Highly Information and Energy-efficient Monitoring Data Transmission in IoT Networks

Bohdan Shevchuk[1], Mykhaylo Geraimchuk[2], Orest Ivakhiv[3,*] and Yuriy Brayko[1]

[1]*Glushkov Institute of Cybernetics, National Academy of Sciences of Ukraine, 40 Academician Glushkov av., Kyiv 03187, Ukraine*
[2]*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37 Peremohy av., Kyiv 03056, Ukraine*
[3]*Lviv Polytechnic National University, 12 Bandera str., Lviv 79013, Ukraine*
E-mail: incors@ukr.net; geraimchuk@kpi.ua; orest.v.ivakhiv@lpnu.ua
[*]*Corresponding Author*

Received 12 November 2020; Accepted 19 March 2021;
Publication 18 June 2021

Abstract

The components of technologies of increasing information and energy efficiency of IoT monitoring networks subscriber systems with protected transfer functioning of reliable packets of information with the increased information capacity are described. In the places of formation of network flows, i.e. in the places of installation of object and on-board systems the realization of a complex of adaptive filtering algorithms, compression and protection of samples of monitoring signals and video data frames with the subsequent adaptive formation and transmission of highly informative code-signal sequences is offered. It is proposed a signal approach as a basis for inputting and compact coding of signals and video data frames of the reliable samples. The signal approach is proposed, according to which the amplitude-time or amplitude-number parameters of the most informative samples of signals and video signals are determined in the rate of input of monitoring data. These are extremes and points of inflection or points of curve movement change. The obtained data are subject to data compression with controlled information

Journal of Mobile Multimedia, Vol. 17_4, 465–498.
doi: 10.13052/jmm1550-4646.1741

loss and lossless compression-protection. According to the proposed information technology for building effective IoT networks for crypto protection of monitoring data arrays by processors of object and on-board systems, the use of disposable ciphers is proposed, which are the rules and parameters for generating crypto-resistant pseudo-random data arrays of a certain length. These rules and parameters are known only to the subscriber-transmitter and the subscriber-receiver of information packets and are used by network subscribers in the process of data compression with losses and without losses, in the process of crypto-resistant and noise-resistant information packets forming of limited duration with increased information capacity. Energy-efficient data packet transmission is based on a significant reduction in the output streams of protected highly informative monitoring data packets and the implementation by object and on-board systems processors a set of algorithms for processing, encoding, encrypting and transmitting data minimized by computational complexity.

Keywords: Packet data transmission, information efficiency, packet transmission, energy efficiency of data transmission, data compression-protection operational algorithms, secure information packets with increased information capacity, managed pseudo-random data transmission.

1 Introduction

The rapid development and application of the Internet of Things (IoT) is based on advances in microelectronics, energy-efficient processors, on-chip data acquisition systems, digital sensors, radio modules and routers [1–9]. Depending on the tasks and purpose of IoT networks, data transmission range, it is necessary to distinguish radio modules and routers of ISM frequency band [5–9], local-regional mobile networks (radio modules and routers LTE IoT, NB-IoT) and specialized stations and repeaters of satellite networks [8–11]. The wireless sensor, local-regional and global (satellite, microsatellite) IoT networks belong to packet radio networks. With the advent of protocols for the operation of branched and cellular packet radio networks with self-organization of information packet retransmission [5, 6, 12], it is provided the data transmission by IoT networks from various sensors, smart devices and systems within large areas covering hundreds of thousands of subscriber systems for various purposes. Depending on the tasks and problem orientation the IoT network are widely used in the construction of smart buildings and municipal property objects, in telemedicine, sports

medicine, to control the safety of movable and immovable objects, eco-monitoring of objects and territories, in industry (industrial networks and devices IoT), in energy, for information exchange and control of the mobile robots and drones as well as in other human activity areas [5, 6, 12–19].

It should be noted that Internet of Things (IoT) are essentially monitoring networks [20, 21]. The Internet of Things means are usually focused on long-term selection and transmission of measurement signals samples and various indicators. The monitoring signals and indicators are entered (selected) using digital and analog sensors. Monitoring of events, phenomena, processes, as well as various objects and subjects (hereinafter – monitoring and control objects, abbreviated – MCO) provides the implementation at the origin of network flows, i.e., at the monitoring objects, a set of long-term measurement and computational operations for selection and transmission to remote databases, cloud environments the most informative, accurate and reliable long-term monitoring data. Accordingly, the high-performance object systems, usually of wireless monitoring networks, are installed on or near the monitoring objects. Such objects systems operate under many limitations, including limitations on power consumption, CPU performance, radio transmitter power, object and on-board devices and systems weight and dimensions.

In this way, monitoring data is entered from digital and analog sensors that are installed at long-term monitoring facilities and subjects. Depending on the problem orientation of IoT tools and networks, the measurement data are temperature, pressure, humidity, output signals of multi-coordinate accelerometers, gyroscopes, sound signals, biomedical and biomechanical signals, two-level messages from motion sensors, proximity, perimeter crossing, etc. Important and informative monitoring data on MCO behavior are video frames and videos of limited duration with a predetermined (selected) image quality. The key requirements for effective IoT tools are long-term operation of on-board systems and devices using autonomous power supplies, reliable, crypto-resistant and interference-immune transmission of reliable monitoring data from served objects to remote databases and cloud environments.

2 Research Task Purpose Description

Given the parameters of channel resources (parameters of the IoT networks radio paths), the efficiency of IoT monitoring networks primarily depends on the information and energy efficiency of object and on-board systems and

devices. There are the on-board systems of IoT networks that convert the input monitoring data into the output information packets of the monitoring information. The purpose of the article is to substantiate the implementation of information-efficient and energy-efficient transmission of monitoring data in local (sensor), local-regional and global (satellite) IoT networks, taking into account: the formation of reliable primary monitoring data; minimization of calculations in the process of encoding and encryption of samples of monitoring signals and video data frames; formation of protected, i.e., crypto-resistant and noise-resistant, information packets with increased information capacity in places of network flows. This approach is the basis for minimizing information flows of monitoring data packets in the common channel resources of IoT networks, filling the channels with reliable data, ensuring the reliability and confidentiality of transmission and delivery of monitoring data taking into account the increased duration of object and on-board IoT networks.

3 Foundation of the Information and Energy-Efficient Transmission Implementation of the Monitoring Data Protected Packages

In monitoring radio networks, the effective transmission of information packets is achieved by solving a set of tasks in the places of installation of object systems (OS) of monitoring networks [20, 21]. These tasks are related to filtering and compression of monitoring signals and images, protection of compact arrays of monitoring data and transmission of information packets (IP), considering the operating protocols adopted as the basis of wireless data networks. Wireless sensor networks (WSNs), which typically operate according to the IEEE 802.15.4 standard with the ZigBee stack, are widely used to build such IoT networks. Also, the mobile LTE networks (LTE IoT), wireless IoT networks using LTE data transmission technologies NB-IoT, LoRaWAN have become widespread. Space networks of SpaceX company will be launched soon to build global IoT networks and promising microsatellite networks are under development. Obviously when using standardized and specialized data transmission networks with their protocols for transmission and retransmission of IPs, object and on-board systems (BS) of such IoT networks provide input of monitoring data, their compression with information loss, lossless compression and crypto protection of received data arrays. Symmetric cryptographic algorithms AES 128, AES 256 have become

widespread in processor modules for cryptographic data protection in the places of network flows origin.

Objects monitoring by means of IoT networks OS requires the decision of long measuring and computing operations complex for supervision over changes of monitoring objects parameters, express analysis of data of monitoring, estimation and forecasting of objects states for the purpose of detection and prevention of their abnormal (threatening) states MCO. An important task of data processing by OS processors is the analysis of the reliability of the entered monitoring data, determining the most informative areas of signals and fragments of video frames in order to primarily transfer information data to remote databases. In order to minimize the output flows of data packets by each OS and fill the packets with reliable and up-to-date monitoring information, it is important to analyze the information states of MCO and optimize data transmission taking into account the current state of MCO [19]. Accordingly, the adaptation of algorithms for the operation of the OS to solve the problems of processing, encoding and transmission of monitoring data is a necessary condition for improving the information and energy efficiency of the OS and BS IoT networks. Information efficiency is characterized by maintaining the maximum possible speed of transmission of informative and reliable monitoring data in radio channels of IoT networks, and energy efficiency determines the maximum duration of OS and BS from autonomous power supplies, providing monitoring data in micropower radio transmitters.

