

# Impact of Network Security on Speech Quality

MIROSLAV VOZŇÁK

Received 3.12.2008

## Abstract

This technical report deals with impact of secured network environment on speech quality. There are presented the results of the analyzing of voice over secure communication links based on TLS, specially in OpenVPN solution. The using of secure network environments can affect a speech quality. There is the performance comparison of cipher algorithms and description how the used security mechanisms influence the final R-factor. The presented results are based on experiments which have been performed in real IP network.

*Keywords:* TLS, OpenVPN, E-model

## 1 Introduction

The security becomes a necessity of current corporate networks and two solutions appear either based on IPsec or TLS and therefore, this topic has been chosen for our research in area of speech quality. The research regarding to Voice over IPsec has been performed at University of Milan [1], so I decided to focus on TLS. Together with my colleagues from Milan we realized our real platform, in order to understand how the voice services in IP network are affected by using the secure IP environment. The real performance test was implemented between VŠB-Technical University of Ostrava and University degli studi of Milan. We pointed out the advantages and the disadvantages of the adopted security measure. We described two virtual testbed, one developed using a traffic emulator and the second one based on a network simulator. Both the virtual environments were implemented in secure and insecure way. The executed measurements proved the obvious impact of some secure solutions on the voice quality, the results has been published [2] but without an exact calculation. A method of calculation describing the overall impact of security on speech quality is published in this technical report, the method is valid for TLS and has been tested with OpenVPN.

Virtual Private Network (VPN) is a technology to construct a private network over public networks. OpenVPN is one of the most popular software-based VPN products and has high flexibility. The usability of OpenVPN is high because offers a open-source, cost-effective and widely tested solution, not requiring expert knowledge. Software VPN products are popular, because they don't need any appliance and OpenVPN provides such solution which is based on matured protocols. The OpenVPN security model is based on SSL (Secure Socket Layer), the industry standard for secure communications via IP network. OpenVPN implements transport secure network extension using the TLS protocol (Transport Layer Security).

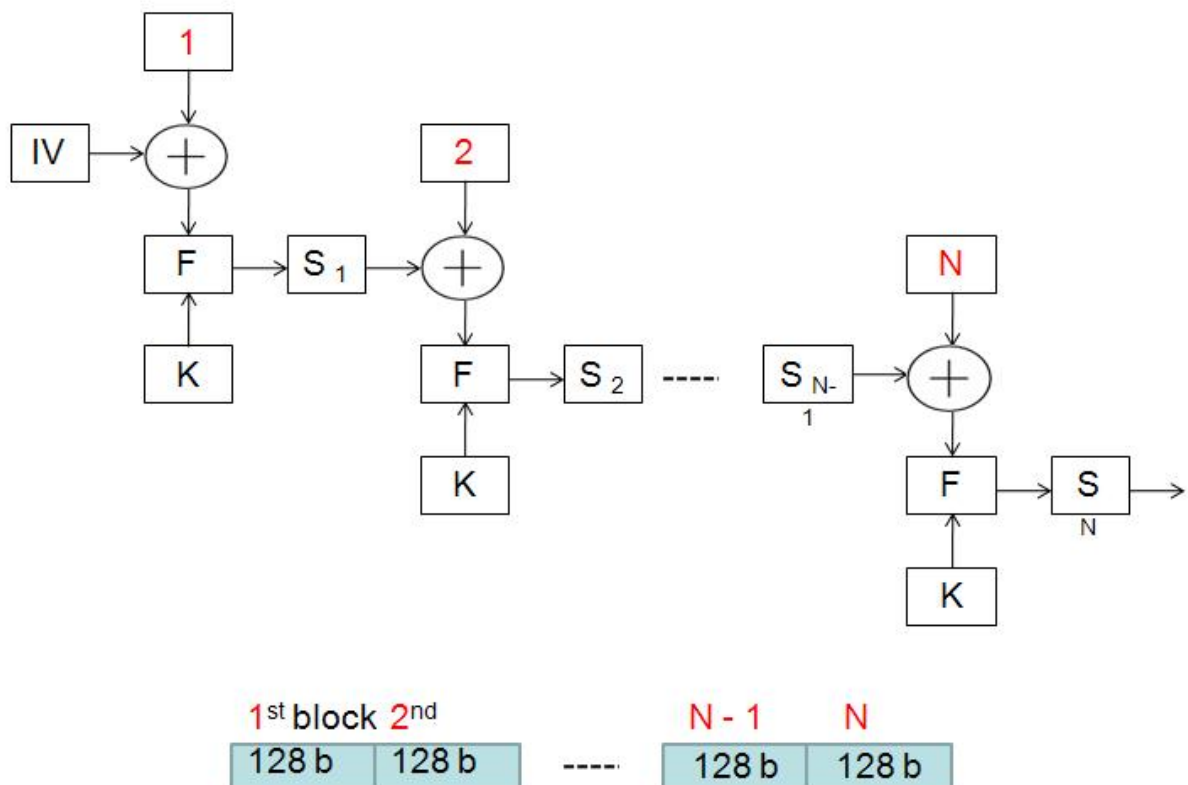
On the other side the using of OpenVPN increases an overhead which is affected by encryption and this overhead can influence overall speech quality [3]. This

