Journal of Theoretical and Applied Information Technology
31st March 2020. Vol.98. No 06

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RADIO COMMUNICATION CHANNEL INTERACTION METHOD, MAINTAINING TRAIN PERFORMANCE INFORMATION SECURITY

[1] SANSYZBAY K.M., [1] BAKHTIYAROVA YE.A., [1] KUANDYKOV A.A., [2] VLASENKO S.V. MAMYRBAYEV O. ZH.

[1] International university of information technologies, Almaty, Kazakhstan

[2] Berlin technical university, Berlin, Germany

[3] Institute of Information and Computational Technologies, Almaty, Kazakhstan

E-mail: [1]kanibek@list.ru, [1]baelag@mail.ru, [1]abu.kuandykov@mail.ru, [2]vlassenko2000@mail.ru, [3] morkenj@mail.ru

ABSTRACT

The work herein considers the principles of radio communication channel data transfer, aims of information security maintenance as well as threats when transmitting information over a radio channel. For experimental determination of the data on channel capacity, batches transit time, data on batches loss in radio net there have been carried out the experiments of interaction with a train along the digital communication channel with account of requirements to information security. Conducted experiments show, that at any size of the batch in the standard digital radio communication system upon increasing the load on the system, the batches transit time is increased. By means of the experiment it has been proved, that the system meets the requirements to batches transit time with the transfer rate up to 1,4 Kbit /s. Starting from the load 1,6-2,0 Kbit /s the batches transit time becomes unacceptably big and simultaneously with that, the lost batches percentage grows. The issues of communication between the radio block center and the TETRA switching center, linking the radio block center with electrical centralization systems, upgrading the locomotive's onboard equipment, and checking the operation algorithms of onboard and stationary equipment were examined during the experiment. It is established that the operational characteristics of the TETRA digital radio communication system lead to regular failures of the SIRDP-E system (system of interval regulation of train traffic on the basis of the radio channel).

Keywords: *Information security, Digital channel, Train performance control system, Batches transit time, Radio network.*

1. INTRODUCTION

Railway transport is of strategic significance for the Republic of Kazakhstan. Kazakhstan's geographical position (absence of direct access to the sea, availability of navigable rivers), territory vastness, production raw structure and location of productive forces, road transport infrastructure underdevelopment make the role of railway transport extremely important for the country's economy [1].

For the recent 10 years the information technologies have become a dynamic participant of enterprises activity all over the world, maintaining their effective operation and optimizing the processes. The message states a complex task on developing traditional basic branch, as logistics, through all round introduction of the Fourth industrial revolution elements. In the result, the RK Government has been assigned the task to elaborate the set of measures on technologic rearmament of key branches till 2025, which has become an initiator of the State program «Digital Kazakhstan» [2] (hereinafter referred to as Digital Kazakhstan). In the framework of the Digital Kazakhstan there will be actively put into action the technologies of the Fourth industrial revolution: automation, robotics, artificial intelligence, interchange of «big data», etc.

Nowadays the Republic of Kazakhstan conducts an active work on reforming the republic's transport complex.

Location of Kazakhstan in the center of Eurasian continent, between large and dynamically developing markets of Europe and South-East Asia,

Journal of Theoretical and Applied Information Technology
31st March 2020. Vol.98. No 06

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

allows, in prospect, for domestic railway transport uncover the transport-logistics potential of the Republic of Kazakhstan [3].

Thus, economic space unity, nationhood entity, country defense and security to a great degree depend on sustainable and reliable railway transport operation.

Upgrading the work of the railway transport under new economic conditions is impossible without reliable, high quality communication as the base of implementing the up-to-date computer-aided control system and maintaining timely and regular information, necessary for traffic process management and control over its fulfillment.

The program of Kazakhstan railway transport development contains a long-term perspective implementation of the advanced information technologies, which is of high priority. With account of qualitative, fast-moving and volumetric characteristics, the contemporary telecoms will not merely solve the problems of providing the traditional services of trains movement railway communication, goods and passengers traffic, but also allow essentially broaden the services spectrum at the expense of the traffic process automation program implementation, providing freight advance following up and other services types, rendering of which at present time is limited due to engineering capabilities of existing communication devices [4].

At present the railway system JSC «National company «Kazakhstan Temir Zholy» (JSC «NC «KTZh») receives sufficient volumes of important confidential information by means of different communication data system. Logistic information on traffic schedule and trains location represents appreciated commercial value. Basis for securing the train operation security is the systems of railway automation and telemechanics (RATS) [5].

RAT system represents a complex of engineering means, providing control and management with an established level of traffic safety with stationary traveling and mobile objects of railway transport, in which the role and requirements to information channels are sufficiently ramped up. Information channels development tendency on the basis of foreign and domestic experience denotes, that apart from traditional tools, for instance, track circuits, it is necessary to use new systems, for example, digital radio channels. Thereat, by no means unimportant factor is the aspects of information security and wireless systems interference immunity [6]. Information security is one of prime importance factors of train movement safety maintenance.

Information security provision aims for trains movement control system and group of threats to information security [7] are shown on the Figure 1.

In modern RAT system to secure safety trains movement it is necessary to transfer important information along several independent channels.

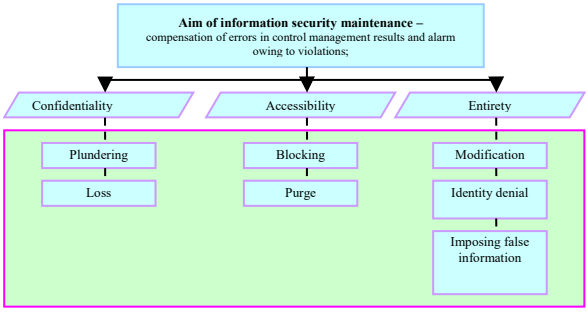

Figure 1: Threats to information security

At that, the information shall be reliably protected both from interferences and from intended impacts, directed to its destruction, distortion or reading [6].

Types of threats to information security in information-telecommunication systems are given in the Table 1.

