**ARCHIVES OF TRANSPORT** *ISSN (print):* *0866-9546*
*Volume 66, Issue 2, 2023* ***e-ISSN (online):*** *2300-8830*
***DOI:*** *10.5604/01.3001.0016.3237*

# TRANSMISSION SYSTEM MODEL IN THE TRACK-VEHICLE RELATIONSHIP BASED ON LONG TERM EVOLUTION TECHNOLOGY

**Marcin CHRZAN[1], Paweł PIROSZ[2], Jacek PAŚ[3]**

[1] *Faculty of Transport, Electrical Engineering and Information Technology, Kazimierz Pulaski University of Technology and Humanities in Radom, Radom, Poland*

[2] *Faculty of Computing and Telecommunications, Poznan University of Technology, Poznań, Poland*

[3] *Division Electronic Systems Exploitations Manager, Military University of Technology, Warszawa, Poland*

## *Abstract:*

*Because of degradations of the wired infrastructure connecting the element of railroad control systems, and related primarily to their destruction, the use of the radio transmission medium for independent management of railroad traffic control devices is increasingly being considered. An undoubted problem in implying such solutions is the security of transmission in such systems. It should be noted that security at a certain level of transmission is currently already offered by the radio transmission systems themselves, which has also been used in the GSM-R standard. The creation of a separate dedicated system for railroads involves huge expenditures for the design, testing, certification and, finally, construction and implementation of such technology. Therefore, in the opinion of the author of this dissertation, it is possible to use public open radio networks for the needs of railroads, which significantly reduces costs, since such a system is based on existing infrastructure. It is necessary to develop a way of transmitting information that meets the requirements of secure transmission in the sense of railroad traffic control systems. The task is to develop a general model for open radio transmission in traffic control systems based on the latest public radio standard, which is LTE, 5G or Future Railway Mobile Communications System (FRMCS). The article will present the concept of data transmission in the track – vehicle relationship with the use of LTE (Long Term Evolution) technology. It will show the concept of transmission based on the PN-EN50159:2011 standard and the results of the tests conducted during control trips on the railway route. The main element that will be subject to the research will include the transmission safety and its delay. The impact of a type of transmission encryption on its delay will be estimated with the assumed blocks of data sent during the transmission. A probability distribution and density functions of the transmission delay probability distribution with the message sizes in the range from 16B to 10 kB with four ways of the signal encoding according to the PN-EN50159:2011 standard will be also analysed.*

***Keywords:*** *control, operation, rail traffic, safety, telecommunications, transport*

## *To cite this article:*

*Chrzan, M., Pirosz, P., Paś, J., (2023). Transmission system model in the track-vehicle relationship based on Long Term Evolution technology. Archives of Transport, 66(2), 89-108. DOI: https://doi.org/10.5604/01.3001.0016.3237*

**Contact:**
1) m.chrzan@uthrad.pl [https://orcid.org/0000-0003-4181-4847] – corresponding author; 2) pawel.pirosz@put.poznan.pl [https://orcid.org/0000-0001-9264-1099]; 3) jacek.pas@wat.edu.pl [https://orcid.org/0000-0001-8900-1445]

## 1. Introduction

The rail traffic control systems (SRK) are an element of the railway transport system that significantly affects the safety and organisation of traffic of rail vehicles moving on the track systems in an organised manner in the process of people and cargo transport [Białoń & Gradowski, 2009; Chrzan, 2020; Chrzan, 2021; Gago & Siergiejczyk, 2020, Toruń et al., 2019]. Elements and systems used in the rail traffic control systems should be characterised by a high degree of reliability, especially when their operation depends on the traffic safety of passenger trains travelling at high speed or when high traffic efficiency is required [Chrzan et al., 2018; Jacyna et. al., 2018]. In order to meet the modern demands, the rail traffic management systems are built on the basis of a technologically and functionally advanced computer and telecommunication technology. By tracking the development of management systems in the European management boards, it is possible to observe that such systems were created, and then, they were operated mainly in the area of a given country. Since the beginning of the 90's of the last century, within the framework of the European Union, the joint railway and industry work related to the implementation of the ERTMS/ETCS (European Rail Traffic Management System/European Train Control System) harmonised train control system and the GSM-R (Global System for Mobile Communication – Railway) railway communication system have been implemented [Rosberg et al., 2021; Białoń & Gradowski, 2007].

## 2. Literature review

The ETCS system is largely based on digital signal transmission between the track and vehicle. The transmission can be carried out through Eurobalises, Euroloops, digital radio channel and specialised transmission modules. Depending on the level and configuration, trackside devices are prepared to perform only a specific function range. This range is determined while designing the railway line equipment in ETCS taking into account, among others, the railway line needs (expressed by, e.g. required railway line capacity, train speed, required passenger comfort) and costs of investments and operation [Kornaszewski et. al., 2017; Pawlik et.al., 2017].

The theoretical and practical aspects of the rail traffic control systems taking into account the solutions used in Poland, were presented in papers [Kukulski et al., 2019; Chrzan, 2021; Chrzan, 2020; Białoń & Gradowski, 2009]. However, these papers do not include solutions based on data transmission open systems.

The theoretical analysis and the one of modelling broadband signals, also in the LTE system, for various areas of application were presented in publications [Chrzan, 2021, Garcia et al., 2019]. The propagation of broadband signals and the related issue were widely discussed in them, but railway issue was not considered in these positions.

The research methodology, as well as the results and analyses of computer simulation on mathematical modelling of the transmission communication system and channel, paying attention to ensuring the adequate system capacity and reliability and taking into account the issue of the train movement were described in [Bocanegra et. al., 2019]. All the considerations were related only to the LTE system without taking into account the specificity of the wave propagation and safety in the rail traffic control systems [Chrzan, 2020].

The LTE/MIMO system architecture and issues related to the transmission of broadband signals were standardised in [3GPP, 2020; Shirly & Malarvizhi, 2020, Wu & McAllister, 2017]. However, the possibility of use in the railway systems was not indicated there.

Currently, the tests on the LTE system application in railway tasks are carried out in an advanced manner in Asian countries (China, India, Indonesia) [Changqing et. al., 2020; Kunai, 2019; Jian, 2019] and also on the European continent in the Western Europe countries (Spain, Sweden) [Karthika & Indumathi, 2020; Alemayehu & Gared, 2019]. However, it must be emphasised that the work is advanced in the field of audio-video transmission. The work on the transmission of signals controlling the railway automation devices is not carried out.

Any research work in the field of modern telecommunications technologies currently carried out in the Polish railways focuses on the implementation of the next stages of the ERTMS system (1 and 2 level) and the system applied for communication in the track-vehicle relationship standardised as GSM-R. In the world, the research work has been conducted and the solutions to replace the GSM-R system with the LTE system have been tested for years. Unfortunately, no one in Poland has not attempted to address this issue so far [Białoń & Gradowski, 2009; Kornaszewski

et. al., 2017; Siergiejczyk & Rosiński, 2019]. The activities to determine the impact of the LTE technology on the possibility of the transmission of telegrams in the relationship between the trackside devices were taken [Chrzan, 2021]. Therefore, in the further part of the article, the developed original signal transmission method in the track – vehicle relationship with the use of an original method taking into account the LTE technology in the presence of phenomena reducing transmission at higher speeds of the train will be presented.

## 3. Radio transmission model structure

In order to model the system of open radio transmission of telegrams between the rail traffic control devices and the local control centre, like in the PN-EN50159:2011 standard, the following assumptions were adopted:

- there are rail traffic control devices with a specific functionality at the level of SIL-4 in the system,
- rail traffic control devices have operating approvals and safety certificates at the specified level SIL (*Safety Integrity Level*) – SIL-4,
- radio transmission changes the transmission medium from wired to wireless, which results in the situation that the behaviour of these devices should not change – their parameters are determined,
- radio transmission takes place in the LOS and NLOS conditions,
- radio transmission takes place in open systems,
- constant train speed of 160 km/h (conditions for Poland)
- network load is a natural load, no impact on network traffic generated by the measurement system – actual conditions, in which the system is to operate,

in order to model, the GSM-R transmission parameters are adopted with the assumption that the fulfilment of these conditions meet the transmission safety conditions.

In order to make measurements on the existing telecommunications infrastructure in Poland, a transmission model for the LTE open system, shown in Figure 1, was built. In order to conduct the research, the system will be used as in [Chrzan, 2020], in which the transmission takes place at the first stage of research between the software virtual LCS (Local Control Centre), and the virtual rail traffic control device, located on the train route.

In order to send information, the methodology of the telegram creation and its sending is presented in Fig. 2.

The measurement involved sending an encrypted message from the LTE mobile station (Fig. 1) located on the train to the local control centre located at the Faculty of Transport and Electrical Engineering of Kazimierz Pułaski University of Technology and Humanities in Radom. The messages with the sizes of 16B, 32B, 64B, 128B, 256B, 512B, 1024B, 2048B, 4096B, 6144B, 8192B and 10240B were sent. The measurements related to the message transmission delay in a given period of time, which was 900 s. The entire time needed to send the message involved the following factors: message encoding time, message transfer time by the mobile network and the message decoding time.

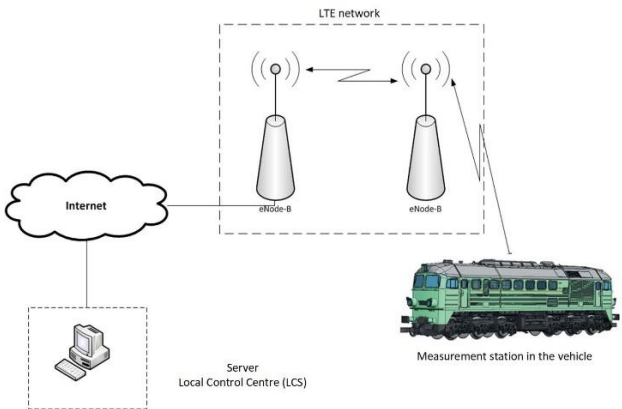


Fig. 1. Measuring diagram

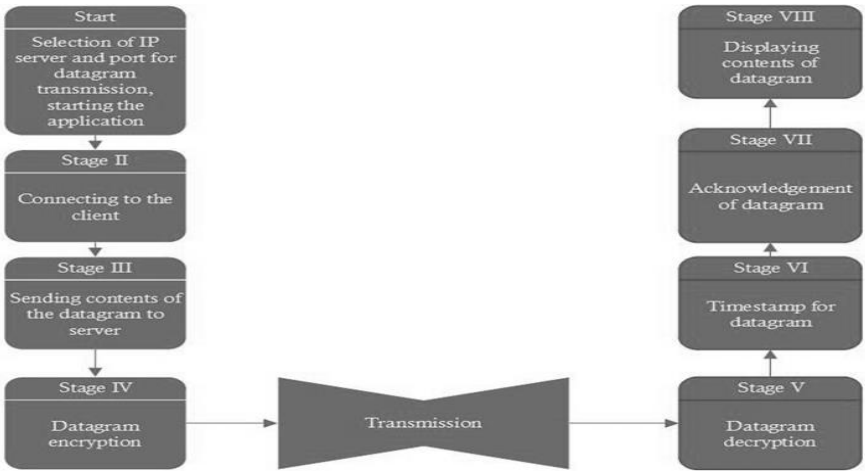

Fig. 2. Telegram service diagram in the measurement system [Chrzan, 2021]

In order to encrypt random railway messages with different sizes, the following algorithms were applied:

- AES CBC (Advanced Encryption Standard – Cipher Block Chaining),
- AES ECB (Advanced Encryption Standard – Electronic Codebook),
- DES CBC (Data Encryption Standard – Cipher Block Chaining),
- DES ECB (Data Encryption Standard – Electronic Codebook),
- RSA (Rivest–Shamir–Adleman) with a key length of 1024 and 2048 bits.