paper contains a description of OpenVPN and its possibilities regarding a configuration, than there is explained a core of the matter which is the splitting of a RTP packet to equally divided blocks.

## 2 OpenVPN and encryption

TLS ensures a secured connection which is encrypted and decrypted with the keys negotiated during a phase of keys exchange. The key exchange and authentication algorithms are typically public key algorithms but subsequent data exchange is usually done by symmetric ciphers because of considerably faster processing. Of course, symmetric encryption is more suitable for IP telephony and this paper deals only with this type of ciphers [4]. TLS involves three main phases such as negotiation of supported algorithms, keys exchange and authentication and in the end symmetric encryption of transmitted data.

The endpoint establishing VPN tunnel are declared one as server and the other as client. Before establishing the VPN, the client first reaches the server on a specific port, whereas the server doesn't need to reach the client. Configuration files are located in directory */etc/openvpn* as *server.conf* or *client.conf*. The tunnel can be established on UDP or TCP, unfortunately TCP protocol is more widespread although UDP is more effective because of real-time applications. The most important information in configuration files is the type of cipher algorithm because it affects the number of blocks and overhead as is shown in Figure 1.



**Figure 1.** The number of blocks affected by CBC mode.

Figure 1 above illustrates the splitting of one RTP packet to N blocks. Every block has the same length which contains in case of AES (Advanced Encryption Standard) 128 bits although the key size can be not only 128 bits, but also 192 or 256 bits. If another algorithms are applied such as DES (Data Encryption Standard), Triple DES or BF (Blowfish), then the block size is set to value 64 bits. A complete list of supported cipher algorithms can be obtained as a result of command *openvpn --show-ciphers*. The following ciphers and cipher modes are available for use with OpenVPN. Each cipher shown below may be used as a parameter to the *-cipher* option.

*DES-CBC 64 bit default key (fixed)*  
*RC2-CBC 128 bit default key (variable)*  
*DES-EDE-CBC 128 bit default key (fixed)*  
*DES-EDE3-CBC 192 bit default key (fixed)*  
*DESX-CBC 192 bit default key (fixed)*  
*BF-CBC 128 bit default key (variable)*  
*RC2-40-CBC 40 bit default key (variable)*  
*CAST5-CBC 128 bit default key (variable)*  
*RC2-64-CBC 64 bit default key (variable)*  
*AES-128-CBC 128 bit default key (fixed)*  
*AES-192-CBC 192 bit default key (fixed)*  
*AES-256-CBC 256 bit default key (fixed)*

The default key size is shown as well as it can be changed with the *-keysize* directive, using a CBC mode is recommended. CBC means Cipher-block chaining, in this mode of operation, each block of plaintext is XORed with the previous ciphertext block and afterward is encrypted, that is why an initialization vector IV must be used in the first block, see Figure 1.