Table 1. Types of threats to information security

External threats							Internal threats			
Natural		Artificial								
		Intended					Unintended			
				Software-hardware means						
Disasters	Electro-magnetic emission	Intended interferences	Viruses and embedded defects	Unauthorized access	Wire tap	Loss	Loss or forfeit	Unintended action	Operating error	Access violation
	Destruction			Distortion	Disclosure	Data leak			Access violation	
	Information loss and breakdown of transport system functioning sustainability									

Upon analysis of information security and interference immunity of railway transport technological radio channels there should be considered three main types of intended threats, bringing to railroad engine sustainable operation breakdown: unauthorized access, information wiretap and loss. Those threats are eliminated with engineering measures complex, jointly applied at protected data transmission [7]. At that, the main danger is unauthorized access to railroad engine management radio channels, in the result of which there also can be realized other threats – information wiretap and forfeit.

Techniques of data transmission to railroad engine devices and their variety at European and Asian railroad transport nets complicate railroad

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

engine on-board systems and lead to their appreciation. Different approaches to trains movement organization and railroad automation systems greatly aggravate running through of trains across national boundaries of Europe: results in speed reduction, additional travelling cost. Moreover, with increase of railway traffic mid-speed (development of high speed railway traffic) the performance of existing signaling systems decreases. By 80-ies of the XX century only in Europe there existed 14 railroad automation national systems, which turned out to be a serious obstacle for creating pan-European railroad net. Difference in European countries railroads infrastructure resulted in increase of delays in international railroad communication (accordingly, in speed reduction and increase of travelling cost). The situation worsened due to increased competition from automobile and air transport, providing speed delivery of passengers and freight [8].

In that connection there appeared the problem of railroad automation national systems compatibility for developing common railway space, as it turned out to be possible to unite railways into a single net and arrange interaction with Eastern Europe countries roads, which are the exits to Asia – it complies with the main aims of European Community [9].

To cut the costs on different locomotive signaling systems and train traffic speed raising in international communication there has been made a proposal to develop systems of signaling, blocking centralization at railway transport in Europe. The project of creating the European rail traffic control system (ERTMS) was initiated in 1995 by the European commission. The project core is the system of control and train traffic security assurance. ERTMS/ETCS (ERTMS – European Rail Traffic Management System; ETCS – European Train Control System) [10].

System ERTMS/ETCS is based on continuous and point data transmission between wayside devices and train, on-board computer modular architecture and smart sensors, which allow the train define own location at the line with high accuracy.

ETCS is a part of ERTMS, which contains, as well, train operation management components, passengers' information system, car gathering, train energetically optimized running, etc. The aim of ETCS elaboration is standardizing the systems of information exchange between train and track side facilities. The system consists of a responsor Eurobalise, driving belt Euroloop, radio communication means Euroradio, locomotive equipment Eurocab.

The system ERTMS/ETCS envisages three levels.

1-level system provides train speed control dependent on the transmitted from the track to the train the data, formulated, based on track signals indices. The system, apart from the train location traditional control means (track circuit or axial pins meters), is added with two responsors, controlled with a signal.

2-level system represents an accomplished system without using the track signals, but maintaining strict breaking down the line into block -sections. At this stage the data on the train situation is continuously transferred to a locomotive along the radio system GSM-R. Third type responsors, point-contact automation communication line driving belts and blocks LEU might be dismounted. The trains fix their location by means of the 1st type responsors. At ETCS second level there remain traditional devices of the train location control (track circuits and axles meters). At the same time, the automatic continuous cab signaling commands, entering along the radio channel, send to the train the main information on the permitted traffic speed. Remained at this stage on-ground stoplights are admitted as a reserve [11].

To upgrade between station travel time devices (automation blocking), upon appropriate engineering substantiation, excluding the stoplights at station-to-station block, it is recommended to apply ETCS 2nd level standard using axles meters, Eurobalise with point-contact coding or other track sensors for finding the running unit at the block (including, as well, track circuits with c uninterrupted coding) [9].

The ETCS 2nd level is characterized with uninterrupted information exchange along the double type digital radio channel of GSM-R standard between rolling equipment and radio blocking center (dispatch control). Eurobalise sends to the train only its coordinates. On-board system constantly defines the train location, based on the latest received coordinates from the balise and the path, passed after it, computed with odometer. This data is continuously sent to a radio blocking center, where the input data is compared to the train traffic schedule. Comparison results are sent along the digital radio communication net to the board information control system to inform a locomotive driver about departure from the traffic schedule for subsequent decision taking on railway traffic management. Availability of on-ground stoplights, at that, is not required. To control the train passage

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

in completion, as well as at the first level, there used the devices of wage wheels or track circuits calculation. Information about area freeness is transmitted to the electric centralization tower, then it enters into radio blocking center, and from there along radio communication is dispatched to the following train. Uninterrupted radio exchange allows cut the interval of traffic compared to SCB traditional systems.

ETCS third level is a complete system of control and railway traffic security maintenance without using on-board signals and with mobile block-sections. ETCS third level standards and technologies are under the development. The train location definition and control over its completion are fulfilled with on-board facilities. Railway traffic regulation at the third level is executed exclusively along the radio channel. Traditional devices of on-board rolling stock location control are not used nowadays. There is no need to use on-board signals due to unavailability of fixed block-section [10].

The system of interval control over railway traffic on the basis of radio channel is directed to upgrading the railway transport operation performance at the expense of raising the line capacity, cutting operation cost and energy consumption, as well, deterioration of track rolling stock.

Upon [8] new lines construction in Kazakhstan in recent years there started applying (SIRDP-E) Bombardier transportation, using uninterrupted data transmission along the radio channels «TETRA» (ETCS third level). The system herein has been constructed on the new lines, put into operation recently. The accepted system of data transmission of different manufacturers often glitches and function not sufficiently reliably.

Upon complex reconstruction of physically and morally deteriorated RAT system devices at existing railway areas it is recommended to use radio blocking facilities of the 2nd or 3rd levels, integrated into microprocess centralization systems at adjacent stations [12].

It is possible to apply the 2nd level ETCS system without using on-board signals, but maintaining strict breaking down the line into block-section. At the stage herein the data on the train situation is transmitted continuously to a locomotive along the radio system GSM-R.

There exist the digital technologies and communication standards, qualified to solve the system's separateness problem and maintain communication at high speeds. Those are the standards of digital mobile communication, such as, TETRA, CDMA, LTE and specially developed in 2000 the standard GSM-R for railway communication aims [11].