The basis of efficient data transmission in packet wireless networks, which are IoT networks, is the adaptation of algorithms for input, processing and encoding of monitoring data to the level of input noise in the measuring units of the OS and BS wireless networks. Also, the efficiency of OS and BS is influenced by algorithms for data protection, cryptographic data encoding and the formation or selection of channel sequences of the IP, taking into account the level of interference in the radio line "packet transmitter-subscriber – packet receiver-subscriber". Taking into account long-term operation from autonomous power sources and transmission of reliable and accurate monitoring data, processor OS and BS in the origin of network flows must implement a set of algorithms optimized for speed and accuracy of processing, encoding, encryption and transmission of various data [19].

General sequence of operations for encoding, encrypting and generating the monitoring data output packets is as follows:

(1) the adaptive filtering of signals and video data (video signals) compression with allowable information loss, including:

(1.1) the selection of one of the algorithms for determining the amplitude-time (number) parameters of the most informative, essential samples of signals and pixels of video data (global and local extremes, inflection points of bypass signals or video signals), including: with high accuracy; without filtering (i.e., without distortion); with adaptive filtering; with limited accuracy (without visual distortion of bypass signals and video signals); with a minimum number of essential samples or essential pixels (i.e., with the most compact data encoding without significant bypass signal distortions);

(1.2) the compact coding of parameters of essential samples (essential pixels);

(2) the operational compression-protection of data without losses, including compression of common binary sequences and adaptive compression of sequences using a dictionary; at the final stage there is the protection of compressed data using disposable ciphers (gamification of compressed data with crypto-resistant pseudo-random sequences);

(3) operational and adaptive noise-tolerant encoding of encrypted data and formation with masking in the output array of verification codes;

(4) adaptive formation of protected (crypto-resistant and noise-resistant) code-signal sequences of information packets with increased information capacity.

The nature of most processes to be monitored and studied is a continuous temporal function. Each input signal is characterized by minimum and maximum values of amplitude and frequency parameters, respectively, $X_{\min}$, $X_{\max}$, $f_{\min}$, $f_{\max}$. The most informative (essential) signal samples or video signals pixels are extremes (E) and inflection points of curve (IPC), namely, points of change of the convexity of the envelope. In addition to the amplitude-time values, the signals essential samples (ES) or the video signals essential pixels (EP) are characterized by additional parameters such as current input signal-to-noise ratio in the vicinity of ES (EP) $\delta^N_{in\,i}$ and the parameters of the current dynamics of the envelope signals and video signals [19], i.e., a current estimation of the value of the input signal-to-noise ratio in the vicinity of the ES (EP) is as follow:

$$\delta^N_{in\,i} = \Delta X^N_i = |X^F_{ES\,i} - X^N_i| -, \tag{1}$$

where $X^F_{ES\,i}$ – is the current significant sample of the filtered signal, X^N_i – is the current input sample of the noisy signal, $i = 1, 2, 3, \ldots$ is the number of the current sample.

When entering video data frames by video sensor means the arrays of *R*-, *G*- and *B*-frames are formed. The set of pixels of the latter horizontally and vertically form a video signal. The current parameters of the dynamics of the signal envelops and video signals are characterized by the current difference between neighboring samples filtered signal

$$\Delta X_i^F = |X_i^F - X_{i+1}^F| \tag{2}$$

or the difference between neighboring essential samples ES (pixels EP)

$$\Delta X_{ES\,i} = |X_{ES\,i} - X_{ES\,i+1}| \tag{3}$$

For reliable signal input, its sampling frequency f_s is chosen significantly increased considering the expression:

$$f_s = k \cdot f_{sN} = 2k f_{\max}, \tag{4}$$

where $k > 5 \ldots 10$ is the sampling rate increase factor taking into account the parameters of the input low-pass filter and requirements for the reliability of the lower bits of the analog-to-digital converter, f_{sN} is the signal sampling frequency according to Nyquist theorem [12], f_{max} is the highest informative frequency of the signal spectrum.

At the maximum number of bits of the analog-to-digital bit converter $q_{\max} \geq 10 - 12$ bits there is the factor $k > 10 - 12$. Therefore, in order to quickly implement the adaptive signal filtering, the thinning factor of the input samples without loss of coding accuracy of the signal envelops $k_t = 2 - 3$. The parameters of the implementation of adaptive filtering are determined depending on the promptly calculated current slope of the signal in relation to the maximum expected (predetermined) slope, i.e.

$$\Delta X_i^F \leq X_{i\,\max}^N. \tag{5}$$

In the process of entering data from long-term monitoring objects, it is important to control the conditions of input of signals and video signals and the degree of their distortion by noise and interference. After signals filtering and compression the data of optimization of processing of input data are fixed in the service information, namely, noise-free fragments of signals (video signals) are coded qualitatively, i.e., with the increased frequency of data input and the maximum necessary quantity of ADC bits, areas with noise are identified, filtered by simplified algorithms, thinned out and coded less accurately. For a more detailed analysis of the signal readings reliability, the

value ΔX_i^N is analyzed at appropriately defined signal areas (for example, in the duration of informative signal complexes or segments of a given duration in the vicinity of extremes and inflection points) or for the duration of the entire monitoring data sample.

After signals filtering, the ΔX_i^N indicators are used in the process of concise coding of the amplitude-time parameters of the most informative, essential signal samples. Taking into account the defined values ΔX_i^N, in the process of data encoding with allowable information loss, the number of valid bits is calculated for each essential count of the current sample. Based on the obtained data, noise-free signal areas, signal areas with different levels of input noise are determined and encoded.

For simplicity of coding, considering the peculiarities of applied research, it is advisable to determine and encode noise-free (reliable) and noise-distorted (less reliable) areas of signals. The coding results of the monitoring networks object systems are transmitted to the central station of the radio network for a more detailed analysis of signal samples and final decisions. Also, according to the instructions of the central station, on request, object systems can transmit primary data without filtering. It should be noted that the distortion of the waveform is significantly affected by the methods and algorithms of signal (video signals) filtering. Distortions of the shape of the analog signal curve also significantly depend on the choice of the sampling frequency of the analog signal and the metrological characteristics of the ADC.

As for the distortion of video data, i.e., the output data of video sensors, it is necessary to note the following. As a rule, video modules with the set characteristics of quality of reproduction of the fixed video frames and moving video in the conditions of presence of daylight and its absence are chosen for video monitoring. Modern video modules are characterized by a focus on a variety of tasks and provide pre-processing of the output data of the video sensor. The processor means of the video module primarily provide the formation of the output R-, G-, B-data based on the averaging of the digitized output source data of the sensitive elements of the corresponding color of the matrix of the video sensor. That is, already at this stage of video data processing there is a distortion of the original video data. Processors of video modules can also filter the output video data, compress it and quickly process video data frames. It should be noted that in many applications, the filtering of video data (i.e., primary R-, G-, B-data arrays, which are essentially video signals) and their compression with certain losses is not allowed (in space monitoring tasks, in monitoring using unmanned aerial vehicles, in security

monitoring systems of objects and subjects, etc.). This approach is important when recognizing small image details and small objects in the video frame. In such cases, video modules with improved image reproduction quality (4K, 8K, etc.) are used. However, such video modules are less energy efficient.

In the case of video modules with video filtering, which is determined by the feasibility of selecting such video modules, there is no possibility of prompt quality control of input video and subsequent compression of loss data, it is important to encode/decode the amplitude-time data without distortion. It is necessary to accent that convenient data compression algorithms usually deformed parameters of the ES. Therefore, in specialized monitoring video systems adaptive filtering, optimized for computational complexity and accuracy of video data encoding, is preferred). For widespread use of IoT networks with video monitoring, it is advisable to encode video data without the use of energy-intensive video codecs, which also significantly distort video data. To minimize the information flow when transmitting video data on radio channels with limited data rates (for example, when using radio modules of ISM-frequency band), it is reasonable to periodically transmit compressed video data with quality video frames and videos of limited duration and quality.

In order to quickly and accurately filter the signals depending on the steepness of the signal among the samples falling into the current window of analysis and data processing, it is advisable to compare the amplitude values of current samples to identify the input samples largest and smallest amplitude values samples and ignore them in further data averaging or search median. Accordingly, samples quantity that affect the filtering result is limited, for example 3 or 5, and characterize the tendency to change the signal envelops. The result of averaging the remaining samples in the current window of analysis and processing of data, which in amplitude is close to the median, is the result of filtering and is determined by the expression:

$$X_i^F = (X_b^N + X_c^N + \cdots + X_d^N)/l_i, \tag{6}$$

where X_b^N, X_c^N, X_d^N is a selected number of input samples with noise that is close to the median amplitude, $l_i < l_a$, l_a – is the size of the analysis window and the averaging of the input samples (depending on the steepness of the signal the value $l_a = 3, 5, 7, 9$). To determine the median based on comparisons of the amplitude values of the respective samples in the window of analysis and data processing, the samples are ordered, for example, in increasing amplitude. After samples arranging, the central count l_a is determined among the l_a samples.