### 3 Used techniques of measurement

The presented results are based on series of measurements which has been performed in real network with OpenVPN and IxChariot<sup>1</sup>, a scheme is shown in Figure 2.

Whole traffic carried out between OpenVPN client and server was captured by Wireshark and individual packets were analyzed. IxChariot is a software, produced by Ixia, which consists of the IxChariot console and IxChariot endpoints. The IxChariot console allows a selection of several test configurations, such as the used codec, timing, number of concurrent calls, test duration and so on. The test is initialized at the console, the conditions are uploaded into endpoints and consequently the test is performed. The results are sent back to the console. There was observed an influence of OpenVPN-TLS on overhead which has been increased and hence the required bandwidth has been affected.

<sup>1</sup> <http://www.ixiacom.com/>

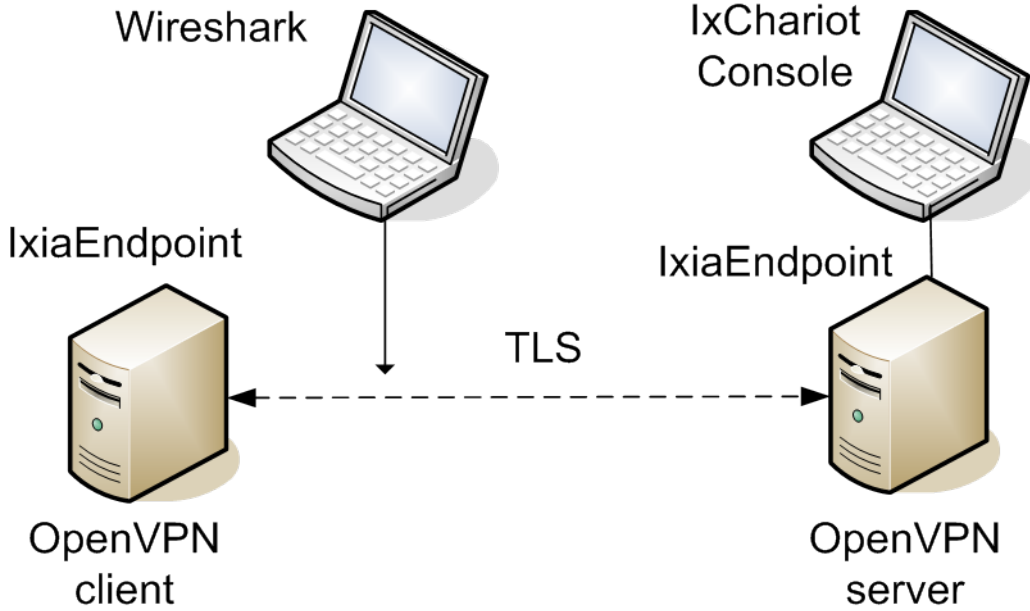


Figure 2. Logical scheme of testbed.

#### 4 Bandwidth requirements

The basic steps of speech processing on a transmission side are encoding and packetizing [5], [6]. RTP packets are sent in dedicated times and a difference between them depends on timing. This process of packetizing is given by the following basic equation:

$$\Delta t = \frac{P_S}{C_R} \quad (1)$$

where  $\Delta t$  [s] is timing in seconds,  $P_S$  [b] is a payload size and  $C_R$  [bps] represents a codec rate. The timing can be derived from content of RTP packet as a difference of two consecutive timestamps, see Equation 2. Typical value of a sampling frequency is 8 kHz.

$$\Delta t = \frac{\text{timestamp}_{\{N+1\}} - \text{timestamp}_{\{N\}}}{\text{sampling\_frequency}} \quad (2)$$

It is necessary to express the packet size at application layer which might be defined by the following formula:

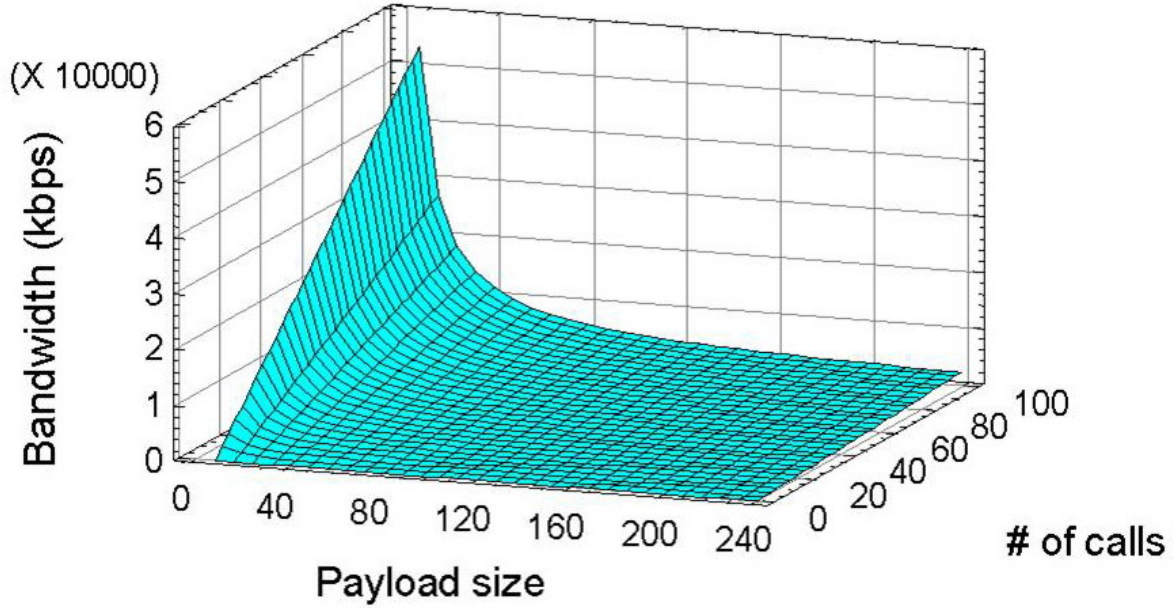
$$S_{AL} = H_{RTP} + P_S \quad (3)$$

where  $S_{AL}$  [b] is the expected size that consists of a RTP header  $H_{RTP}$  [b] and a payload size  $P_S$  [b]. Equation 4 determines the size of the  $S_F$  [b] frame at the link layer.

$$S_F = S_{AL} + \sum_{j=1}^3 H_j \quad (4)$$

$S_F$  [b] includes a packet at the application layer and the sum of lower located

headers of the OSI model where  $H_1$  [b] is media access layer header,  $H_2$  [b] internet layer header and  $H_3$  [b] is transport layer header.



**Figure 3.** Bandwidth as a function of payload size and concurrent calls.

Figure 3 illustrates the relation between bandwidth, payload size and number of concurrent calls.

$$(5) \quad BW_M = \sum_{i=1}^M \frac{S_{Fi}}{\Delta t_i}$$

In Equation 5 we expressed total bandwidth  $BW_M$  [kbps] required in case of  $M$  concurrent calls. If we now apply Equations 1, 2 and 4 to Equation 5, we obtain the following result:

$$(6) \quad BW_M = MC_R \left( 1 + \frac{H_{RTP} + \sum_{j=1}^3 H_j}{P_S} \right)$$

We have to realize that TLS is located between two layers of OSI model, between application and transport layer and therefore we apply  $S_{TLS}$  instead of  $S_{AL}$ . This replacement should be done in respect of explained location of TLS and we define a new parameter  $S_{TLS}$ , size at TLS layer.  $S_{TLS}$  is expressed in Equation 7.

$$(7) \quad S_{TLS} = C_0 + \left\lceil \frac{S_{AL}}{B_S} \right\rceil \cdot B_S$$