TETRA represents the standard of digital trunked radio communication, consisting of several specifications, developed by European Telecommunications Standards Institute. TETRA standard was created as common pan-European digital standard. Therefore till April 1997 the abbreviation TETRA meant Trans-European Trunked Radio. However, due to the big interest, shown to the standard in other regions, the territory of its functioning is not limited by Europe only. That is why, presently the TETRA decoded as (Terrestrial Trunked Radio) [13].

Standard TETRA has been developed based on engineering solutions and GSM standard recommendations and it is oriented to creating the communication systems, effectively and economically supporting joint usage of radio communication nets by different users groups securing secrecy and information security. Special attention in the standard has been paid to public security services interest.

Presence in TETRA net of data transmission method with channels commutation, availability of PRI interface of ISDN net to switch on RBC to radio communication net, as well, meeting the requirements to call connection duration (less than 5 seconds for 95% calls), to maximum data transmission delay between two edge devices (no more, than 0,5 seconds), to link disconnection recognition time (no more, than 1 second), allows to use the TETRA net for problems of rolling stock management. JSC «National company «Kazakhstan temir zholy» uses the TETRA net in batch transfer regime [8].

2. RELATED WORK

At present to upgrade information transmission process performance along the radio channel here has been developed and widely used the code radio channels noise masking method, implemented by means of combined random coding the transmitted messages.

Along with creating the digital systems there has been developed the combined code parameters selection algorithm for information transmission along the radio channel with noise masking, which makes possible to obtain results independent on definite coding schemes and correcting codes, simultaneously securing noise immunity upgrading and radio channels information security and information transmission control [14].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Let's consider the principle of data transmission along radio channel. There are following distinctions from alternative means of digital data transmission, typical of other closed systems [15]:

1. Hierarchical nets with ring-type structure. Centralization computer as a control element, has been separated from the ring-type structure, though all executive units are united according to the closed-loop principle by means of copper (SHDSL) or fiber optical cable. Outstep from classic scheme of star-like compounds according to the principle «point – point» allows:

- reduce need in cable;
- by means of a ring provide two independent data transmission paths.

2. Backbone with fiber-optical cable of Ethernet standard, consisting of two independent channels and connecting the computer with rings, which secure control over the group of located nearly wayside devices via their object controllers. The given redundancy type guarantees the system's vitality upon damage of any physical links. The backbone length might reach dozens and even hundreds kilometers.

3. Scheduled in the object controllers diagnostic tasks. Thanks to placement of executive digital elements directly at wayside devices or even inside them, the computer tower gets exhaustive information on the state of management and control objects «at first hand». At that, it is indispensable to distinguish the management/control problems from diagnostics, envisaging the priority principles in the being considered data transmission network.

4. Network modules before every managing or executive element.

Their tasks consist in defining the top-priority, in respect of data flow transmission path in the real time mode and using the lowest priority channel for transmitting diagnostic messages from wayside devices. Moreover, the network modules maintain dual connection with the backbone, transform the protocols (Ethernet on top of SHDSL), filter traffic, having limitations in data transmission volume to linear ring bus, and they are digital signals boosters, which secure high range communication.

5. Upon transmitting the commands along both channels, the network module of executive element, having received the first message, records its number and runs the command. Arrived afterwards along the reserve channel the second message with similar number is deleted in the network module.

6. In prospect, the fiber-optical communication line's backbone can be replaced with a radio channel (for instance GSM-R), and network modules will be switched on to corresponding radio communication transmitters.

7. With account of elaborating the advanced energy saving technologies, as well, alternative sources of local electric power supply, the feeding network will gradually loose its significance, and local power sources will be enough for off-line operation of the devices, remoted from the devices tower.

It should be taken into consideration, that while transmitting the data, inside the digital centralization any incorrect message or errant command might bring the system to dangerous state. To exclude it, in the protocols stack TCP/IP there is separated the zone, responsible for signals transfer, and it is not critical in relation to security. Thus, responsible security functions are at applications level, and a transport level together with a backbone, linear ring bus and network modules (Figure 2) fulfill the tasks of highly reliable data transmission path [16, 17].

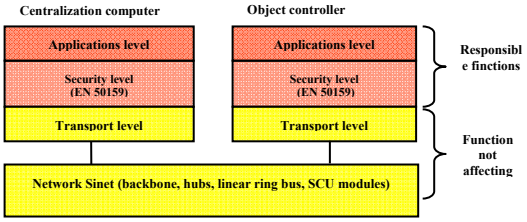

Figure 2: Multilevel model of data safety transmission

In practice the code noise masking method of radio channels is implemented by means of combined random coding of the messages, being transmitted, which represents combination of noise-immune and stochastic coding.

Principle of transmission protection level upgrading upon using the method of code noise masking is clarified on the Figure 3. Digital information transmission quality is assessed with probability of errant accepting the messages $P_{ош}$, which shall not exceed the required (maximum permissible) magnitude $P_{ош.\ треб}$. Magnitude $P_{ош}$, in its turn, is defined with the probability of errant accepting the the information symbol p_0, linked with communication channel characteristics and parameters of the error-correcting code, being used. Let during the interval time from t_1 to t_2 in the communication channel there is fulfilled information transmission [18].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

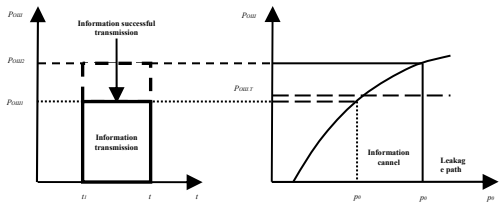

Figure 3: Principle of information transmission protection level upgrading, using method of code noise masking

Correcting code parameters are selected in the way, that in the information transmission channel a legal subscriber with prescribed probability of errant accepting the information symbol p_{01} is secured the condition $P_{ош1} < P_{ош. треб}$, which complies with successful information transmission, but excess of $P_{ош.треб}$ over $P_{ош1}$ shall be minimal. Then in the leakage path, characterized with the probability of errant accepting the information symbol $p_{02} > p_{01}$, probability of errant messages accepting will exceed the required ($P_{ош2}>P_{ош.треб}$) and trespasser will have complications with unauthorized access to the information being transferred [7].