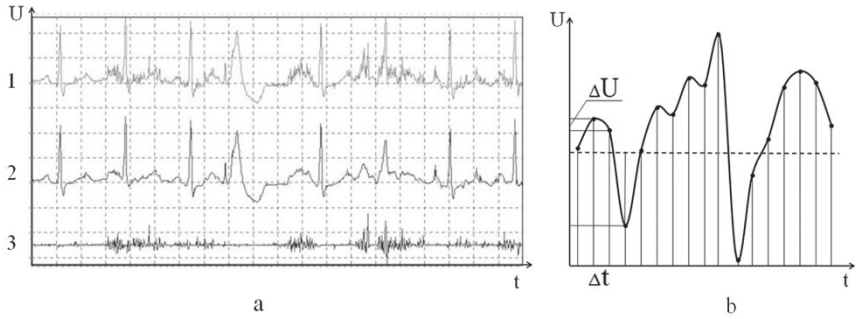


Figure 1 Filtration of the electrocardiographic signal monitoring and its essential samples determination.

To explain the processes of operational control of the reliability of the entered data and compact coding of monitoring signals by means of the OS, consider the curves shown in Figure 1. The curve 1 (Figure 1, a) shows the electrocardiographic signal (ECS) obtained during the daily monitoring of the cardiovascular system of the human body. Certain areas of such a signal may be distorted by input noise. After filtering, there is obtained a filtered signal (Figure 1, a, curve 2), in certain areas of which (in areas of ECS with noise) there are unaccounted distortions. That is, the data obtained after filtering are inaccurate. Prompt determination of such distortions of the envelope of the filtered signal is possible based on the analysis of the difference signal (Figure 1, a, curve 3). Indirectly, the difference signal characterizes the level of input noise. The location of significant samples of the filtered signal is shown (Figure 1, b).

Thus, in order to minimize computational operations during the processing, encoding and transmission of long-term monitoring data, it is important to organize a compact coding with allowable (controlled) losses of measurement signals information, video data (moving frames and still images), as well as rapid analysis of input data and for operative detection of the most informative arrays of monitoring data and operative transfer to the central server of the monitoring network. Since information about events, natural phenomena, research results and monitoring of various objects and subjects, the quality of technological processes and research results are introduced into the data network of computer systems in the form of signals and video signals during the processing and encoding inputs data it is important to identify the most informative and reliable readings of the signal envelop (video signals), i.e., ES or EP. The accuracy of coding of amplitude-time parameters of ES

(EP) significantly depends on the features of applied research, data entry conditions (absence or presence of noise in the measuring links of object systems, the presence of vibrations, etc.), functional orientation of object systems of computer networks and is selected adaptively, for example, among the following signal encoding modes:

(1) The accurate coding of amplitude values of extremums with the maximum number of bits and the maximum signal frequency (this mode is used to ensure reliable and accurate information flows in the network).
(2) The accurate coding of ES (EP) parameters and intermediate ES (EP) parameters on the most informative signals areas with high polling frequency.
(3) The less accurate coding of the amplitude values of the extremums and some ES-IPC (essential samples – inflection points of curve) with fewer ADC bits and the minimum polling frequency, while low-amplitude extremes and some adjacent ES are ignored, taking into account the minimal distortion of the visual characteristics of the signal envelop coding of signal areas with noise).
(4) The less accurate coding of extremum parameters (to minimize information flows).
(5) The accurate coding of ES (SP) of the output data of sensors and video modules with filtering of signals and images.

Accordingly, when inputting and processing the signals and video data frames, the amplitude-time characteristics of the most informative signal and video signals readings, including global and local extremes and signal inflection points, are operatively determined and compactly encoded. The basis of compression and high-quality signal recovery is the signal envelop characteristics preservation, considering the requirements and features of applied tasks, areas of application of adaptive data coding algorithms. Herewith, in the process of ES (EP) parameters compression with allowable (controlled) information loss, it is advisable to determine quickly the most informative signal (noise-free) areas, where ES (EP) parameters are encoded as accurately as possible and less informative areas with noise in which maximum data compression is achieved (due to less accurate data coding).

When restoring the bypass signals due to the operative classification of signal sections, a message is formed for researchers (experts) about the type of curve (reliable/less reliable). In order to optimize the coding of signals with allowable information loss, it is advisable to introduce several modes of ES (EP) coding, for example, with high accuracy of ES (EP) parameter coding,

i.e., without signal filtering (any signal filtering leads to envelope distortion), with adaptive filtering signals, with limited accuracy of ES (EP) (for example, with a smaller number of ADC bits), with the formation of the minimum number of ES (EP), i.e., in this mode, the maximum data compression is achieved with allowable information loss.

When encoding video signals generated by video sensors in video data frames (on rows and columns), it is important to accurately transmit the amplitude-numerical parameters of the extremes and inflection points of video signals. As a result, when decoding compressed video data (with allowable losses and without losses), the envelopes of video signals in moving and still video frames are accurately restored, which is the basis for reliable reproduction of encoded video data.

In the case of adaptive filtering in the process of the signals operational processing and coding based on the signs analysis of difference values ΔX_i^F and $\Delta(\Delta X_i^F)$ it is determined the amplitude-time parameters of the signal envelop ES, including extremes and inflection points of the curve, where, for example, the current variance of neighboring samples X_i^F and X_{i-1}^F of the filtered signal is as follow

$$\Delta X_i^F = X_i^F - X_{i-1}^F, \tag{7}$$

where $i = \overline{1, v}$ is the numbering of the current input samples of the signal, v is the samples maximum number that can be accumulated in the RAM of the object system processor module. Depending on the operationally determined indirect estimates of the input signal-to-noise ratio in the vicinity of the ES is as follows

$$\Delta X_{ES\,i}^N = |X_{ES\,i}^N - X_i|. \tag{8}$$

And depending on the following condition existence

$$\Delta X_{ES\,i}^N \leq \delta_d^N \text{ or } \Delta X_{ES\,i}^N > \delta_d^N, \tag{9}$$

compressed arrays of difference amplitude-time parameters of the signal ES are formed. The signal area formed by two or more neighboring ES, for which the condition $\Delta X_{ES\,i}^N < \delta_d^N$ is fulfilled, is considered as noise-free. Accordingly, the signal samples form sequences of noise-free signal regions (reliable signal regions) or noise-distorted signal regions (less reliable signal regions). Based on the adaptation of the input data encoding depending on the quality of data input (reliable/less reliable areas of signals), it is fulfilled accurate (with more ADC bits $q_{\max}$) or less accurate (with fewer ADC bits $q_{\min}$) amplitude parameters signal ES coding.

Thus, a significant advantage of the compact coding algorithm of the signals samples and video signals using the signaling approach is the fact that in the process of analog signals compression provides a reasonable decision on the coding accuracy of the most informative signals (video signals) samples, which are used on the receiving side for accurate recovery of analog signals envelop. By minimizing computational operations, compact data encoding algorithms with controlled information loss are optimized for speed and coding accuracy. After the implementation of operational adaptive filtering of the signal samples and determination the amplitude-time parameters of the ES-extremums, there is obtained the ES parameters at the signal areas with noise. The ES parameters related to clean areas are subject to further refinement. Depending on the type of coding of the monitoring data, including the coding with filtering, the coding without filtering, the coding with $q_{\max}$ use, the coding with $q_{\max}$ and $q_{\min}$ use, the stream of output compact data is coded as a stream of service and information monitoring data [19].

When encoding data only with $q_{\max}$, for example, in the encoding mode of input data without performing adaptive filtering (in the case of transmission of input data without distortion or in the case when sensors or video modules output data with filtering) the sequences of bit streams with a field of common service information and difference bit streams of amplitude and time values of ES signals or ES video signals are formed. When encoding signal samples and frames of video data with adaptive filtering and use $q_{\max}$ and $q_{\min}$ the sequences of bit streams of general service information and compressed data of the corresponding signals or video signals areas (areas free from noise and areas with noise or vice versa) are formed. In this case, the compressed data of the signal areas (video signals) are encoded with the field of service information of the adaptation parameters and the field of the difference bit data of the amplitude and time values of the ES (EP).

The obtained data stream after the signal samples and video data frames compression is subject to operational compression without loss and protection of compressed data arrays using disposable ciphers. The obtained data stream after compression of signal samples and frames of video data is subject to operational compression without losses, protection of compressed data sets using disposable ciphers and noise-resistance encoding [20, 21]. As a result of complex coding and encryption of monitoring data, signal samples and video data frames are transformed into protected compact pseudo-chaotic arrays of informative break-even data. The resulting arrays can be stored in object or on-board drivers and are the input data for the formation of the output IP of the IoT networks object and on-board systems.

