating the effect of encryption on the blur effect. The maximum values obtained for this artifact definitely do not mix within the acceptable range, making the image almost impossible to recognize. In addition, it is worth emphasizing that for an encrypted connection using the SRTP protocol, the average value of all the obtained results was the lowest.

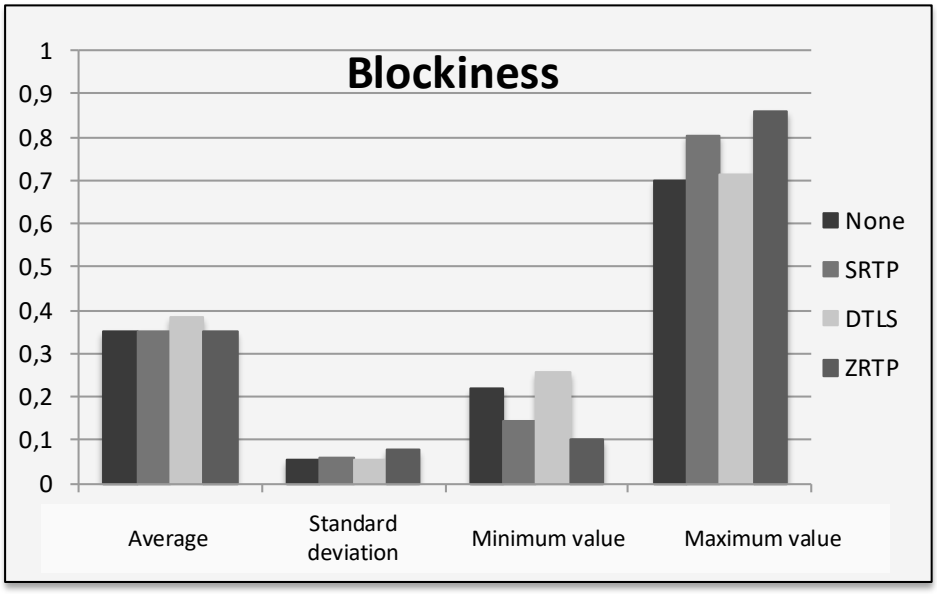

Fig. 6. Characteristic measurement values obtained for the block effect

The last series of results is shown in fig. 8, which refers to the assessment of the impact of encryption on the contrast indicator. The measurement values obtained for the contrast index are definitely below the criterion (0,15). The image contrast for the tested video connections was insufficient, causing the phenomenon of "merging" of similar image colors. The best results were obtained for the SRTP protocol and then for the connection without encryption. This confirms the advantages of using the SRTP protocol.