Upon information transmission along the radio channels the probability of errant information symbols p_{01} and p_{02} depends on the being used signals structures, and they are defined with energetic potential of information transmission paths and leakage. At correcting code fixed parameters the difference in the messages accepting quality in the information transfer paths and leakage will be all the more, than bigger the difference between the magnitudes p_{01} and p_{02}, at that, increase of probable multiplicity errors, detected and corrected with the correcting code, brings to their multiplication in the leakage channel. Thereat, upon practical implementing the code noise masking method the problem consists in selecting the parameters k, r and l of the combined code, providing realization of the information transmission protection level upgrading principle, having been considered [7].

The most practical interest in implementing the method of code noise masking is the usage of correcting codes, putting right the errors. In that case, the probability of errant accepting the message, transferred with a dual code, is connected with possibility of the information symbol errant accepting and parameters of the correcting code, which is shown with the expression below

$$P_{ош} = \sum_{i=q_И+1}^{n} C_n^i p_0^i (1-p_0)^{n-i}, \qquad (1)$$

where $q_и$ – multiplicity of the errors being corrected. At $p_0=p_{01}$ the expression (1) provides the magnitude $P_{ош1}$ in the information transmission path, and at $p_0=p_{02}$ – magnitude $P_{ош2}$ in the leakage channel. It is necessary to select the parameters of the combined code k, r and l in such a way, that for prescribed n and k there is executed the condition $P_{ош1} < P_{ош. треб}$ and $P_{ош2} > P_{ош. треб}$.

Codes, correcting the errors, are characterized with parameters n, k, r, q_u, as well, with a generalized parameter d – code distance (Hamming distance). The basic task of constructing the correcting codes with prescribed parameters is establishing the correlation between their ability to detect or correct the errors and redundancy. At selecting the parameters of combined code, first of all, proceeding from expected communication conditions, there shall be selected the correcting code parameters, and afterwards, they shall be added with stochastic code, filling in the code combinations positions. At that, there used the dependencies between correcting code parameters d, n, k, r and $q_и$, being specified with bounds linking them, which allows define the codes required parameters independent on concrete coding schemes, implementing any given codes. There exist bounds (upper and lower bounds), connecting the code distance d with multiplicity of being corrected errors $q_и$, bounds, linking the overall amount n and checking symbols amount r with multiplicity of errors being corrected q_u.

The bound, connecting the code distance of the dual code with multiplicity of errors being corrected, has a view $d\geq 2q+1$. That bound is used in respect to already selected codes, for which the code *distance* d is known. Upon selecting the correcting codes for realization of the code noise masking method it is necessary to use the bounds, connecting an overall symbols amount n and checking symbols amount k in the code combination. At that, in case of selecting the correcting code parameters to implement the code noise masking method, there exist the peculiarities of applying those bounds, connected with appearing of additional parameter – amount of stochastic code symbols in the code combination l. If for conventional usage of correcting codes, $n=k+r$, then in case of using the correcting codes in the combined makeup upon code noise masking, $n=k+l+r$.

Boundary conditions for the codes, correcting errors are defined with the following inequalities [19]:

- upper Hamming bound

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$n-k-l \geq \log_2\left(1+\sum_{i=1}^{q_и} C_n^i\right); \quad (2)$$

- lower Gilbert – Varshamov bound

$$n-k-l > \log_2\left(1+\sum_{i=1}^{2q_и-1} C_{n-1}^i\right). \quad (3)$$

Hamming bound (2) is an upper boundary for the code distance d at checking symbols amount $r=n–k–l$, prescribing the minimal code redundancy with existence of the correcting code, having minimal code distance and assuredly correcting the errors with multiplicity $q_и$. Gilbert – Varshamov bound (3) is a lower boundary, which shows, at what amount of checking symbols $r = n – k – l$, *and* there definitely exists the code, reliably correcting the errors of multiplicity $q_и$.

Solving the task of combined code parameters selection to implement the code noise masking method consists in selecting, by means of expression (1) and boundary conditions (2) and (3), the parameters of correcting r and stochastic l codes, maintaining for the prescribed n, k, p_{01} and p_{02} the fulfillment of the condition $P_{ош1} < P_{ош.\ треб}$, $P_{ош2} > P_{ош.\ треб}$ and, if possible, $P_{ош2} >> P_{ош.\ треб}$.

The initial data for solving the tasks is parameters of messages source n and k, information transmission paths and leakage p_{01} and p_{02}, as well, $P_{ош.\ треб}$. Outcome of the task solution is parameters of correcting r and stochastic l codes, maintaining implementation in the prescribed conditions of code noise masking method. Magnitudes $P_{ош1}$ and $P_{ош2}$ are computed according to a formula (1). In case of solution absence, at which there simultaneously fulfilled inequalities $P_{ош1} < P_{ош.\ треб}$ и $P_{ош2} > P_{ош.\ треб}$, which is possible by virtue of discrete-continuous character of dependencies, connecting the magnitudes being analyzed, there should be changed (specified) initial data [19].

3. IDENTITY VERIFICATION AND KEYS GENERATION UPON DATA TRANSMISSION ALONG RADIO CHANNEL

The main requirement to the railway transport is security. Data protection maintenance in control systems is the problem, affecting the system's security. Therefore, the data, transmitted along the radio channel, shall be protected from unauthorized influence and distortions. Upon considering the system security, there analyzed potential threats. In compliance with the standard EN 50159 upon data transmission there are possible the following threats [20]:

- message iteration;
- message delete;
- message insertion;
- change of messages succession order;
- message distortion;
- message delay;
- message masking.

The threats thereof have been defined by European standard EN50159-2 [21] and it describes all known for the current moment threats to information transmission.

For protection assurance from the enumerated threats there used special security techniques [20] and data transmission implemented in the protocol.

To protect from such threats as message iteration, message delete and change of messages succession order there is applied the method, under which as additional field is introduced into the protocol– the message's serial number, which allows easily detect the given type threats.

To protect from messages delays a field is added into the protocol – time stamp, which allows control over the message delivery delay.

To protect from message distortion and message masking there is used cryptographic protection methods.

To protect from messages insertion there added the fields – source and receiver identifiers.

