CONTENT
Vol. 6. No. 4-2020

Published quarterly since 2015.

ISSN 2664-066X (Print)
ISSN 2664-0678 (Online)

Publisher
Institute of Radio and Information Systems (IRIS), Vienna, Austria

Address:
1010 Wien, Austria,
Ebendorferstrasse 10/6b
media-publisher.eu/
synchroinfo-journal

MOBILE SOFTWARE PLATFORM FOR RADIO INFORMATION SYSTEMS STATISTICAL MODELING

Alexander A. Totilas,
Department of Nanotechnology in Electronics, Kazan National Research Technical University named after A.N. Tupolev-KAI, KNRTU-KAI,Kazan, Russia;
German-Russian Institute of Advanced Technologies (GRIAT), totilas.aleks@gmail.com

Renat F. Zaripov,
Department of Nanotechnology in Electronics, Kazan National Research Technical University named after A.N. Tupolev-KAI, KNRTU-KAI, Kazan, Russia;
German-Russian Institute of Advanced Technologies (GRIAT), rfzaripov@kai.ru

Marat M. Fatykhov,
Department of Nanotechnology in Electronics, Kazan National Research Technical University named after A.N. Tupolev-KAI, KNRTU-KAI, Kazan, Russian Federation;
German-Russian Institute of Advanced Technologies (GRIAT), mmfatykhov@prof.kai.ru

DOI: 10.36724/2664-066X-2020-6-4-2-10

ABSTRACT

For the static research purposes in the field of radio signals reception under freely fluctuating interference conditions, specialized software for the Android platform based on the Kotlin language has been developed using. The program design allowing to work with both the information recorded by the radio receiver analog system and the signals obtained using the simulation model. CDMA system operation under Gaussian white noise and chaotic pulse interference conditions has been simulated. The dependences of the bit error probability on additive radio channel effects of a different nature were obtained. The work originality is an attempt to implement a software-defined binary signal processing system on an accessible platform.

KEYWORDS: *software defined radio, chaotic pulse interferences, code division multiple access, the clean architecture, mobile platform.*

I. INTRODUCTION

Nowadays, telecommunications such as mobile cellular communication networks and wireless local area networks (WLANs) are actively developing. The number of users in such networks is constantly increasing, and at the same time, the requirements applied to communication systems, necessary for comfortable communication, are growing - for voice, text messages, image transmission, video communication, the Internet surfing and other services. Over time, the load on the network grows the requirements for speed and quality of data transferring. At the same time, more and more wireless networks are appearing, which leads to very limited frequency resource decrease and rising cost, as well as to an increase in noise and interference in the used radio frequency ranges. All of this makes the research in the field of wireless data transmission efficiency improving very relevant.

A promising and relevant solution to the above problems is the use of so-called complex signals, including broadband signals, which allow occupied frequency bands to be used, while introducing minimal interference to existing systems.

The use of such signals is associated with complex processing, calculations that are difficult to implement with analog elements, but which are easily solved using digital systems. In addition, the rejection of analog processing in favor of digital allows achieving a number of advantages, such as increased noise immunity, long range with relatively low transmitter power, data encryption, and much other functionality. [1]

One of the ways to study the digital communication network capabilities is its computer simulation. It provides available tools with minimal cost and sufficient accuracy for determining the characteristics, for experiment on models close to real objects, when thy are inaccessible.

DESIGNING A SOFTWARE-DEFINED RADIO SYSTEM

Software Defined Radio System

A software-defined radio (SDR) system is a radio communication system where the most of the components (amplifiers, mixers, filters, detectors, etc.) are implemented on a personal computer, embedded system or other programmable digital equipment instead of hardware. Such systems require great computing capabilities, however, modern personal computers, gadgets, embedded systems with their relatively low cost and wide distribution have a sufficient number of processor cores with high clock frequencies - up to 5 GHz per core.

The simplest SDR system can consist of a personal computer with a sound card (or other analog-to-digital converter), which has connected radio-frequency receiving system. A significant part of the signal processing is supported by the processor, not in specialized hardware components (electrical circuits). This design allows you to receive and transmit a very large number of different radio protocols only on the single software basis.

Software-defined radio systems are widely used for military purposes, as well as in cellular mobile communication networks, since they must serve a wide range of radio protocols in real time.

According to engineers, software and hardware developers, providers from the International Organization for Wireless Innovation (The Wireless Innovation Forum, formerly SDRForum), in the long run, SDR will become the dominant technology in radio communications. In addition, SDR, together with programmable antennas, allows cognitive radio -the further telecommunications development.

Previous types radio systems developers had to deal with such problems as the limited frequency resource, its occupancy and the presence of mutual interference. However, software-defined radio systems can be flexible enough to get around these problems in various ways, for example, using spread spectrum technologies that allow multiple transmitters to transmit at the same time at the same frequencies with very little mutual interference. In addition, error detecting and correcting algorithms are introduced that make it possible to completely get rid of the interference effect.

Turning in the signal direction Software-defined antennas application allows receivers to better suppress interference from other directions, and therefore receive weaker signals.

In cognitive radio technologies, each system measures the current spectrum conditions and transmits this information to other similar systems, so transmitters can avoid mutual interference, for example, by choosing unused frequencies. Also, each radio system, according to this technology, is associated with a geolocation data for given area spectrum occupancy information obtaining and tuning the effective frequencies and transmitter power.

Based on the communication with the receiver, transmitter power dynamic tuning reduces it to the required minimum, solving the near-far problem and reducing interference, as well as reducing the power consumption from transmission on portable devices.

System design general principles

In the system development, it is very important to pay attention to its architecture. So, if the system is designed as a single block, it is not free for expansion, modifications. It is difficult to test it, verify all its functions reliability, but it is easy to allow a flaws and shortcomings. Any change in one part of it requires processing of the entire system, and this introduces additional labor and financial costs. In addition, the design of such system carries a high complexity itself.

The modularity concept, based on the problem decomposition helps to help solve these problems. According to it, the system must be divided into functionally complete modules. Thus, the system can be easily supplemented and improved by adding and/or changing these blocks.

At the highest level, the SDR system can be divided into hardware and software parts. It is assumed that in this way each of them can be developed independently. In their turn, these parts should also be decomposed.

Historically, equipment has been developed from functionally complete units, thereby fulfilling the principle of modularity. However, this mainly concerns only design, but often does not apply to the period of operation. The components of the finished product are usually rigidly connected with each other and the environment structure that unites them (circuit board): the procedure for replacing them (soldering) is relatively complicated and time-consuming, and it is also difficult to configure the functionality. In part, these problems are solved by connecting parts - connectors and interfaces connecting devices to each other.

Therefore, in this projected system, the hardware is completely represented as several interchangeable modules having a single unified connector for connection. The hardware module is completely replaced depending on the task and the required functional purpose.

In the developed system, the equipment is divided into a data source (for example, radio frequency) and a digital processing center. Different source implementations may, for example, work with different frequencies and powers, but must have the same connectors and a single interface for "communication" with the digital part.

A digital device can also be easily replaced in the next cases: it has the same connection interface, supports software for data generating and processing, and has sufficient performance for real-time operation.

The software part takes over most of the functions previously performed by the hardware equipment, which significantly reduces the size and cost of the device. Also, software with proper design is divided into modules, which sometimes makes it possible to change the functionality and processing algorithms on-line, and in the future will make it easy to expand and modify. In addition, the modular architecture of the software simplifies its testing, which means entire system overall reliability and accuracy increase.

System elements implementation

The developed system in its hardware part contains two devices: the first is the data source for the system, and the second is processing and display device.

An important part of the system is the equipment devices interaction interface. For physical wiring task, a universal serial bus interface is suitable as a version, since it is widespread - it is the standard for most modern digital devices, also, it can have high data transfer speeds - up to 20 Gb / s (for USB 3.2 Gen 2x2) [2]. An important connector feature is also power transmission to the device. In cases where the wired connection between devices is impossible, irrational or inconvenient and the distance between them is no more than 10 meters, wireless connection through Bluetooth modules can be used.

A common digital interface between parts of the equipment allows using a wide design implementations range, depending on the task and capabilities.

For example, if the goal is radio data receiving and subsequent processing (in this case, the devices act as an SDR real-time system), then a RF device is connected to the digital equipment. In general, an RF hardware can have one or more antennas, a preselector, a local oscillator and a mixer for transferring the signal to an intermediate frequency, a band-pass filter for suppressing the mirror channel, an ADC, a USB converter, and/or a Bluetooth module. The radio receiver of the system is generally connected to the processing device via USB for a more reliable connection and power supply.

There may be situation when a radio signal is received by some device and its digitized data is stored in memory, but processing at the reception time is impossible (for example, due to the fact that the ADC has high bit depth and the processing device has low performance - thus the data stream does not manage to be processed in real time). The solution to this problem is to use a storage device, such as a flash drive, as a data source. Then the processing device reads the information directly from the memory via the USB connector.

A data processing device can be any computing device that supports system software and is capable of performing the necessary calculations in a reasonable amount of time. It is possible to use:

- single-board computers;
- FPGA
- PC
- mobile devices (smartphones).

Single-board computers are mobile and cheap, but they usually have low performance and RAM.

FPGAs are portable and have a great performance, but require much more time for software development, while programming uses hardware description languages that do not allow developing a complex user interface.

