Journal scientific and applied research, vol. 20, 2021
International Journal

Original Contribution

ISSN 1314-6289

ANALYTICAL STUDY OF THE DELAY INTRODUCED AS A RESULT OF ENCRYPTION/DECRYPTION OF VOICE TRANSMITTED OVER A VPN NETWORK

Daniel R. Denev

KONSTANTIN PRESLAVSKI UNIVERSITY OF SHUMEN, 115 UNIVERSITETSKA , SHUMEN 9700,
E-mail: slimshady33@abv.bg

ABSTRACT: *The purpose of this article is to evaluate the impact of the decoding/encoding process on the IP based voice transfer. A short analysis of the decoding/encoding algorithm has been made. Using the result from the conducted analysis evaluation model has been created. A series of simulations have been performed and the results are represented in graphical form*

KEY WORDS: *VPN, G. 711, G. 729*

Although there are a number of technologies that allow connectivity between different offices and locations, Internet-based VPN's have recently developed as the most secure and cost-effective way to connect enterprise hubs with their remote offices and mobile employees. They provide the highest level of security by using modern, standardized security protocols, such as the Triple Data Encryption Standard (3DES) for encryption and IP Security Protocol (IPSec) for tunneling, as well as a variety of authentication methods that protect data from unauthorized access. and abuse.

IPSec ensures the security of the transmitted data, the identification header and encryption/ decryption of the basic data in the packet on both sides of the transmission line. This process of encrypting/decrypting the information adds an additional delay in the distribution of packets.

At present, standards based on the ITU H.323 protocol stack have been adopted for the use of voice transmission technology. The H.323 protocols mainly

provide the transmission of video and audio data over IP networks and the Internet. H.323 is recommended by the International Telecommunication Organization (ITU) as a standard for transmitting multimedia information over a network that does not support QoS. Part of the H.323 stack are the G.711 and G.729 codecs, which are mainly used for voice transmission over the Internet.

The encapsulation of an IPSec voice transmission packet in tunnel mode is shown in Fig. 1. The ratio of the added information to the packet size itself varies between 35% for a 160 bytes (64 kb/s) packet encoded according to the G. 711 standard and 81% for a 20 bytes (8 kb/s) packet encoded according to the G. 729 standard. It is obvious that the addition of additional information to the fixed packet size will reduce the performance of QoS mechanisms in voice transmission.

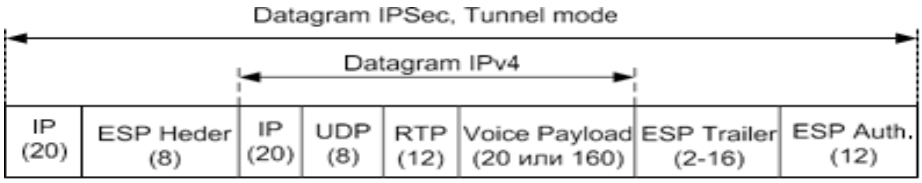

Fig. 1. Encrypted packet structure

The process of encrypting/decrypting data in routers takes some time Δt. We assume that this time is the same for all routers with an architecture. It is this time Δt that is the additional delay that is introduced during the encryption/decryption process in the system. This delay can be estimated by the following formula:

(1) $$I_{sec} = \frac{S_{packed}}{R}$$

Where S_{packed} is the packet size (bit) and R is the encryption/decryption rate of the routers (bit/s)

Regardless of protocol use, the end-to-end delay I_{ee} is the sum of the following components: delay imported from using the I_{code} codec, from the distribution of packets in the transmission medium I_{prop} , transmission delay (time required for the packet to reach its destination) I_{trans} .

The total delay can be calculated as follows: When using the G.729 codec, the imported delay is $I_{code} = 23$ ms. The packet propagation speed in a standard environment (copper cable) is 5 $\mu s/km$ for a distance of 350 km (Sofia - Shumen) is approximately $I_{prop} = 2$ ms. The time to pass a 160 bytes packet over a 4 Mb/s

line is approximate $I_{trans} = 0{,}3$ ms. The expression for the total delay in this case, using the IPv4 protocol acquires the following form:

(2) $$I_{beIP} = I_{code} + I_{prop} + I_{trans} + I_{queue}$$

Where I_{queue} is the delay introduced by the buffer queue service. If IPSec formula (2) is used, it will look like:

(3) $$I_{beIPSec} = I_{code} + I_{prop} + I'_{trans} + I'_{queue} + 2I_{scc}$$

Where I_{sec} is the delay inducted by the information of the encryption/decryption processes. The most variable compound is I_{queue}. We assume that in the considered system there are N intermediate routers between the source and the receiver. The delay introduced by the request for processing in every router is I_i , then the total delay from the processing of queues in the system is I_{queue}:

(4) $$I_{queue} = \sum_{i=1}^{N} I_i$$

To calculate I_i several assumptions will be made: the intermediate routers have an implemented mechanism for processing the incoming queues on their ports, the processing scheme is FIFO. The routers are connected via a transmission line with a capacity of C and accept for processing on M incoming streams. It is known that human speech can be represented as a sequence of intervals containing information and pauses, and their distribution is exponential (ON - OFF model). This type of incoming traffic is defined as self-similar and with long-term dependencies. It can cause overflow of the buffers of the service devices, and this process cannot be predicted by the traditional methods with the Poisson and Markov models.