Based on cryptographic methods there implemented identity verification in the protocol Euroradio, used in the system ETCS. Detailed description of cryptographic protection method execution is given in [22]. Messages entirety in the protocol Euroradio is protected with a special code of message authenticity MAC (message authenticity code), which represents the number, hindering a trespasser to forge a message. MAC value is computed based on the secret key and message text. Any change of message text demands MAC value alteration, which is computed by means of a secret key unavailable to a trespasser. Actually, the message authenticity code is a function, accepting at the inlet two arguments: a secret key K of the fixed length and random length message. In theory, an ideal function of a message authenticity code computation is a random mirroring of all possible inlet values by dozens of n-bit outlet values. In the protocol Euroradio as MAC function there used the method on the basis of the block cipher, called CBC-MAC. The main idea of the algorithm CBC-MAC consists in the message cryptogram be means of block cipher in the mode of chaining the coded blocks (CBC – cipher block chaining) and casting-out all coded text blocks,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

except the last one. For the message, consisting of blocks $P_1,\ldots,P_k$, MAC value is computed, based on the following formulae:

$$\begin{aligned} H_0 &= 0; \\ H_i &= E_k\left(P_i \oplus H_{i-1}\right) \\ MAC &= H_k. \end{aligned} \tag{4}$$

Upon establishing the session at the instant of switching on, there takes place identity verification procedure, shown on the Figure 4.

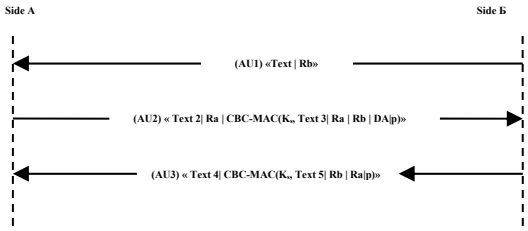

Figure 4: Sequence of identity check and keys generation

Side Б sends a random number Rb with a length of 64 bits, which is generated with Б. Number Rb is saved at the side Б. After obtaining that message the side A generates a random number Ra with a length of 64 bits and computes MAC along the field of Text 3, random numbers Ra and Rb, of DA indicator and MAC padding bit (message authentication code), which represents the number, hindering a trespasser to forge the message. Actually, message authenticity code (MAC) is a function which accepts at the inlet two arguments (key K of the fixed length and message m of random length) and yield the value of fixed length.

To compute the MAC there is calculated the sessional key Ks, based on the parameters Ra, Rb and authentication key Kab in compliance with the following procedure:

- numbers Ra, Rb are divided into 32 bit blocks.

$$\begin{aligned} R_A &= R_A^L \left| R_A^R \right. \\ R_B &= R_B^L \left| R_B^R \right. \end{aligned} \tag{5}$$

Three 64 - bit keys Ks1, Ks2, Ks3 are computed according to the formulae:

$$\begin{aligned} K_{s1} &= MAC\left(R_A^L \left| R_B^L, K_{AB}\right.\right) = DES\left(K_3, DES^{-1}\left(K_2, DES\left(K_1, R_A^L \left| R_B^L\right.\right)\right)\right) \\ K_{s2} &= MAC\left(R_A^R \left| R_B^R, K_{AB}\right.\right) = DES\left(K_3, DES^{-1}\left(K_2, DES\left(K_1, R_A^R \left| R_B^R\right.\right)\right)\right) \\ K_{s3} &= MAC\left(R_A^L \left| R_B^L, K'_{AB}\right.\right) = DES\left(K_1, DES^{-1}\left(K_2, DES\left(K_3, R_A^L \left| R_B^L\right.\right)\right)\right) \end{aligned} \tag{6}$$

where $KMAC = \left(K_1, K_2, K_3\right)$.

MAC computation in the protocol Euroradio is based on using cryptographic standard TripleDES, which is symmetric to block. Upon protocol designing for the needs of JSC «National company «Kazakhstan temir zholy» is has been assumed to replace TripleDES with the standard of symmetric coding of GOST 28147-89 «Systems of information processing. Cryptographic protection. Algorithm of cryptographic transformation».

In the system ETCS protection of being transmitted data is fulfilled with the protocol Euroradio, designed for transmitting the data, connected with security, along the radio channel, using the open communication networks.

Protocol thereof has been constructed based on the standard EN 50159-2 [21], which regulates protection upon critical data transmission along open networks. Protocol Euroradio has been constructed based on the model OSI and has following models (Table 2):

Table 2. OSI levels of Euroradio protocol

Name	Implementation
Applications level	Subset-026 (7,8)
Security level	Euroradio (Subset-037)
Transport level	Protocol X.224
Net level	Protocol T.70
Channel level	Protocol HDLC
Physical level	Modem GSM/GSM-R

At channel level there is used bit-oriented protocol HDLC (High-Level Data Link Control) of OSI network model, having been developed with ISO. The current standard for HDLC is ISO13239. HDLC is the protocol for data transmission channel control and it implements control tool over the flow be means of uninterrupted sliding window. HDLC supports half-duplex and full-duplex transmission, single-point and multipoint configurations, as well, dial-up and unswitched channels.

In Euroradio HDLC protocol there is used connection type 'point-point' of combined stations, which match up the functions of leading and leaded and produce both commands and responses. Each of the stations at every instant can be in one of three logic states:

- state of logic disconnection;
- initializing state;
- state of information transmission.

Protocol HDLC supports three regimes of logic connection. For HDLC realization in Euroradio protocol makeup there is used asynchronous balanced regime, in which transmission might be initiated from any side and in the full duplex. In the regime thereof both devices are equivalent and they exchange frames, which are

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

divided into frames-commands and frames-responses.

HDLC frames can be transmitted, using synchronous and asynchronous connections. The connections themselves do not have tools of defining the frame start and end, it is fulfilled with unique, within the protocol, bit sequence (FD – Frame Delimiter) «01111110» (0x7E in hexadecimal presentation), placed at the begin and end of every frame. Indicator's unique character is secured with byte-staffing usage.

Upon byte-staffing there is used special sequence, hereby–«01111101» (0x7D in hexadecimal representation), that is the byte FD(0x7E) in the middle of the frame is replaced with sequence of bytes (0x7D, 0x5E), and byte (0x7D) –with sequence of bytes (0x7D, 0x5D). HDLC frame structure is shown in the Table 3.