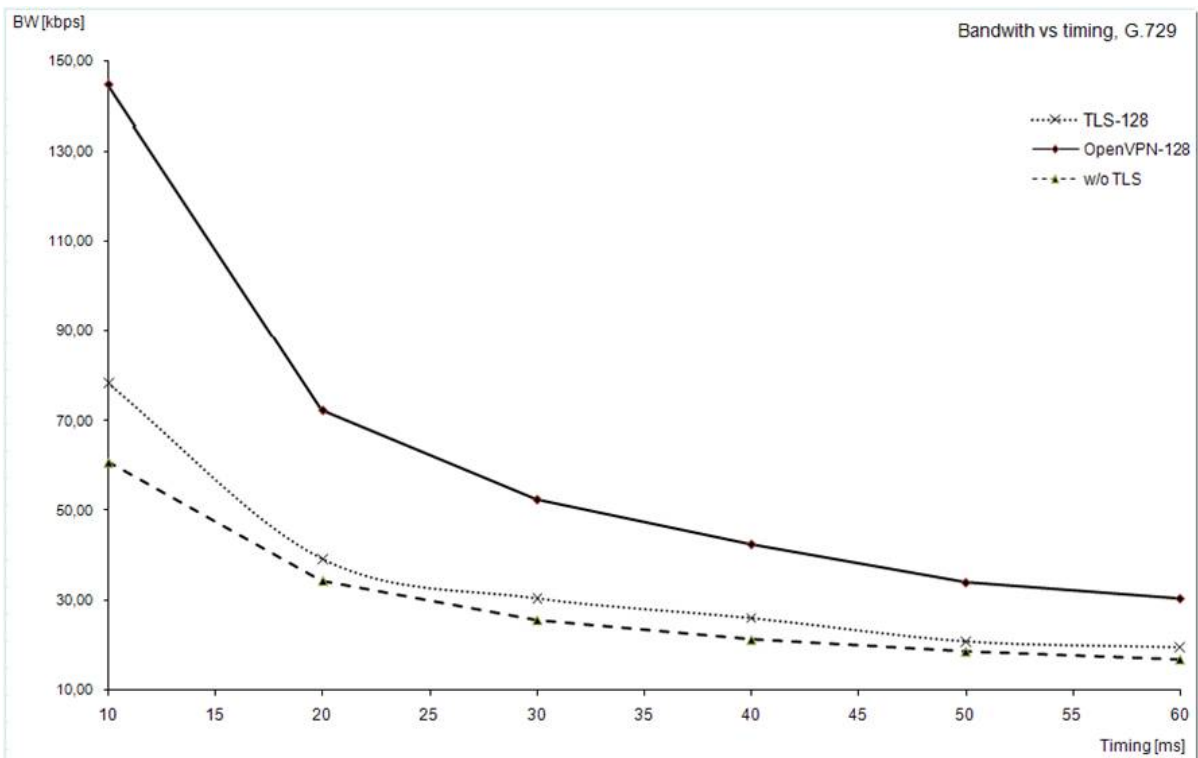
where we used the ceiling function which gives the smallest integer greater than or equal to its argument:

$$(8) \quad \lceil x \rceil = \min\{n \in \mathbb{Z} \mid x \leq n\}$$

The ceiling function was defined by M. Schroeder in 1991 [7] and the symbol was coined by K. Iverson in 1994. The parameter  $B_S$  represents a block size which has been explained in Figure 1, its value is 64 or 128 bits and depends on applied cipher algorithm (AES, DES, Triple DES or Blowfish).  $C_0$  is a constant and equals to zero in case of clear TLS unfortunately OpenVPN adds supplementary overhead that is included in  $C_0$ . The value has been achieved by performing experiments, see Figure 2. We can claim that this constant  $C_0$  is 83 bytes in case of block size 128 bits and 75 bytes in case of block size 64 bits.

## 5 Achieved results

Relations stated in previous chapter have been confirmed by experiments, Figures 4 and 5 illustrate how required bandwidth is affected by TLS and OpenVPN.