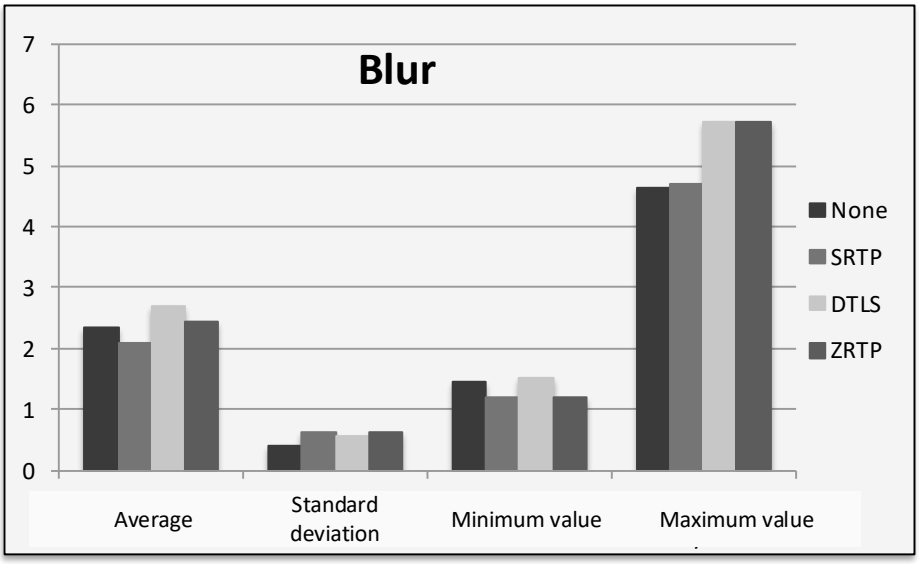

Fig. 7. Characteristic measurement values obtained for the blur effect

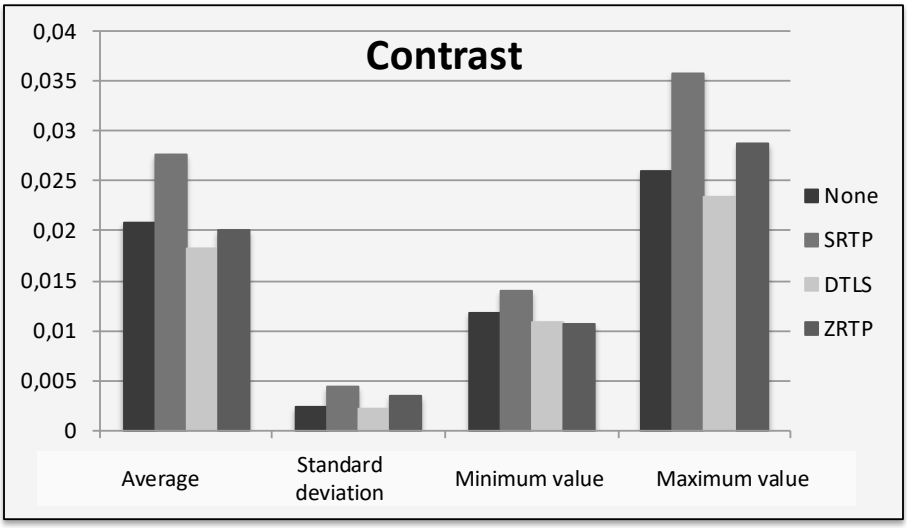

Fig. 8. Characteristic measurement values obtained for the contrast effect

Finally, based on the mathematical analysis, the indicator of the probability of obtaining a video communication service with a specified and defined quality level P_{sz} was determined (fig. 9). It has been assumed that a satisfactory level of service quality is achieved when the MOS rating reaches a value not worse than 3. At a level higher than 40%

probability, a cut-offline shaping the user satisfaction threshold has been marked. However, it should be noted that the presented function only takes into account the overall impact of encryption (the basic configuration of encryption protocols was used during testing), and does not include the impact of other factors related to operator or network behavior. Hence, it is easy to see that it is highly dependent on the timing of video sequences.

However, the analysis of the results shows that all protocols allow us to obtain a satisfactory level of video service quality, and the probability indicator fluctuates in the middle range of the considered range.