Table 3. HDLC frame structure

Indicator FD	Address	Control field	Information field	FCS	Indicator FD
8 bits	8 bits	8 or 16 bits	0 or more bits, fold 8	16 bits	8 bits

Indicators FD – opening and shutting down indicators, indicating the codes 01111110, edging the HDLC-frame, allowing the receiver define begin and end of the frame. Thanks to those indicators in HDLC-frame there is no frame length field. Sometimes an indicator of one frame end (but not obligatory) might the starting indicator of the next frame.

Address fulfills its usual function of identifying one of several possible devices merely in configuration 'point-multipoint'. In double - point configuration HDLC address is used to denote the transmission direction – from the network to a user's device (10000000) or vice-versa (11000000).

Control field occupies 1 or 2 bytes. Its structure depends on being transmitted frame type. Frame type is defined with the control field first bits: 0 – information, 10 – control, 11 – unnumbered type. Control field of structure's all types frames contains a bit P/F, it is in different ways used in frames-commands and frames-responses. For instance, station receiver upon getting from station-transmitter the frame-command with an established bit P shall immediately response with a control frame-response, having determined bit F.

Information field has been designed for transmitting along the network of overlaying protocols batches – network protocols IP, IPX, AppleTalk, DECnet, rarely – applied protocols, when those thereof lay own messages directly in channel level frames. Information field might be absent in the control frames and some unnumbered frames.

Field FCS (Frame Check Sequence) – control sequence, indispensable for detecting the transmission errors. Its computation, is mainly, executed with method of cyclic coding with generating polynom X16+X12+X5+1 (CRC-16) in compliance with recommendation of CCITT V.41. Obtained CRC is bit-wise inverted and recorded in inverted sequence. It allows detect all possible errors tuple with length up to 16 bits, caused with a single error, as well 99,9984 % all kinds of longer errors tuple. FCS is compiled from the fields: Address, Control field, Information field. Rarely there used other methods of cyclic coding. After checking FCS on the receiver side, it responses with a positive or negative acknowledge. Frame repetition with transmitting side is executed with arrival of negative acknowledgment or upon expiring the time-out.

Network level Euroradio protocol has been implemented on the base of the so-called coordinating functions and protocol T.70. Coordinating functions maintain synchronization mechanisms, required upon using B/Bми protocols stack by signaling protocol stack.

Coordinating functions fulfill the following tasks:

- recording with inquired GSMPLMN;
- creating the network connection with signaling protocols GSM 07.07 and ETS300102;
- mirroring of QoS quality inquired parameters;
- connection deviation upon call, when applicable;
- connection closing by means of GSM07.07 and ETS 300102 signaling protocols;
- processing GSM/ISDN additional service information.

Transport level is represented with the protocol X.224 of TP2 level and it secures reliable batch transmission between the modules, fulfilling the following services:

- messages connection and spacing;
- partition and desectorizing;
-multiplexing and demultiplexing;
- evident flow control.

Security level is based on the document [23] and on the procedure of authentication and CBC-MAC computation.

Upon upgrading the system of monitoring and diagnostics of railway infrastructure condition there is possible to transfer to radio blocking

Journal of Theoretical and Applied Information Technology
31st March 2020. Vol.98. No 06

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

system without track circuits, but with train entirety control.

Radio blocking system is recommended to apply, if at the adjacent area there is already the mentioned system and at running rolling units are already equipped with on-board units, tail sensor inclusive.

Auto blocking system selection or radio blocking is fulfilled based on engineering task upon executing the design works on upgrading a concrete area.

4. EXPERIMENTS AND RESULTS

Radio blocking system practical application has been considered at the area Zhetygen – Altynkol of Almaty department of mains [8]. Upon practical application there have been considered the issues of radio blocking and commutation TETRA, centers connection, coupling the radio blocking center [7] with electric centralization systems, locomotive's on board equipment renovation, on-board and stationary equipment algorithms control.

At the first stage the experiments are carried out according to the scheme, presented on the Figure5.

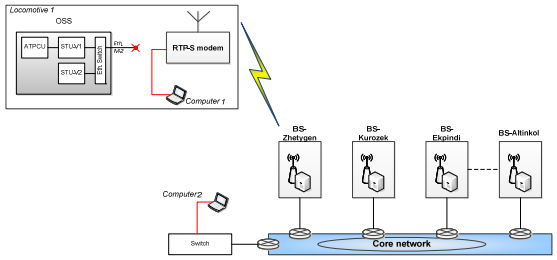

Figure 5: Scheme of experiments conduct – stage 1

Computer 1 is connected to the radio modem RTP-S on the locomotive, computer 2 is switched on to the TETRA backbone via the switch at EC tower of Zhetygen station [8].

On both computers there have been installed the software («receiver» on computer 2 and «transmitter» on computer 1, fulfilling transmission of UDP different lengths at various speeds. Batches amount increasing or decreasing brings to the change of the load on radio channel.

During the experiments on computers 1 and 2 there is triggered a specialized software, providing transmission and receipt of UDP batches. Locomotives, participating in the experiments, are motionless, traffic along SIRDP-E of other equipped locomotives is not fulfilled.

During the experiments there have been used setting ups, submitted in the Table 4.

Table 4. Results, obtained during the first stage

Batch size, byte	Load on data transmit channel, Kbit /s	Test duration, min.
46	1.2-2.0	105
64	1.2-2.4	30
76	1.2-2.4	30
86	1.2-2.8	105
106	1.2-2.8	30

Results of measurements, including the data on the channel capacity, batches transit time, data on batches loss in TETRA radio network are given on the Figures 6-8.