Furthermore, if one looks at the codec mechanism (e.g. G.729), it will be found that the size of the incoming packets is fixed and therefore the resulting service time μ is determined. In the literature, this type of traffic is investigated by a G/D/1 queuing system, which allows to calculate the total delay of voice transmission over IP. To calculate the delay in such a system, we need to know: λ and the change of incoming self-similar traffic $\sigma 2$, the Hirst N parameter and the service time μ. If the Weibull law is used for distributing purpose, then a

certain number of packages will have size S_{packed} where the queuing can be calculated by the formula:

(5) $$L_i \cong exp - \frac{U_t^{2H}(C-\lambda)^{2H}}{2\alpha\lambda H^{2H}(1-H)^{2-2H}} S_{packed}^{2-2H}$$

Where Ut is the duration of the interval and $\alpha > 0$ is the coefficient of variation. Then the delay in the i-th router can be calculated by:

(6) $$I_i = \mu . L_i = \frac{S_{packed}.L_i}{C}$$

We consider two types of voice traffic, one encoded according to the G.711 standard and the other encoded according to the G.729 standard. Assume that the number of intermediate routers N = 8 (the value is accepted after executing the command tracert IP address of a server located in Sofia). In order for the quality of the transmitted voice to be acceptable and to meet international specifications, the delay must be less than 150ms. The parameters and architecture used for the simulation are shown in Table 1 and Fig. 2.

Table 1. Parameters used for the analysis

Parameter	Value
λ	8/64 kb/s
C	1/2 Mb/s
α	0,6
H	0,7
Information part of the package	20/160 bytes
N	8

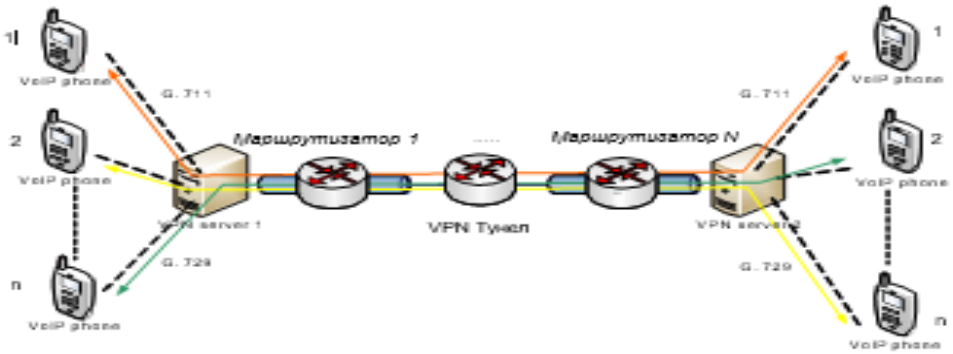

Fig. 2. Simulation staging

The analytical results of the voice delay in the IPv4 protocol and IPSec are shown in Fig. 3.

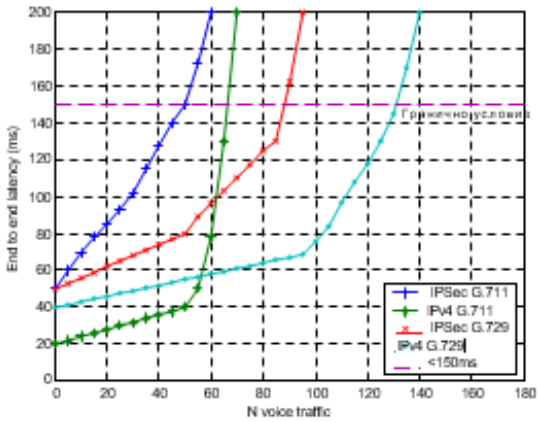

Fig. 3. Results obtained from the analytical study

As can be seen from the figure, the number of flows under the boundary condition when using IPSec is 40% less compared to the cases where the IPv4 protocol is used. These results are obtained for all coding rates of the input streams.

Therefore, in order to maintain the quality of the broadcast voice and to meet international standards, it is necessary to limit the number of voice sessions to a certain level.

Reference:

[1] Barberis A., Casetti C., Martin J.C., Meo M. A Simulation Study of Adaptive Voice Communications on IP Networks. Computer Communications, no. 24, pp. 757– 767, 2001.

[2] Beritelli F., Ruggeri G., Schembra G. TCP-Friendly Transmission of Voice over IP. European Transactions on Telecommunications, vol. 14, Issue 3, pp. 193–203, 2003.

[3] Qiao Z., Sun L., Heilemann N., Ifeachor E. A New Method for VoIP Quality of Service Control Use Combined Adaptive Send Rate and Priority Marking. Proceedings of IEEE International Conference on Communications, vol. 3, pp. 1473–1477, Paris, 2004.

[4] Iliev T., Hristov G. Evaluation of video quality after network transport.