PCs have high performance, but high cost and large size. In addition, they are stationary, tied to a general power supply system.

Modern mobile devices have several advantages - they are portable, have small dimensions, a large amount of RAM, low cost, and are quite productive (a mid-range smartphone usually has 8 processor cores with a clock speed of about 1.8-2 GHz) and combine a display device. In addition, due to their widespread prevalence, they are so included in the everyday life of people that almost every person has it. Thus, a mobile phone (smartphone) was selected for use as system data processing equipment.

An important feature of the smartphone is the presence of a built-in touch screen, which not only allows you to display the information necessary for the operator, but also serves as a controlling element, which means it allows the user to interact with the software. This provides software configuration depending on the task and the type used data source.

Currently, smartphones with operating systems (OS) iOS and Android are common. The choice of platform is considered from the device and software development opportunities availability point of view - devices with the iOS operating system are much more expensive and less common [3]. In addition, for the software full development and distribution, this platform requires a PC with a similar OS from the manufacturer, which requires huge additional costs. Thus, an Android device was chosen due to its widespread use, low cost and the free unlimited software development possibility.

SOFTWARE DEVELOPMENT

Based on the processing system hardware digital part implementation - a mobile device based on the Android operating system - software can be developed in the Java, Kotlin, and JavaScript programming languages (through the React Native framework).

JavaScript is not officially supported by the Android platform, the React Native framework does not have the same functionality as native languages, in addition, it is unstable and often leads to application inoperability. Therefore, this language is not suitable for the mobile devices complex and resource-intensive software package development.

Java is the official programming language for Android, stable and has a large number of libraries from third-party developers, which allows quickly adding various functionality to the application. However, this language also has a number of drawbacks: it is strongly typed and verbose, requires a lot of development time.

Kotlin is also the official (and recently, the main) programming language for Android applications. Compared to Java, it is concise, so the amount of code base is significantly reduced, which means that development time is also reduced. In addition, it contributes to a significant reduction in the number of errors, which means it increases the stability of the software. Also, this language, like Java, is compiled into byte code for the Java Virtual, therefore it allows the use of third-party libraries written in the Java language.

Thus, based on the advantages described above, Kotlin has been chosen for software development.

Software architecture

The system software design based on the “The Clean Architecture” [4] concept, proposed by engineer Robert Martin (Fig. 1).

This concept means dividing the entire program into several main layers representing various program areas:

- Entities layer - the core of the architecture, contains business logic objects. This can be either classes with methods or sets of data structures. They contain the most general, high-level rules.
- Layer of business rules — application-specific laws and processes that manipulate data flows between entities.
- Interface layer - an intermediary between entities with business rules and an implementation layer, designed to transform data into a form suitable for layers.
- Implementation layer - includes elements of an objects specific implementation, a graphical interface, external libraries and frameworks, a connection to the network and external interfaces, databases - that is, everything that depends on the platform.

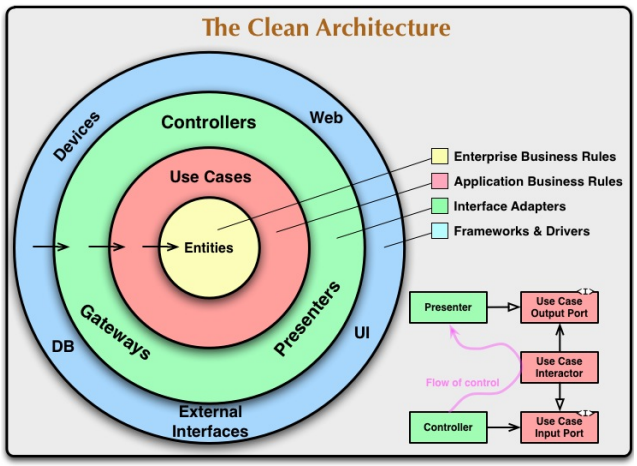


Fig. 1. "The Clean Architecture" concept by Robert Martin

Between layers it is necessary to observe the following Dependency Rule: external layers depend on internal, but not vice versa. For example, the business logic layer uses the central layer entities, while the latter do not interact with the business logic in any way.

Thus, this architecture fulfills the following requirements necessary for reliable, easily extensible, and modifiable software:

- the software core does not depend on third-party libraries, frameworks, databases;
- the software core does not depend on the user interface execution;
- software is easy to test.

Through this architecture and JVM-based language, the software core can be distinguished and used both for a mobile solution and for use in a desktop PC.

Data source

The designed system is developed both for practical purposes, such as the complex radio signals reception and processing, and for research - the study of multi-user access by encoding with orthogonal or pseudorandom sequences and their noise immunity under the noise, interference, and reflections conditions. Therefore, the system software implements two types of operation modes corresponding to two types of data source:

- received signal processing mode (data "from the outside");
- simulation mode (software data generation).

For the SDR system, the data source is a radio signals transmitted through radio channel with noise and interference. The mixture of noise, interference and signals received by the RF device antennas can pass through pre-filtering, then it is digitized in the hardware ADC. Thus, a digital signal with a flow rate equal to the ADC sampling frequency is received at the mobile device input via USB or Bluetooth, while the number of bits in the word that determines the signal level is equal to the ADC bit depth.

The software is developed for receiving and modeling radio signals with various parameters used in communication systems (including nonstandard ones), therefore a large number of various settings are provided in the data source module:

- ADC sampling rate;
- ADC bit depth;
- channel code type;
- carrier frequency;
- number of channels;
- data flow rate;
- frame length;
- number of frames;
- code length.

For modeling purposes, it is also possible to generate additive white Gaussian noise (AWGN) with given signal to noise ratio and chaotic pulse interferences (CPI) with a scarcity factor.

First, according to the user entered settings, the software generates random digital data for each channel with a uniform zero probability distribution.

Then, in the encoder module, data is encoded with a code corresponding to each channel. Encoding is the modul 2 addition for each data frame bit a with the entire sequence of code. Thus, the length of the encoded data is:

$$L_{cd} = L_d \cdot L_c \qquad (1)$$

where L_d – data frame length, L_c – code sequence length.

The encoded data from each channel undergoes a change in the bipolar form. In this case, the pulse durations correspond to half the data flow rate selected by the user (the symbol rate is a half the bit rate). Then the bipolar pulse sequences are linearly combining, forming a group signal.

Next, the generator block creates a carrier harmonic with a frequency specified by the user, which, at the same time as the signal from the encoder, is supplied to the QPSK modulator block. The following operations are performed here:

- The pulse sequence is divided into two streams: even pulses go to channel I, and odd pulses go to channel Q (given that the numbering starts from zero).
- Channel I data is multiplied with the carrier harmonic, and channel Q data is multiplied with the same harmonic, but 90 degrees out of phase.
- Q and I components add up to form a QPSK signal and are output.

Obtained signal is additively combining with noise and interference. The mixture is displayed on the oscilloscope on the source module page and is forwards to the demodulator unit.

Noise and interference generation

In the signal source module simulation section, the user has the ability to turn on/off the noise and interference under the radio channel simulation, as well as configure their parameters.

When the noise is turned on, the user adjusts the signal-to-noise ratio. Each time the parameter is changed, an AWGN is generated. Generation is based on the function included in the Kotlin programming language standard library. All samples obtained by this function have the same probability density of the form of a Gaussian distribution with zero mean and unit dispersion. The noise power is controlled by multiplying the density of the noise power coefficient by a random value obtained by the above function.

For the continuous analog white noise according to the formula [5]:

$$P_N = \int_{-\infty}^{\infty} S_N(f)df = \int_{-\infty}^{\infty} \frac{N_0}{2}df = \infty \quad (2)$$

the dispersion is infinite, however, in this case, the noise is represented by discrete samples, and the frequency range at which the noise is considered white is limited. Thus, its dispersion is finite, and noise can be implemented by software.

The required noise power calculation based on the user specified SNR and bit rate, as well as the known QPSK signal average power. SNR in software is interpreted as the normalized signal-to-noise ratio in decibels, therefore, based on the formula:

$$\frac{E_b}{N_0} = \frac{S}{N}\frac{W}{R} \quad (3)$$

where the energy of the bit E_b is the energy per one bit of information [6]:

$$E_b = ST_b = \frac{S}{R} \quad (4)$$

and the spectral density of the noise power N_0 is the power per unit frequency interval in the noise spectrum having an energy amount.

Then, the power spectral density is expressed as follows:

$$N_0 = \frac{E_b}{SNR_{lin}} = \frac{S}{10^{\frac{SNR_{dB}}{10}} \cdot R} \quad (5)$$

Thus, when interferences are turned off and there are no channel signals in the simulated broadcast, white Gaussian noise is observed, in which the power spectral density is directly proportional to the signal-to-noise ratio.

When interferences are turned on, the user has the ability to adjust the sparseness coefficient and signal-to-noise ratio. Turning on and changing the parameters starts the generation of CPI in the simulated radio channel.

First, for simulation each data point, taken with a sampling frequency (specified by the user), the value of the same function, which was used to generate the AWGN, from the Kotlin library is calculated. Then it is compared with the sparseness coefficient, which in this case is the threshold of the pulse – if the function value is greater than the coefficient, then it goes on for further processing, otherwise the generation process for this data point is completed and the interference pulse does not occur.