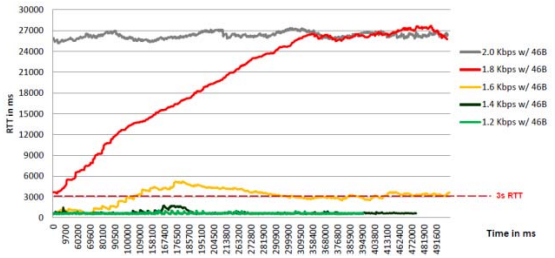

Figure 6: Transit time of a batch with 46-byte size

As it is seen from the graphs on the Figure 4 for 46 bytes size batches the experiments have shown the following:

- at speeds 1,2-1,4 kilobit /s the batches round trip time (RTT) in both sides constitutes about 1-2 seconds, at that the transit time is stable and it practically does not change within the overall test duration;
- at speed 1,6 kilobit /s round trip time in both sides amounts to 6 seconds;
- at speed 1,8 kilobit /s transit time starts from 3 seconds and within the test time grows up to 27 seconds;
- at speed 2.0 kilobit /s batches RTT is about 26 seconds within overall test duration.

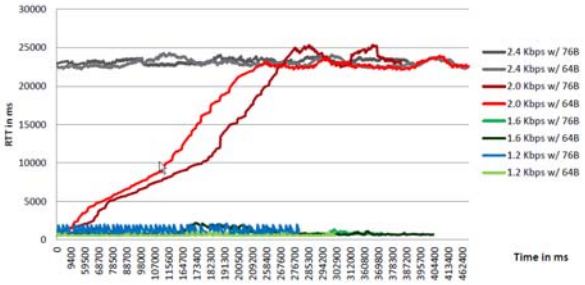

Figure 7: Transit time of a batch with 64 bytes and 76-bytes size

As it is seen from the schemes on the Figure 5 for 64 and 76- bytes size batches the experiments have shown the following:

- at speeds 1,2-1,6 Kbit/s batches RTT varies from 1 to 3 seconds during the whole test;
- at speeds 2,0 Kbit/s batches RTT reaches

Journal of Theoretical and Applied Information Technology
31st March 2020. Vol.98. No 06

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

25 seconds, at that, in length of time from the experiment starting instant the transit time increases;

- at speeds 2,4 Kbit/s batches RTT is about 25 seconds during the whole test.

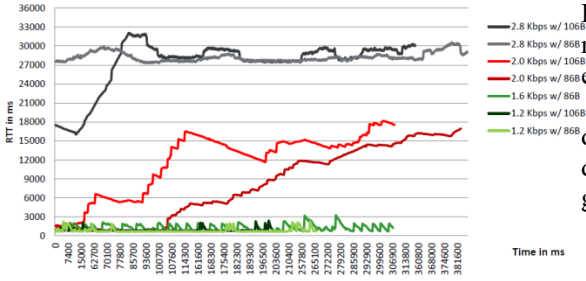

Figure 8: Transit time of a batch with 86 and 106- bytes size

As it is seen from the graphs on the Figure 5 for 86 and 106- bytes size batches the experiments have shown the following:

- at speeds 1,2-1,6 Kbit/s batches RTT varies from 1 to 3 seconds during the test overall duration;

- at speed 2,0 Kbit/s batches RTT reaches 18 seconds, thereat, in length of time from the experiment starting instant the transit time increases;

- at speed 2,8 Kbit/s batches RTT is about 30, at that for 106 bytes size batches the transit time at the beginning of the test constituted about 18 seconds, and then sharply increased up to 32 seconds.

At the second stage the experiments are carried out according to the scheme, presented on the Figure 9.

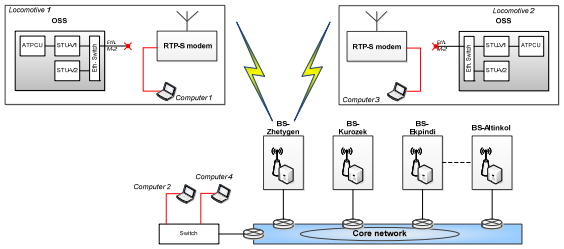

Figure 9: Scheme of experiments conduct – stage 2

Computers 1 and 3 are connected to radio modem RTP-S at locomotives 1 and 2 accordingly, computers 2 and 4 are switched on to опорной TETRA backbone via switch EC tower of Zhetygen station.

All computers are installed with software («receiver» at computers 2 and 4, «transmitter» at computers 1 and 3), executing transmission of UDP different lengths batches at various speeds. Decreasing or increasing the number of batches brings to changing the load on the radio channel.

Batches exchange occurs in pairs, between computers 1 and 2, 3 and 4.

During experiments on all 4 computers there is launched a specialized software, providing transmitting and accepting UDP batches. Locomotives, participating in the experiments, are motionless, traffic along SIRDP-E of other equipped locomotives is not fulfilled.

Results of measurements, including the data on the channel capacity, batches transit time, data on batches loss in TETRA radio network are given on the Figure 10.

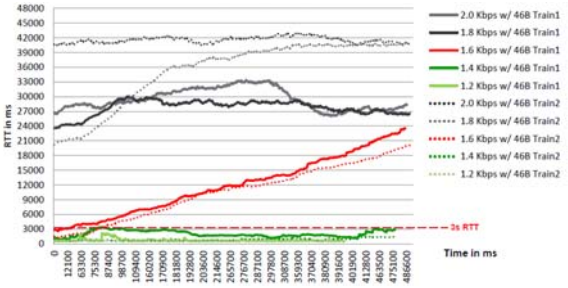

Figure 10: Transit time of a batch with 46 bytes size

As it is seen from the graphs on the Figure 7 for 46- bytes size batches the experiments have shown the following:

- at speeds 1,2-1,4 Kbit/s batches RTT for modems, installed at both locomotives, varies from 1 to 3 seconds within the test duration;

- at speed 1,6 Kbit/s the time reaches 21 seconds, thereat, in length of time from the experiment starting instant the transit time increases. This regularity is typical of both modems, installed at locomotives;

- at speed 1,8 Kbit/s batches RTT at the first locomotive reached 30 seconds, at the second locomotive – 40 seconds;

- at speed 2,0 Kbit/s the batches RTT at the first locomotive reached 33 seconds, at the second locomotive – 42 seconds.

Batches loss percentage in the radio network is presented on the Figure 11.

Figure 11: Percentage loss of batches in radio net

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

As it is seen from the graph, simultaneously with c the transit speed increase and patches delivery time there grows, as well, their loss percentage (up to 50% at speed 2,4 Kbit/s) [24].

Thus, according to requirements to digital radio communication system, the required capacity shall be no less, that 4.8 Kbit/s, the batches transit time to one side shall not exceed 0,5 seconds, to both sides 1 second, accordingly.