## 4. Results and discussion

The constructed measurement programme consists of two modules: Server (which is an LCS simulator) – Fig. 3 – and the Client (as a transmission receiver) – Fig. 4. The Server programme allows to connect with the Client programme after setting of the common transmission parameters, such as: IP address, TCP protocol port number, and determination of the signal encoding method. In case of RSA transmission with the use of a key – the server programme allows to generate a key on the basis of the entered password. The Server programme receives the sent telegram, decodes it, checks integrity and sends back the acknowledgement of receipt to the Client (Fig. 5). The programme that initiates the exchange of transmission with the specified data encryption is the Client's programme. In addition, it allows to:

- send a fixed message (telegram) with a cyclically specified length, in a specific time period,
- send a variable message, generated separately for each server connection with a fixed length, cyclically generated in a given time,
- send a single message with a specified length.

The telegram sent from the client to the server is designed in such a way as to meet the safety requirements for the open and closed transmission systems included in the PN-EN50159:2011 standard, which is connected with the use of the applied equipment and software operating on it. The provision of the appropriate level of the telegram transmission safety should be carried out in a way that makes it possible to detect the signal transmission errors from the sender to the recipient, and in case of a break in transmission over the above specified time, the system should result in the transition to the state providing safety. In this dissertation, it was achieved by securing the telegram with the use of encryption.

The radio interface used in the tests was based on the public network of the LTE system, which was the dissertation's assumption. Owing to the fact that the radio interface operates in the open system, the measurements were conducted with the use of actual transmission parameters of the LTE network and the unknown system load capacity. According to the author's assessment, it constitutes a determinant to assess the open system suitability for tasks related to

the rail traffic control in accordance with the criteria specified in the PN-EN 50159 and PN-EN 50129 standards.

Figures 6 – 11 present the measurement results of the random railway message transmission delay in the time function for the extreme message sizes of 16B and 10kB with AES CBC, AES ECB and RSA encryption algorithms of the signal sent from the train moving at the speed of 160 km/h to the local control centre with the use of the LTE infrastructure [Chrzan, 2021].

Summary of measurement results in Table 1.

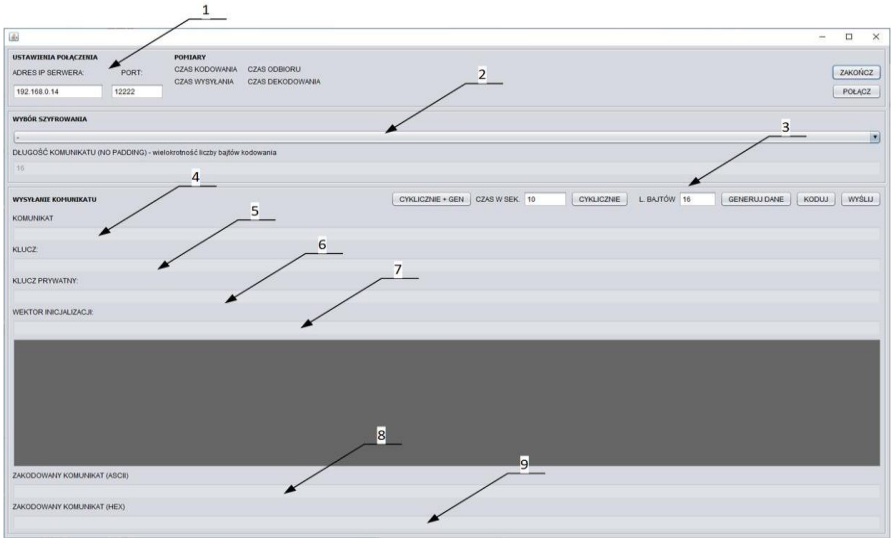


Fig. 3. Measurement programme window – client (1 –port for TCP/IP transmission, 2 – the choice of encryptionx algorithm, 3 – the length in bits, 4 – data logging (data are logged to text file), 5 – key, 6 – private key, 7 – initiation vector , 8 – coded message (ASCII))

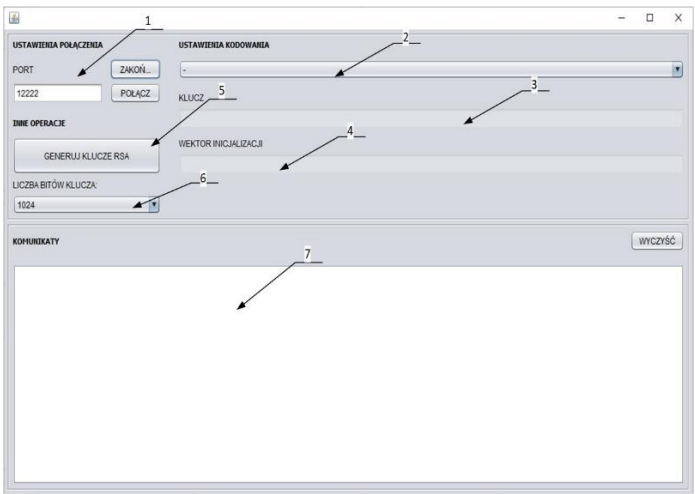


Fig. 4. Measurement programme window – server (1 – port for the transmission, 2 – the type of encryption algorithm mode, 3 – key, 4 - initiation vector, 5- RSA key generator, 6 – number of key bits, 7 – message received)

| | A | B | C | D | E | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ENC | SEND | DEC | RECEIVE | SIZE (byte) | UNIX TIME | | czas [s] | opóźnienie [ms] | |
| 2 | 1138 | 25002 | 67260 | 29647 | 64 | 1,44E+12 | | 0 | 98,045 | |
| 3 | 2914 | 29681 | 74368 | 44203 | 64 | 1,44E+12 | | 0,33 | 121,485 | |
| 4 | 485 | 37584 | 111368 | 99312 | 64 | 1,44E+12 | | 0,697 | 211,165 | |
| 5 | 732 | 33403 | 46163 | 68904 | 64 | 1,44E+12 | | 0,995 | 115,799 | |
| 6 | 809 | 37866 | 53362 | 28531 | 64 | 1,44E+12 | | 1,309 | 82,702 | |
| 7 | 1771 | 23215 | 46616 | 20125 | 64 | 1,44E+12 | | 1,612 | 68,512 | |
| 8 | 1231 | 43067 | 49577 | 30613 | 64 | 1,44E+12 | | 1,925 | 81,421 | |
| 9 | 1058 | 47341 | 53303 | 38666 | 64 | 1,44E+12 | | 2,239 | 93,027 | |
| 10 | 1069 | 19464 | 52687 | 41350 | 64 | 1,44E+12 | | 2,553 | 95,106 | |
| 11 | 1067 | 31838 | 49444 | 34389 | 64 | 1,44E+12 | | 2,865 | 84,9 | |
| 12 | 1427 | 47431 | 59516 | 47577 | 64 | 1,44E+12 | | 3,175 | 108,52 | |
| 13 | 1073 | 47664 | 54045 | 27648 | 64 | 1,44E+12 | | 3,485 | 82,766 | |
| 14 | 1055 | 28119 | 45427 | 40099 | 64 | 1,44E+12 | | 3,904 | 86,581 | |

Fig. 5. Record of the telegram transmission parameters

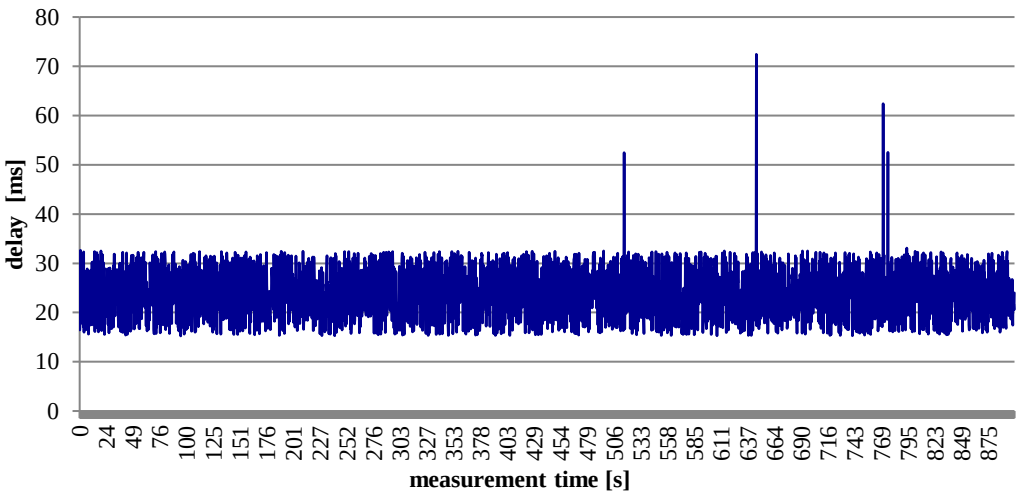


Fig. 6. Transmission delay relationship in the measurement time function for messages with a length of 16 B encoded with the use of the AES CBC method