4 Adaptive Formation and Transmission of Highly Informative Protected Packages

Highly informative transmission of compressed and crypto-protected monitoring data in IoT networks is achieved by increased information speed of information transmission R_i with limited channel speed R_c, i.e.,

$$R_i = k \cdot R_c, \tag{10}$$

where k – is the coefficient of exceeding the information rate of data transmission in relation to the channel data rate $k \gg 1$. Providing high information efficiency of data transmission in packet radio networks is achieved by maintaining the maximum possible current data rate R_i, i.e., $R_i \rightarrow R_{i\,\max}$ using the means of the OS and OBS [12]. With a limited value of the operating frequency band F, the maximum channel data rate is determined by the expression as follows:

$$R_{c\,\max} \leq 2F/k_s = 1/k_s \cdot T_b, \tag{11}$$

where, $F = 1/T$, $T = 2T_b$ – is the bit sequence repetition period, T_b – is the bit sequence duration, $k_s > 1.4$ – is the coefficient taking into account the quality of digital (two-level) signal edge restoration [12] (i.e., for high-quality digital signal transmission of digital signals in the radio channel, part of the operating frequency band must be allocated for the pulse signals with steep edges transmission).

It should be noted that the minimum duration of bit sequences is limited, respectively $T_b \geq T_{b\,\min}$. Therefore, a significant increase in data rate $R_i \gg R_{c\,\max}$ is achieved through the implementation of object and on-board processors and specialized means of compression of monitoring data with loss of insignificant information and without loss, the formation of code-signal sequences (PCB) packets with increased information capacity [20, 21]. The maximum data rate $R_i \rightarrow R_{i\,\max}$ in radio networks significantly depends on the energy signal to noise ratio in the radio channel E_{is}/J_0 [12], where E_{is} – is the energy of the useful signal (energy of IP coded signal sequence CSS), J_o – is the energy of total noise and interference in the radio channel. In this case, to ensure the maintenance of a given errors probability level in data transmission P_n (for example, $P_n \leq 10^{-6}$) requires support by OS and BS and timely correction of the minimum required energy ratio $(E_{is}/J_0)_n$ in the radio channel. That is, it needs to maintain the energy of the radio channel. With limited power of radio transmitters OS and OBS, the energy of the radio

channel significantly depends on the base of the useful signal B [12], where $B = F \cdot T_{is}$.

Thus, the implementation of information-efficient transmission of IP is achieved through the maximum compact data encoding at the information level of OS and BS means, the choice of the minimum required base $B_{\min}$ of channel signals to support the ratio $(E_{is}/J_0)_n$ in the radio channel, the implementation of effective methods of noise-immune IP data encoding. Depending on the noise level in the radio channel, the speed increase $R_i \rightarrow R_{i\,\max}$ is achieved on the basis of data transmission using multi-position signals with T_b duration and $B \leq 1$ base, two-level interval signals with the base $B \geq 1$, parallel data transmission using independent L code mono channels in the operating frequency band F at $B > 10$ [20]. Taking into account the service data of the IP and the need for support by subscribers in the radio channel the value $\gamma_n = (E_{is}/J_0)_n$ by selecting the minimum base CSS IP $B_{\min} = f(\gamma_n)$, the speed of information transfer is determined by the expression:

$$R_{i\,\max} = \frac{K_{ci}(\delta_d^N) \cdot L}{k_{ds} \cdot k_s \cdot T_b \cdot B_{\min}(\gamma_n)}, \tag{12}$$

where $K_{ci} = k_1 \cdot k_2 \cdot k_3$ is the total data compression ratio by means of BS and OS information level of IoT networks, $k_1 = k_{1\,c}(\delta_d^N)$ – is the compression ratio of signals and video data with allowable information loss, which significantly depends on the assessment of the allowable level of input noise δ_d^N in the vicinity of ES (EP) of signal or video signal envelopes, k_2 – is the data compression ratio without losses, $k_3 = k_3(n, B_{\min})$ is the coefficient of the IP duration reduction in the process of CSS packets forming, which corresponds to the additional lossless compression ratio in the process of IP transmitting, n – is the number of bits transmitted by the CSS packets, $k_{ds} \geq 1.1$ – is the factor that takes into account the IP service information, $B_{\min}(\gamma_n)$ – is the minimum required base of CSS IP for the implementation of noise-immune data transmission.

Thus, taking into account the change in the energy of signal to noise ratio in the radio channel to a large extent to ensure reliable and high-speed transmission of data packets (IP) by processor means OS and BS of monitoring wireless networks (MWN), it is necessary to implement the adaptive choice of noise-immune coding algorithms and the structure of the channel sequences of the IP taking into account the noise level in the radio channel. Therefore, the coefficient of exceeding the information data rate in relation to the channel data rate significantly depends on the total data

compression ratio K_c, the base B of the channel sequences of the IP and the service data ratio $k_{sd} > 1$, which takes into account additional losses in the formation of noise-immune data arrays and data packets transmitting. In the first approximation it is obtained as follows:

$$k = R_i/R_c = K_c/B \cdot k_{cd}, \tag{13}$$

where $K_c = K_{c\,i} \cdot K_{crt}$, K_{ci} – is the data compression ratio at the information level of OS and BS of monitoring wireless networks, K_{crt} – is the data compression ratio at the radio level of OS and BS means. This ratio considers the number of mono channels in frequency, code or spatial separation of data channels.

Accordingly, the reliable and secure information transmission in radio networks is ensured by network subscribers maintaining the minimum required signal-to-noise energy ratio in the radio link, providing conditions for reliable synchronization of code-signal sequence CSS IP reception and their recognition on the receiving side, implementation of object (on-board) processors of subscriber systems of radio networks of high-speed and operational algorithms of filtering, compression and protection of monitoring data [19], noise-tolerant data coding and formation of protected IPs. The efficiency of IP transmission in wireless networks is achieved by filling the information frames of packets with reliable monitoring data, reducing information flows in places of installation of OS and BS IoT networks by adapting the encoding of input data depending on data input quality with increased information capacity [20].

In the process of input, processing and coding of signals it is important to determine their reliability (reliability of current samples and signal areas) and depending on the indirectly determined noise level in the measuring links to organize economic data coding. Operational calculation of the monitoring signals sampling indicators and their analysis allows to estimate the data reliability and determine the information status of MCO in the places of IoT networks installation. Based on aperture control of statistical, spectral, correlation, chaotic and entropic characteristics of signals operatively information states of objects are operatively defined and coded and minimization of information streams in monitoring networks is reached.

Along with minimizing the original reliable and secure flows of monitoring data packets in the places of their formation, in order to ensure the reliability of communication, it is necessary to provide favorable conditions for radio communication. The range of radio communication depends significantly on the conditions of direct radio visibility. For the transmission of data

packets over long distances, the technology of self-organization of packet transmission between registered subscribers of cellular and cluster networks has become widespread. It should be noted that the self-organization of the transfer leads to a significant (almost an order of magnitude) reduction in data rate. Therefore, an effective solution for the implementation of reliable data transmission over long distances (tens of kilometers or more) is to install in each cell high-altitude repeater subscribers with directional antennas for data retransmission in the main and backup directions of data transmission. The power of transmitters is minimal (tens of miliWatt), any subscriber of the respective cells has the addresses of intermediate subscribers-repeaters, and the self-organization of packet transmission is implemented in the local areas of the respective cells.

In case of failure of one or more repeaters, considering the location of operating repeaters, their current energy reserve, according to the previously calculated options for the formation of address directions, the transmission of packets to remote subscribers. Efficient repeaters are energy-independent mini-balloons with power supply via a strong and light cable. Stationary repeaters at appropriate heights with retractable telescopic antenna systems are possible. In radio networks of long-term monitoring of facilities for the use of subscribers-repeaters of mobile and satellite networks, microsatellite networks, considering the delays in the retransmission of packets, the transmission of monitoring data over long distances (hundreds of thousands of kilometers).

An important component of information processing and encoding at monitoring facilities is the protection of data from unauthorized access and their substitution by unauthorized users of the computer network. It is important for pairs of subscribers (subscriber-transmitter and receiver of an individual entrepreneur) to encrypt data at the same level with a high degree of data protection and send them to the means of interconnection. Preference should be given to combined methods of information protection, which provide both software and hardware implementation of the formation and transmission by subscribers of the monitoring network of protected information packets at the information level and at the level of channel sequences. In this case, with each transmission of the current information packet, the rules of cryptographic data protection must be variable.