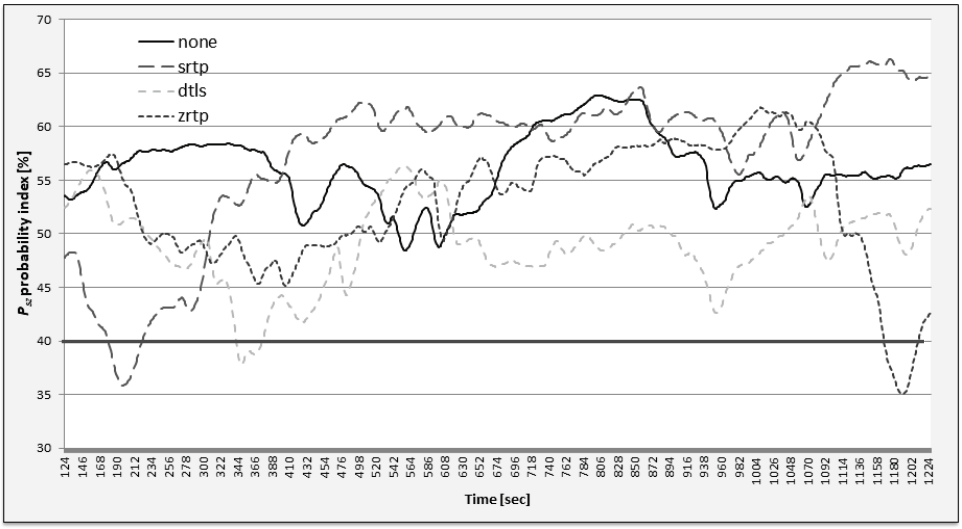

Fig. 9. The probability of getting a video call with satisfactory quality

6. Conclusions

The results obtained clearly indicate the impact of encryption on the quality of the VEoIP connection, and therefore also indicate the dependence of quality on the encryption algorithm. Further work in this area should include the configuration parameters of encryption protocols, the impact of network parameters and the level of knowledge of the system operator.

The proposed research methodology together with the proposed research environment can be the basis for further research to assess the impact of not only encryption algorithms, but also heterogeneous environment parameters on VEoIP services. Moreover, the research methodology proposed in the article can also be used to determine the impact on multimedia communication of other factors, including factors related to the operation and maintenance of the telecommunications system as a comprehensive technical facility.

7. References

1. Andre L., et al: An Evaluation of Secure Real-time Transport Protocol (SRTP) Performance for VoIP. 2009 Third International Conference on Network and System Security, 2009.
2. Bronzino F., et al: Inferring Streaming Video Quality from Encrypted Traffic: Practical Models and Deployment Experience, Proc. ACM Meas. Anal. Comput. Syst., Vol. 3, No. 3, Article 56, December 2019
3. Dimopoulos G., Leontiadis I., Barlet-Ros P., Papagiannaki K.: Measuring Video QoE from Encrypted Traffic. IMC '16, November 14–16, Santa Monica, CA, USA, 2016.
4. ITU-T P.910: Subjective video quality assessment methods for multimedia applications, 1999.
5. ITU-T P.912: Subjective video quality assessment methods for recognition tasks, 2008.
6. ITU-T Rec. P.800: Methods for subjective determination of transmission quality, 08, 1996.
7. ITU-T Recommendation X.805: Security architecture for systems providing end-to-end communications, 2003.
8. Janowski L., Leszczuk M., Papir Z., Romaniak P.: Ocena postrzeganej jakości usług strumieniowania wideo w scenariuszu bez referencji ze skalowaniem przepływności. Przegląd telekomunikacyjny, nr 8-9, 2009.
9. Kowalski M., Magott J., Nowakowski T., Werbińska-Wojciechowska S.: Exact and approximation methods for dependability assessment of tram systems with time window. European Journal of Operational Research, vol. 235, iss. 3, 2014.
10. Laskowski D., et al: Anthropo-technical systems reliability. Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014, CRT Press, A Balkema BOOK, 2015.
11. Leszczuk M.: Jakość usług multimedialnych w zastosowaniach użytkowych. Przegląd Telekomunikacyjny – Wiadomości Telekomunikacyjne, nr 8-9, 2014.
12. Lubkowski P., et al: Provision of the reliable video surveillance services in heterogeneous networks. Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014, CRT Press, A Balkema BOOK, 2015.
13. Pan W., Cheng G.: QoE Assessment of Encrypted YouTube Adaptive Streaming for Energy Saving in Smart Cities. IEEE Open Access, vol. 6, 2018.
14. Raport z prac realizowanych w ramach memorandum w sprawie współpracy na rzecz podnoszenia jakości usług na rynku telekomunikacyjnym [Report on the work carried out under the memorandum on cooperation to improve the quality of services on the telecommunications market]; wersja 1.04, z dnia 2014.02.07, Warszawa 2014.