The measurements of the secured voice communication quality in a broadband radio channel

Piotr Lubkowski*[a], Rafal Polak[b], Robert Sierzputowski[b]
[a]Military University of Technology, Faculty of Electronics, Gen. Sylwestra Kaliskiego 2, 00-908 Warsaw, Poland; [b]Transbit Sp. z o.o., Lukasza Drewny 80 str., 02-968 Warsaw, Poland

ABSTRACT

SCIP (Secure Communication Interoperability Protocol) is the basic solution introduced by NATO to ensure secure communication (voice and data) through heterogeneous networks. It provides interoperable end-to-end connectivity in military radio communication systems, traditional telephone systems, satellite communication channels, VoIP connections and mobile telephony. It is also designed to operate at the application layer with minimal dependency on the characteristics of the lower layers. The protocol supports transmission in narrowband and broadband radio channels in point-to-point and point-to-multipoint modes. The main challenge related to ensuring communication in radio channels is to guarantee a defined level of security, availability and quality of services provided. The implementation of any encryption algorithm in nowadays heterogenous networks with restricted bandwidth can lead to degradation of the voice quality due to increased loss packets and packet latency resulting from the deterioration of radio channel conditions. This paper show the results of measurements including the impact of end-to-end SCIP encryption on the quality of VoIP communication in a wideband radio channel. The measurements were carried out using the MultiDSLA tester and PESQ and POLQA methods. The results of laboratory tests indicate what effect does SCIP encryption-based security has on the voice communication quality over radio channel.

Keywords: voice quality testing, SCIP encryption, broadband radio communication, SDR.

1. INTRODUCTION

Provision of adequate level of data and voice transmission security in secured communication systems is one of the most important aspect in contemporary alliance and coalition communication. The SCIP protocol allows the use of cryptographic mechanisms for encryption the transmission of voice and data in a standardized way, ensuring interoperability of existing and newly formed allied and coalition communication systems dedicated to voice and data transmission. The SCIP protocol operates using the classic VoIP service model, which is its undeniable advantage. Requirements for real-time transmission over secure channels (i.e. voice communication) are defined around functional and quality constraints. An important set of QoS-specific parameters including parameters related to the establishing, disconnecting and call-blocking of connection is defined in ITU-T Recommendation G.1010 [1]. However, the assurance of quality at the network level (QoS) is extremely important because it allows prediction of the size of the available bandwidth and the level of losses at the application layer.

As far as the confidentiality, integrity and authentication of VoIP application is considered the reduction of effective bandwidth should also be noticed. It could lead to the overall reduction of QoS for VoIP quality in terms of packet ratio lost, jitter and latency. The problem of bandwidth availability is particularly noticeable in radio communication systems, so characteristic for tactical military communication. Radio communication channel are degraded according to Doppler and multi-path spreading, low Signal to Noise Ratio (SNR), fading and high level of interference. Additionally, in contrast to narrowband radio channel, the broadband radio channels are characterized by smaller range of operation and lower immunity to targeted interference which may negatively affect the quality of communication. The article presents the results of the assessment of the quality of VoIP traffic encrypted with the SCIP protocol in a broadband radio channel. A measurable effect of the conducted research is the methodology developed for testing the impact of encryption protocols on the quality of voice communication over radio channels.

* piotr.lubkowski@wat.edu.pl; phone +48 261 837-897; fax +48 261 839-038; wat.edu.pl

Radioelectronic Systems Conference 2019, edited by Piotr Kaniewski, Jan Matuszewski, Proc. of SPIE
Vol. 11442, 114420R · © 2020 SPIE · CCC code: 0277-786X/20/$21 · doi: 10.1117/12.2564573

The remaining part of this paper is organized as follows. In Section 2 an overview of the SCIP protocol is described. Next, basic information about broadband radio communication and its implementation in R-450C station are given. Section 4 describes the testbed environment with reference to VoIP QoS issues. The results of research are presented in the fifth section along with discussion and recommendation for future work. Finally, the paper ends with the conclusions.

