Determination of Error Probability of Cryptography and Safety Codes for Safety-Related Railway Applications

Maria FRANEKOVA[1], *Marek VYROSTKO*[1], *Peter LULEY*[2]

[1]Department of Control and Information Systems, Faculty of Electrical Engineering, University of Zilina, Univerzitna 8215/1, 010 26 Zilina, Slovak Republic
[2]Electrotechnical Research and Projecting Company, Trencianska 19, 018 51 Nova Dubnica, Slovak Republic

maria.franekova@fel.uniza.sk, marek.vyrostko@fel.uniza.sk, luley@evpu.sk

Abstract. *The paper deals with the problem of determination of error probability of cryptography and safety codes used within the safety-related railway applications with increasing safety integrity level (SIL). In the paper are also described requirements for cryptographic block code and safety linear block code in safety-related communications for railway application. The main part is oriented to the description of mathematical apparatus for the error probability of the cryptography and safety block codes for communication between two safety-related devices across GSM-R communication channel. The practical results are related to the quantitative evaluation of an average error probability of the cryptography and safety codes for several lengths of safety-related messages which are expanded about determination of the cryptography degradation with using GMSK modulation scheme.*

Keywords

Cryptography, error probability, safety codes, safety-relevant.

1. Introduction

Nowadays in railway applications, with respect to high requirement to Safety Integrity Level (SIL) of an interlocking and a communication system, the safety of subsystems cannot be demonstrated only by tests but also by theoretical models based on quantitative analysis. Standards for railway applications define four levels of the safety integrity (SIL 1 to SIL 4) depending on the safety requirements [1], [2]. For individual SILs are recommended procedures to be carried out in various life cycle phases of the system to achieve the ability to perform desired function with regard to so-called RAMS (Reliability, Availability, Maintainability, Safety) parameters. Negative influence also results from the fact that a generally acceptable theoretical apparatus for risk analysis and safety level evaluation is missing. Such apparatus would objectify the whole process of safety consideration. Mutual information exchange leads to opinion to unify the safety certification. This leads to problems with minimisation of the acceptation advisement results by reciprocity.

The genesis of the problem is based on the fact, that single European countries developed philosophically different signalling systems and interlocking systems. Those systems have been developed basically at the national level with different types of signals and devices. Today it is very difficult to harmonise these devices.

Future issues shall be solved by a unified system ETCS (European Train Control System) developed in Europe, although implementation of individual application levels of the ETCS system depends on the economic conditions of each European country [3]. Principle of ETCS L2 level is shown in Fig. 1. Within this level is assumed the communication via a GSM-R (Global System Mobile for Railway) network and via communication protocol EURORADIO which already contains the cryptographic mechanisms to ensure authentication procedures of railway participants and integrity of the transmitted safety-related data, for example OBU (On Board Unit) communication in a train with RBC (Radio Block Centre) and RBC-RBC communication. Within communications via GSM-R network is necessary to fulfill the following safety-related functions.

In track part:

- registration of each ETCS train in RBC,
- tracking the position of each ETCS train in RBC,

- determination of drive permission in accordance with data from a train protection system individually for each train,
- determination of drive permission individually to each train.

In board part (see Fig. 1):

- 1: transmission of train position with regard to balise to the RBC,
- 2: calculation of the dynamic speed profile,
- 3: comparison of the current speed with a speed limit,
- 4: on-board signalization for driver.

In case there is expected attack on the messages (as in the case of GSM-R network) it is possible to protect the safety-related messages in the safety-related applications by using of cryptographic and channel coding techniques. Standard EN 50159 [4] recommends the usage of the message transmission model B0 respectively B1. UNISIG development teams involved in the development of ETCS system and in the development of safety-related communication protocol EURORADIO were motivated with the B1 model and offered to secure the message sources authorization, securing the integrity and securing the safety-related messages during the transmission based on commercially available authentication technology MAC (Message Authentication Code) [5]. For reason of increasing the safety level is recommended applying CBC-MAC (Cipher Block Chaining MAC) by using the symmetric block cipher algorithm 3-DES [6].