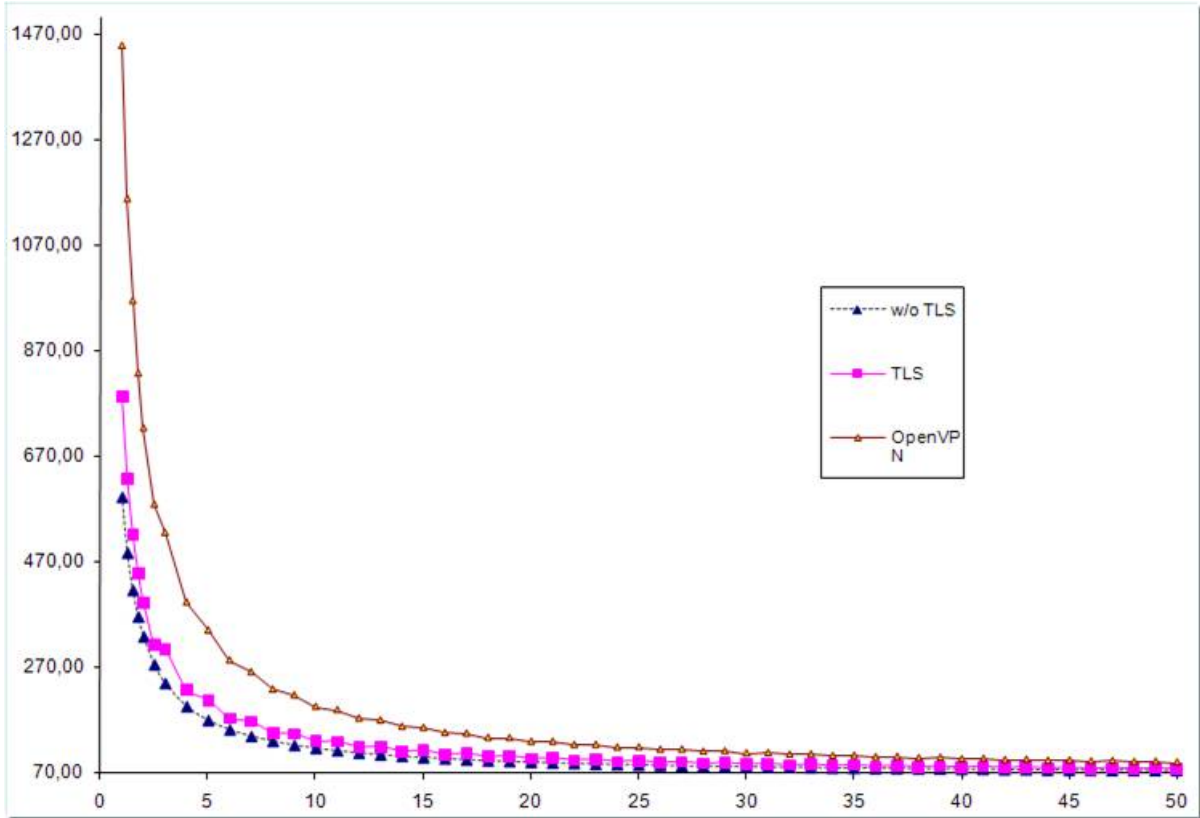


**Figure 4.** Comparison of bandwidth for codec G.729 without TLS, with TLS and OpenVPN,  $B_S=64$  bits

The first column of Table 1 contains codec G.729 and both variants of G.723.1. Block size has a length either 64 bits or 128 bits. Table 1 provides the results for Ethernet without TLS, with TLS and with OpenVPN [8], [9].