In this case, information about the current rules of encryption and decryption of data (private and session keys) should be known only to the transmitter and receiver of packets. In the case of packet transmission between remote subscribers of the local-regional and global network with

the help of intermediate subscribers, the current session keys are formed and distributed. To change the keys by wireless network subscribers, it is advisable to use asymmetric cryptography methods. The prospect of information protection by object and on-board systems of IoT networks is a combination of cryptography, noise-resistance coding and computer steganography, the joint application of which allows to organize efficient radio transmission with noise presence of crypto-resistant and noise-resistant data packets. Given the great computational complexity of the implementation of asymmetric methods of information protection limited in the OS and BS processor means performance, it is advisable to use the combined information protection at the level of information compression-protection algorithms, the noise-resistance coding of data arrays as well as at the level of formation, the CSS IP transmission and reception.

With the rapid development of high-performance processors, computers, and supercomputers, the resources of which are used to decrypt data, the degree of information protection by MCO subscribers of the monitoring wireless network depends on the areas of application of MCO, requirements for the duration of guaranteed time cryptographic protection (hours, days, months, years) . The degree of protection depends on the length of the private key L_{sc}, which is known only to a single subscriber, and on the lengths of the current session key. For practical reasons, the degree of protection of information is calculated by the following formula

$$P_p = 2^{L_{sc}}, \tag{14}$$

so to access the received encrypted information, attackers need to use a search method to analyse all possible combinations of relevant bit sequences in data arrays of a certain volume.

To effectively decrypt the data, it is necessary to have a large amount of additional data, including information about the structure of the current IPs, their number, the length of private and session keys, etc. parameters. To increase the possible combinations of bit sequences, it is advisable in the protected data sets to provide for the appearance of various bit sequences from the most possible combinations. Given the high rate of development of high-performance processors, specialized computers and supercomputers, the emergence of quantum computers, it is necessary to choose large enough, for example, 4096 bits.

It should be noted that the radio channel is open to any subscriber of the radio network who owns a specialized receiver. However, the reception of CSS protected packets is possible if subscribers have a significant amount of

a priori information and data decryption rules. Therefore, for effective protection of information in radio networks, it is advisable to change the parameters of data encryption of information frames, the formation and transmission of CSS IP, the amount of information transmitted by the current packet, etc. package parameters. Effective protection of information in wireless networks is the use of blockchain technology [16], which allows to control all traffic for a particular subscriber, for various ways of relaying data and the network as a whole. Based on the calculation of the hash functions of primary transactions, the conditions for detecting the facts of intrusion of intruders into the network by means of authorized wireless network subscribers are provided. Some important information should be transmitted in the mode of covert data transmission in the noise of the radio channel using noise-like CSS IP (CSS-NLS) with a large base B(NLS means noise-like signals). Without knowledge of the rules and parameters of the formation and transmission of such CSS-NLS the third-party subscribers of the radio network will not be able to receive hidden in the noise channel sequences.

To ensure the reliability and efficiency of reliable IP transmission, it is important to implement by object and on-board systems of the wireless networks the adaptive methods and algorithms for noise-immune coding of data transmitted in the radio channel with noise. Since the energy signal to noise ratio in the radio channel varies widely, for reliable and efficient IP transmission (on the first attempt and with minimal loss and amount of service data) with a predetermined probability of erroneous reception of the code sequence P_n, the wireless networks subscribers must adaptively select the algorithms of noise-immune coding and forming noise-immune CSS IPs to maintain the minimum required signal to noise energy ratio in the radio channel and packets with a minimum duration transmission.

In practice, a combination of noise-resistance coding, data mixing, and noise-immune channel signal (CS) algorithms is effective, including the use of CS with entropy signal manipulation methods. A promising direction of noise-resistance coding is the introduction of a priori information in the IP by encoding data frames (DF) packets using pseudo-random sequences (PRS), including the use of dependencies between PRS bits on the transmitting and receiving sides, such as Galois field codes [21], with the formation of signal correction sequences.

For efficient data transmission of a pair of subscribers (transmitter and receiver of an individual entrepreneur) of a wireless network that have access to the radio channel, using session secret codes and by monitoring the current state of the radio channel, provide the formation of crypto-stable

and noise-immune IP based on the transformation of compact data sets into chaotic data using procedures for the formation of crypto-stable controlled chaos. Thus effective noise-resistant coding and data recovery by means of OS and OBS is reached on the basis of the complex approach to the decision of problems of correction of errors in the course of data transmission on radio channels taking into account the a priori information which is laid by the subscriber-transmitter of the IP in concise, crypto-stable and noise-immune data and using the accepted verification codes of the IP. One of the ways to increase the efficiency of radio networks with limited frequency resources is to increase the informativeness (information capacity) of data packets [20] based on the transmission of short-duration IP with pseudo-chaotic selection of key protected CSS packets.

The proposed technology of the information-efficient radio networks formation is one of the approaches to creating promising cognitive networks for secure transmission of information in the Internet of Things, to build networks for multi-day monitoring of subjects and objects, creating intelligent sensors and video modules with effective software video codecs for their installation on mobile robots, unmanned aerial vehicles, vehicles and persons with long-term monitoring need. For reliable, secure and noise-immune data transmission on each OS and BS, which is the source of packets, it is important to minimize the number of limited duration IP transmissions and increased information capacity. The solution of this problem is based on determining the most informative, signal essential samples and video data frames pixels, compression and protection of monitoring data arrays, as well as by express processing of monitoring data by OS processors to determine the most informative data arrays to be transmitted to remote servers and databases.

Due to the constant analysis of the noise level in the radio channel and the adaptive choice of the minimum base of the CSS ($B_{\min} = 1$, $B_{\min} \geq 1$, $B_{\min} > 10$) by the two subscribers conducting the packet transmission, the required signal to noise ratio in the radio channel is maintained. Additional coding to increase the IP transmission noise immunity is the introduction of a preliminary relationship between the bit sequences of the current CSS and signal characteristics transmitted to the modulator (manipulator) of the OS (OBS) radio transmitter, the formation and transmission of CSS verification codes of PI with increased base. Also effective mixing of data in the process of forming the CSS group of the IP in order to fight with error packets, when the channel interference affects a large number of CSSs of one or more packets, making additional dependencies between a group of adjacent bits

of the data array, the use of a priori information embedded in compressed and encrypted data arrays, use of hidden numbering of ES signals and EP of video data frames, transmission of IP with a previously known amount of CSSs or with a fixed amount of information, formation of intermediate verification codes at each stage of data coding before IP transmission (after compression of data with allowable losses, after compression-protection of data without losses, after mixing of data, after coding with introduction of dependences between group of the next bit data, after formation of CSS IP), the use of efficient and fast algorithms for noise-immune data coding in order to combat single and multiple errors detected on the receiving side.

Given the available channel resources (operating frequency band F, number of frequencies L_f, code L_k and spatial L_p mono channels) information is transmitted in short portions of information, the length (value) of which is mainly variable and is measured in thousands of bits. The efficiency of the radio network is characterized by the current maximum transmission rate of the IP $R_{\max}$, the value of which significantly depends on the quality and system indicators of channel resources (values F, $L_\Sigma = L_f + L_k + L_p$, the energy of the signal to noise ratio in mono channels) and parameters of adaptive processing, coding and data transmission, i.e.,

$$R_{\max} = f(F, L_\Sigma, P_n, (E_b/J_o)_r,\ 1/B, K_c). \tag{15}$$

where P_n is the probability of erroneous code sequence, $(E_A/N_o)_r$ is the required energy signal to noise ratio in the mono channel, K_c is the total data compression ratio, including data compression before the formation of the IP (compression with allowable loss of signals/video signals and compression of bit sequences without loss), as well as data compression in the process of formation and transmission of the IP.

Depending on the choice of the CSS base to support the energy of the radio channel (maintenance of the energy ratio $(E_A/J_o)_H$) and the method of the current CSS IP forming, the maximum data rate $R_{i\ \max}$ is variable. In the presence of significant noise and interference in the radio channel in order to ensure monitoring data packets reliability (delivery) from remote MCO by means of OS and OBS it is necessary to form a loss CSS SP with NLS. This leads to sharp drop in the speed of information transmission in IoT networks. A further increase of the information transmission speed in radio networks with NLS is associated with an increase in the number of code mono channels of data transmission with NLS, which complicates the digital multi-channel NLS receiver and requires the use of high-performance multiprocessor microcontrollers and specialized FPGAs.

5 Energy Efficient Transmission of Data Packets in IoT Networks

The implementation of information-efficient packet transmission in radio networks [19] is the basis for the energy-efficient data transmission in IoT networks. Due to the maximum compact coding of monitoring signals samples with preservation of high accuracy coding of the most informative and reliable samples of signals and frames of video data, operative compression-protection of data arrays, formation of the minimum duration of crypto-stable and noise-immune information packets with the increased information capacity [20] the minimization of IP output streams by each OS (BS) in places of origin of input network streams is reached. Minimization of energy spending is also achieved using simplified radio modules in the means of OS and BS (radio modules for widespread use of ISM frequency band).