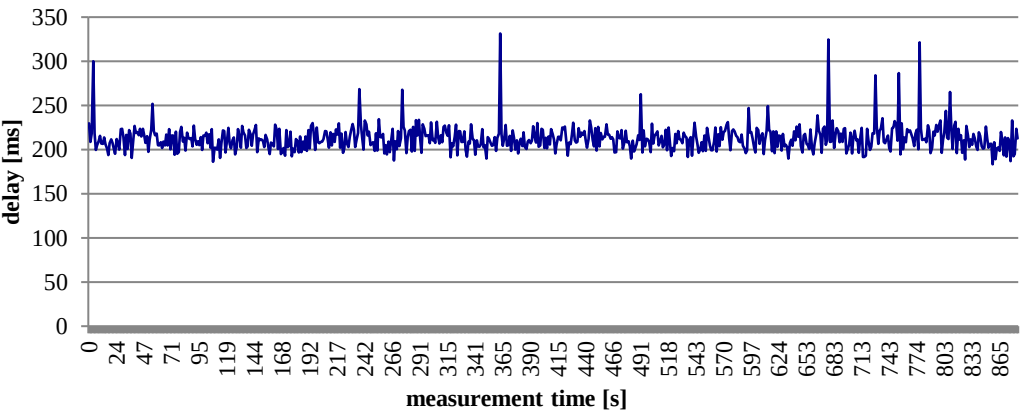


Fig. 7. Transmission delay relationship in the measurement time function for messages with a length of 10240 B (10 kB) encoded with the use of the AES CBC method

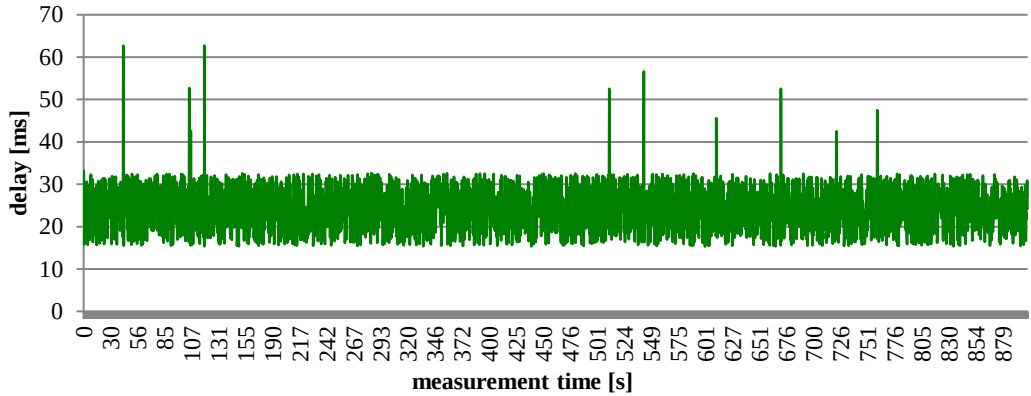


Fig. 8. Transmission delay relationship in the measurement time function for messages with a length of 16 B encoded with the use of the AES ECB method

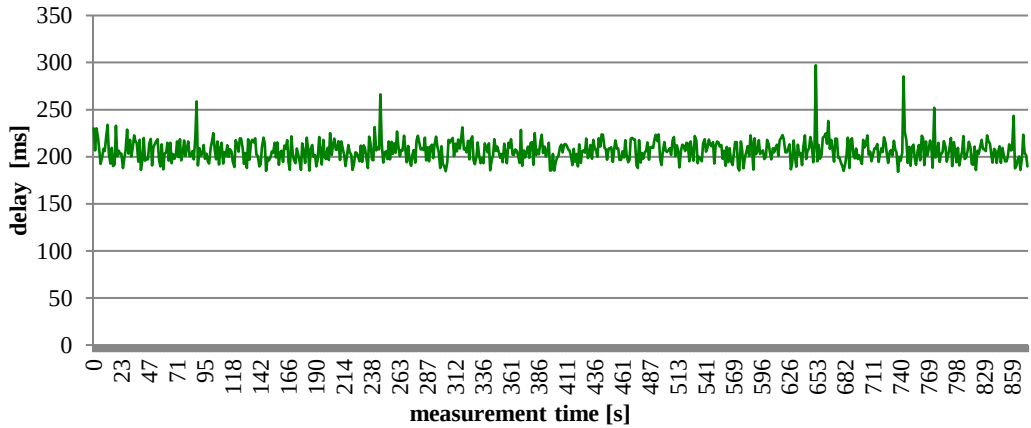


Fig. 9. Transmission delay relationship in the measurement time function for messages with a length of 10240 B (10 kB) encoded with the use of the AES ECB method

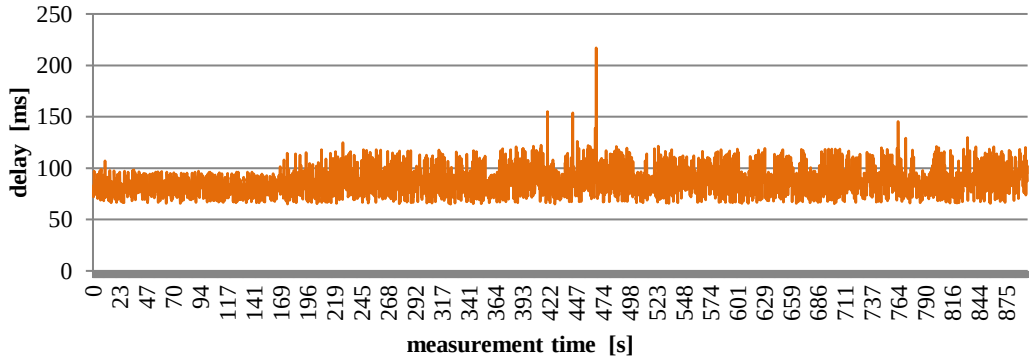


Fig. 10. Transmission delay relationship in the measurement time function for messages with a length of 16 B encoded with the use of the RES key with a length of 1024 bits

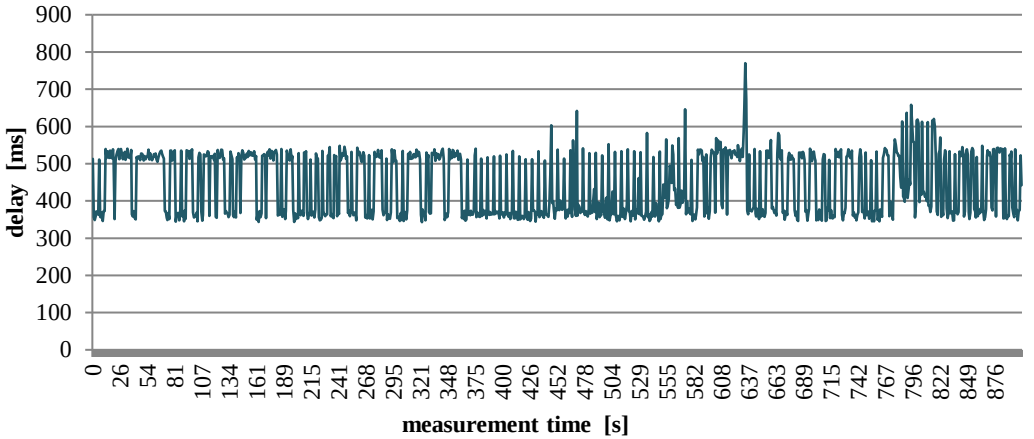


Fig. 11. Transmission delay relationship in the measurement time function for messages with a length of 16 B encoded with the use of the RES key with a length of 2048 bits

Table 1. The comparison of the transmission delay of messages with variable lengths in the range of 16B – 10kB with different ways of encoding

| Message Length [B] | Average delay $\bar{x}$ [ms] | | | | | |
|---|---|---|---|---|---|---|
| | AES CBC | | AES ECB | | DES CBC | |
| | $\bar{x}$ | σ | $\bar{x}$ | σ | $\bar{x}$ | σ |
| 16 | 24,011 | 5,096 | 24,195 | 5,201 | 24,012 | 5,120 |
| 32 | 26,063 | 4,609 | 24,104 | 5,332 | 26,172 | 4,514 |
| 64 | 26,954 | 4,887 | 26,350 | 4,558 | 26,787 | 4,930 |
| 128 | 27,691 | 5,168 | 27,932 | 5,243 | 27,695 | 5,494 |
| 256 | 29,978 | 6,160 | 29,910 | 6,099 | 29,966 | 6,232 |
| 512 | 32,712 | 6,846 | 33,168 | 6,746 | 32,559 | 7,115 |
| 1024 | 39,608 | 8,038 | 39,481 | 7,986 | 39,485 | 8,480 |
| 2048 | 49,966 | 9,807 | 49,478 | 9,937 | 49,884 | 10,020 |
| 4096 | 74,977 | 11,723 | 73,984 | 10,502 | 74,049 | 10,841 |
| 6144 | 107,533 | 12,958 | 107,186 | 10,761 | 111,451 | 15,415 |
| 8192 | 154,259 | 14,582 | 150,367 | 13,973 | 152,047 | 13,265 |
| 10240 | 212,673 | 14,689 | 206,338 | 11,823 | 209,598 | 15,073 |
| **Message Length [B]** | **AES CBC** | | **AES ECB** | | **DES CBC** | |
| | $\bar{x}$ | σ | $\bar{x}$ | σ | $\bar{x}$ | σ |
| 16 | 24,189 | 5,346 | 87,421 | 13,717 | 441,881 | 83,783 |
| 32 | 26,246 | 4,529 | 93,372 | 16,359 | 474,947 | 84,147 |
| 64 | 27,072 | 5,072 | 94,426 | 15,518 | 476,346 | 86,334 |
| 128 | 27,839 | 5,285 | not tested | --- | not tested | --- |
| 256 | 29,994 | 6,302 | not tested | --- | not tested | --- |
| 512 | 32,968 | 7,051 | not tested | --- | not tested | --- |
| 1024 | 39,730 | 8,474 | not tested | --- | not tested | --- |
| 2048 | 49,459 | 10,277 | not tested | --- | not tested | --- |
| 4096 | 73,761 | 12,692 | not tested | --- | not tested | --- |
| 6144 | 108,728 | 13,585 | not tested | --- | not tested | --- |
| 8192 | 150,715 | 15,626 | not tested | --- | not tested | --- |
| 10240 | 207,205 | 14,070 | not tested | --- | not tested | --- |

The comparison of average values of the transmission delays with different methods of the message encoding with lengths from 16B to 10kB was presented in Fig. 12 and 13.
In case of the messages with a length of 16 B, the LTE network parameters has the greatest impact on the delay, however, in case of the messages with a length of 10 kB, the message encoding and decoding time has the greatest impact on the transmission delay.
Histograms of the size of absolute transmission delays for the AES-CBC encoding, for various sizes of data of the message sent by the LTE open system for 16B and 10kB were presented in Fig. 14 and 16, however, Figures 15 and 17 presented a step function of the $F_n(x)$ transmission delay frequency, where: $F_n(x)$ – empirical distribution function from the formula (6).
Similar results were obtained for other encodings: AES-ECB, DES-CBC and DES-ECB.
The above histograms (Fig. 14 and 16) presented the size of the transmission delays, and the above step functions (Fig. 15 and 17) presented the delay frequency with transmission with the use of a symmetric block cipher. Figure 18 and Figure 20 presented the transmission delay histograms with the message size of 16B, and Fig. 19 and 21 presented the transmission delay step functions with the use of an asymmetric cryptographic algorithm with a RSA public key.