Further, values exceeding the threshold are multiplied by a power factor expressed from a known signal-to-noise ratio.

Thus, when the noise is turned off and there are no channel signals on the air, a sequence of pulses with chaotic amplitude and an interval between them is observed, the average value of the pulses occurrence frequency being inversely proportional to the rarefaction coefficient, and the amplitude is directly proportional to the signal/noise ratio. It should also be noted that the number of generated pulses for the considered time interval approximately corresponds to the Poisson distribution law.

Demodulation

The signal data received through USB or Bluetooth, or generated by the program, enters the demodulation module.

In it, QPSK demodulation is carried out in two channels, each of which is a demodulation of the BPSK signal. Thus, in the module, data is divided into two streams:
I-channel and Q-channel. The input signal in the I-channel is multiplied with the signal of the harmonic signal generator generating the cosine. The frequency of the generator is user-configurable and must be equal to the carrier frequency of the input QPSK signal for proper demodulation. As a result of multiplication, the sum of the double frequency harmonic and the constant component, proportional to the phase difference between the signal of the generator and the input signal, is formed [7].

Next, the resulting mixture enters a digital FIR filter, where noise is suppressed and a constant component is extracted. It is programmed to operate as a low-pass filter (LPF) using the ideal pulse response formula:

$$\begin{aligned} &h_d(n) = 2f_c \frac{\sin(n\omega_c)}{n\omega_c}; n \neq 0 \\ &h_d(n) = 2f_c; n = 0 \end{aligned} \quad (6)$$

The ideal filter characteristic is an infinite decaying series of values, however, for practical FIR use, this series must be limited, and the so-called Gibbs phenomenon appears – a transitional frequency band appears between the suppression and transmission bands, and emissions forms on the transfer characteristic.

Multiplication the pulse response by the window smoothing weight function helps to solve this problem. For this, the following are used [8]:

- Hannah function

- Hamming function
- Gauss function
- Blackman function

For each window, the resulting signal spectrum minor lobes level is different, and can act as a parameter characterizing the quality of filtering.

The filtering part is also user-configurable – its order, cutoff frequency and weight function are set.

After filtering, the signals from both channels enter the data processing module. Since the filter introduces a delay, the processing start time is also software-based delayed to avoid errors.

In the module, the signals are divided into time sections of length T_s, each of them is integrated over time. Thus, data array that carries information about the average signal value at each such section is obtained. Next, two arrays of in-phase and quadrature channels are combined as follows: $D = [i_0, q_0, i_1, q_1, \ldots, i_n, q_n]$, where i_k is the kth value of the in-phase values array, q_k is the kth value of the quadrature values array.

Then, the resulting data array passes to the decoder module.

Decoding

A digital values array is supplied to the input of the decoding module, which is a group signal – a mixture (linear sum of encoded data) of each active communication channel information.

To decode data, it needs first to be determined which channels should be processed. The developed software allows defining channels in several ways:

- manual channel definition;
- all possible channels identification;
- automatic channel detection.

In the manual user determination case, the channel codes that need to be decoded are manually entered. When selecting all channels for subsequent processing, all possible channels are determined for a user-selected family of codes of a specified length: for example, for Walsh codes of length 16, 16 channels with all possible codes (including service sequences) are determined. If the user selects the automatic channels detection, the program sets the channels whose codes give the maximum response to the cross correlation function, determined by the beginning of the transmitted sequence.

To highlight the transmitted information messages of each channel, their code sequences are converted into bipolar values according to the following rule: "-1" corresponds to the zero bit, and "1" corresponds to the single bit.

The values of the group signal are multiplied by the values of the bipolar code sequence with a period equal to the length of the code. The result of the multiplication will depend on the presence of a channel message: if the information has been transmitted through channel, then a bipolar sequence was obtained, where each value corresponds to a channel information bit (a threshold considered is a zero level: a negative value is a zero bit, a positive is a single), otherwise the output is a sequence of zeros.

Under the influence of noise and interference, the group signal is distorted. If we assume that the total set of noise is distributed according to the Gaussian law according to the expression of the probability density:

$$p(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{1}{2}\left(\frac{x}{\sigma} \right)^2 \right) \quad (7)$$

where σ is a root-mean-square deviation, and σ^2 is a process dispersion, demodulated mixture defines as:

$$x(t) = S_i(t) + n(t), i = 1..k \quad (8)$$

where $S_i(t)$ is an information signal in the form of binary bipolar symbols with amplitude a, $n(t)$ is zero-mean AWGN.

Based on the last 2 expressions, the nominal probability densities of receiving signals S_1 and S_2 can be expressed as:

$$p(x \mid S_1) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{1}{2}\left(\frac{x - a_1}{\sigma} \right)^2 \right) \quad (9)$$

$$p(x \mid S_2) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{1}{2}\left(\frac{x - a_2}{\sigma} \right)^2 \right) \quad (10)$$

These densities are called the likelihood densities of signals and show the probability density of the random signal $x(t)$ provided that the corresponding symbols are transmitted (Figure 2).

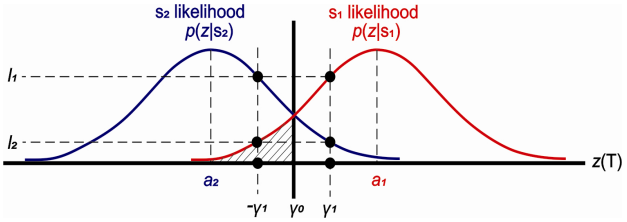


Fig. 2. Symbols receiving nominal probability densities [9]

As can be seen from the graphs (Fig. 2), the densities do not have clear boundaries and intersect with each other, as a result of which errors may occur in determining which symbol was received. Despite this, the final solution (choice of hypothesis) is still issued in comparison with the threshold – the zero level (γ_0).

The program decoding module enables the display of bits that are supposedly erroneous. This is done by entering another threshold value that defines the zone of uncertainty ($\pm\gamma_н$). All values are compared with this threshold: a value is considered erroneous if it's modulo less than the $\gamma_н$. Erroneous bits are remembered by the system and are subsequently highlighted in red when displayed. It is possible to use the error correction scheme in further.

Statistics collection

The statistics module displays the data collected as a result of coding, modulation, demodulation and decoding, as well as graphing the digital communication network characteristics.

If the signal source is channels generated by the program, then some parameters of the system are known in advance, in the case of signal processing from an external device or from a data file, some parameters are determined during the program operation.

The statistics window shows the number of active channels, the total number of transmitted bits and received bits per communication session (includes a certain number of frames), the number of bits detected by the decoder as erroneous, and the percentage of erroneous bits to the total number of received (which is the current bit error probability).

The module has the ability to collect statistics for plotting the BER/SNR dependence. The input parameters entered by the user in this case are the initial and final values of the SNR in decibels, and the desired graph samples number. The counting process is carried out by repeating the simulation of the reception session with the parameters of the source, demodulator and decoder specified in advance, and at each iteration, noise power is swiped corresponding to the current SNR:

$$SNR_i = SNR_0 + i\frac{(SNR_K - SNR_0)}{K} \quad (11)$$

where $i = 0...K-1$ is the iteration number; SNR_0 – initial SNR; SNR_K – final SNR; K – number of graph points.

It is necessary to note that it is not recommended to specify a large number of points – this entails a long processing, collecting statistics and plotting.

RESEARCH IN DEVELOPED SOFTWARE

The developed software for a software-defined radio system allows researches in the field of noise immunity and data transmission using the multiple access method such as code division multiplexing (CDMA), when several communication channels are operating simultaneously.

Initial data for the study

Data Source Settings:

A. Operation mode: simulation.
B. Sampling frequency: 10 MHz.
C. Channel settings:

- Number of channels: 4.
- Channel codes type: Walsh codes.
- Code length: 4 bits.
- Carrier frequency: 500 kHz.
- Data transfer rate: 100 kBit / s.
- Information parcel length: 100 bits.
- Number of frames: 1.

Demodulator Settings:

A. Generator frequency: 500 kHz.
B. FIR Filter Settings:

- Order: 10.
- Cutoff frequency: 1000 Hz.
- Weight function: Blackman.

C. Filter delay compensation: 0.1.
D. Information parcel length: 100 bits.
E. Code Length: 4 bits.
F. Data transfer rate: 100 kBit.

Decoder Settings:

A. Detection mode: manual.
B. Number of channels: 4.
C. Channel codes type: Walsh codes.
D. Code Length: 4 bits.
E. Threshold signal level: 0.3.

Noise immunity study

The performance calculation module calculates the theoretical BER_{theor} and practical BER in percent, the theoretical system throughput in kbit/s and the real system transmission rate D in kbit/s at various levels of the E_b/N_0 ratio. AWGN acts as a noise model.

The theoretical bit error probability for systems with coherent QPSK modulation is calculated using the following formula:

$$P_{err.theor.} = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \quad (12)$$

$$Q(x) = \frac{1}{2\pi}\int_x^{\infty}\exp\left(-\frac{t^2}{2}\right)dt \quad (13)$$

Theoretical throughput is calculated by Shannon's theorem as follows:

$$C = W\log_2\left(1+\frac{E_b}{N_0}\right) \quad (14)$$

where $W \approx 1/T_b$ is available bandwidth in Hz.