A significant increase in the information and energy efficiency of monitoring data transmission is possible based on the value $K_{ci} \rightarrow \max K_{ci}$ optimization by achieving maximum data compression ratios with allowable information loss and without losses, where K_{ci} – is the total data compression ratio at the information level before transmission and during transmission. First of all, this problem is solved by reducing the number of ESs in signal areas with noise based on the selection of the most high-amplitude ES in the current ES group, which are found in the vicinity of global and local extremum and inflection points on the filtered curve, ignoring inflection points in highly dynamic areas signals and video signals, as well as the choice of a reasonable minimum number of ADC bits in the process of compact coding of ES areas of the signal with noise. In such cases, it is important to provide encoding and recovery of bypass signals and video signals without significant visual distortion with a minimum number of ES extremes.

As a result of complex data compression, the flows of monitoring data to be transmitted are reduced at least tens to hundreds of times. This in turn significantly saves the energy of the autonomous power supply OS and BS due to the minimal use of subscriber radio transceivers. A significant reserve for reducing energy consumption by OS and BS is the use of processor algorithms for compressing and protecting arrays of monitoring information, converting n-bit sequences of crypto-stable and noise-immune data arrays in CSS IP of minimum duration with minimal computational operations [19].

6 Discussion of Analysis and Research Results

The analysis of expressions (4) and (12) identifies ways to minimize the network flows of monitoring data in their places of origin, as well as approaches to improving the information and energy efficiency of IoT networks. Significantly increase the efficiency of IP transmission in IoT networks is possible on the basis of optimizing the amount of data compression $K_{ci} \to \max K_{ci}$ at the information level of the OS and BS by achieving the maximum value of the coefficient with allowable information loss $k_1 \to k_{1\,\max}$. The optimal solution to this problem is to minimize the number of ES (EP) signals and video signals, considering the requirements to avoid visual distortion of the bypass. Except for unique monitoring tasks that require the use of high-metrological sensors and ultra-high-resolution video modules, the most IoT applications require timely, reliable and secure delivery of monitoring data for further detailed analysis. Therefore, taking into account the peculiarities of application tasks, parameters of measuring signals and output data of sensors and video modules, it is necessary to select appropriate parameters for input signals and images, indicators of input data evaluation and on their basis to provide compact coding and transmission of reliable monitoring data.

Given the choice of too redundant frequency of signal input, considering the maximum informative frequency on less dynamic and sloping sections of the bypass signals, it is advisable to increase the interval of interrogation and analysis of signals. This can be done based on the analysis of the differences between the current readings of the signals and will reserve the time of the OS and BS processor for complex encoding and data encryption. Accordingly, the increase of the data compression ratio and the speed of compact coding is achieved due to prompt selection of the maximum allowable sampling interval and analysis of the current samples; reduction of the number of ES (EP), especially in less reliable (in areas with noise) and sloping areas of the signal; determination of IPC only on noise-free areas of the signal (on highly dynamic areas of signals and video signals of IPS can be ignored); by sampling less reliable parts of the signal with the maximum allowable interval, which guarantees the achievement of the minimum required data compression ratio $K_{c\,\min}$.

In the process of long-term monitoring of MCO states it is formed the samples of input data $\{X_{ik}^{N}\}$, where $i = \overline{1,s}$, s – is the maximum number of the channels for monitoring data input, $k = \overline{1,r}$, r – is the maximum number of signal readings of the current data sampling for i – *th* input data channel. The amount of the input data significantly depends on the

areas of application of the OS and BS and their functional orientation, the accuracy of coding of input signals and images and the time of data entry to form the necessary samples of monitoring data. Due to the execution of OS and BS CPU of current computational operations with using input data and filtering operations, the data compression with allowable information loss, lossless compression and the data crypto-protected, noise-immune coding and formation CSS of output SP from the input data array $\{X_{ik}^{N}\}$, the arrays of filtered data $\{X_{ik}^{F}\}$, the compressed data with loss of information $\{X_{ik}^{CL}\}$ and without loss $\{X_{ik}^{CWL}\}$, the crypto-protected $\{X_{ik}^{CDP}\}$ and noise-immune $\{X_{ik}^{NDP}\}$ data, from which are formed sets of information packets CSS, where $b = \overline{1,p}$, $c = \overline{1,f}$, $d = \overline{1,h}$, $f < p < k$, $h > f$.

That is, in the process of performing of a computational operations sequence, the volumes of entered, filtered and compressed monitoring data are reduced, which, after crypto-protected and noise-resistance encoding, are the basis for forming and transmitting CSS IP of appropriate duration, usually variable. In the presence of conditions of direct radio vision of the monitoring network subscriber systems and clean from noise and interference the radio channel, the duration of the IP is selected as the maximum, for example, units-tens of thousands of intervals T_b. In the presence of interference, the duration of the IP is chosen to be much shorter. The current value $R_{i\,\max}$ should be determined during the transmission of each packet as the amount of information of the information frames of the packets in bits, which is transmitted during the current employment interval of the radio channel t_3, i.e.

$$R_{\max} = N_{V:}/t_3 = N_{ik}/(t_{dp} + T_{in} + T_{nk}), \tag{16}$$

where N_{ik} is the number of IR bits, t_{dp} – is the access interval to the radio channel, T_{in} is the duration of the IP, T_{nk} – is the duration of the verification code.

Regarding the values of the data compression ratio at the information level of the OS and BS the value $K_{ci} = k_1 \cdot k_2 \cdot k_3$: k_1 is determined by the features of applied research and tasks. The value of the compression ratio of signals and images k_1 significantly depends on the dynamic properties of the bypass and the accuracy of ES (EP) coding. In practice, the minimum value $k_{1\,\min} = 2 - 3$ is greater. Minimum value $k_{2\,\min} \approx 1.4 - 2$ and more [19]. Research of transcoding of the pseudo-chaotic break-even data into IP code-signal sequences have shown both when $B \leq 1$ $k_3 \geq 4-5$ (4–5-bit sequences are transmitted by signal of T_b duration); and when $B \geq 1$ $k_3 = 1.6 - 2.3$ (provided that the formation of k_l – is the interval of two-level CSS) [20],

where the value k determines the minimum number of intervals of the CSS IP ($k = 2$ or $k = 3$), and the value l specifies the maximum number of possible CSS intervals in the range from $T_{\min} = T_b$ to $T_{\max} = T_b + (l-1) \cdot \Delta T$, where $\Delta T = k_s \cdot T_b$, and $k_s < 1$ is selected depending on the level interference of the radio channel (for example $k_s = 0.125$; 0.15; 0.2; 0.25). To implement a pseudo-chaotic data transmission, the parameters of the k_l – interval of the two-level CSS are selected within the following limits: $k = 2; 3$; $l = 3 - 6$; $n = 4 - 8$ [20].

Achieving higher coefficients of compact data coding k_3 in the process of CSS IP forming with minimum duration and increased information capacity is carried out under the condition of reducing the number of varieties n – bit sequences in a compressed and protected data array. Some reserve for increase the value k_3 is the replacement of the n – bit sequences of the most common IP information frames with the two-level CSS of the shorter duration. As a result of such data recoding the coefficient k_3 increases approximately in 1.2–1.4 times. In the case of the value $B > 10$ of CSS IP, the transmission of the monitoring data is lossmaking (the main purpose of such data transmission is to ensure the delivery of data to subscribers of the upper levels of monitoring networks).

In real conditions of the objects states long-term monitoring, the coefficient k_1 must meet the condition as follows $k_1 > k_{1\ \min}$. Significant reduction of information flows by means of OS and BS is achieved based on the MCO information states determining [19] and in case of the object normal states, abbreviated codes of such states are sent to the network. Therefore, in real conditions, the reduction of information flows by means of the monitoring networks OS and BS should be expected tens to hundreds of times or more, which leads to a significant reduction in the output flow of packets of each OS and BS of IoT.

Due to the pseudo-random (almost chaotic) change of the correspondence of the n-bit sequences of the IP information frames to the optimally selected CSS IP, the reliable data protection in the radio channel is provided. In this case, the rules for the CSS IP formation are known only to the IP subscriber-transmitter and the IP subscriber-receiver.