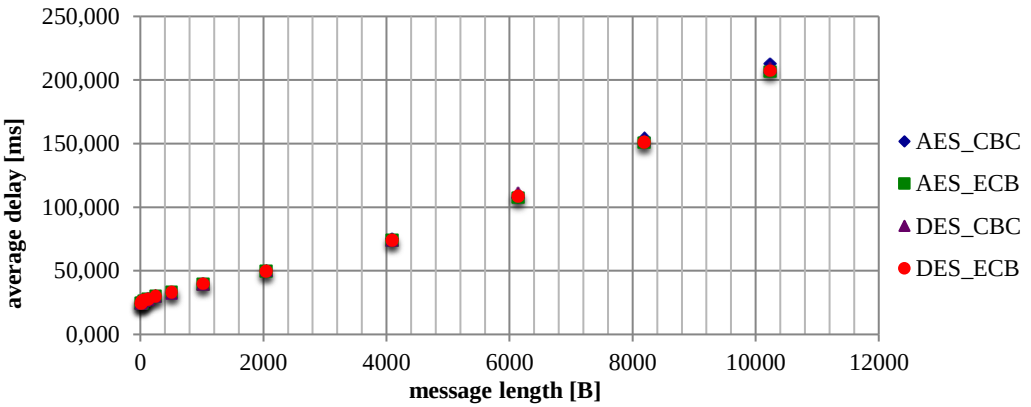


Fig. 12. The comparison of average values of the transmission delays with different encoding methods of the messages with lengths within the range of 16B – 10kB

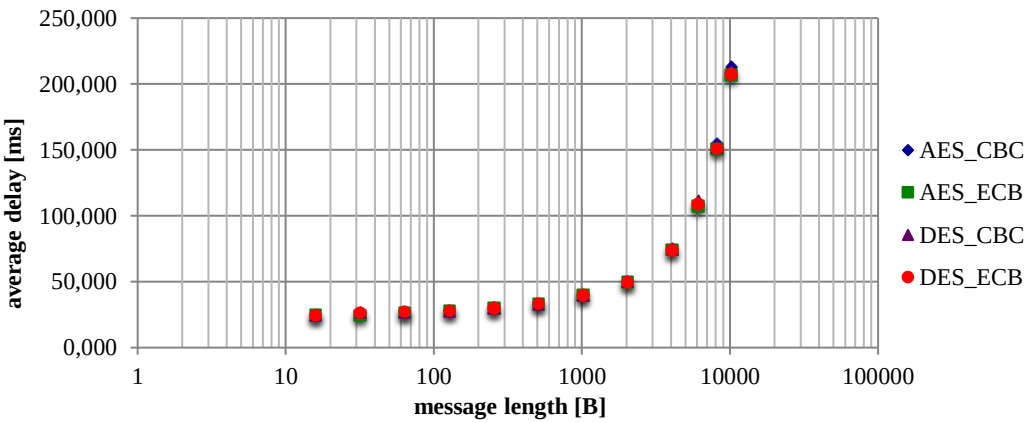


Fig. 13. The comparison of average values of the transmission delays with different encoding methods of the messages with lengths within the range of 16B – 10kB (logarithmic scale)

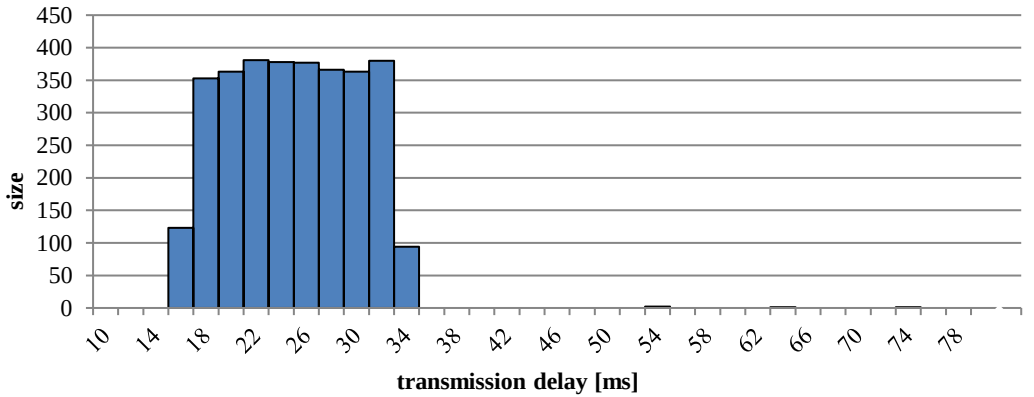


Fig. 14. Histogram of the absolute size of the AES-CBC transmission delays for the 16B message

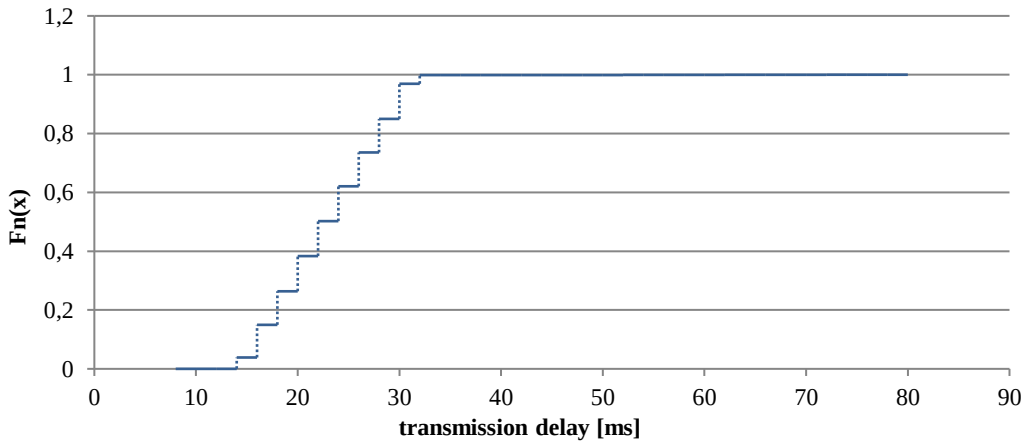


Fig. 15. Step function of the AES-CBC 16B transmission delay frequency

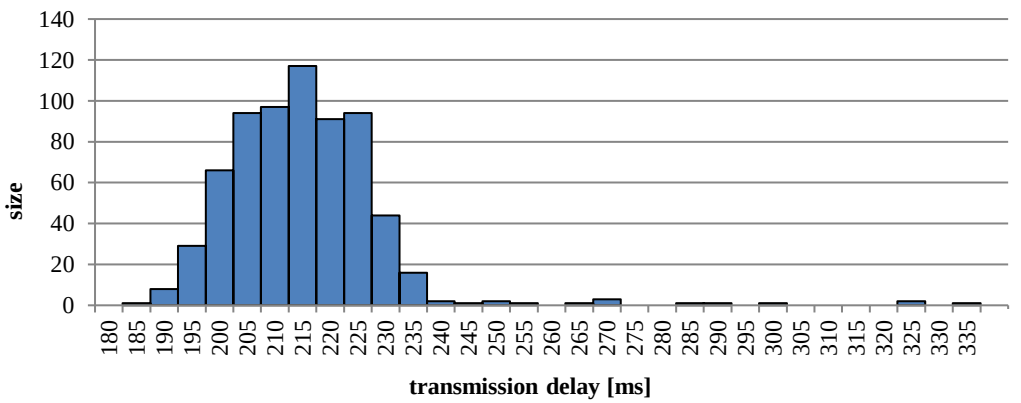


Fig. 16. Histogram of the absolute size of the AES-CBC transmission delays for the 10kB message

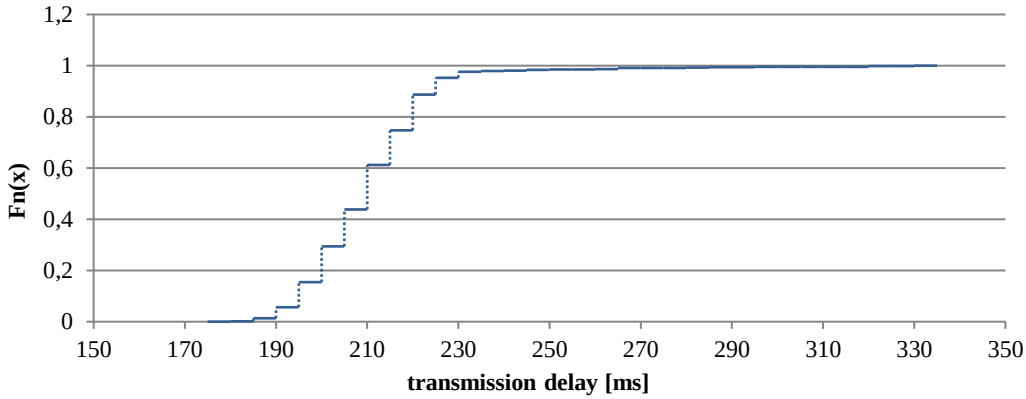


Fig. 17. Step function of the AES-CBC 10kB transmission delay frequency

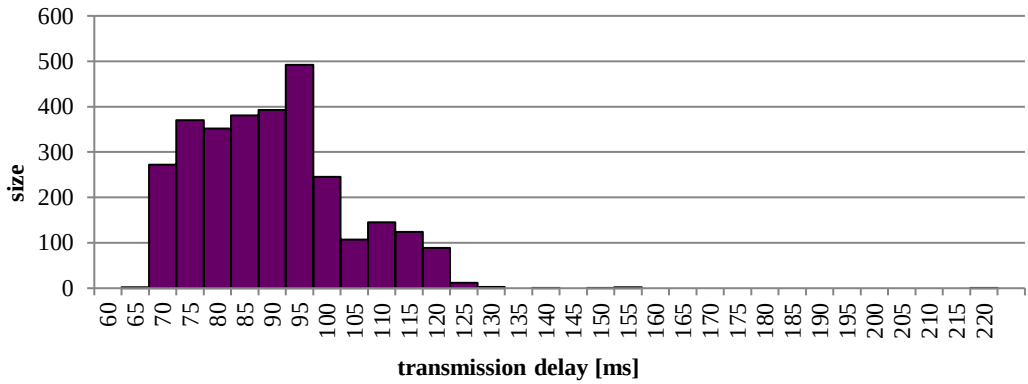


Fig. 18. Histogram of the absolute size of the transmission delays with a 1024-bit RSA key for the message with a size of 16B