2. Requirements for Cryptography and Safety Codes of Safety-Related Communications

Concerning to the application of safety codes within safety-related communication system the linear block detection codes are recommended with the decoding principle based on syndrome technique of determination. These requirements the group of channel block codes satisfy, from which for the purpose in view cyclic codes based on cyclic redundancy check (CRC) are the most recommended. In the last terms the possibilities of error correction of block codes are subjected to research, primarily if the safety codes algorithms are effective and very well known, e.g. Hamming codes, eventually non binary Reed Solomon codes, up to now with the use of their decoding possibilities [7]. Safety-related application requires that one safety code assures the messages of different lengths.

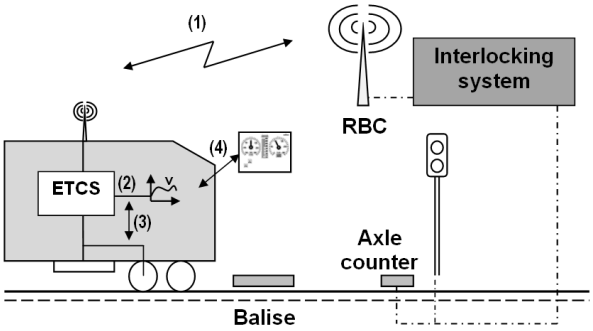

Fig. 1: Safety functions of ETCS L2.

Cryptographic techniques are aimed at the elimination of masking from unauthorized sources respectively are used to ensure the confidentiality of the transmission. In case of encrypted messages transmission via a noisy communication channel is the influence of EMI (Electromagnetic Interference) eliminated by usage of the safety code but the noise does influence the transmission of the encrypted code word. The level of safety integrity and the nature of the safety-related process shall according to [4] prove the adequacy of:

- technical choice of cryptographic techniques (enforced are the block ciphers techniques with private key),
- key management (key generation, testing, transfer, archiving and replacement).

Cryptographic algorithm must be applied for all user data and can be used for any additional data which shall not be transferred but are known for the sender and also for the recipient, so-called implicit data. It is recommended to use standardized techniques and standardized procedures, e.g. recommendations by ISO/IEC 10116, when using cryptographic techniques and key management methods. For the safety-related applications is not recommended the use of electronic coding book (ECB) mode for input length exceeding the block length of encryption algorithm. To improve the safety is recommended to use CBC (Cipher Block Chaining) mode. Cryptographic algorithms can be registered in accordance with the international standard ISO/IEC 9979 but registration itself does not guarantee the strength of the algorithms.

To simplify the issue we can describe the communication system on the end-to-end link as shown in Fig. 2. Communication system consists of the safety-related equipment SRE 1 and the safety-related equipment SRE 2 (in ETCS it can be for example RBC and on-board unit in the train part) with untrusted

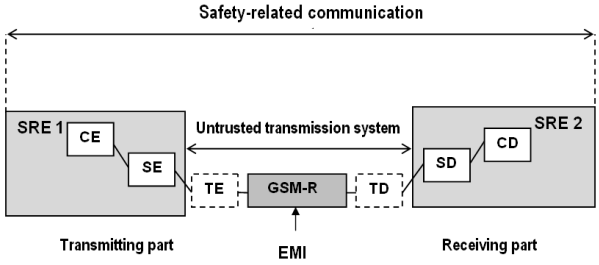

Fig. 2: Safety-related communication system.

transmission system which consists of transmission encoder/decoder and GSM-R communication channel. Meaning of abbreviations from Fig. 2 is as follows:

- CE/CD: Cryptographic encoder/decoder,
- SE/SD: Safety encoder/decoder,
- TE/TD: Transmission encoder/decoder,
- GSM-R: Global System Mobile for Railway,
- EMI: Electromagnetic Interference.