After data compression and protection, there is obtained the resulting array of compressed and protected reliable monitoring data in the form of pseudo-chaotic non-redundant data. As example it is shown the results of the electrocardiogram coding (Figure 2, a) as well as the chaosgram of such an array (Figure 2, b). The chaosgram is the dependence of the current *i*-th q-bit symbol of the data array from the next $(i + 1)$-th symbol. The chaosgram

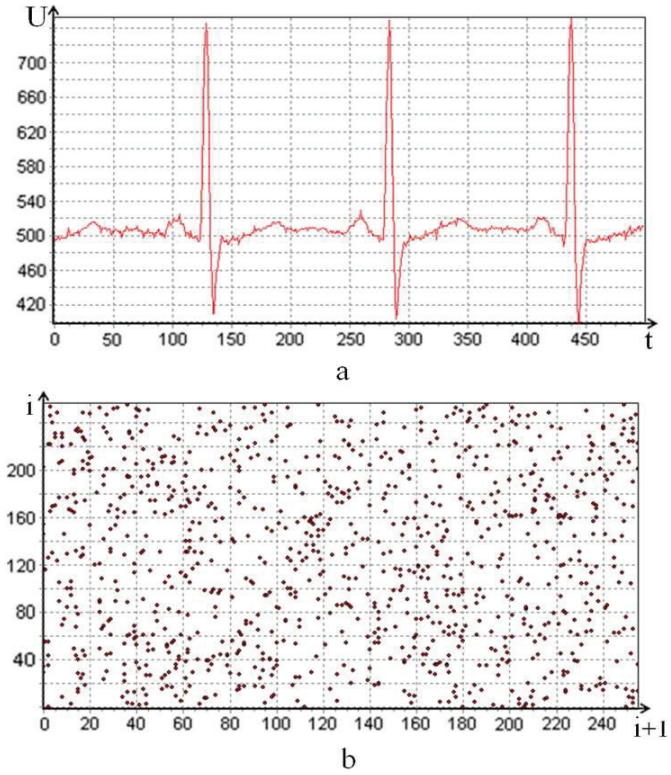


Figure 2 Electrocardiogram coding.

displays the results of the data encoding and encryption. It is noticed that the pseudo chaotic data are scattered over the entire range of q-bit data $(q = 8)$.

The next example (Figure 3) shows the results of the video signal encoding There are both a less dynamic video signal and a more dynamic video signal.

It is shown the envelope of. bypassing (Figure 3, a and Figure 3, c, respectively) one of the lines of the video frame. Less dynamic video signals are characterized by fewer EPs, and more dynamic by more EPs, respectively, by the larger streams of compressed data. As well as the proper chaosgrams of encoded and encrypted video signals at $q = 7$ (Figure 3, b and 3, d, respectively).

Thus, regardless of what monitoring data is transmitted to the OS and BS of IoT networks (samples of monitoring signals, video data frames, compressed data arrays), the information frames of data packets are filled

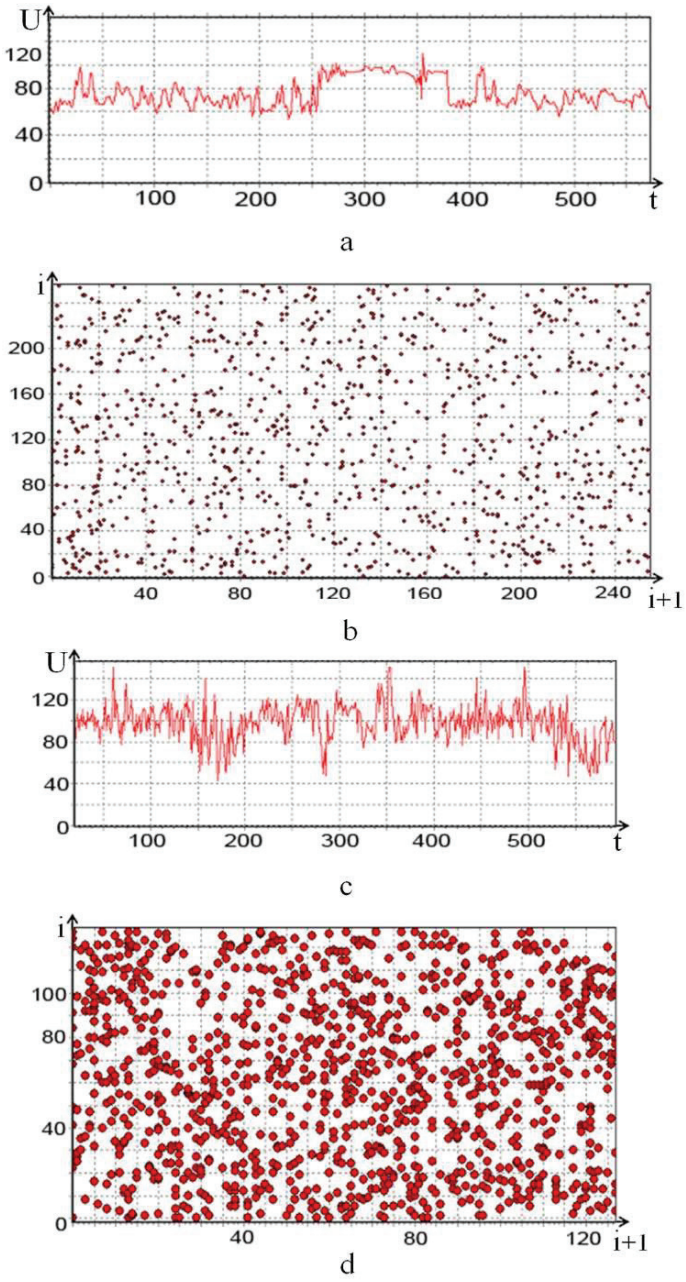


Figure 3 Envelopes and chaosgrams of encoded and encrypted video signals.

with the protected non-redundant and chaotic data. It is possible to decrypt such data only if the subscribers of the IoT network have the appropriate private keys.

The novelty of the proposed and described information technology is that limited computing resources such as microcontrollers or in the complex "processor-specialized devices", provide both minimization of calculations in places of formation of IoT network flows by means of OS/BS and formation/transmission of protected compact packets of monitoring data with increased information capacity. The advantages of the technology are the prompt determination and formation of reliable monitoring data, i.e., essential samples (ES) of signals and essential pixels (EP) in the frames of video data with confirmation of their reliability. The obtained data are the basis for compact coding of signals and images, filling of radio channels of IoT networks with non-redundant and reliable data and restoration of both monitoring signal and video signal envelopes without distortions. The proposed adaptation to the noise level in radio channels provides the formation and transmission of highly informative information packets of the minimum duration. At the same time, object and on-board means of IoT networks do not require the use of energy-intensive processors, specialized codecs and video codecs. The technology does not require the use of high-speed and energy-intensive radio modules and is focused on the building of OS, BS, intelligent sensors and video modules with radio communication for long-term (days, weeks, months and more) monitoring of objects and subjects.

7 Conclusions

Networks and tools of Internet of Things are usually focused on the long-term monitoring of objects of the various nature and functional purpose, the data acquisition from sensors and the control of various remote mechanisms. In this case, network devices, i.e., object and on-board systems of IoT networks, are installed in the places of the formation of network flows and work in conditions of many restrictions. The main limitations are in the devices and systems power consumption as well as restrictions on the performance of object and on-board processors. Also, object and on-board systems of IoT networks must work as long as possible from autonomous power supplies, carry out input monitoring signals and images in the presence of industrial interference, the input noise in the measuring units of sensors, to transmit the monitoring data in the presence of interference in radio channels and in the absence of direct visibility conditions of antenna systems of IoT subscribers.

The fundamental requirement for the quality of the IoT networks with the wide application functioning is the reliability and security (crypto stability and noise immunity) of the information transmission in the network. Considering the above requirements, a new information technology is proposed to increase the information and energy efficiency of the IoT networks object and on-board systems.

The basis of information technology is a set of algorithms for processing, encoding and transmission of monitoring data (signals samples, video data frames and data arrays) taking into account the minimization of OS and BS of the output crypto-protected information packets and the implementation of high-speed algorithms for the filtering, encoding, data compression monitoring, formation and transmission of information packets with increased information capacity, provided a minimum number of computational operations.

Effective methods and algorithms of compact coding of signals and frames of video data are based on the signal approach, according to which, taking into account the peculiarities of applied tasks, application areas of adaptive compression algorithms of signals and video signals with allowable information loss it is effectively implemented operational coding/decoding of the most informative essential samples of signals and pixels of video signals (extremums and inflection points or points of change of curve motion) with accurate restoration of the amplitude-time parameters of the latter in the process of the memorizing, transmitting and decoding data and the high-quality recovery of bypass signals and video signals.

In order to maximize the compression of signals, only those parts of signals and video signals that are classified as less reliable (areas with noise) are less qualitatively restored, and when restoring bypass signals, researchers (experts) receive information about the type of curve (reliable/less reliable, i.e., with noise).