Comparing the results obtained experimentally with previous works, it should be noted that the results can be applied in the development of the national KTCS system (Kazakhstan Train Control Systems) to ensure the information security of the railway network of the Republic of Kazakhstan.

5. CONCLUSIONS

1. Conducted experiments show, that at any batch size in the system of TETRA standard digital radio communication upon increasing the load on the system, the batches transit time grows accordingly. For transmission speed up to 1,4 Kbit/s the system meets the requirements to batches transit time. Starting from the load 1,6-2,0 Kbit/s batches transit time becomes unacceptably big and reaches 30-40 seconds, which does not meet demanded requirements.

2. Concurrent with that, the lost batches percentage grows (up to 50%), thereat, there is observed the loss of several batches in succession.

For the future it is planned to carry out other experiments for specifying the operational characteristics of TETRA standard digital radio communication system upon working with the being elaborated national system of train performance security.

3. The results obtained experimentally will allow us to further determine the operational characteristics of the TETRA digital radio communication system in the development of the national KTCS system to ensure information security of the railway network of the Republic of Kazakhstan.

REFERENCES:

[1] State program of development and integration of RK transport system infrastructure till 2020. Approved by the decree of the President of the Republic of Kazakhstan as of January13, 2014 # 725. (revised and expanded by the Decree of RK President, dated May 26, 2015 # 30)

[2] State program «Digital Kazakhstan». Program is approved by the decree of RK Government # 827, dated 12.12.2017.

[3] Bakhtiyarova Ye.A., Sansyzbai K.M. «Analysis in case of failure to grade-up the existing RAT systems in the Republic of Kazakhstan» *Proceedings of all-Russian scientific-technical conference with international participation / Omsk state university of communications*, Omsk, Russia 2019, p.p. 97-104

[4] Program of developing Kazakhstan railway transport for long-term perspective http://miid.gov.kz/ru/pages/koncepciya-proekta-zakona-respubliki-kazahstan-o-zheleznodorozhnom-transporte-0

[5] Engineering policy of Automation, telemechanics and telecommunication department for a period from 2017 to 2022. JSC «National company «Kazakhstan temir zholy», Astana, Kazakhstan 2017, p.p.4-5

[6] A. Tolegenova, P. Kisla, A. Zhetpisbayeva, O. Mamyrbayev, B. Medetov «Experimental determination of the characteristics of transmission spectrum of tiled fiber Bragg gratings» *Metrology and measurement systems*, Vol.26 Issue 3, Poland 2019, p.p./ 581-589

[7] A.A. Kuandykov, K.M. Sansyzbay «Methods of information protection in railway automation and telemechanics systems» *Herald of the Kazakh – British technical university*, Vol. 16 issue 3, Almaty, Kazakhstan 2019, pp. 353-359.

[8] Concepts of modernization and production of RAT systems. Astana, Kazakhstan 2018. – p.p. 88 – 90.

[9] K.M. Sansyzbay, A.A. Kuandykov «The development of the national microprocessor system «KTCS»» *Proceedings of international scientific-practical conference «Auezov readings– 15: Third modernization of Kazakhstan – New concepts and modern solutions», dedicated to 120 years of Mukhtar Omirkhanovich Auezov,* Shymkent, Kazakhstan, April 13-14, 2017, p.p. 276-279

[10] Teyega G., Vlasenko S.V. Automation and telemechanics systems at the world railways, M.: Intext, 2010. – p.p. 261 – 274.

[11] A. Geisder, M. Schwah «ETCS of level 2 with alternative radio communication systems» *World railways,* Vol. 10, 2013, p.p. 57 – 63.

[12] K.M. Sansyzbay, A.A. Kuandykov Providing information security of train traffic through

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the introduction of the national system «Kazakhstan Train Control Systems» on the country's railways. *Proceedings of V International scientific-practical conference «Smart information and communication technologies – means of implementing the third industrial revolution in light of the strategy «Kazakhstan -2030», Eurasian national university, named after Gumilyev L.N.* Astana, Kazakhstan, February 22, 2018, p.p. 460-463

[13] Locomotive board terminal of TETRA standard. Engineering requirements. Astana, Kazakhstan 2012, p.p. 3-8

[14] E.A. Bakhtiyarova, B.Zh. Kemel'bekov, Zh.M. Bekmagambetova, M. A. Lipskaya, T. O. Chigambaev, A. K. Orazymbetova, N. A. Ospanova, A. K. Mekebaeva, V. A. Khan, V. Ye. Mamilov. «Quality of speech reproduction using stochastic digital systems of information transfer with its statistical compaction» *Russian Physics Journal*, Vol. 60, #1, 2017, p.p.190-195.

[15] André Lisker, Kersten Kanis. Inbetriebnahme des DSTW Annaberg-Buchholz Süd. SIGNAL+DRAHT | Ausgabe 04/2018.

[16] Smagin Yu.S., Yefremov A.Yu. «First digital system of interlocking system in Germany» *World railways* , Vol.8, 2018.

[17] Vlasenko S.V., Lunev S.A., Sokolov M.M. «Centralized and decentralized architecture of stations control tower» *Automation, communication and informatics*, Vol.03, 2019.

[18] Zolotzryev V.V., Ovechkin G.V. «Protective coding. Methods and algorithms»: *reference book - M.: Hot line – Telecom*, 2004. - 126 p.

[19] Adadurov A. S. Means of information protection and upgrade interference resistance in radio channels of controlling traction rolling stock // Herald of All-Russian Scientific Research Institute of Railway Transport – 2009. – #3. p.p. 32-36.

[20] EN 50159 Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems.

[21] EN 50159-2 Railway applications - Communication, signaling and processing systems - Security related electronic systems for signaling.

[22] Ferguson N., Schnaer B. Practical cryptography.: Translation from English. – M.: Publishing house Williams, 2005г. – 424 p.

[23] Euroradio FIS Subset-037 v2.3.0 http://www.era.europa.eu/Document-Register/Pages/New-Annex-A-for-ETCS-Baseline-3-and-GSM-R-Baseline-0.aspx

[24] Engineering analysis of loading tests of TETRA standard radio communication system. Almaty 2016. – p.p. 15-16.