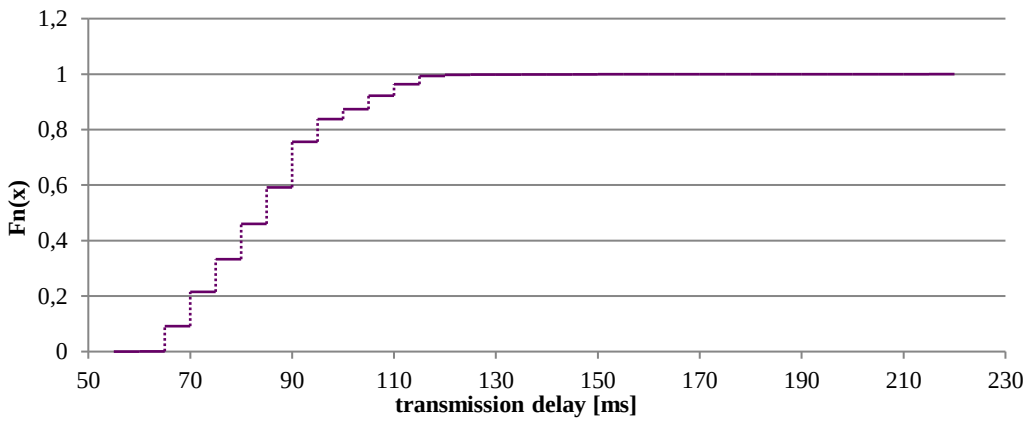


Fig. 19. Step function of the transmission delay frequency with a 1024-bit RSA key for the message with a size of 16B

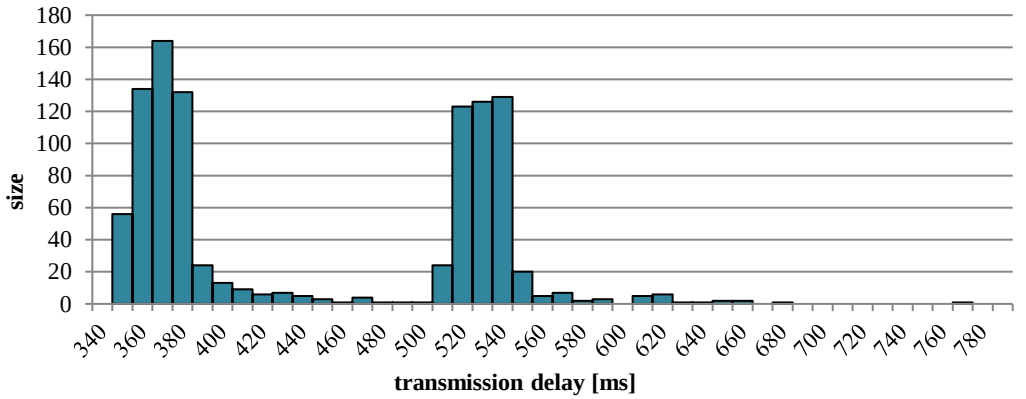


Fig. 20. Histogram of the absolute size of the transmission delays with a 2048-bit RSA key for the message with a size of 16B

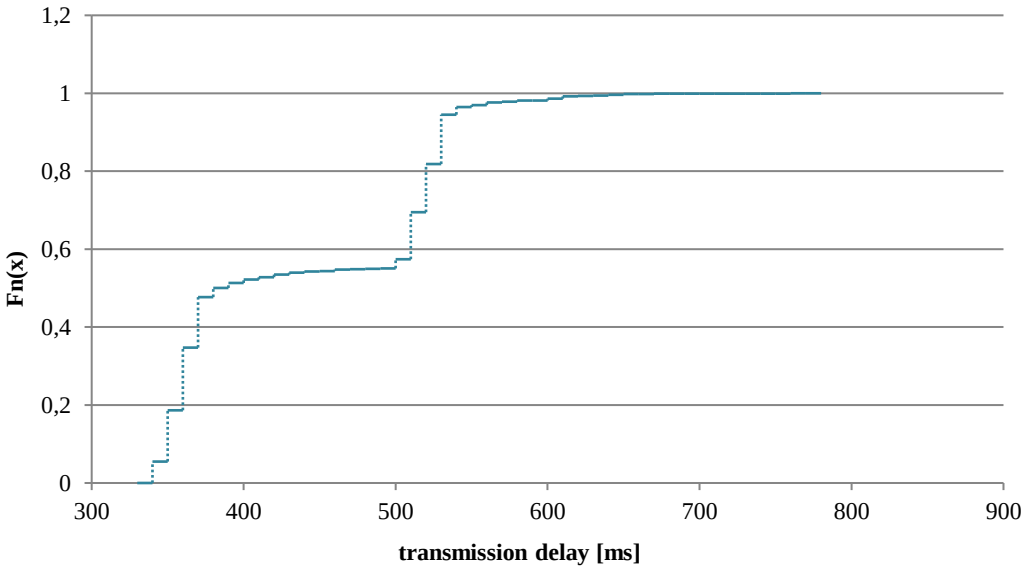


Fig. 21. Step function of the transmission delay frequency with a 1024-bit RSA key for the message with a size of 16B

The probability distribution of the transmission delay can be described by the density function (1):

$$f(x) = \begin{cases} 0 & ,x < a \\ p_1 \dfrac{2(x-a)}{(b-a)^2} & ,x \in [a,b] \\ p_2 \dfrac{1}{c-b} & ,x \in (b,c] \\ p_3 \lambda e^{-\lambda(x-c)} & ,x > c \end{cases} \quad (1)$$

where:

$$p_i > 0, \ \sum p_i = 1, \lambda > 0$$

and it is a convex combination (mixture) of three probability distributions [Rogowski, 2012]:

– triangular distribution,
– uniform distribution,
– exponential shifted distribution,

where:
it is assumed that $x_1$, $x_2$, ..., $x_n$ is a simple sample, $n_1$ is the number of elements in the sample less than b, $n_2$ is the number of elements in the sample greater than *c*. Then:

$$a = \min_{i=1,\dots,n} x_i - \varepsilon$$

$$p_1 = \frac{n_1}{n}$$

$$p_3 = \frac{n_2}{n}$$

$$p_2 = 1 - p_1 - p_3$$

$$\lambda = \frac{n_2}{\sum_{x_i > c} x_i - c \cdot n_2}$$

If we do not apply the Anderson – Darling test, then $\varepsilon = 0$, otherwise, $\varepsilon$ is a possibly small number, at which there is a value ln $F(x_0)$, where:

$$x_0 = \min_{i=1,\dots,n} x_i,$$

$F(x)$ is a distribution function of the rectangular triangular distribution (2):

$$(x) = \begin{cases} 0 & ,x < a \\ \dfrac{(x-a)^2}{(b-a)^2} & ,x \in [a,b] \\ 1 & ,x \geq b \end{cases} \quad (2)$$

The values *b* and *c* are selected ("trial and error" method) so as to minimise the value of the test statistics. It can be initially adopted that *a* is equal to a quantile of 0.01 of the sample, and *b* is equal to a quantile of 0.98 of the sample. In case of using the Anderson – Darling test, the estimation of *a* and *b* cannot constitute the values belonging to the sample (Fig. 22), where: The random variable has a triangular distribution in the section [*A, B*], in which *A*<*B* and with a vertex *C*, where $-\infty < A \leq C \leq B < \infty$, if the probability distribution density $g_1(x)$ is determined by the formula:

$$g_1(x) = \begin{cases} 0 & ,x \notin (A,B) \\ \dfrac{2(x-A)}{(B-A)(C-A)} & ,x \in (A,C] \\ \dfrac{-2(x-B)}{(B-A)(B-C)} & ,x \in (C,B) \end{cases} \quad (3)$$

The random variable has a uniform (rectangular, even) distribution in the section [*A, B*], in which $-\infty < A < B < \infty$, if the probability distribution density $g_2(x)$ is determined by the formula:

$$g_2(x) = \begin{cases} \dfrac{1}{B-A}, x \in [A,B] \\ 0 \quad ,x \notin [A,B] \end{cases} \quad (4)$$

The random variable has a exponential shifted distribution, if the probability distribution density $g_3(x)$ is determined by the formula:

$$g_3(x) = \begin{cases} 0 & ,x \leq D, \\ \lambda e^{-\lambda(x-D)}, & x > D, \lambda > 0, \lambda = const, D > 0 \end{cases} \quad (5)$$

where: *D* – distribution shift
In order to determine the distribution compliance with a given model distribution, the tests were used for continuous distributions:

– λ Kolmogorov, in which the test statistics is described by the following formula:

$$\lambda = \sqrt{n} D_n \qquad D_n = sup_{-\infty < x < \infty} |F_n(x) - F(x)|$$

where:
λ – Kolmogorov statistics,
$D_n$ – test statistics,
*n* – sample size
$F_n(x)$ – empirical distribution function of the step function
$F(x)$ – distribution function of the distribution in the presented null (hypothetical) hypothesis, where – for the formula:

$$F(x) = \int_{-\infty}^{x} f(t)dt \quad (6)$$

– Cramer – von Mises, in which the test statistics is described using the formula [Rogowski, 2012]:

$$W^2 = \frac{1}{12n} + \sum_{i=1}^{n} \left( F(X_i) - \frac{2i-1}{2n} \right)^2 \quad (7)$$

where:
$X_i$ – *i* observed value in the value arranged in an ascending order

$F(x)$ – distribution function of the continuous distribution
$n$ – sample size

– Watson, in which the test statistics is described by the following formula:

$$U^2 = \frac{1}{12n} + \sum_{i=1}^{n}\left(F(X_i) - \frac{2i-1}{2n}\right)^2 - n\left(\left(\frac{1}{n}\sum_{i=1}^{n}F(X_i)\right) - 0{,}5\right) = = W^2 - n\left(\left(\frac{1}{n}\sum_{i=1}^{n}F(X_i)\right) - 0{,}5\right) \quad (8)$$

where:
$X_i$ – $i$ observed value in the value arranged in an ascending order
$F(x)$ – distribution function of the continuous distribution
$n$ – sample size

– Anderson – Darling, in which the test statistics is described by the following formula:

$$A^2 = -n - \frac{1}{n}\sum_{i=1}^{n}(2i-1)\left[\ln F(X_i) + \ln\left(1 - F(X_{n+1-i})\right)\right] \quad (9)$$

The critical values for individual tests of significance used for testing the empirical distribution compliance with the assumed one were given in Table 2.