Information-efficient transmission of the monitoring data by means of IoT networks of OS and BS is based on the adaptation to the input data with noise, determination of amplitude-time (numbering) parameters of essential samples of bypass filtered signals or video signals pixels, compression-protection of the determined reliable data and the adaptive choice of the base and structure of code-signal sequences of the increased information capacity packets, taking into account the current level of the interference in the radio channel. Energy efficiency of the monitoring data transmission is achieved by the minimizing the output streams of the highly informative data packets at the installation sites of the object and on-board systems and

by processors performing a set of high-speed algorithms for the processing, encoding, encrypting and transmitting data with minimized computational operations.

The proposed information technology is focused on the construction of the small and efficient object and on-board systems of the sensor, local-regional, mobile and global (microsatellite) IoT networks with a focus on the long-term monitoring of various stationary, mobile objects, industrial facilities, for telemedicine monitoring of athletes, operators, patients, to build safety networks of facilities and entities, to eco-monitoring of facilities and territories, to build networks of smart homes, smart cities and roads.

References

[1] Gartner: The Internet of Things, Report, accessed on 17 November 2015 from http://www.gartner.com/technology/research/internet-of-things
[2] M. Chiang and T. Zhang, 'Fog and IoT: An Overview of Research Opportunities', in IEEE Internet of Things Journal, vol. 3, no. 6, Dec. 2016, pp. 854–864.
[3] S. A. Hinai, A. V. Singh. 'Internet of things: Architecture, security challenges and solutions'. 2017 International Conference on Infocom Technologies and Unmanned Systems (Trendsand Future Directions) (ICTUS), Dubai, 2017, pp. 1-4.
[4] Z.-K. Zhang, M. C. Y. Cho, and S. Shieh, 'Emerging Security Threats and Countermeasures in IoT', Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security – ASIA CCS '15, 2015, pp. 1–6.
[5] W. Dargie W., C. Poellabauer. Fundamentals of wireless sensor networks: theory and practice. John Wiley and Sons, 2010. 330 p.
[6] Z. Shelby, C. Bormann. 6LoWPAN: The Wireless Embedded Internet. WILEY, 2009. 223 p.
[7] www.ti.com
[8] 8.www.st.com
[9] www.nxp.com
[10] www.simcom.com
[11] www.teltonika-networks.com
[12] B. Sklyar. Digital Communication. Theoretical Foundations and Practical Application, 2nd ed.: Moscow: Williams Publishing House, 2003. 1104 p.

[13] Eileen Kuehu, Matthias Prelwitz, Maurus Rohrer, Juergen Sieck, 'Distributed middleware for applications of the internet of things', Proc.7-th IEEE Int. Conf. Intel. Data Acquisition and Advanced Comp. Syst.: Techn. and Applicat., IDAACS'2013, Berlin,Germany, September 12–14, 2013, pp. 517–520.

[14] Chen Yang, Weiming Shen, and Xianbin Wang, 'The internet of things in manufactoring. key issues and potentional applications', IEEE Trans. Syst. Man Cybern., pp. 6–15, Jan. 2018.

[15] S. K. Sharma and X. Wang, 'Live Data Analytics With Collaborative Edge and Cloud Processing in Wireless IoT Networks', in IEEE Access, vol. 5, pp. 4621–4635, 2017.

[16] M. Singh, A. Singh and S. Kim, 'Blockchain: A game changer for securing IoT data', 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51–55. doi: 10.1109/WF-IoT.2018.8355182

[17] M. Ermes, J. Parkka, J. Mantyjarvi, and I. Korhonen, 'Detection of daily activities and sports with wearable sensors in controlled and uncontrolled conditions', IEEE Trans. Inf. Technol. Biomed., vol. 12, no. 1, pp. 20–26, 2008.

[18] T. Shah and S. Venkatesan, 'Authentication of IoT Device and IoT Server Using Secure Vaults', 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, 2018, pp. 819–824. doi: 10.1109/TrustCom/BigDataSE.2018.00117.

[19] B.M. Shevchuk. 'Theoretical and Algorithmic Foundations of Improving the Efficiency of Packet Data Transmission in High-Speed and Secure Radio Networks'. Cybernetics and Systems Analysis. 2016, January, Vol. 52, Issue 1. pp. 151–159.

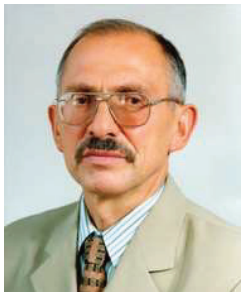
[20] B.M. Shevchuk, V.K. Zadiraka, S.V. Fraier. 'Data transfer optimization in the information efficient sensory, local-regional and microsatellite wireless networks', in Optimization Methods and Applications. In Honor of Ivan V.Sergienko's 80th Birthday, Butenko S., Pardalos P.M., ShyloV., (Eds.), Springer, 2017. pp. 465–480.

[21] Dikshita Sarma, Manash Pratim Sarma, Kandarpa Kumar Sarma and Nikos E. Mastorakis. 'Implementation of Galois Field for Application in Wireless Communication Channels', MATEC Web of Conferences 210, 03012 (2018), https://doi.org/10.1051/matecconf/201821003012 CSCC 2018.

Biographies

Bohdan Shevchuk graduated in 1978 from the Radio Engineering Faculty of the Lviv Polytechnic Institute in the radio engineering and during 4 years worked at the Lviv Research Radio Engineering Institute as a radio engineer. In 1984 he entered and in 1987 graduated as PhD from the Institute of Cybernetics named after V.M. Glushkov National Academy of Sciences of Ukraine. Since 2018 he received Doctor of Technical Sciences degree. Now he works with the department of the numerical methods optimization in the Institute of Cybernetics as a leading researcher, specializing in processing, encoding, encryption and transmission of signals and images, construction of monitoring information-efficient radio networks, including sensor, local-regional, micro-satellite networks. and Internet of Things. He has more than 160 scientific works, including 4 monographs, 7 copyright certificates and 2 patents of Ukraine for inventions.

Further theoretical and practical developments of the author are aimed at building secure (crypto-resistant and noise-resistant) high-speed radio networks for various purposes, operating in many constraints, data compression, transmission of highly informative and pseudo-chaotic information packets, creation and implementation of experimental wireless telemedicine networks and networks. industrial monitoring, ecomonitoring, security networks, object and on-board means and wireless intelligent sensors, energy efficient intelligent video modules.



Mykhaylo Geraimchuk, Doctor of Technical Sciences, professor of the Instrument Making Department of the National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine. He graduated from the Kyiv Polytechnic Institute in 1974, the Department of Precision Mechanics, where he has worked since 1974. From 1988 to 2001 he was the Deputy Dean of the Instrument-Making Faculty, from 2001 to 2019 he was the Head of the Instrument-Making Department, and now he works as a Professor at this Department. Received more than 15 patents. He has more than 150 scientific works, including more than 10 monographs and books, more than 30 publications indexed in international Scopus databases, more than 11 textbooks and guidelines. He has collaborated with China, Algeria, France and other countries. He has scientific interests in the fields of instrument making, artificial intelligence, sensor networks; inertial sensors, mechatronics and robotics, unman vehicles and also participates in projects on psychology of creativity, computer programs of training and stimulation of genius and others.

Orest Ivakhiv is from Lviv, Ukraine. Professor O.Ivakhiv received his M.A. Sc. in Electrical Engineering from The Lviv Technical University

(Ukraine), the Ph.D. in Communications from The Moscow Aviation Institute (Russia), the Sc. D. in Electrical Instrumentation from Lviv Polytechnic National University (Ukraine). Orest Ivakhiv was a visiting professor at the Department of Electrical and Computer Engineering at The University of Toronto (Ontario, Canada) in 1994 and in Gdansk University of Technology (Poland) in 2019. Since 1968 professor O. Ivakhiv is a faculty member at the Computer Technology, Automation and Metrology Institute of Lviv Polytechnic National University. Now Orest Ivakhiv is a Head of the Intelligent Mechatronics and Robotics Department. Orest Ivakhiv has more than 300 publications, 12 patents. His research interests include electrical measurement and instrumentation, informative measurement theory, adaptive data processing, data compression, enumerative coding, communication theory and mechatronics.

Yuriy Brayko graduated from the National Technical University of Ukraine "Kyiv Polytechnic Institute" in 1973 with a degree in Information and Measurement Technology. Now he works at the Glushkov's Institute of Cybernetics of the National Academy of Sciences of Ukraine, as the researcher, specializing in the development and creation of distributed and autonomous data collection and processing systems for environmental, medical and industrial monitoring. He has 115 scientific papers, 8 patents.