## 6 Impact on R-factor

Lack of bandwidth causes a loss in the first place hence the estimation of its impact on R-factor is explained in this chapter. The maximum value of R-factor for narrowband codecs is 94, the overall quality (R-factor) is calculated by estimating the



**Figure 5.** Comparison of bandwidth for codec G.711 without TLS, with TLS and OpenVPN,  $B_S=128$  bits

signal to noise ratio of a connection ( $R_0$ ) and subtracting the network impairments ( $I_S, I_D, I_{E-EF}$ ) and by adding Advantage factor  $A$ .

$$(9) \quad R = R_0 - I_S - I_D - I_{E-EF} + A$$

The first item  $R_0$  is derived from original SNR, the second  $I_S$  considers non-optimum sidetone, quantizing distortion, overall loudness and other impairments which occur more or less simultaneously with the voice transmission. The delay impairments are included in the parameter  $I_D$  as a mathematical summary of transmission delay, talker echo and sidetone. The effective equipment  $I_{E-EF}$  is an equipment impairment that considers the influence of used codecs and impairments due to packet loss and rejection. The packet loss distribution can be modelled using a Markov process. A multi-state Markov Model is used to measure the distribution of lost or discarded packets or frames, and to divide the call into “bursts” and “gaps”. The call quality is calculated separately in each state and then combined using a perceptual model, such as in VQmon [10]. The mentioned VQmon does incorporate G.107 compliant implementation of the E-Model. However, I applied a very simple method described in the last revision of G.107 from 2005 [11]. The impairment factor values  $I_E$  under packet-loss were tabulated for particular codecs. Robustness Factor  $B_{pl}$  is defined as codec-specific value and can be described as the robustness of the codec to packet-loss. Both values are listed in Appendix I of ITU-T G.113 and are available for several codecs. If we consider the Packet-loss Probability as  $P_{pl}$ , the  $I_{E-EF}$  impairment factor can be calculated using the formula:

**Table 1.** Values of required bandwidth for various environments

codec	block size [bits]	timing [ms] [ms]	w/o TLS BW [kbps] [kbps]	w TLS BW [kbps] [kbps]	w OpenVPN BW [kbps] [kbps]
23.1/6,3	128	30	24	30,4	52,53
23.1/6,3	128	60	15,2	17,33	28,4
23.1/5,3	128	30	22,93	26,13	48,27
23.1/5,3	128	60	14,13	17,33	28,4
23.1/6,3	64	30	24	28,27	50,4
23.1/6,3	64	60	15,2	17,33	28,4
23.1/6,3	64	30	22,93	26,13	48,27
23.1/6,3	64 bits at block	60	14,13	16,27	27,33
29	128	10	60,8	78,4	144,8
29	128	20	34,4	39,2	72,4
29	128	30	25,6	30,4	52,53
29	128	40	21,2	26	42,6
29	128	50	18,56	20,8	34,08
29	128	60	16,8	19,47	30,53
29	64	10	60,8	72	138,8
29	64	20	34,4	39,2	72,4
29	64	30	25,6	30,4	52,53
29	64	40	21,2	24,4	41
29	64	50	18,56	20,8	34,08
29	64	60	16,8	18,4	29,47

$$I_{E-EF} = I_E + (95 - I_E) \cdot \frac{P_{pl}}{\frac{P_{pl}}{BurstR} + B_{pl}} \quad (10)$$

$BurstR$  is the so-called Burst Ratio, when packet loss is random  $BurstR=1$  and when packet loss is bursty  $BurstR>1$ . For packet loss distributions corresponding to a 2-state Markov model with transition probabilities  $p$  between a "found" and a "loss" state, and  $q$  between the "loss" and the "found" state, the Burst Ratio can be calculated as:

$$BurstR = \frac{1}{p + q} \quad (11)$$

Once the  $I_{E-EF}$  factor is calculated, it is not difficult to determine R-factor as an output of E-Model using implicit values of recommendation ITU-T G.107, which are  $R_0=94,7688$ ,  $I_S=1,4136$  and  $A=0$ . Hence the Equation 9 can be modified to

$$R = 93,3553 - I_D - I_{E-EF} \quad (12)$$

The model used to estimate  $I_D$  is described in [12], where it is explained that the effects of delay are well-known and easily modelled. Delays of less than 175 ms have a small effect on conversational difficulty, then  $I_D=4T$  where  $T$  is the delay in ms.