On the basis of the formula (1) and significance tests, the distribution parameters of the probability density function of the transmission delay distribution with the message sizes in the range from 16 B to 10 Kb with four ways of the signal encoding, presented in Tables 3 – 6, were obtained.

The probability distribution density function parameters for AES-CBC encoding were provided in Table 3.

Based on Table 3, the test values indicate that at the significance level of α=0.05, there is no grounds for rejecting the hypothesis for λ Kolmogorov, Cramer–von Mises and Anderson–Darling tests. This condition is not satisfied only with the message size of 4096B in the Watson test for the significance level from Table 2, and in the remaining three tests, the critical values of a given test are met.

By using the formula (1) and the probability distribution density function parameters of the transmission delay for AES-CBC encoding provided in Table 3, the graphic representation of this function, as shown in the sample diagrams 23 and 24 for 16 B and 10KB, were prepared.

The probability distribution density function parameters for AES-EBC encoding were provided in Table 4.

Based on Table 4, the test values indicate that at the significance level of α=0.05, there is no grounds for rejecting the hypothesis for Cramer–von Mises and Anderson–Darling tests. This condition is not satisfied only with the message size of 4096B in the Watson test, but it meets the critical values at the significance level of α=0.01. A similar situation occurs in the λ Kolmogorov test, where the condition at the significance level of α=0.025 is satisfied for the message size of 6kB.

The probability distribution density function parameters for DES-CBC encoding were provided in Table 5.

Based on Table 5, the test values indicate that at the significance level of α=0.05, there is no grounds for rejecting the hypothesis for λ Kolmo-gorov, Cramer–von Mises and Anderson–Darling tests. This condition is not satisfied only with the message size of 6kB in the Watson test at the significance level of α=0.05, but it is met at the significance level of $\alpha$=0.025.

The probability distribution density function parameters for DES-EBC encoding were provided in Table 6.

Based on Table 6, the test values indicate that at the significance level of α=0.05, there is no grounds for rejecting the hypothesis for Cramer–von Mises, Watson and Anderson–Darling tests. This condition is not satisfied only with the mes-sage size of 6kB in the λ Kolmogorov test at the significance level of α=0.05, but it is met at the significance level of α=0.025.

Figures 25 – 28 present the probability distribu-tion density function for the delay in the message transmission with the size of 16B with AES-CBC, AES-ECB, DES-CBC and DES-ECB encryption.

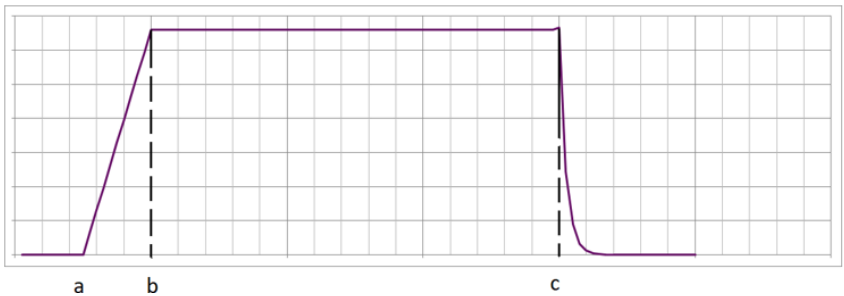

Fig. 22. Illustration of the designated probability distribution density function f(x)

Table 2. Critical values for tests of significance with a given significance level $\alpha$ [107]

| **Test** | **α = 0,15** | **α = 0,1** | **α = 0,05** | **α = 0,025** | **α = 0,01** |
|---|---|---|---|---|---|
| λ Kołmogorowa | 1,13 | 1,22 | 1,35 | 1,48 | 1,63 |
| Cramera-von Misesa | 0,28406 | 0,3473 | 0,46136 | 0,58061 | 0,74346 |
| Andersona-Darlinga | | 1,933 | 2,492 | 3.070 | 3,857 |
| Watsona | 0,1312 | 0,15176 | 0,18688 | 0,222 | 0,26842 |

Table 3. Estimation of the probability distribution density function parameters (1) of the transmis-sion delay for AES-CBC encoding and the values of the applied compliance tests

| **B** | **p1** | **p2** | **p3** | **a** | **b** | **c** | **λ** | **Kołmogorowa** | **Cramera-von Misesa** | **Watsona** | **Andersona-Darlinga** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **16** | 0,004 | 0,994 | 0,002 | 15,0 | 13,36 | 32,5 | 0,063332 | 0,797958 | 0,086081017 | 0,044133 | 0,551973 |
| **32** | 0,013 | 0,982 | 0,005 | 18,43 | 18,75 | 33,43 | 0,269067 | 1,082068 | 0,24784024 | 0,116469 | 1,489447 |
| **64** | 0,003 | 0,993 | 0,004 | 18,55 | 18,87 | 35,0 | 0,065713 | 0,958642 | 0,11892971 | 0,089907 | 1,743776 |
| **128** | 0,004 | 0,995 | 0,001 | 18,79 | 19,1 | 36,0 | 0,167498 | 0,541768 | 0,05702398 | 0,049756 | 0,467304 |
| **256** | 0,003 | 0,989 | 0,008 | 19,27 | 19,63 | 39,9 | 0,099524 | 0,716028 | 0,13016827 | 0,092909 | 1,235739 |
| **512** | 0,018 | 0,977 | 0,005 | 20,29 | 22 | 43,2 | 0,201427 | 0,677301 | 0,06953514 | 0,040781 | 0,647521 |
| **1024** | 0,052 | 0,921 | 0,027 | 23,5 | 27,4 | 52,51 | 0,287764 | 0,750045 | 0,08322517 | 0,073557 | 0,725571 |
| **2048** | 0,027 | 0,956 | 0,017 | 32,0 | 34,5 | 66,0 | 0,095229 | 1,041422 | 0,25017683 | 0,150875 | 2,052405 |
| **4096** | 0,036 | 0,871 | 0,093 | 54,0 | 57,9 | 88,35 | 0,103504 | 1,065766 | 0,35275153 | 0,344052 | 2,061448 |
| **6144** | 0,036 | 0,915 | 0,049 | 85,6 | 90,8 | 122,8 | 0,053465 | 1,308153 | 0,25727716 | 0,183546 | 1,837507 |
| **8192** | 0,07 | 0,845 | 0,085 | 130,1 | 138,8 | 167,2 | 0,082021 | 1,086976 | 0,2371365 | 0,214683 | 2,15533 |
| **10240** | 0,235 | 0,633 | 0,132 | 183,2 | 203 | 223,8 | 0,082021 | 0,923394 | 0,11980214 | 0,118611 | 1,692118 |

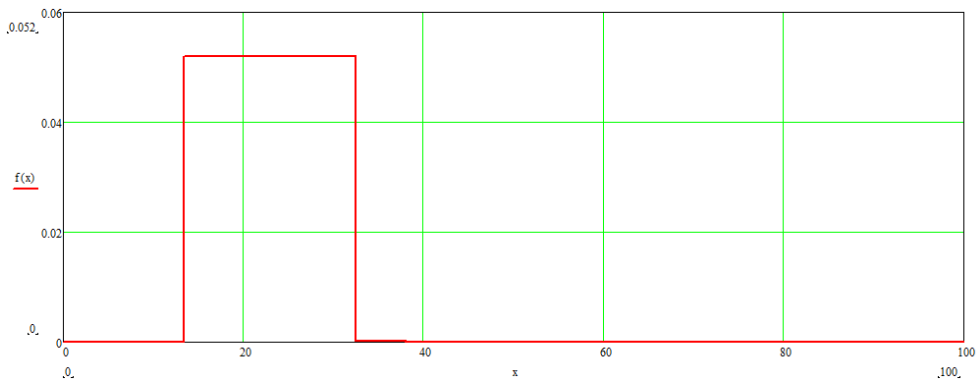

Fig. 23. Probability distribution density function of the transmission delay with the message size of 16B

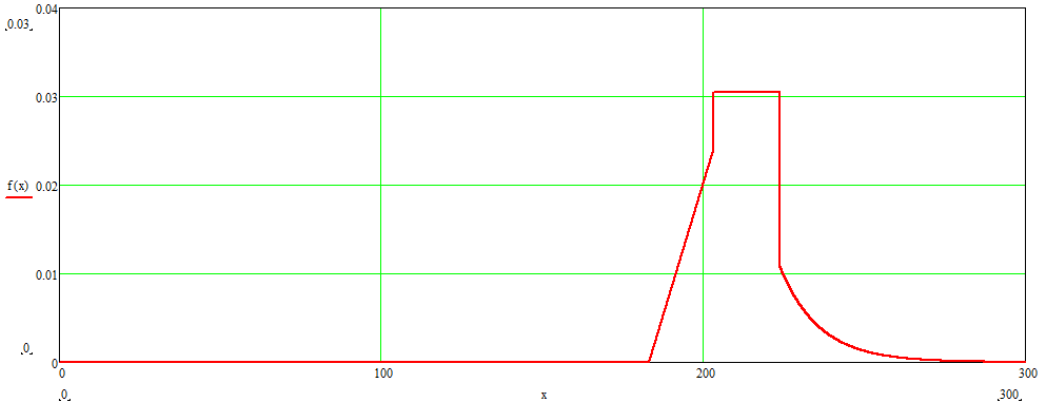


Fig. 24. Probability distribution density function of the transmission delay with the message size of 10kB