Numerical simulation results are collected in Table 1.

Table 1

BER dependence from E_b/N_0

E_b/N_0, dB	$P_{err.theor.}$ (BER_{theor}), %	P_{err} (BER), %	C, kbit/s	D, kbit/s
0.0	9.571986	3.5	100.000	96.500
1.0	7.087514	3.0	117.564	97.000
2.0	4.914345	0.5	137.010	99.500
3.0	3.138237	0.75	158.268	99.250
4.0	1.806955	0.25	181.225	99.750
5.0	0.913139	0.25	205.737	99.750
6.0	0.391355	0.0	231.646	100.000
7.0	0.136200	0.0	258.781	100.000
8.0	0.036432	0.0	286.979	100.000
9.0	0.006988	0.0	316.080	100.000

The obtained dependencies are presented in Fig. 3 and 4.

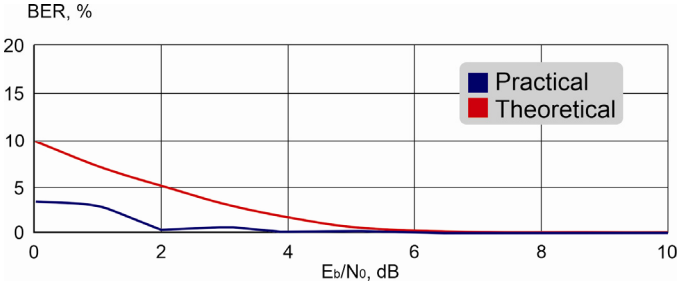


Fig. 3. Theoretical and practical BER dependencies on the E_b/N_0 ratio Graphs

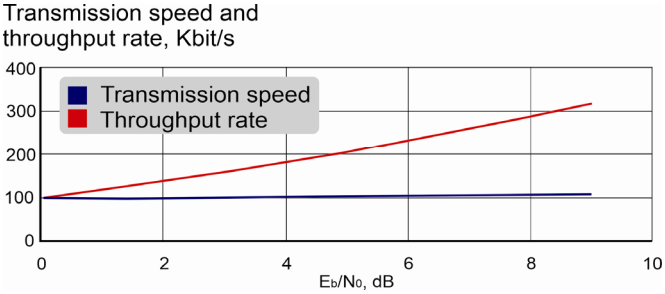


Fig. 4. Bandwidth and bit rate dependencies on the E_b/N_0 ratio

Thus, according to the obtained results, developed model does not meet theoretical expectations. In practice, the simulation program achieved half of the probability bit error over the entire E_b/N_0 range. This phenomenon can be explained by a very limited selection and a small amount of transmitted data (100 bits for each of the four channels), as well as imperfect program algorithms. At the same time, the transmission speed drops slightly with a high noise level compared to the declared one, but does not exceed the bandwidth values, which is normal.

As a result, according to the developed model, the system is capable to correctly receive, demodulate, and decode data transmitted by at least four channels in one frequency band under noise conditions with an E_b/N_0 ratio more than 6 dB.

Since the software can simulate not only AWGN, but also CPI in the radio channel, we study the effect of chaotic pulse interference on the system with the same settings. In this case, this interference is a model of other radio transmitters that may interfere with signal transmission.

Measurements are taken in the absence of background white noise in order to investigate only the interference effect. The simulation program allows adjusting the interference by changing the ratio of the energy of the bit E_b to the spectral density of the interference power P_0 and the so-called sparseness coefficient K_s inversely proportional to the interference pulses appearance frequency, that is, the higher its value, the wider pulses appear in the channel. Studies are conducted to these parameters combining in order to identify an influence to the system tendency for each of them. The results are listed in Table 2.

Table 2

Bit errror probability depending on CPI parameters

№	E_b/N_0, dB	K_s	P_{err} (BER), %
1		0.4	4.00
2		0.6	3.75
3		0.8	2.50
4		1.0	2.75
5		1.2	2.00
6		1.5	1.00
7		0.4	1.00
8		0.6	1.00
9		0.8	1.00
10		1.0	0.50
11		1.2	0.00
12		1.5	0.00
13		0.4	0.00
14		0.6	0.00
15		0.8	0.00
16		1.0	0.00
17		1.2	0.00
18		1.5	0.00

According to the results of the study, it is clear that with an increase in the E_b/N_0 ratio, the error probability decreases, and at the level of 6 dB the system no longer produces influential amount errors. That is, the probability is too small to detect it with a selected transmitted information amount. The study also shows that with decreasing rarefaction coefficient, the error probability increases.

In general, the error probability with CPI on the communication channel is lower compared to the influential AWGN for the same signal-to-noise and noise ratio, respectively.

The smaller CPI influence on the system compared to the AWGN can be explained by the fact that pulsed noise occupies a smaller band in the spectrum and is narrow-band compared to the broadband signals used in CDMA systems.

Conclusion

During the project implementation, the processes modeling theoretical basis, the nature of complex signals, noise and interference was studied. The wireless digital communication systems receivers and transmitters generalized structural diagrams were studied and the main characteristics of such systems were also considered. Phase manipulation and, in particular, quadrature modulation, which has great potential and is widely used in existing wireless networks, were examined in detail. The basic multiple access methods, necessary for the systems with a large number of users (subscribers) developing possibility were studied. Code separation of channels was considered in more detail as the most interesting, relevant and effective channels separation solution, and also some actual groups of channel codes with their implementation methods were studied.

The result of the work is the developed software, primarily intended for broadband CDMA signal receiver using QPSK at the presence of AWGN and CPI in the radio channel modeling. The program implements the data, noise and interference generation processes, channel coding and decoding, QPSK modulation and demodulation, statistics collection and system characteristics graphing versus S/N ratios.

The software product, in addition to modeling, also acts for receiver digital data processing – it has the ability to read and process the received signal digitized by the ADC data from a memory (file with UTF-8 encoding). After refinement and optimization, for some cases, the software can process data not only from memory, but also directly from an external radio module connected via a USB interface to the processing device – thereby

forming a software-defined radio system. For SDR, the program is a key link – in addition to performing most of the work previously carried out using a large number of analog devices, it enables the operator to configure the entire system while performing to solve a wide range of problems, which also significantly reduces the final cost, facilitates easy development and the rapid spread of SDR.

Another important feature of the developed system is the platform on which it is built. The software operates on the mobile devices basis, which gives a number of advantages compared to traditional stationary equipment solutions. This makes the system:

- Portable – it has small dimensions and weight of devices.
- Modular – an easy replacement individually for both the radio module and the processing device.
- Cheap – relatively low prices for devices sufficient to operate the system.
- Affordable – mobile devices widespread use on the market, as well as their availability for almost every system user; easy distribution and installation of lightweight software; the ability to transfer the current configuration to the other devices.
- Productive – because of presence of a sufficiently powerful multi-core processor, a large amount of RAM in modern mobile devices.

Studies have been conducted to the system noise immunity at the certain settings. As a result of measurements with AWGN in the radio channel, the bit error probability indicators turned out to be less (better) than theoretical ones - this is explained by the small amount of transmitted information in the experiment, as well as the imperfection of the program algorithms. At the same time, the transmission speed slightly decreased with strong noise, but did not exceed the declared speed and throughput, which is normal. The bit error probability with the CPI in the radio channel was also measured at various interference settings. As a result of the study, it turned out that CPIs have less effect on the system than AWGN, due to the narrow-band interference. Moreover, with the tendency of the rarefaction coefficient to zero, CPI in form and parameters tends to AWGN.

Thus, the developed system is relevant for private research and practical purposes. It has great possibilities and, after refinement and optimization, can serve as the basis for educational or commercial use.

References

[1] Fajzullin, R.R. (2011), An integrated approach to solving the mobile infocommunication systems signals processing multiprocessor devices structural synthesis problem [“Kompleksnyj podhod k resheniyu zadachi strukturnogo sinteza mul'tiprocessornyh ustrojstv obrabotki signalov mobil'nyh infokommunikacionnyh sistem”] *Nelinejnyj mir*, Vol. 9. No , pp. 78-85.

[2] USB Implementers Forum, Inc. (2019). USB 3.2 Specification Language Usage Guidelines from USB-IF. [online] Available at: https://www.usb.org/sites/default/files/USB_3_2_Language_Product_and_Packaging_Guidelines_FINAL.pdf [Accessed 6 Dec. 2019].

[3] StatCounter (2020). Mobile Operating System Market Share Wordwide (1999-2020). [online] StatCounter Global Stats. Available at: https://gs.statcounter.com/os-market-share/mobile/wordwide [Accessed 10 Jun. 2020].

[4] Martin, R.C. (2019). The Clean Architecture. [online] Cleancoder.com. Available at: https://blog.cleancoder.com/uncle-bob/2012/08/13/the-clean-architecture.html.

[5] Nadeev, A.F., Podkurkov, I.A. (2015), “Adaptive estimation of non-Gaussian interference distribution parameters based on the application of the EM algorithm and its modifications”, [“Adaptivnaya ocenka parametrov raspredeleniya negaussovskih pomekh na osnove primeneniya EM-algoritma i ego modifikacij”] *Nelinejnyj mir*, Vol.13. No 8. pp. 64-72.