2. SCIP OVERVIEW

The SCIP is an international standard developed for the provision of secure voice and data communication [2]. The protocol belongs to the group of application layer protocols, which makes its operation independent of dependencies occurring in the lower layers of the reference model. The basic transmission mode is point-to-point transmission, which is dedicated to support voice communication via narrowband HF/VHF radio channels at a rate of 2.4 kbps. The second of the supported modes of operation is point-to-multipoint, which in turn is used for multimedia data transfers at speeds up to 10 Mbps. It is also worth noting that user data encryption via the SCIP channel is implemented with minimal bandwidth requirements, and encryption requires bit transparency for signaling and data. The SCIP protocol uses the classic model of VoIP services, which creates the possibility of its implementation in a wide spectrum of end terminals used in VoIP communication. The diagram of signaling procedures for setting up and disconnecting a connection for VoIP service using the SCIP protocol is presented in Figure 1. Session Initiation Protocol (SIP) and Real – Time Protocol (RTP) are both used by SCIP terminals to establish an IP connection between SCIP terminals. A crypto – sync message is used for establishing a secure mode of voice/data transmission within a SCIP session.

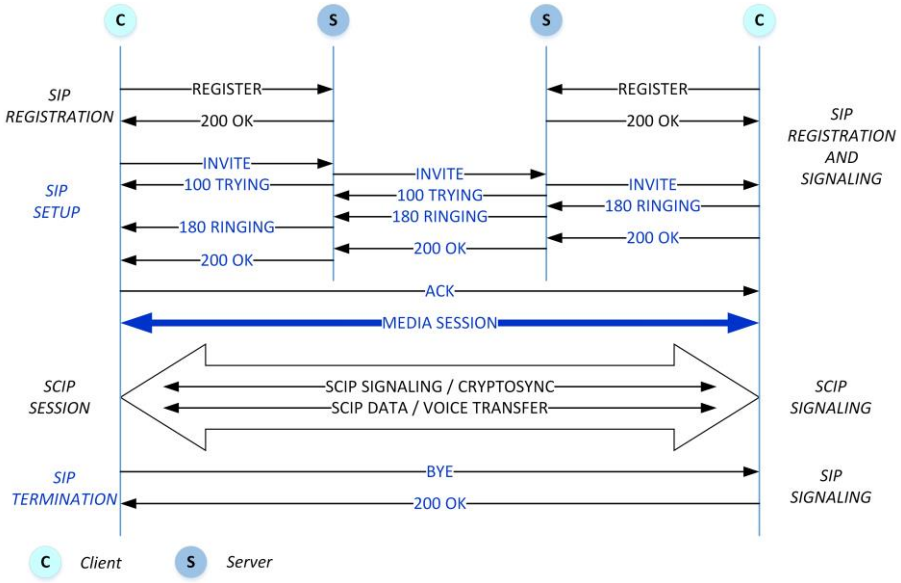

Figure 1. Signaling procedures for SCIP communication.

The SCIP technology makes it possible to establish a voice connection in the SECURE VOICE mode. This is intended for voice transmission in a strictly defined way which allows the use of one out of two codecs: MELPe (Mixed-Excitation Linear Predictive enhanced) or G.729D [3].

In the case of SCIP protocol implementation presented in the paper, two variants of the MELPe codec - Blank & Burst and Burst without Blank (Bw/oB), characterized by a 2.4 kbps bandwidth, were developed.

Both variants use the structure of the so-called "super frame" consisting of the Sync Management frame (SM) and the frame of the MELPe codec. The SM frame contains information enabling subsequent cryptographic synchronization and sustaining this synchronization during voice transmission.

In the Blank & Burst variant, the first frame of the MELPe codec is periodically replaced by a SM frame, whereas in the Burst w / o Blank variant the SM frame is inserted periodically before the first frame of the MELPe codec.

Secure transmission using the MELPe codec in the Blank & Burst version is carried out using a "super frame" consisting of a 54-bit SM frame and 23 frames of MELP vocoder 54-bit size each. In the case of the MELPe codec in the Bw/oB

version, the "super frame" structure consists of a 56-bit SM frame and 24 56-bit MELP vocoder frames (54 bits of MELPe vocoder + 2 bits). In view of the above, the Bw/oB variant requires a transmission channel with a capacity greater than 2.4 kbps.