The base of a trusted communication system is an untrusted communication channel GSM-R, which is classified as open transmission system. It is assumed the usage of GSMK (Gaussian Minimum Shift Key) modulation where a bit error rate P_b is defined in [8] by the empirical formula:

$$P_b = \frac{1}{2} erfc\left(\sqrt{\frac{\alpha E_b}{2N_0}}\right), \tag{1}$$

where E_b is the energy per one bit, N_0 is the power spectral density of white noise and *erfc* is the complementary error function of Gaussian noise. The parameter $\alpha/2$ is the efficiency degradation of GMSK (with prescribed relative bandwidth of frequency filter WT_b) in the corporation with the MSK (Minimum Shift Keying) modulation. Safety-related messages are secured by cryptographic block code with a private key (length of block k is chosen according to current computation-secure cryptographic standards of block ciphers $k = 64$, 128 and 256 bits) and safety code, e.g. CRC-r, where r represents the number of redundant bits. According to [4] it is assumed that CE/CD can be a part of safety-related equipment or can be implemented in the separated safety layer on the input of untrusted transmission system for example as a part of the firewall. Encoder and decoder of cryptographic and safety codes must be realized on the fail-safe principle.

A part of the transmission system is the communication channel which is influenced by EMI. Safety-related messages source authorization is provided by safety procedures of shared keys exchange during every relation. Safety-related messages are also assured by a safety code. We assume independence of the safety and cryptographic encoders/decoders.

3. Mathematical Apparatus for Error Probability Determination of Cryptographic and Safety Codes

As it is well known in the process of the safety evaluation of the block linear codes are used two parameters: minimal Hamming distance of code d_{min} and the probability of undetected/uncorrected error of the code words with lengths w.

The probability of error of the code word P_w is depending on the bit error rate P_b of used transmission channel. In practice the different types of transmission channels have different values of P_b and different behavior of noise in concrete media. In many cases the model of binary symmetric channel (BSC) or q-nary symmetric channel (q-BSC) are assumed.

If the linear block safety code with minimal Hamming distance d_{min} is applied that the code is able to detect α errors in code word of length w whereby must be true that $d_{min} \geq \alpha + 1$ and correct β errors in code word of length w, whereby must be true that $d_{min} \geq 2\beta + 1$. For determination of the probability of uncorrected errors P_w in the code word w when the BSC channel with bit error rate P_b is assumed that is valid:

$$P_w \leq \sum_{\|i=\beta+1\|}^{w} \binom{w}{i} P_b^i (1-P_b)^{w-i}, \tag{2}$$

what is possible to approximate by:

$$P_w = \binom{w}{\beta+1} P_b^{\beta+1} (1-P_b)^{w-\beta-1}. \tag{3}$$

If we assume the independence of errors in the input of the cryptography decoder in Fig. 2 it is possible to calculate the relations for probability of error of cryptography word Pcw, what is described in the next part.

According to the recommendation from the standard for communications in the railway applications [4] for determination of the cryptographic decoder error probability is necessary to consider the set of block cryptography encoder with the private key where the safety-related message of length n bits is divided into the words with the length of k bits and after that encrypted with the agreed algorithm. During transfer via the untrusted communication channel GSM-R there is interference by EMI (during analysis we assumed the impact of Gaussian noise). The plaintext is restored on

the output of the cryptographic decoder after transmission and receiving on the receiving part of communication system.

No c_w (Cipher Word) is incorrect until the blocks of received encrypted code contains an error in more than one out of n bits. If we assume independence of the blocks with errors on the input of the cryptographic decoder then the error probability of encrypted word $\vec{P}_{cw}$ depends on the communication channel bit error rate P_b and is defined as:

$$\vec{P}_{cw} = \vec{P}(w|be)\left[1-(1-P_b)^n\right], \tag{4}$$

where $\vec{P}(w|be)$ is the conditional error probability of the output word w if there is an error block on the input of the cryptographic decoder.

According to [9] by repeating of the analysis for a sufficient amount of output bits we can make a conclusion that the average error probability in the word with the length of k bits in the simple encrypted block on the output (in case there is no error block on input) is:

$$\vec{P}(w|be) = 1 - \prod_{i=1}^{k} \frac{2^{n-1}-1}{2^{n+1-i}-1} = \frac{1-2^{-k}}{1-2^{-n}}. \tag{5}$$

By substitution of this formula into (4) we can calculate the ensemble-average word error rate probability for the block cipher:

$$\vec{P}_{cw} = \left(1-2^{-n}\right)^{-1}\left(1-2^{-k}\right)\left[1-(1-P_b)^n\right]. \tag{6}$$