[6] Kadushkin, V. V. (2016), “CDMA systems non-Gaussian channel optimal receiving algorithm considering intersystem interference.” [“Algoritm optimal'nogo priema v negaussovskih kanalah CMDA sistem s uchetom vliyaniya vnutrisistemnyh pomekh”], *Zhurnal radioelektroniki*, No11, available at: http://jre.cplire.ru/jre/nov16/index.html.

[7] Fajzullin, R.R., Kadushkin, V.V., Zaripov, R.F. (2015), Poly-Gaussian algorithm for mobile communication systems channels joint demodulation-decoding [Poligaussovskij algoritm sovmestnoj demodulyacii-dekodirovaniya v kanalah mobil'nyh sistem svyazi] *Nelinejnyj mir,* Vol.13. No 8, pp. 4-9.

[8] Kadushkin, V.V., Fatyhov, M.M., Zaripov, R.F. (2016) “Sufficiency of a poly-Gaussian approximation of arbitrary probability distributions in the communication systems with mobile objects radio links”, New Technologies, Materials and Equipment of the Russian Aerospace Industry: All-Russian Scientific and Practical Conference with International Participation, Collection of reports. Vol. 2 [“O dostatochnosti poligaussovoj approksimacii proizvol'nyh veroyatnostnyh raspredelenij v radioliniyah sistem svyazi s podvizhnymi ob’ektami.” Novye tekhnologii, materialy i oborudovanie rossijskoj aviakosmicheskoj otrasli: Vserossijskaya nauchno-prakticheskaya konferenciya s mezhdunarodnym uchastiem. Sbornik dokladov. Vol 2] Izd-vo Akademii nauk RT, Kazan, pp. 521-523.

[9] Sklar, B. (2016). Digital communications: fundamentals and applications. Upper Saddle River, Nj: Prentice Hall Ptr.

[10] Lerner, I.M., Fayzullin, R.R. and Chernyavskii, S.M. (2018), “To a Matter of Increasing the Spectral Efficiency of Phase Radio-Technical Data Transmission Systems Operating under Strong Intersymbol Interference”, Russian Aeronautics. Vol. 61, No.1, pp. 120-126.

[11] Zaripov R.F., Fayzullin R.R., Fatykhov M.M. and Kaduskin V.V. KNRTU-KAI. (2017), Programma dlya modelirovaniya algoritmov obrabotki signalov v mobil'nyh sistemah svyazi [A program for simulation of signal processing algorithms in mobile communication systems], Russian Federation, Patent № 2017615223.

STABLE IONISTOR BATTERY FOR COMMUNICATION SYSTEMS

Study of technological possibilities of creating ionistor batteries to ensure the transceiver systems operation stability

Denis R. Ivanov, Ilya M. Lerner, Sergey V. Spiridonov,
Department of Nanotechnology in Electronics,
Kazan National Research Technical University named after A.N. Tupolev-KAI, KNRTU-KAI, Kazan, Russian Federation;
German-Russian Institute of Advanced Technologies (GRIAT), aviap@mail.ru

DOI: 10.36724/2664-066X-2020-6-4-11-17

ABSTRACT

The article describes a stable ionistor battery for infocommunication systems creating procedure. Based on a comparative analysis, the most balanced in terms of electrical characteristics, processability and availability components were selected. Using vacuum thermal resistive spraying, electrodes with a nanostructured carbon coating were manufacturedd. For this method, a structure with a high specific surface area obtaining technology has been formulated. Using two assembly methods, a cell of a stable ionistor battery has been built. It is possible to fully evaluate the physical and operational characteristics of the obtained ionistor batteries during long-term tests.

KEYWORDS: *ionistor, structured carbon coating, supercapacitor, thermal vacuum resistive spraying.*

INTRODUCTION

One of the reasons for the transmitting, receiving and information converting modules parasitic signals formation is supply circuits power fluctuations. The use of unstabilized power sources, pulse converters and power elements with a large spread of output parameters leads to the appearance of noise and errors in the information channels.

At the moment, there are two solutions for this problem - the use of stabilized sources powered by an external circuit, or the use of autonomous batteries [1, 2, 3]. The latter have several advantages – they are quite cheap, allows you to operate the equipment in hard-to-reach places and provide high power stability. But there are serious disadvantages, such as a limited service life and low environmental friendliness. Currently, electrochemical batteries are the most widely used. But a short service life (3-5 years), a small number of charge/discharge cycles, toxicity of components and severs requirements for operating conditions make them disadvantageous for most practical tasks.

As one of the alternative approaches to solve the tasks, caused by posed problems, is the energy storage devices new types creation [2, 4, 5]. In this paper, we examine the possibility of creating a storage device – an ionistor battery with nanostructured electrodes. The proposed design makes it possible to ensure power stability, a long service life and the ability to work in difficult climatic conditions with used the technologies high environmental safety.

STATEMENT OF THE PROBLEM AND THEORETICAL JUSTIFICATION OF THE STUDY

A. Design rationale

Due to the of double electric layer (DEL) ionistor structure high performance characteristics [2, 4, 6], this technology is used to build an ionistor battery with nanostructured electrodes.

The simplest ionistor cell with a DEL construction is presented on the Fig. 1.

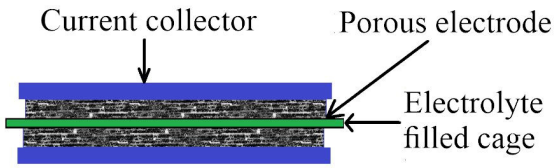


Fig. 1. Simple ionistor cell construction

A porous electrode paired with an electrolyte is involved in charge accumulation at the phase boundary. The current collector is necessary to ensure structures high charge-discharge currents. The separator electrically isolates the porous electrodes from each other while simultaneously providing high ionic conductivity for electrolyte ions.

B. Electrode material selection

Based on the chosen design, materials for the electrodes manufacturing were selected, which make an important contribution to the electric charge storage entire system efficiency [2, 6, 7]. Since the design of the electrodes can conditionally be classified as the active part (in which the charge accumulates directly) and the passive (current collector), then each of them has different requirements, and therefore the materials and manufacturing technology selection must satisfy different criteria.

The active part of the electrode is the most important and the most attention is paid to it. Analysis of existing active electrode layers materials (given in Table 1) showed that the best performance in combination with low cost are ensured when using carbon coatings. They have high conductivity and mechanical strength, a sufficient specific surface area and the technology does not require large expenditures in production.

Active electrode layers based on rare-earth materials and conductive polymers are in some cases more effective than carbon-based ones, but much more expensive or technologically less profitable.

In this work structured carbon materials were used as the main material component for electrode manufacturing, since they combine accessibility, environmental safety with high electronic conductivity (Table 2) [2, 6]. In addition, the proposed technology made it possible to achieve a high specific surface area, which critically affects the unit capacitance of the ionistor.

Table 1

Supercapacitor (ionistor) electrode materials contrastive analysis

Electrode material		**Operating voltage, V**	**Specific capacity, F/g**
Carbon-base materials	Activated carbon	1,5	40
	Graphitic carbon	3,0	12
	Carbon aerogel	3,0	160
	Ctructural carbon materials	1,5	140
	Mesoporous carbon	0,9	180
	Meso/macroporous carbon	0,8	130
	Single-walled carbon nanotube	2,3	50
	Multiwall carbon nanotube	2,5	13
Transient metal oxides	$RuO_2 \cdot H_2O$	1,0	650
	RuO_2, on carbon	0,8	1000
	MnO_2	0,8	261
	MnO_2, on activated carbon	2,2	29
	$Ni(OH)_2$	0,8	578
	$Ni(OH)_2$, on activated carbon	0,9	194
Conductive polymers	Poly (3-methylthiophene)	3,6	25
	Poly (3-methylthiophene), on MnO_2	1,0	381

Table 2

Carbon materials comparison

Material	**Specific surface area**	**Conductance**	**The cost or synthesis complexity**	**Mechanical strength and stability**	**Remarks**
Activated carbon	Very high	Very low	Very low	Very low	Requires conductive additive compounds, polymer binders, extrusion or casing to enhance some characteristics, often with damage to others
Colloidal carbon	**Low**	H		Low	More commonly used as an additive component
Disperse nanostructures (carbon nanotubes, fullerenes, etc.)	Medium	**High**	H	Low	Requires a similar approach as activated carbon, because of the high cost often used in small quantities as an additive component.
Carbon fabrics or array of carbon nanotubes	High	High	Very high	High	It is extremely expensive and difficult to achieve high reproducibility
Black lead powder	Medium	High	Low	Low	It has advantages and disadvantages specific to dispersed material, but particles have a high electrical conductivity/

Material	Specific surface area	Conductance	The cost or synthesis complexity	Mechanical strength and stability	Remarks
Structured carbon coating	Medium	High	Medium	High	Controlled morphology and structure
Carbon aerogel (black lead, graphene)	Very high	High	Very high	Very high	It was possible to obtain only in recent years, potentially extremely productive material

The structured carbon coating provides the best combination of characteristics, and further, the synthesis of this active electrode layer particular type is considered.

The second part of the electrode is the frame collector layer, sometimes called the current collector. The current collector material choice is given in the Table 3. The main criteria for this layer were: high electronic conductivity, mechanical stability, chemical inertness to the cell components, and availability.