In turn, data transmission using the G.729D codec is based on a "super frame" with a structure identical to Bw/oB variant supplemented with an additional Encrypted Speech (ES) header placed periodically between the vocoder frames. Thus, the "super frame" consists of a 64-bit SM frame and eight frames carrying an encrypted speech signal. Each of the speech signal frame includes a 24-bit header and four 64-bit frames containing G.729D codec data. The scrambled speech header frame allows resynchronization between the SM frames. A channel with a capacity of at least 7.2kbps is required to carry out the transmission.

An integral part of SCIP technology is cryptographic mechanism. Cryptography in the SCIP standard defines an interoperable set of methods and algorithms, which are necessary to establish a secure connection, encryption of transmitted data, methods responsible for the verification process of integrity, authentication and identity of the parties of the connection. Currently, there are two groups of cryptographic algorithms used in military communication: Mercator and Medley algorithms as well as AES algorithm. Identification of cryptography compliant with the coalition standard is performed via the Keyset Type (KT). Therefore, one of the conditions for establishing a secure transmission of information between two devices with the implemented SCIP standard is that they have a common subset of KT values.

3. BROADBAND RADIO COMMUNICATION SYSTEM

Dynamic development of Command and Control (C2) systems results in dynamic demand for broadband services including voice and video transfer in real time. Broadband radio communication systems seem to be solution broadband radio systems seem to be the solution. However, they have also some limitations concerning a small range and high transmitter activity associated with the generation of maintenance traffic, which makes it easier to detect the radio emission.

The R-450C radio is an excellent example of such a broadband communication solution which was used in research environment. It is a universal, programmable SDR (Software Defined Radio) device, designed to work in the I-band (225 to 400 MHz), using radio channels with 1, 2 and 4 MHz band. [4] The standard mode of operation is TDMA mode, which is used in military systems with closed network topology. It is characterized by a constant short delay, high efficiency of transmission medium usage, controlled allocation of resources, the ability to adjust the size of the slot to the amount of information sent.

CSMA/SC mode is another mode of operation, which allows for optimization of the working channel parameters (type of modulation, forward error correction level, adaptive power level selection). Operation in CSMA/SC mode ensures its resistance to interference in narrowband channels. In this mode the transmission of each packet is followed by a fast (about a few dozen - several hundred microseconds) signaling process (calling the correspondent). It consists of a Ready To Send (RTS), Clear To Send (CTS) and CTS Ack messages. Upon completion of signaling phase, data are carried out. The CSMA/SC mode is equipped with the mechanism of adaptation of the bit rate to the current spectral situation. Unfortunately, the main disadvantage of this mode is the variable delay depending on the network occupancy and operating conditions.

The third mode of operation is the CSMA/MC mode (Figure 2). It allows the adaptive selection of radio channel parameters and the selection of the channel (frequency) which is characterized by the best propagation conditions. A characteristic feature of this mode of operation is the analysis of all assigned channels. This operation is carried out in real time and enables the creation of the so-called awareness of the spectral (cognitive) environment. It is used in the process of optimizing decision making on the occupation of channels, selection of transmission parameters, etc. To avoid interference, in this radio mode, each packet can be transmitted on a different frequency.

In contrast to the CSMA/SC mode in CSMA/MC mode, a pilot, preamble and channel parameters are transmitted in the RTS frame, thanks to which the receiving radio knows the spectral situation on a given channel. It offers a high data rates for individual relationships as well as for entire network. This mode is immune to intentional interferences by current analysis of the quality of work channels and selection of a channel or group of channels that are not disturbed now. Unfortunately, it has slightly lower bit rates for individual relationships than for CSMA/SC mode [5].