To increase the safety of cryptographic communication system is used a suitable coding system with the error detection (in the Fig. 2 it is a safety code) in the trusted communication system. Then, considering the conditions in [9], it is possible adjust formula (6) to:

$$\vec{P}_{cw} = \left(1-2^{-n}\right)^{-1}\left(1-2^{-k}\right)\left[1-(1-P_w)^{n/k}\right], \tag{7}$$

where P_w is the error probability of unencrypted code word and the integer n/k is the amount of words in the block. A Taylor-series expansion yields the approximation:

$$\vec{P}_{cw} \approx \left(1-2^{-n}\right)^{-1}\left(1-2^{-k}\right)\frac{n}{k}P_w, \tag{8}$$

which is accurate in case if:

$$P_w << 2k\,(n-k)^{-1}. \tag{9}$$

The error probability of unencrypted code word can be calculated using the mathematical model applicable to the BSC model (see e.g. [10] or there can be used a pessimistic approach for calculation of P_w by approximation of the value 2^{-r} where r represents the amount of redundant bits of the safety code).

If we would like to consider in the probabilistic cryptographic code analysis also the energy ratios of encrypted transmission we have to develop a further consideration. The bit error probability P_b in the unencrypted binary communication (plaintext) is a function of average energy per bit E_b and the white noise power spectral density N_0:

$$P_b = f(E_b/N_0). \tag{10}$$

After incorporating these values into the formulas we can calculate the cryptographic code word error probability by a formula which is the function of E_b. When we use basic formula of the BSC model where the error probability of unencrypted code word with length k is:

$$P_w = 1-(1-P_b)^{-1}, \tag{11}$$

we can express the increase of the energy required for the same error probability when using cryptographic system by assuring with corresponding unencrypted system. This increase provides a quantitative measure of a cryptographic degradation which is defined:

$$\begin{aligned} D[dB] &= 10\log_{10}E_{b1} - 10\log_{10}E_b = \\ &= 10\log_{10}\left(\frac{E_{b1}}{E_b}\right), \end{aligned} \tag{12}$$

where E_{b1} is the energy required to produce the desired value of $\vec{P}_{cw}$ which is equal with the value of P_w when the energy is E_b. For low values of P_b in the formula (6) can be this formula approximated:

$$P_w \approx kP_b, P_b << 2\,(k-1)^{-1}. \tag{13}$$

Then the summary variable error probability of cryptographic code word has the form:

$$\vec{P}_{cw} \approx g(n,k)P_w, P_b << (n+k-2)^{-1}, \tag{14}$$

where $g(n,k)$ is a function representing the relation between the amount of all bits in the message n and the amount of bits in block k. For block cipher applies:

$$g(n,k) = \frac{(1-2^{-k})n}{(1-2^{-k})k}. \tag{15}$$

With respect to the formula E_{b1} is implicitly in relation with E_b:

$$\vec{P}_{cw}(E_{b1}) = \vec{P}_{cw}(E_b). \tag{16}$$

As was already mentioned the bit error probability of GMSK modulation is given by the formula (1) which after adjusting for E_b/N_0 small enough is:

$$P_b = \frac{1}{2}\exp\left(-\frac{\alpha E_b}{2N_0}\right), \tag{17}$$

since $\alpha/2$ is not depended on E_b, but depends on the type of modulation. By substitution (14) into (13) for E_{b1}/E_b and by using the result from (9) we obtain:

$$D = 10\log_{10}\left[1+\frac{\ln g(n,k)}{(\alpha E_b/2N_0)}\right]. \tag{18}$$

4. Practical Part

Let assume that the safety code is detection cyclic linear block code working on the principle of CRC (Cycling Redundancy Check), CRC-16. Further we assume that the probability of undetected error of code word $P_w = 2^{-16}$ (according to standard [4], so called the worst case). The ensemble-average cryptographic word error probability $\vec{P}_{cw}$ was realized according to equation (7). The results of $\vec{P}_{cw}$ for different length of code word on the input of ciphering encoder ($k = 64$, 128, 192, 256) and different length of input plaintext ($n = 1 \cdot 10^4$, $5 \cdot 10^4$, $1 \cdot 10^5$, $5 \cdot 10^5$, $1 \cdot 10^6$, $5 \cdot 10^6$) are illustrated in Tab. 1.