Table 3

Current collector materials analysis

	Conductivity	Price	Processing ability	Chemical resistance
Aluminum		Low	High	Medium
Copper	y high	Medium	High	High
Precious metals (Ag, Au, Pt)	High or very high	High or very high	High or very high	Very high
Iron (steel)	Very low	Very low	Low	Low

All considered materials provide the necessary strength characteristics. Therefore, from Table 3 it follows that the most preferred materials for solving the task are aluminum and copper, as materials with the highest conductivity, availability and chemical resistance.

C. Electrolyte selection

To carry out the next step, an electrolyte for an ionistor cell capable of providing high charge-discharge currents was selected [2, 4, 9].

Existing electrolytes for super condenser with DEL comparative analysis is shown in the table below (Table 4).

Aqueous electrolytes have high ionic conductivity, are very available, and characterized by small ion sizes, which increases the electrolyte permeability into the pores of the active part of the electrode.

Aqueous electrolytes, in their turn, are also classified into several groups (Table 5).

Table 4

DEL super condensers electrolytes analysis

	Ion conductivity, S/cm	Voltage range, V	Accessibility	Ion sizes
Aqueous electrolyte	Up to 0,8	Up to 1,23	Very high	Small
Organic electrolyte	Approx. 0,02	Up to 5	Low	Large
Ionic liquids	Approx. 0,01	Up to 6	Low	Small

Table 5

Aqueous electrolytes classification

Salines	KNO_3, $AlCl_3$
Strong acids	$HClO_4$, $HClO_3$, HNO_3, H_2SO_4, HCl, HI, HBr
Alkalis	NaOH, KOH, CsOH, RbOH, $Sr(OH)_2$, LiOH, $Ba(OH)_2$, $Ca(OH)_2$

Basing on the information about conductivity (Table 6), availability and environmental friendliness, there were considered to use KOH-based electrolyte.

Table 6

Aqueous solutions peak molar mobility ($S \cdot m^2 \cdot mol^{-1}$) at 25 °C

Cation	$\lambda_i^\infty \cdot 10^4$	Anion	$\lambda_i^\infty \cdot 10^4$
H^+,H_3O^+	349,8	$½Pb^{2+}$	70
Li^+	38,7	$½Fe^{2+}$	53,5
Na^+	50,8	$⅓Fe^{3+}$	68
K^+	73,5	$½Ba^{2+}$	63,6
Rb^+	77,8	$½Ca^{2+}$	59,5
Cs^+	77,2	$½Sr^{2+}$	59,5
Ag^+	61,9	$½Ba^{2+}$	63,6
NH_4^+	73,6	$½Zn^{2+}$	54
$½Cu^{2+}$	56,6	$½Cd^{2+}$	54
$½Mn^{2+}$	53,5	$⅓Al^{3+}$	63
$½Mg^{2+}$	53,0	$⅓Pt^{3+}$	69,8
OH^-	198,3	$½CrO_4^{2-}$	85
F^-	55,4	$½C_2O_4^{2-}$	74
Cl^-	76,35	$½SO_4^{2-}$	80
Br^-	78,1	$½HPO_4^{2-}$	57
I^-	76,8	$⅓H_2PO_4^-$	12
HS^-	65	HC^-	54,6
NO_3^-	71,5	$C_2H_5COO^-$	35,8
HCO_3^-	44,5	CH_3COO^-	40,9
ClO_4^-	67,3	$C_6H_5COO^-$	32,3
$½CO_3^{2-}$	69,3	$¼[Fe(CN)_6]^{4-}$	110,5
$½SO_4^{2-}$	79,8	$⅓[Fe(CN)_6]^{3-}$	100,9

The target electrolyte concentration was determined based on the dependence shown in Figure 2.

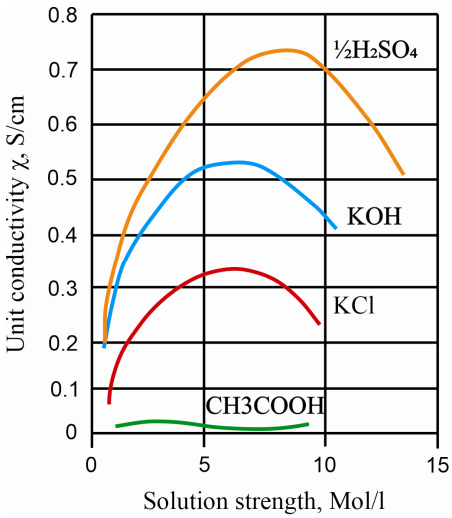


Fig. 2. Conductivity versus electrolyte concentration

Based on the graph, the highest conductivity of the KOH electrolyte is achieved at a concentration of 6 mol/L [10].

D. Separator material selection

The last element of the design is a separator – a porous material that provides electrolyte retention and opposite electrodes electrical insulation. Among the separation materials intended for electrochemical current sources, the main ones are the polypropylene, polyethylene, fiberglass, pulp and paper and fluoroplastic materials. It was found that the electrode material specific capacitance weakly depends on the nature of the separator. A weak correlation is also traced between the thickness of the separator and its impedance. Only porosity has a marked effect on impedance. Thus, the main criteria for the separator are high porosity and small thickness [11].

Based on the available commercial separator models, it was decided to use the YN-BS001 fiberglass separator (Fig. 3). Its thickness is about 300 microns, and porosity is not less than 85%.

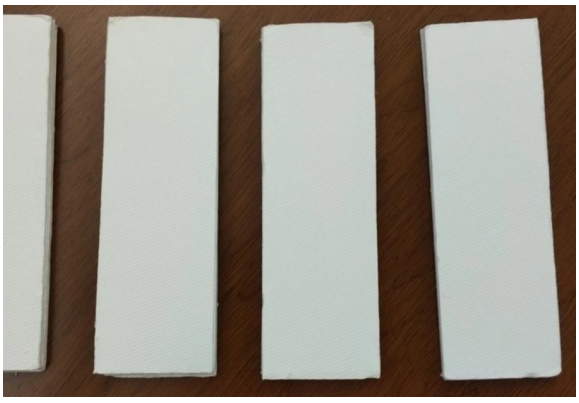


Fig. 3. YN-BS001 separator

PRACTICAL ASPECTS OF CONSTRUCTION PROBLEM SOLUTION

The main task of the technological cycle of the work was the active layer of electrodes structured carbon coating formation. The considered methods for evolved carbon coatings producing have led to the conclusion about the promising possibilities of direct thermal vacuum resistive spraying [8]. This method allows obtaining both flat films and evolved crystallite-based structures depending on the spraying mode. For this reason, in further work this approach was chosen as the main one.

As the electrodes current collector frame layers, aluminum and copper foil with a thickness of 20 μm and a purity of no worse than 99.5% were used. Before applying the active layer, the surface of the foil was subjected to cleaning in a solution of ethanol (C2H6O, 95%) and drying in an oven for 15 minutes at a temperature of 85 °C.

Substrates prepared in this way were placed in the working chamber of the Type Jee thermal vacuum-deposition system. This system implements two methods of thermoresistive spraying – indirect heating and direct evaporation of carbon material. The second method was used in the work to form a defined carbon structure.

Fig. 4. Vacuum Evaporator Type Jee thermal vacuum-deposition system

As the vaporized substance, graphite rods of 99.99% purity are used. They are sharpened in order to minimize the diameter of the mutual contact. The rods were placed in the chamber at a distance of 10-15 cm from the substrates (Figure 5).

Fig. 5. Preparation before spraying

Spraying was performed at a vacuum level of about 10-5 mm Hg. Before spraying, graphite rods were annealed with a closed shutter at a current value of 15A (900–950 °C) for 5 minutes. Temperature control was carried out using a remote infrared pyrometer.

The main spraying process was carried out in two stages - the carbon sublayer creation and the developed carbon surface formation. The sublayer was deposited for 90 minutes at a current of 15A (900–950 ° C). This stage is necessary to ensure the required adhesion and passivation of the foil surface in order to minimize the electrolyte influence on it. The second stage of spraying was carried out at a current of 24 A for 180 minutes. The temperature of the rods reached 1500 °C. Thus, the total spraying time was 4 hours 30 minutes.

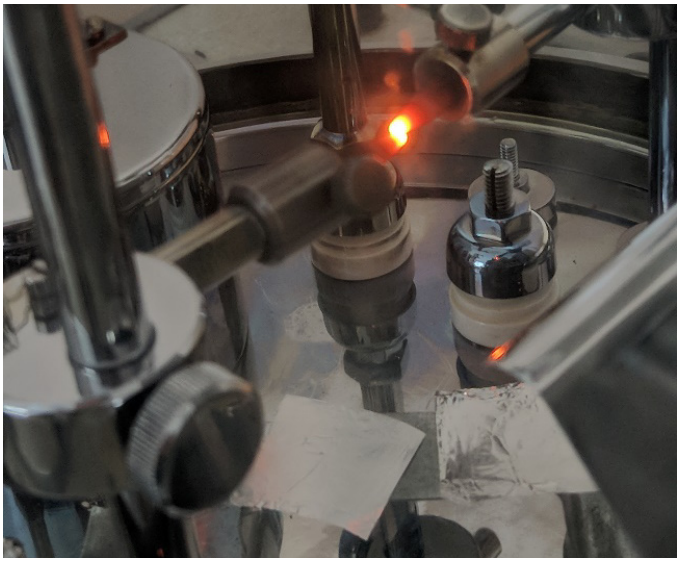


Fig. 6. Evaporation on the conducting foil process

OBTAINED SPRAYING RESULTS INVESTIGATION

To evaluate the presented technology recovery results, scanning electron microscopy with the elemental composition energy-dispersive analysis possibility were used. The study was carried out using a Carl Zeiss Auriga CrossBeam microscope.