Table 4. Estimation of the probability distribution density function parameters (1) of the trans-mission delay for AES-EBC encoding and the values of the applied compliance tests

| B | p1 | p2 | p3 | a | b | c | λ | Kolmogorowa | Cramera-von Misesa | Watsona | Andersona-Darlinga |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **16** | 0,004 | 0,993 | 0,003 | 15,11 | 13,97 | 32,82 | 0,067154 | 0,798123 | 0,08523721 | 0,042109 | 0,523798 |
| **32** | 0,008 | 0,988 | 0,004 | 16,36 | 15,57 | 33,02 | 0,199112 | 1,109473 | 0,18973762 | 0,100158 | 1,349812 |
| **64** | 0,003 | 0,992 | 0,005 | 18,01 | 18,68 | 34,09 | 0,072398 | 0,917532 | 0,12866113 | 0,088544 | 1,432561 |
| **128** | 0,005 | 0,992 | 0,003 | 18,82 | 19,31 | 37,03 | 0,168239 | 0,576352 | 0,09983471 | 0,065382 | 0,673219 |
| **256** | 0,004 | 0,989 | 0,007 | 19,02 | 19,67 | 39,95 | 0,100065 | 0,778524 | 0,12376988 | 0,094479 | 1,198724 |
| **512** | 0,016 | 0,980 | 0,004 | 21,34 | 22,67 | 43,16 | 0,227351 | 0,694362 | 0,07398733 | 0,050004 | 0,653215 |
| **1024** | 0,050 | 0,925 | 0,025 | 24,05 | 28,33 | 51,06 | 0,296542 | 0,786541 | 0,09863288 | 0,088524 | 0,768271 |
| **2048** | 0,028 | 0,954 | 0,018 | 33,20 | 34,88 | 67,08 | 0,105292 | 1,076622 | 0,25998534 | 0,176545 | 1,986505 |
| **4096** | 0,034 | 0,887 | 0,079 | 55,05 | 58,8 | 87,54 | 0,108723 | 1,076212 | 0,37235166 | 0,244146 | 2,087655 |
| **6144** | 0,035 | 0,928 | 0,037 | 87,03 | 92,65 | 126,8 | 0,066563 | 1,421111 | 0,26877862 | 0,177621 | 1,910872 |
| **8192** | 0,068 | 0,849 | 0,083 | 128,2 | 139,9 | 169,2 | 0,087219 | 1,070909 | 0,24444718 | 0,217685 | 2,355633 |
| **10240** | 0,225 | 0,645 | 0,130 | 184,2 | 202,1 | 224,9 | 0,088534 | 0,976251 | 0,12398113 | 0,120004 | 1,691187 |

Table 5. Estimation of the probability distribution density function parameters (1) of the transmis-sion delay for DES-CBC encoding and the values of the applied compliance tests

| B | p1 | p2 | p3 | a | b | c | λ | Kolmogorowa | Cramera-von Misesa | Watsona | Andersona-Darlinga |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **16** | 0,004 | 0,993 | 0,003 | 15,54 | 13,55 | 32,11 | 0,098655 | 0,862132 | 0,09542711 | 0,039876 | 0,598676 |
| **32** | 0,011 | 0,984 | 0,005 | 18,33 | 18,66 | 32,98 | 0,269765 | 1,091102 | 0,25561223 | 0,122762 | 1,499912 |
| **64** | 0,004 | 0,994 | 0,002 | 18,29 | 18,98 | 34,98 | 0,070021 | 0,948731 | 0,12008111 | 0,092221 | 1,788833 |
| **128** | 0,004 | 0,993 | 0,003 | 18,99 | 19,14 | 37,08 | 0,167788 | 0,555213 | 0,05903282 | 0,055676 | 0,497876 |
| **256** | 0,005 | 0,986 | 0,009 | 19,57 | 19,98 | 40,02 | 0,109544 | 0,722372 | 0,15567227 | 0,098762 | 1,276389 |
| **512** | 0,020 | 0,972 | 0,008 | 20,18 | 22,98 | 43,97 | 0,233421 | 0,687867 | 0,07002243 | 0,047565 | 0,677877 |
| **1024** | 0,048 | 0,917 | 0,035 | 23,14 | 27,76 | 53,55 | 0,302872 | 0,788778 | 0,11008998 | 0,087676 | 0,701123 |
| **2048** | 0,026 | 0,955 | 0,019 | 32,32 | 35,68 | 68,98 | 0,105228 | 1,055611 | 0,26233483 | 0,166671 | 2,077775 |
| **4096** | 0,030 | 0,881 | 0,089 | 53,05 | 59,7 | 90,32 | 0,104504 | 1,076321 | 0,35779879 | 0,355525 | 2,222761 |
| **6144** | 0,032 | 0,917 | 0,051 | 87,77 | 92,7 | 125,7 | 0,067535 | 1,344651 | 0,27762973 | 0,199987 | 1,889897 |
| **8192** | 0,075 | 0,845 | 0,080 | 133,2 | 139,8 | 169,3 | 0,092024 | 1,086999 | 0,25671365 | 0,284663 | 2,455533 |
| **10240** | 0,242 | 0,612 | 0,146 | 183,1 | 205,3 | 226,7 | 0,102034 | 0,998622 | 0,13280614 | 0,165619 | 1,872116 |

Table 6. Estimation of the probability distribution density function parameters (1) of the transmis-sion delay for DES-EBC encoding and the values of the applied compliance tests

| B | p1 | p2 | p3 | a | b | c | λ | Kolmogorowa | Cramera-von Misesa | Watsona | Andersona-Darlinga |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **16** | 0,004 | 0,992 | 0,004 | 14,98 | 13,32 | 32,71 | 0,076332 | 0,808081 | 0,08987651 | 0,065398 | 0,597968 |
| **32** | 0,012 | 0,984 | 0,004 | 18,53 | 18,84 | 33,54 | 0,257878 | 0,990677 | 0,22784065 | 0,109467 | 1,429453 |
| **64** | 0,005 | 0,989 | 0,006 | 18,95 | 19,52 | 36,33 | 0,078278 | 0,998783 | 0,13764171 | 0,109247 | 1,888664 |
| **128** | 0,004 | 0,993 | 0,003 | 18,88 | 19,57 | 36,47 | 0,188898 | 0,596578 | 0,07223644 | 0,062886 | 0,501305 |
| **256** | 0,006 | 0,987 | 0,007 | 19,28 | 19,67 | 39,95 | 0,109523 | 0,722278 | 0,15556827 | 0,102911 | 1,455736 |
| **512** | 0,017 | 0,975 | 0,008 | 20,88 | 24,03 | 47,34 | 0,276627 | 0,875432 | 0,10753533 | 0,055782 | 0,666681 |
| **1024** | 0,050 | 0,920 | 0,030 | 25,11 | 27,99 | 54,89 | 0,327765 | 0,777005 | 0,10322533 | 0,081555 | 0,743478 |
| **2048** | 0,049 | 0,923 | 0,028 | 32,76 | 36,55 | 69,44 | 0,111129 | 1,231456 | 0,28723871 | 0,203454 | 1,872405 |
| **4096** | 0,035 | 0,866 | 0,099 | 55,00 | 59,11 | 90,57 | 0,123405 | 1,115733 | 0,33335883 | 0,377652 | 2,224454 |
| **6144** | 0,036 | 0,913 | 0,051 | 86,61 | 91,9 | 127,8 | 0,074965 | 1,446792 | 0,28887712 | 0,189877 | 1,899701 |
| **8192** | 0,081 | 0,831 | 0,088 | 135,5 | 142,2 | 172,8 | 0,099234 | 1,208697 | 0,23333548 | 0,245634 | 2,457398 |
| **10240** | 0,222 | 0,639 | 0,139 | 181,5 | 201,3 | 224,5 | 0,082231 | 0,956396 | 0,19876212 | 0,123455 | 1,998127 |

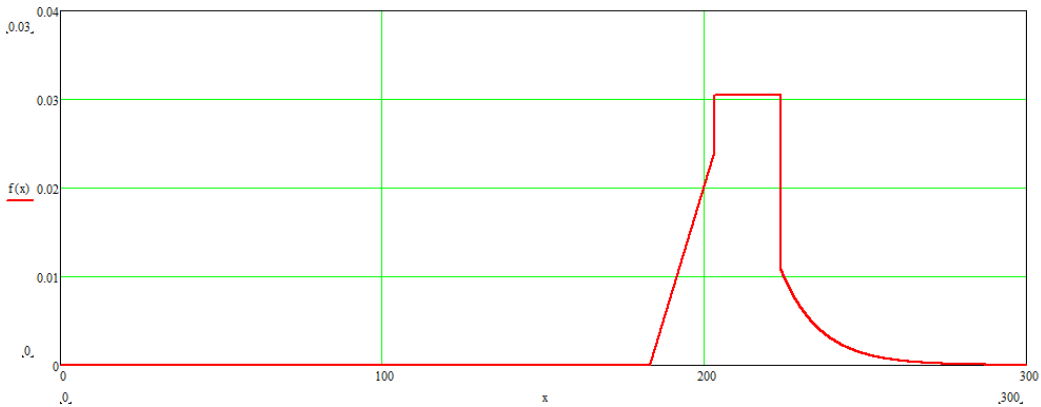


Fig. 25. Probability distribution density function of the transmission delay with the message size of 16B – AES-CBC encoding

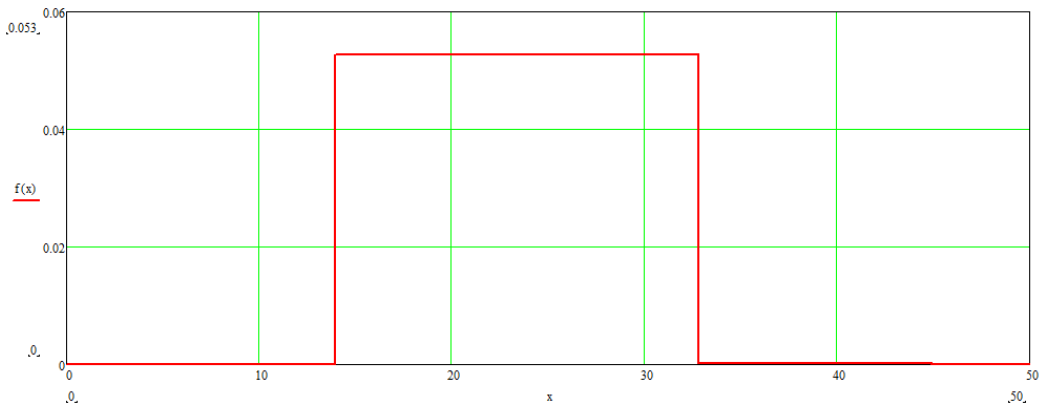


Fig. 26. Probability distribution density function of the transmission delay with the message size of 16B – AES-EBC encoding