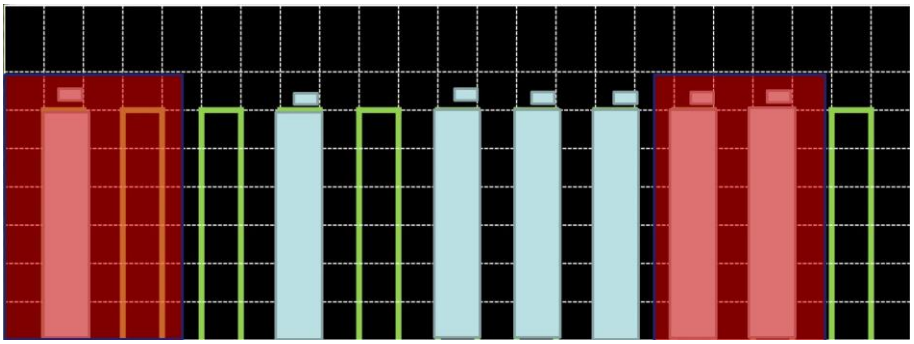

Figure 2. General characteristics of radio channel spectrum in CSMA/MC mode.

4. MEASUREMENT RESULTS

4.1 Measurement environment

The ability of SCIP to operate in heterogeneous networks requires the implementation of the SCIP protocol which is validated in a wide range of network environments. The purpose of the tests is to confirm that the SCIP protocol allows to provide a defined level of security with specified reliability, performance and interoperability. The intent of this paper was to evaluate the quality of voice calls encrypted with the implemented SCIP protocol using the radio channels. The established testbed reflects a realistic heterogeneous communication system [6-7]. The research methodologies were developed and verified in previous work carried out by the authors in relation to testing the real-time services in heterogeneous networks [8-9].

The VoIP service is based on packet switching, which means that all data are transmitted over the network using IP packets transported in a common transmission medium. Implementation of voice calls over IP networks is closely linked to the need to ensure an appropriate level of quality of the service. As far as the voice transfer over IP networks is considered several factors such as end-to-end delay, jitter and packet loos ratio contribute to overall voice quality as perceived by an end user. However, the implementation of security protocols in VoIP requires additional resources which will impact the quality of voice communication. Hence, any disruptions of the network layer may affect the level of the assessed quality of the received voice signal which is expressed in the Mean Opinion Score (MOS). The MOS values are in the range from 1 to 5, with the value of 5 being the best case of the speech quality. The influence of popular encryption protocols on the quality of VoIP connection has been repeatedly analyzed [10-12]. But, up to now, these analyses did not include the impact of the SCIP protocol.

The research concerning an impact of SCIP protocol on VoIP call quality were performed in the applied experimental testbed which consists of two domains, called respectively D_1 and D_2 (Figure 3). Each domain contains the voice terminal VT-10SCIP (marked as DUT – Device Under Test) in which the SCIP protocol was implemented as well as two R-450C radio stations. The VoIP connection is established between VT-10SCIP terminals and voice traffic is send form DUT_1 to DUT_2 over the radio channel with regulated attenuator. The DSLA II tester (Digital Speech Level Analyzer) presented in the diagram together with the MultiDSLA application represents a professional system for measuring and analyzing voice quality. It provides a reference voice signal for DUT-1 and receives a distorted signal from DUT_2. These signals form the basis for estimating the quality of the speech signal using the objective PESQ (Perceptual Evaluation of Speech Quality) and POLQA (Perceptual Objective Listening Quality Assessment) measurement methods. Reference files representing female and male speech with a corresponding signal strength are used for the research. Additionally, the analyzer makes it possible to examines the influence of distortions such as noise, codec types, packet losses, jitter, loss of synchronization and SNR or BER.

During research the following speech codecs supported by DUT_1 were used: G.729D, MELP B&B and MELP Bw/oB. Taking as a basis the developed scenario encompassing encrypted VoIP communication in the radio channel with variable characteristics, the quality of speech signal transmission was evaluated using the PESQ and POLQA methods. The results of the conducted research are presented below, considering the scenarios and assumed determinants.