## 7 Conclusion

The real-time applications are very sensitive to packet loss, and each variation occurring on the network can modify and influence the final result of a real-time data transmission, such as a VoIP call. On the one hand the defence techniques using cryptography such as OpenVPN reduce the danger of security threats but on the other side they affect the required bandwidth of IP telephony which is significantly increased in case of OpenVPN. The presented relations in this paper help us to understand how OpenVPN and TLS can affect the bandwidth of calls and how we can optimize the timing.

For example we can show an optimization at G.723.1 with 6.3 kbps, see Table 1. If we used a timing 30 ms during packetization, we would require 30,4 kbps in case of TLS against 24 kbps in environment without TLS, but we could achieve better result with timing 60 ms, because we would require 17,33 kbps for TLS against 15,2 kbps without TLS and it is really much better ratio. This presented example is valid for AES due to size of blocks but the new created relations help to optimize any CBC encryption.

The new contribution of this paper is the presented method of bandwidth calculation in network using TLS. The achieved results were confirmed in testbed, the bandwidth of any particular call was affected by length of cipher block and didn't depend on key size. The results corresponded with relations stated in chapter 4. This paper is an extension of a previous work on the impact of security on the quality of VoIP calls [2] and [9].

I would like to thank my colleagues Antonio Nappa and Alessandro Rozza from the Milan University for collaboration and especially Filip Řezáč, a student of the VŠB – Technical University of Ostrava, who helped me with configuration of TLS.

## References

- [1] BARBIERI, R. – BRUSCHI, D. – ROSTI, E. *Voice over IPsec: Analysis and solutions*. In Proceedings of the 18th Annual Computer Security Applications Conference, December 2002. Las Vegas, IEEE Computer Society, ISBN 0-7695-1828-1.
- [2] VOZŇÁK, M. – ROZZA, A. – NAPPA, A. *Performance comparison of secure and insecure VoIP environments*. TERENA Networking Conference 2008, Brugge, 19-22 May, 2008.
- [3] VOZŇÁK, M. – NEUMAN, M. *The Monitoring and Measurement of Voice quality in VoIP Environment*. Technical report 18/2006<sup>2</sup>, CESNET, November 2006. 12 p.
- [4] VOZŇÁK, M. *Impact of security on speech quality*, Invited lecture at University of Milan, July.2008.

<sup>2</sup> <http://www.cesnet.cz/doc/techzpravy/2006/voice-quality/>

- [5] HALÁS, M. – KYRBASHOV, V. – VOZŇÁK, M. *Factors influencing voice quality in VoIP technology*, In: 9th International Conference on Informatics' 2007, pp. 32-35, Bratislava, June 2007.
- [6] BAROŇÁK, I. – HALÁS, M. – ORGOŇ, M. *Mathematical model of VoIP connection delay*. In: Telecommunications, Networks and systems, Conference in Lisboa, 3-8 September, 2007.
- [7] SCHROEDER, M. *Fractals, Chaos, Power Laws: Minutes from an Infinite Paradise*. New York: W. H. Freeman, p. 57, 1991.
- [8] NAPPA, A. – BRUSCHI, D. – ROZZA, A. – VOZŇÁK, M. *Analysis and implementation of secure and unsecure Voice over IP environment and performance comparison using OpenSER*. Technical report, 84 pages, published at Università degli studi di Milano, December, 2007.
- [9] VOZŇÁK, M.: *Impact of OpenVPN on speech bandwidth*. In proceedings TSP2008, 31th International conference, 3-4.9 in Paradfurdo, Hungary. Publisher: Aszisztencia Szervező Kft. Budapest, ISBN 978-963-06-5487-6.
- [10] CLARK, A. *Extension to the E-Model to incorporate the effects of time varying packet loss and regency*. ETSI TIPHON committee, TS 101 329-5 Annex E, July 2001.
- [11] ITU Recommendation G.107. *E-model, a computational model for use in transmission planning*, ITU, 2005.
- [12] CLARK, A. *Modelling the Effects of Burst Packet Loss and Regency on Subjective Voice Quality*. 2001.