At the first stage, the electrode main layer surface (current collectors based on aluminum and copper foil) was evaluated. Their surface before spraying can be estimated from the images in the Figure 7:

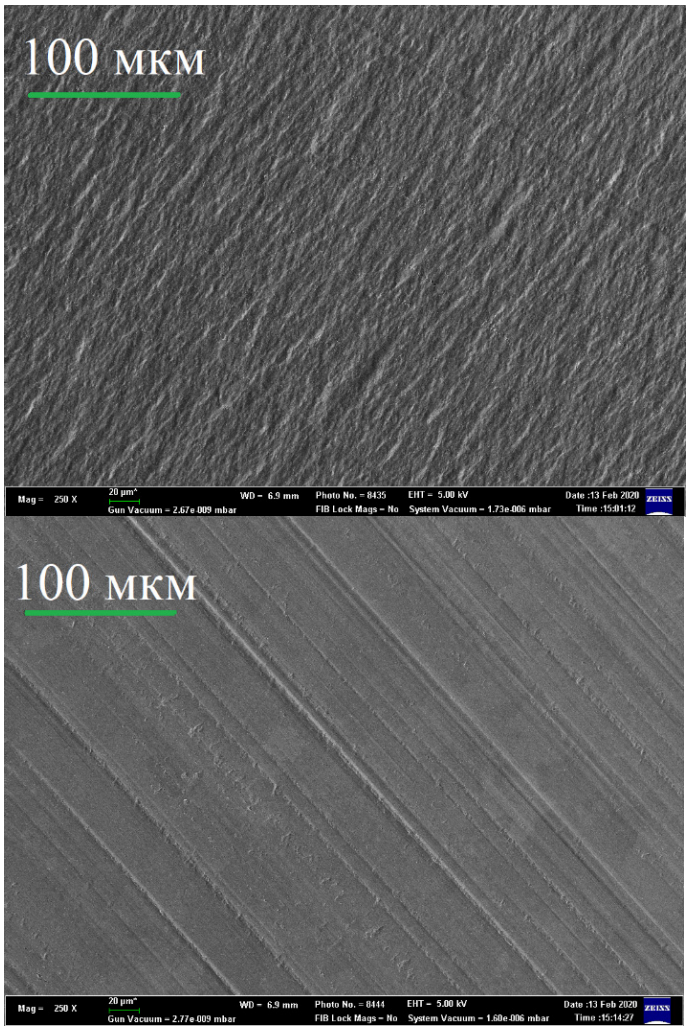


Fig. 7. Aluminium foil SEM images. Matte side exposure on the top, glossy on the bottom

Comparing the images, it can be seemed that the foil matte side has a more evolved and chaotic surface structure, which can affect the resulting coating characteristics.

Next, after carbon coating deposition, SEM images were obtained (Figure 8):

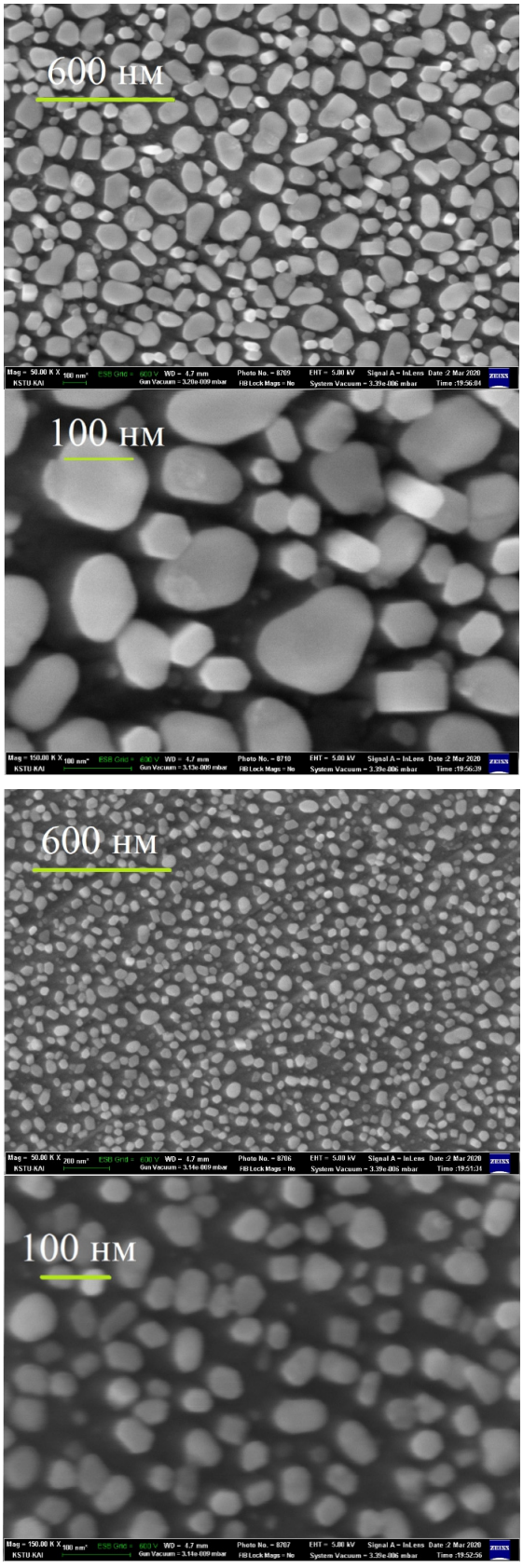


Fig. 8. SEM images of the matte (two on the top) and glossy (two on the bottom) side of an aluminum foil with a nanostructured carbon coating with magnification of 50 and 150 thousand times

The coating consists of submicron diameter crystal-like longitudinal structures. On the matte side formations are denser and larger. A more detailed inspection of the surface of the matte side is shown in the image below (Figure 9).

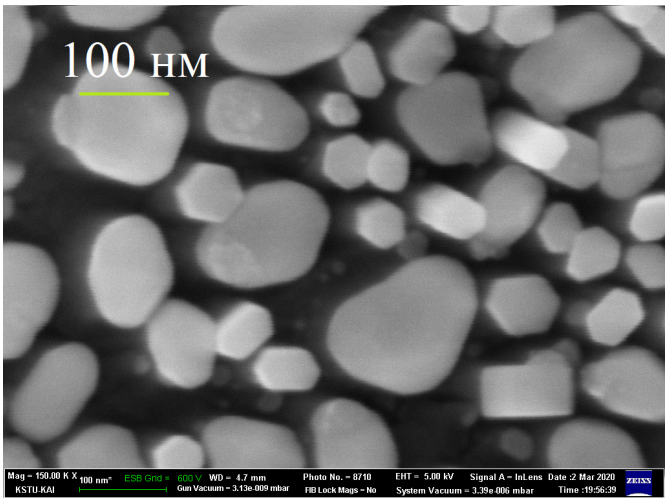


Fig. 9. Structured carbon coating increased 150 thousand times

The diameter of the structures at the baseline varies from 5 nm to 200 nm. The average particle diameter is 60 nm. The average distance between particles is 40 nm. The shape of the particles base varies from an irregular ellipse to a regular hexagon. It can be assumed that particles having the shape of a regular hexagon are a carbon single crystal with sp-2 bond hybridization. Due to the fact that the electron beam falls on the substrate at a slight deviation from the right angle, the dark background formation, indicating an elongated shape, can be seen.

For a more detailed study of the surface, it was carried out using an NT-MDT Nanoeducator II scanning probe microscope. The study confirmed that the structures are in the form of rods with a height of 200 nm to 850 nm.

A preliminary assessment of the resulting structure allows us to conclude that the surface development indicators, hence the specific surface area, are high. The latter is a key parameter that determines the ionistor cell final capacity

Electrolyte preparation

To prepare 25% KOH electrolyte, 100 ml of distilled water and 34 g of chemically pure KOH were used. To accelerate the alkali in water dissolution reaction passage, heating and mixing were carried out using a magnetic stirrer. Next, the solution was isolated from air and settled for 3-6 hours until completely clarified.

ASSEMBLY TECHNIQUE

At the final stage, stacking and coiling ionistor manufacturing technology assembly methods are considered. [2, 4] In simplest case, the cell is assembled as a hermetically

sealed package, with two manufactured electrodes embedded in it, between which there is a separator preventing electrical contact. The electrolyte is poured during the electrodes placement, or after sealing the packet with subsequent hole sealing. Electrical contacts may be formed from an ongoing electrode portion that is hermetically-sealed from the stack. Due to the fact that the electrodes are usually flat, this practically does not affect the tightness of the stack.

When using coiling manufacturing technology, at least four layers are used, two of which are "positive" and "negative" electrodes, and two others are separators. They are located alternating each other so that there is no electrical contact between the electrodes during winding. The current leads can be pre-attached to the current collector (preferably in several places, to reduce the equivalent series resistance), as shown in the design example (Figure 10).