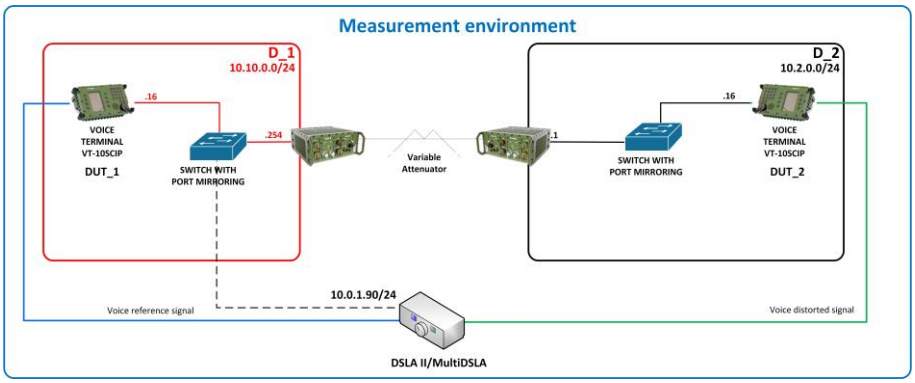

Figure 3. Measurement environment.

4.2 Assessment of the VoIP quality in SCIP encrypted radio connection

The research was focused on measurement of voice quality expressed in MOS scale. The tests began with the determination of initial conditions and determination of radio channel limitations. During this phase, under normal operating conditions of the radio channel, i.e. without interference, a VoIP connection was established using the tested VT-10SICP terminals.

Later, by increasing the attenuation value in the radio channel, the level of suppression for which voice communication becomes unintelligible was determined. This part uses the procedure of subjective assessment of speech quality. Then the attenuation in the radio channel was reduced by 1 dB, thus determining the edge value of the attenuation for further measurements. Subsequent measurements were therefore carried out for the following attenuation values in the radio channel: 5 dB, 7 dB and 9dB.

Tables Table 1 and Table 2 show results for voice quality encrypted with SCIP transmitted in radio channel working in predefined conditions of attenuation. A graphical representation of the results obtained is shown in the following figures (Figure 4-Figure 5).

Table 1. The MOS value measured using the PESQ method.

SNR [dB]	BER	MELPe B&B	MELPe Bw/oB	G.729 D
5	$1{,}7*10^{-2}$	1,24	2,09	2,19
7	$4*10^{-3}$	1,98	2,14	3,16
9	$2{,}13*10^{-4}$	2,47	2,29	3,19

Table 2. The MOS value measured using the POLQA method.

SNR [dB]	BER	MELPe B&B	MELPe Bw/oB	G.729 D
5	$1{,}7*10^{-2}$	1,29	1,78	1,56
7	$4*10^{-3}$	2,04	2,22	3,25
9	$2{,}13*10^{-4}$	2,36	2,37	3,27

The result shows that voice quality for SCIP encrypted traffic over broadband radio channel is quite good even for the very high values of BER (SNR = 5 dB). As the value of BER decreases (SNR = 7 or 9 dB) the MOS values are growing up to a level between 2 and 3. Those are very satisfactory values for so called military coders for which the voice quality can be obtained usually in the range from synthetic to 3,2 [13].

However, long-term persistence of bad channel parameters may lead to significant degradation of the voice connection and even its disconnection. It should be noted that the obtained results are comparable to the results discussed in other publications dealing with the analyzed issue [14].