Graphical results of $\vec{P}_{cw}$ as a function of input bit stream of plaintext n for constant value of code words in input of cryptography decoder is illustrated in the Fig. 3. In the graph illustrated in the Fig. 4 we can see how is changing $\vec{P}_{cw}$ depending on code words $k = 64$, $k = 128$ and $k = 256$ on the input of cryptography encoder.

Cryptographic degradation of the cryptographic system was determined by using the formula (18) assuming the GMSK modulation. The assumed error rate of one bit determined according to (1) assumed that there is present Gaussian noise in the channel. The relative bandwidth of the filter WT_b was set in accordance with the recommendation for GSM applications $WT_b = 0,3$ for which according to empirical graphs from [8] $\alpha/2 = 0,9$. Graphic illustration of the cryptographic degradation for various length of cryptographic code $k = 64$, 128, 256 bits is shown in Fig. 4.

Tab. 1: Result of the average error probability with using cryptography code in accordance with parameter n.

Length of input plaintext n	Average error probability $\vec{P}_{cw}$ if $k = 64$	Average error probability $\vec{P}_{cw}$ if $k = 128$	Average error probability $\vec{P}_{cw}$ if $k = 256$
$1 \cdot 10^4$	3,13E-14	1,56E-14	7,81E-15
$5 \cdot 10^4$	1,56E-13	7,81E-14	3,91E-14
$1 \cdot 10^5$	3,13E-13	1,56E-13	7,81E-14
$5 \cdot 10^5$	1,56E-12	7,81E-13	3,91E-13
$1 \cdot 10^6$	3,13E-12	1,56E-12	7,81E-13
$5 \cdot 10^6$	1,56E-11	7,81E-12	3,91E-12

5. Conclusion

Authors worked with the recommendation for the cryptographic block ciphers according to [4]. They also considered the recommendations for the safety analysis of the encrypted transmission affected with noise environment of GSM-R with GMSK modulation, which has become a prospective medium for transmitting messages in the developing ETCS system. Such a cryptographic system in order to ensure the data integrity during the transmission is always connected with the particular type of safety code which eliminates the interference effect of communication channel. When choosing the parameters for cryptographic and safety code is necessary that the length of transmitted safety-related message was $n >> k$. Recommendation of [8] is $n >> 4k$.

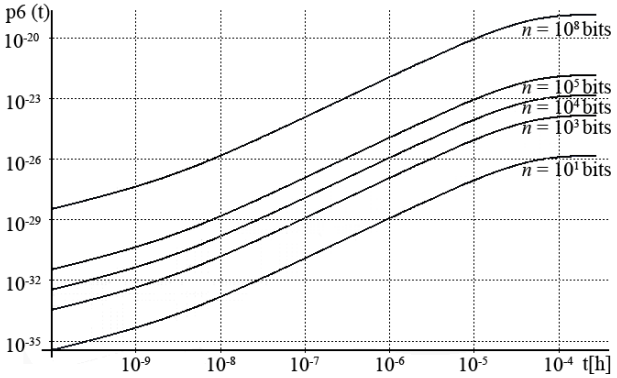

Fig. 3: Average error probability of the cryptography code word in dependence on n.

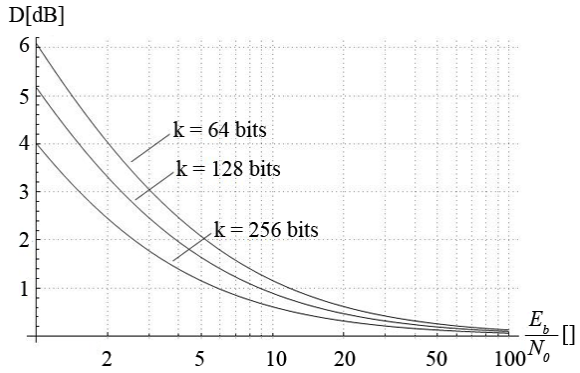

Fig. 4: Cryptographic degradation depending on the E_b/N_0 ratio.