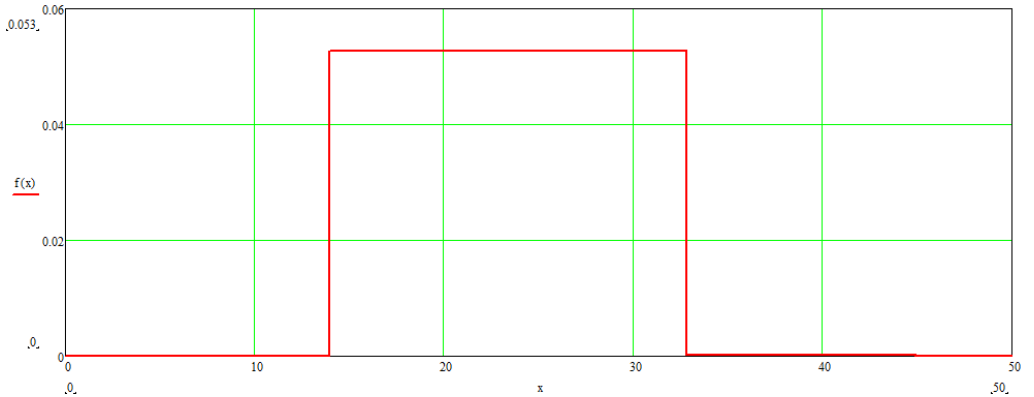


Fig. 27. Probability distribution density function of the transmission delay with the message size of 16B – DES-CBC encoding

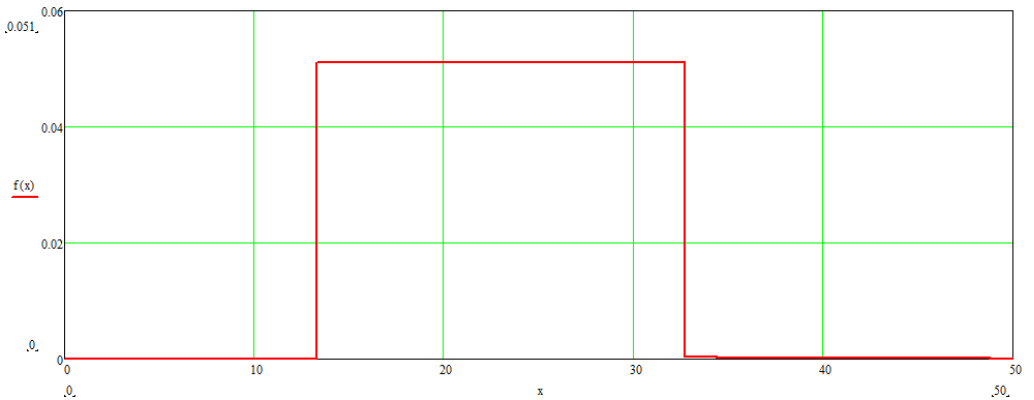


Fig. 28. Probability distribution density function of the transmission delay with the message size of 16B – DES-ECB encoding

On the basis of the data analysis for all the message sizes and encoding methods, the parameters can be chosen in order to make them possible to be described with one distribution, which is a combination of triangular, rectangular (uniform) and exponential shifted distributions. On the basis of the carried-out significance tests, it can be concluded that the uniform distribution is particularly sensitive to the choice of ends of intervals (in the example 1 parameters *b* and *c*).

## 5. Conclusion

The genesis of this article was to assess the possibility of using open, public data transmission mobile networks based on the LTE standard for the transmission of signals used for the rail traffic control, in order to support the existing GSM-R infrastructure. Furthermore, the use of the open systems also provides opportunities to reduce funding for the specialised ICT infrastructure creation for railway purposes and it can constitute a complement to the infrastructure of the rail traffic control devices.

Currently, in the rail traffic control, within the framework of the ERTMS system, it is possible to choose the GSM-R railway infrastructure and the LTE open system, which can be an important aspect at the moment of the GSM-R system operation completion, providing the continuity of operation of the ICT systems in rail traffic.

Based on the carried-out tests and mathematical methods, it can be concluded that with the small message sizes, in which the message transmission

time has the greatest impact on the delay, the probability distribution density function is a convex combination of three distribution types: triangular, uniform and exponential ones. In the current deliberations in the literature, regardless of the size of packages, the normal distribution was adopted.
In case of single kB telegrams, in which the message encoding time has the greatest impact on the transmission delay, the probability distribution density function may show the message encryption features, however, it was not studied in this article and remains as the topic open for further research.
As a result of the carried-out research, based on the assessment of the article authors, it is important to modify the existing PN-EN50159 standard in order to limit the availability of encoding algorithms, leave AES and remove DES because in case of small messages, as shown in Figures 1.12 and 1.13, the encryption does not affect the message transmission delay. Therefore, it is recommended to leave the algorithm with the best encryption effectiveness. The application of the RSA keys becomes useless due to long transmission delay times mostly resulting from the encryption method.

**References**

[1] Alemayehu, B., Gared, F., (2019). Inter cell interference modeling and analysis in long term evolution (LTE). *Ethiop. J. Sci. Technol.* 2019, 12, 107–123.
[2] Białoń, A., Gradowski, P., (2009). ERTMS European Rail Traffic Management System – part I. *Transports Infrastructure,* 4/2009, 14-17.
[3] Białoń, A., Gradowski, P., (2007). Rail traffic management system (ERTMS). *Telecommunications and Traffic Control,* 1/2007, 2-11.
[4] Bocanegra, C., Alemdar, K., Garcia, S., Singhal, Ch., and Kaushik, R., Chowdhury., (2019). NetBeam: Networked and Distributed 3-D Beamforming for Multi-user Heterogeneous Traffic. *In 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN). IEEE,* 1–10.
[5] Changqing, L., Hao, L., Hongli, Z., Shuo, W., Yong Z., (2020). LTE-U based Train to Train Communication System in CBTC: System Desin and Reliability Analysis. Wireless Communications and Mobile Computing. DOI: 10.1155/2020/8893631.
[6] Chrzan, M., (2021). Study of the possibility of using transmission in the LTE system on a selected railway line for the purpose of running railway traffic. *Archives of Transport,* 57(1), 91-101. DOI: 10.5604/01.3001.0015.8150.
[7] Chrzan, M., (2020). The Assessment of the Pos-sibility of Using Open Systems of Radio Trans-mission for the Purposes of Railway Transport. *ICTE in Transportation and Logistics 2019, Springer Nature Switzerland* 2020, 271-278.
[8] Chrzan, M., Kornaszewski, M., Ciszewski, T., (2018). Renovation of Marine Telematics Objects in the Process of Exploitation" *In: Communications in Computer and Information Science, Springer* 2018, 45-56.
[9] Gago, S., Siergiejczyk, M., (2020). Premises for Developing an IT Network Design for Railway Transport in Poland. *Advances in Intelligent Systems and Computing,* 1032, 115–123. DOI: 10.1007/978-3-030-27687-4_12.
[10] Garcia, J., Sundberg, S., Brunstrom, A., (2019). LTE for Trains - Performance Interactions Examined with DL, ML and Resampling. *Conference: International Workshop on Machine Learning for Wireless Communications. Barcelona, Spain.* DOI: 10.1109/ISCC47284.2019.8969727.
[11] Jacyna, M., Szczepański, E., Izdebski, M., Jasiński, S., Maciejewski, M., (2018). Characteristics of event recorders in automatic train control systems. *Archives of Transport,* 46(2), 61-70.
[12] Jian, L., (2019). Research on the new generation urban rail transit signal system. *Urban Rail Transit Research,* 22(7), 71–74.
[13] Karthika, S., Indumathi, P., (2020). Analysis of Dynamic Frequency Reuse Techniques in LTE-A Cellular Network. *In IOP Conference Series: Materials Science and Engineering; IOP Publishing: Bristol,* UK, 2020; 994, 012034.
[14] Kornaszewski, M., Chrzan, M., Olczykowski, Z., (2017). Implementation of New Solutions of Intelligent Transport Systems in Railway Transport in Poland. *In. J. Mikulski (Eds.), Smart Solutions in Today's Transport. TST 2017. Communications in Computer and Information Science, Cham Springer,* 715, 282–290.

[15] Kukulski, J., Gołębiowski, P., Pyza, D., Jachimowski, R., Wychowański, W., (2019). Selected aspects of the selection of data sent to the vehicle in automatic rail vehicle driving systems. *Scientific Journal of Silesian University of Technology. Series Transport*, 103, 43 -52.

[16] Kunai, B., (2019). Research on Wireless Resource and Mobility Management of LTE-U System in Urban Rail Transit. *Beijing Jiaotong University.*

[17] Pawlik, M.; Siergiejczyk, M.; Gago, S., (2017). European rail transport management system mobile transmission safety analysis. *In Risk, Reliability and Safety: Innovating Theory and Practice;* Walls, L., Revie, M., Bedford, T., Eds.; CRC Press: London, UK, 2017; 1791–1794.

[18] Rogowski, A., (2012). *Fundamentals of probabilistic methods in transport.* Monography. Kazimierz Pulaski University of Technology and Humanities in Radom.

[19] Rosberg, T., Cavalcanti, T., Thorslund, B., Prytz, E., & Moertl, P., (2021). Driveability analysis of the european rail transport management system (ERTMS). *Journal of Rail Transport Planning and Management,* 18. https://doi.org/10.1016/j.jrtpm.2021.100240.

[20] Shirly, E., Malarvizhi, S., (2020).Architectural implementation of modified K-best algorithm for detection in MIMO systems. *Mikroprocessors and Microsystems,* 74. DOI: 10.1016/j.micpro.2020.103010.

[21] Siergiejczyk, M., Rosiński A., (2019). Analysis of information transmission security in the digital railway radio communication system. Contemporary Complex Systems and Their Dependability. *Proceedings of the Thirteenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX / Zamojski Wojciech [et al.] (Eds.), Advances in Intelligent Systems and Computing*, 761, 420-429.

[22] Toruń, A., Sokołowska, L., Jacyna, M., (2019). Communications-based train control system - Concept based on WiFi LAN network. *Transport Means - Proceedings of the 23 -rd International Conference. Kaunas University of Technology.* 911 -915.

[23] Wu, Y., McAllister, J., (2017). Bounded Selective Spanning With Extended Fast Enumeration for MIMO-OFDM Systems Detection. *IEEE Trans. Circ. Syst.* 64 (9)(2017) 2556–2568.

[24] PN-EN 50129:2011. (n.d.). PN-EN 50129:2011—Railway Applications—Communication, Signalling and Processing Systems—Safety.

[25] 3GPP Specifications, TS 36-series, Release 99 and later. (2020). *http://www.3g org/specifications/specification-numbering.*