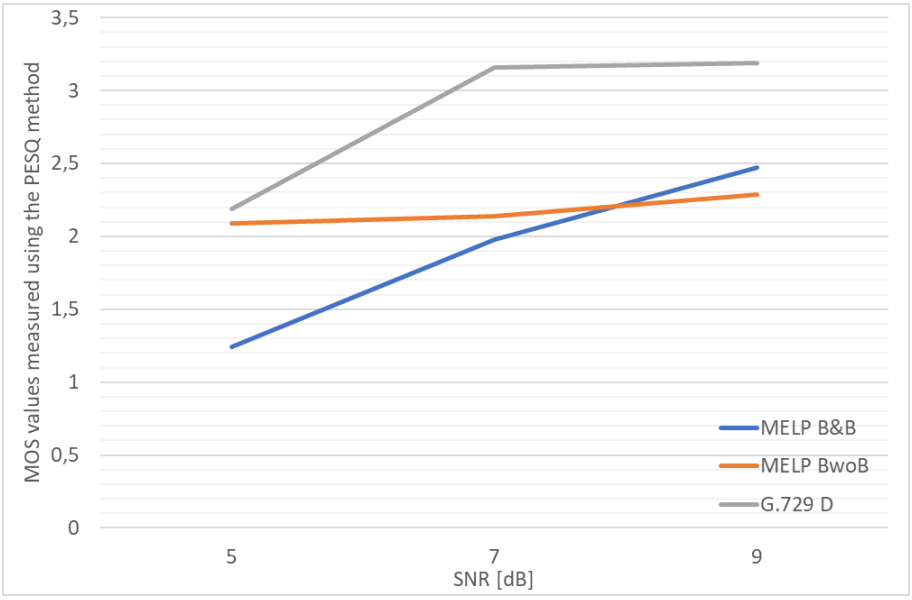

Figure 4. The MOS value measured using the PESQ method for SCIP encrypted voice traffic.

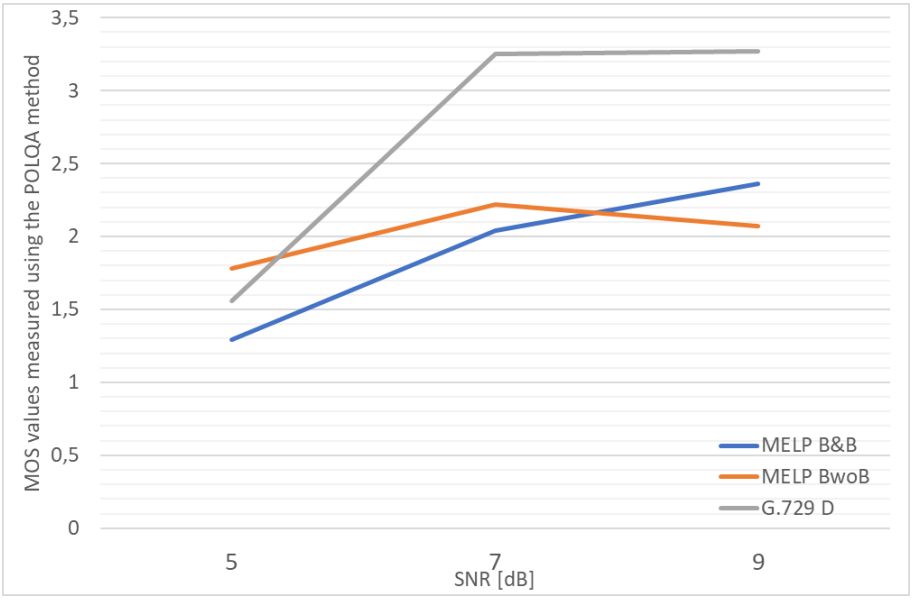

Figure 5. The MOS value measured using the POLQA method for SCIP encrypted voice traffic.

Next figure (Figure 6) presents the measured value of IF (Impairment Factor) for SCIP encrypted voice traffic over broadband radio channel. IF is a rating factor of E-model which reflects the subjective quality of conversation as perceived by the user. It enables of including such parameters as quality of voice coder and frame loss. The high IF values indicate very poor voice quality. As it can be seen the high quality was obtained for G.729 D SCIP encrypted connection even in the poor radio channel conditions. However, also the MELPe Bw/oB SCIP encrypted conversation seems to be satisfactory for the end user. However, it should be remembered that in the case of the IF indicator, the obtained results are valid only for the analyzed case and for other conditions of the implementation of the experiment can take completely different values.

Finally, the impact of SCIP encryption on the quality of the speech waveform was determined for transmission in a non-degraded network. The results of the study are shown in the next figure (Figure 7). As is easy to see, in the low frequency range of the voice signal, encryption causes a deterioration in the quality of the speech signal. This can lead to a general degradation of the quality of the VoIP connection, especially for codecs with a high compression ratio.