Results of the average error probability of cryptographic code word illustrated in the Tab. 1 were determined for messages with the length from $1 \cdot 10^4$ to $5 \cdot 10^6$. In many cases the application offers telegrams with short or long messages. Results of the cryptographic code error probability in the receiving part of a cryptographic system illustrated in the Tab. 1 are determined for the worse assumed noise parameters on the basis of BSC model with $P_b = 2^{-1}$. In case we knew the detailed parameters of the safety code (for example minimum Hamming distance d_{min} or weighing code function A_i) the results of $\vec{P}_{cw}$ would have been much more favorable. The curve of the cryptographic degradation was based on the assumption of using GMSK modulation which is usually applied in the GSM modulation. The curve of cryptographic degradation indi-

cates that the choice of cryptographic communication system parameters is a compromise between E_b/N_0 ratio and the desired value of $\vec{P}_{cw}$ where is an important set this along with the parameter k-length of the block and requested $\vec{P}_{cw}$.

Acknowledgment

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number: 024ZU-4/2012: Modernization of technology and education methods orientated to area of cryptography for safety critical applications.

References

[1] EN 50129. *Railway applications: Safety-related electronic systems*. Brussels: CENELEC, 2003.

[2] EN 50126. *Railway applications: The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS)*. Brussels: CENELEC, 2001.

[3] Ertms.Com. *Ertms.Com* [online]. 2013. Available at: www.ertms.com.

[4] EN 50159: *Railway applications: Communication, signalling and processing systems - Safety - related communication in transmission systems*. Brussels: CENELEC, 2010.

[5] FRANEKOVA, M., F. KALLAY, P. PENIAK and P. VESTENICKY. *Komunikacna bezpecnost priemyselnych sieti*. Zilina: EDIS, 2007. ISBN 78-80-8070-715-6.

[6] BIHAM, E. Cryptanalysis of Multiple Modes of Operation. *Journal of Cryptology*. 1998, vol. 11, iss. 1, pp. 45–58. ISSN 1432-1378. DOI: 10.1007/s001459900034.

[7] KLAPKA, S. *Detection codes in signalling systems*. Prague, 2009. Habilitation work. Czech Technical University in Prague.

[8] HAYKIN, S. *Communication systems*. New York: John Wiley&Sons, 2001. ISBN 0-471-17869-1.

[9] TORRIERI, D. J. *Principle of Secure Communication Systems*. London: Artech House Boston, 1992. ISBN 0-89006-555-1.

[10] FRANEKOVA, M. and K. RASTOCNY. Safety Evaluation of Fail-Safe Fieldbus in Safety Related Control System. *Journal of Electrical Engineering*. 2010, vol. 61, iss. 6, pp. 1–7. ISSN 1335-2547.

[11] FRANEKOVA, M. Evaluation of safety codes used in safety - related communication systems. *International Journal of Engineering: Annals of Faculty Engineering Hunedoara*. 2010, vol. VIII, iss. 2, pp. 43–48. ISSN 1584-2265.

[12] FRANEKOVA, M.: Mathematical apparatus for safety evaluation of cryptography and safety codes used in safety related communication system. In: *Modern transport telematics: 11th international conference on transport systems telematics, TST 2011*. Berlin Heidelberg: Springer-Verlag, 2011, pp. 126–135. ISBN 978-3-642-24659-3.

About Authors

Maria FRANEKOVA was born in Brezno, (Slovak Republic) in 1961. She received her Prof. in 2011 in the field of Automation with orientation to "Safety-related Control and Communication Systems". Her research interests include safety communications, methods of safety evaluation of data transmission on the base of coding and cryptography tools within safety-related applications.

Marek VYROSTKO was born in Kosice, (Slovak Republic) in 1985. He received his Master (MSc.) degree in 2008 in University of Zilina. Currently he is Ph.D. student. His research interests include communication and solution of key management system for cryptography communications within railway applications.

Peter LULEY was born in Ilava (Slovak Republic) in1983. He received his M.Sc. in University of Zilina in 2007. Currently he is Ph.D. student of external form. He works in corporation of EVPU a.s., Nova Dubnica. His research interests include methods of quality assessment of technical communication and control systems.