Thus, it can be stated that it is possible to provide a quality voice transmission in a radio channel with relatively high interference, while providing a defined level of communication security. Further tests aimed at estimating the impact of encryption on the quality of voice communication in a wide spectrum of radio and wire channels will be the subject of further research.

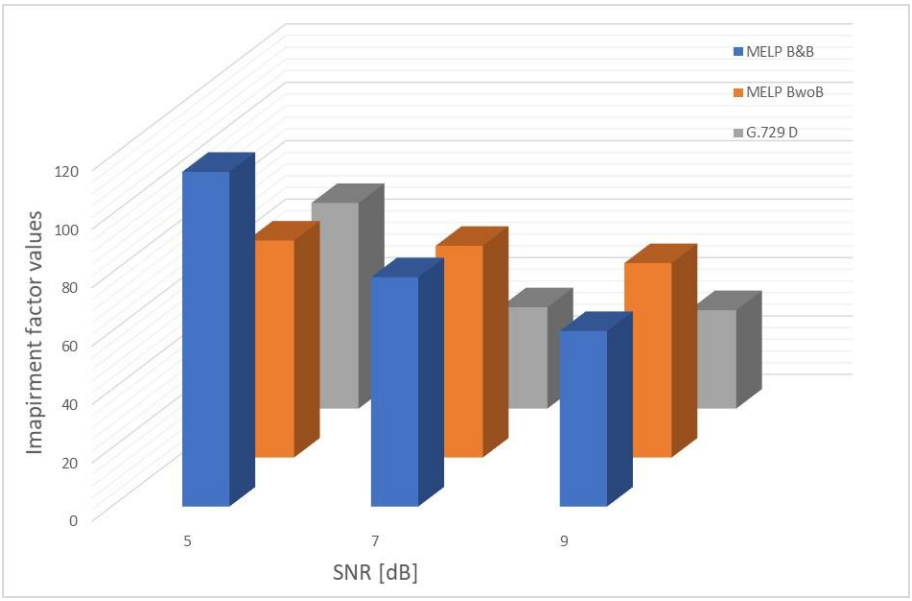

Figure 6. Impairment factor values for different types of military codecs.

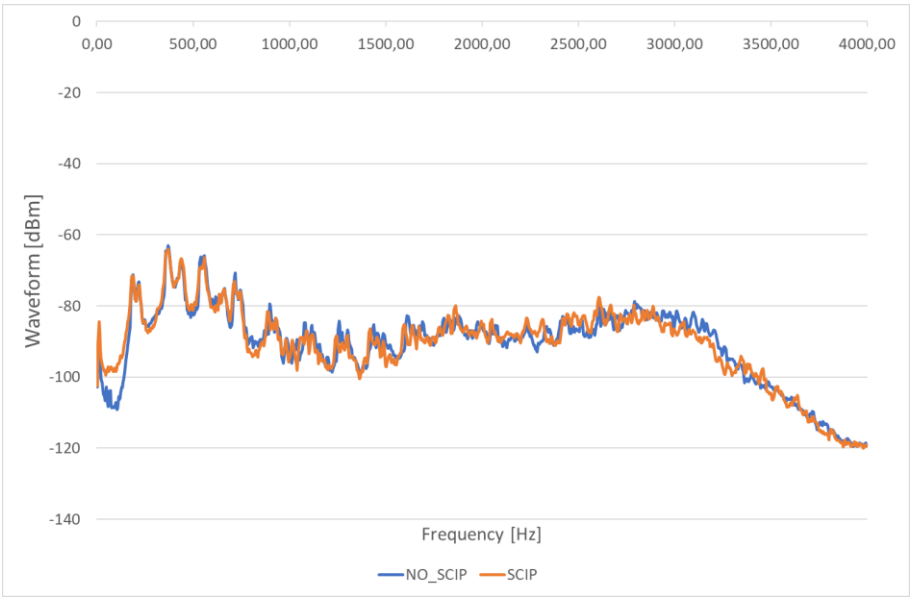

Figure 7. The voice waveform for encrypted and non-encrypted traffic.

5. CONCLUSIONS AND RECOMMENDATIONS

We presented a result of evaluation tests of VoIP quality encrypted with SCIP protocol in broadband radio environment. The obtained results show that even in very poor channel conditions there is the possibility of voice communication of acceptable quality. However, for an SNR of 5dB, the quality of voice communication is rapidly decreasing, leading to a drastic deterioration in the quality perceived by the user, which is at the level of MOS below 2. It can therefore be concluded that the tested implementation of military VoIP codecs with SCIP encryption fits perfectly into military applications characterized by large interferences of radio channel as well as high level of security requirements.

It is also worth noting that the use of the MELPe Bw/oB codec makes it possible to obtain a satisfactory voice connection quality with relatively large disturbances in the radio channel. The best results were obtained for the G.729 D codec, which in these conditions ensures the highest quality of voice communication. However, it should be remembered that the measurements were carried out in relation to broadband radio, which allows the use of this type of codecs. In the case of communication with the use of narrowband channels, there may be problems with the availability of resources.

Analysis of the quality of speech transmission encrypted using the SCIP protocol in narrowband channels determines the direction of further research.

REFERENCES

[1] ITU-T G.1010 Recommendation, "End-User Multimedia QoS Categories Series G: Transmission Systems and Media, " Digital Systems and Networks Quality of Service and Performance - Study, (2001).

[2] Collura, J. S., "Secure Communications Interoperability Protocols (SCIP)," IEEE Military Communications, Meeting Proceedings RTO-MP-IST-054, Neuilly-sur-Seine, France: RTO, Paper 19, 19–1 – 19–10 (2006).

[3] Burke, D., [Speech Processing for IP Networks: Media Resource Control Protocol (MRCP)], Wiley, (2007).

[4] Matyszkiel, R., Polak, R., Kaniewski, P., Laskowski, D., "The results of transmission tests of polish broadband SDR radios," 2017 Communication and Information Technologies (KIT), (2017).

[5] Kaniewski, P., Matyszkiel, R., Kustra, M., Jach, J., "The evolution of transmission security functions in modern military wideband radios," Proceedings of SPIE - The International Society for Optical Engineering, 10418, art. no. 104180E, (2017).

[6] Lubkowski, P., et. al., "On improving connectivity and network efficiency in a heterogeneous military environment," In: Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS 2015), (2015).

[7] Suri, N., Hansson, A., Nilsson, J., et al., "A Realistic Military Scenario and Emulation Environment for Experimenting with Tactical Communications and Heterogeneous Networks," International Conference on Military Communications and Information Systems ICMCIS, (2016).

[8] Lubkowski, P., Laskowski, D., Maslanka, K., "On Supporting a Reliable Performance of Monitoring Services with a Guaranteed Quality Level in a Heterogeneous Environment," Theory and Engineering of Complex Systems and Dependability 365, 275 - 284 (2015).

[9] Lubkowski, P., Sierzputowski, R., Polak, R., Laskowski, D., "Assessment of Voice Call Quality in SCIP Encrypted Traffic," Proceedings of SPIE - The International Society for Optical Engineering, 11055, art. no. 110550E, (2019).

[10] Radmand, P., et. al., "The impact of security on VoIP call quality", Journal of Mobile Multimedia 7 (1), 113 - 128 (2011).

[11] Barbieri, R., Bruschi, D., Rosti, E., "Voice over IPsec: Analysis and solutions," Proceedings - Annual Computer Security Applications Conference ACSAC, 261 - 270 (2002).

[12] Kolahi, S. S., Mudaliar, K., Zhang, C., Gu, Z., "Impact of IPSec security on VoIP in different environments," 9th International Conference on Ubiquitous and Future Networks ICUFN 2017, 979 - 982 (2017).

[13] Hersent, O., Petit, J-P., Gurle, D., [Beyond VoIP Protocols], Wiley, (2005).

[14] Alvermann, J. M., Kurdziel, M. T., Furman, W. N., "Secure Communication Interoperability Protocol (SCIP) over An HF Radio Channel," MILCOM'06, 1 - 4 (2006).