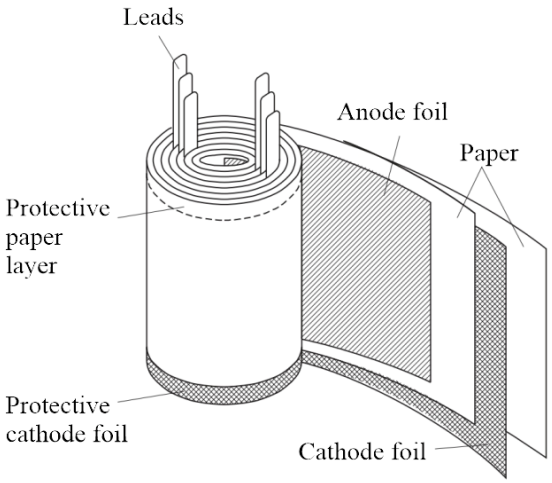


Fig. 10. Ionistor battery construction example [12]

It is also possible to provide such arrangement of electrodes and separators that winding each end surface forms an electrical output of one of the electrodes. Refueling with electrolyte is carried out before winding or when placing the finished structure in a special case. The housing must be hermetically-sealed, durable and chemically inert to the supercapacitors internal environment. Each assembly method has its advantages and disadvantages. In the case of stacking technology, the required voltage inside one battery is easily achieved due to the cells series coupling. Coiling technology is preferable for production due to the ability to scale. Both methods were used in the work.

CONCLUSION

Within the framework of this study, the stabilized autonomous power source based on an ionistor battery creating possibility was considered. The main approaches to such energy storages design were considered. A complete technological study of all stages of finished cell item obtaining is carried out. During experimental work steps, a proprietary approach to electrodes active part obtaining was proposed. All technological steps have been carried out to form the ionistor cell and its assembly elements. Performed operations allow us to conclude the possibility of such power sources cheap and maintainable production. However, a more detailed study of all operational properties is required.

Acknowledgments

The article authors are grateful to the "Prikladnye Nanotehnilogii" (Applied Nanotechnology) core facilities center of Kazan National Research Technical University named after A.N. Tupolev for providing research technical opportunities.

REFERENCES

[1] Wang S., Wei T., Qi Z. (2008) Supercapacitor energy storage technology and its application in renewable energy power generation system. *Proceedings of ISES World Congress 2007*, Vol. I, pp. 2805-2809.

[2] Raza, W., et al.. (2018). Recent advancements in supercapacitor technology. *Nano Energy*, 52, pp.441–473.

[3] Moftah A., Al Shetiti A. (2015) Review of Supercapacitor Technology. *Int. J. Comput. Sci. Electron. Eng.* V. 3(3). pp. 226-231.

[4] Kötz, R. and Carlen, M. (2000). Principles and applications of electrochemical capacitors. *Electrochimica Acta*, 45(15–16), pp.2483–2498.

[5] Gautham Prasad, G., Shetty, N., Thakur, S., Rakshitha and Bommegowda, K.B. (2019). Supercapacitor technology and its applications: a review. *IOP Conference Series: Materials Science and Engineering*, 561, p. 012105.

[6] Lewandowski, A. and Galinski, M. (2007). Practical and theoretical limits for electrochemical double-layer capacitors. *Journal of Power Sources*, 173(2), pp. 822-828.

[7] Tabarov, F.S. (2019). Obtaining and properties of fibrous carbon materials for supercapacitor electrodes. Ph.D. thesis in Engineering Science. 115 p.

[8] Vangari, M., Pryor, T. and Jiang, L. (2013). Supercapacitors: Review of Materials and Fabrication Methods. *Journal of Energy Engineering*, 139(2), pp. 72-79.

[9] Jónsson, E. (2019). Ionic liquids as electrolytes for energy storage applications – A modelling perspective. *Energy Storage Materials*, 25. pp. 827-835.

[10] Svarovskaya, N.A., Kolesnikov, I.M. and Vinokurov, V.A. (2017). Electrochemistry of electrolyte solutions ["Elektrohimiya rastvorov elektrolitov"]. Moscow: Publishing Center of the Russian State University of Oil and Gas (NRU) named after I.M. Gubkin, 66 p.

[11] Chaika, M.Y. (2012). The main types of separation materials in supercapacitors with non-aqueous electrolyte ["Osnovnye tipy separacionnyh materialov v superkondensatorah s nevodnym elektrolitom"]. *Vestnik VGTU*, 6, pp. 57-60.

[12] Popel, O.S., Tarasenko, A.B. and Kolomiets, Y.G. (2012). Electric energy storage devices for use in renewable energy power plants.[" Nakopiteli elektricheskoj energii dlya ih ispol'zovaniya v energoustanovkah na vozobnovlyaemyh istochnikah energii"] Moscow: M.V. Lomonosov Moscow State University, p. 49.

PHYSICAL MODELING OF METAMATEREALS ON THE BASIS OF THE FLAT SPIRAL COIL

Z.R. Idiatullov, I.I. Ahmetov, M.M. Fatyhov, S.V. Spiridonov, I.M. Lerner
Kazan National Research Technical University named after A. N. Tupolev - KAI, Kazan, Russia;
German-Russian Institute of Advanced Technologies (GRIAT)

DOI: 10.36724/2664-066X-2020-6-4-18-30

ABSTRACT

In this work, the problems of physical modeling of metamaterials based on flat spiral coils with different geometric shapes were considered. The main parameters of the structures metamaterial modeling, methods of creation, as well as their unique properties are considered. As a result of physical modeling, structures were obtained that model the metamaterial with different values of dimensions and parameters. On the basis of the experimental data, the best variant of the geometric shape of the structure element was determined, based on the highest transmission coefficient.

KEYWORDS: *metamaterial, electromagnetic interaction, physical modelling.*

INTRODUCTION

In recent years, metamaterials have attracted great attention in connection with the prospects of their practical application for radio masking and the development of antenna technology - the creation of compact flat antennas, high-impedance surfaces, decoupling of antenna array elements. Metamaterials are artificial materials consisting of composite structural elements that acquire their unusual properties that do not exist in nature. A fundamental feature of metamaterials is their ability to provide a strong magnetic response at terahertz and even optical frequencies, where the magnetic permeability of ordinary materials is close to unity.

In accordance with various physical properties, metamaterials can be classified into acoustic, thermal, photonic and electromagnetic (EM) metamaterials. Recently, EM metamaterials that are constructed from subwavelength structural units have received much attention because of their exotic properties, such as the inverse Doppler effect, Vavilov-Cherenkov back radiation, negative refractive index, double negative property, etc. EM-metamaterials simultaneously have negative permittivity and negative permittivity (ie, $e < 0$ and $\mu < 0$) and obey the left-hand rule, which differ from conventional materials.

Currently, the transmission efficiency is strictly limited in a wireless power transmission system (WPT) with conventional materials and therefore new methods are required to increase the transmission efficiency. This problem can be solved with the help of metamaterials, which are special structures. Flat spiral coils can be used as elements for physical modeling, and for predicting the behavior of electromagnetic fields in metamaterials. The relevance of this topic is justified by the fact that today metamaterials have unique properties with which you can increase the efficiency of energy transfer. It is also important to note that it allows you to save money on the transmission and reception of electrical energy, as well as reduce the costs associated with maintaining direct connectors.

THEORETICAL PART

A. Areas of application of metamaterials and their basic properties

According to different values of permittivity and permeability, materials can be divided into four categories (Figure 1).

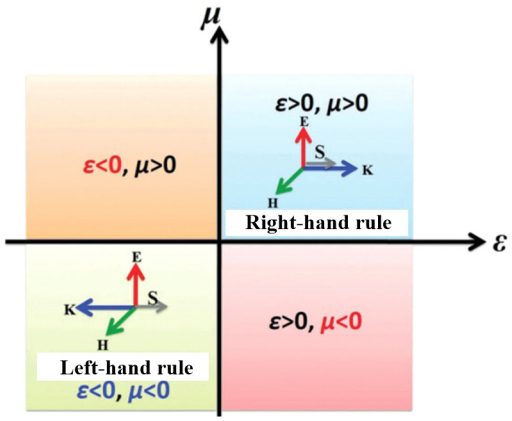


Fig. 1. Categories of materials based on values of different dielectric constant (e) and permeability (m). E, H, K and S – electric field, magnetic field, wave propagation and Poynting vectors

For ordinary materials, dielectric constant and permeability are positive. When the dielectric constant or permittivity is negative (i.e., e < 0 and μ > 0 or e > 0 and μ <0), the materials are called epsilon-negative (e.g. metals, plasma) or μ-negative materials (e.g. gyrotropic magnetic materials). Interestingly, when these two parameters are simultaneously negative, the materials are defined as double negative materials. In fact, a double negative property was originally observed in metamaterials.

When the values of e and m are simultaneously positive or negative, electromagnetic waves can propagate through the medium. For ordinary materials (i.e., e> 0 and μ> 0), the electric vector E, the magnetic vector H and the wave vector K correspond to the right-hand rule. Meanwhile, the Poynting vector S, which is the energy flux density, has the same direction of wave propagation when the energy decays along with wave propagation.

For metamaterials with a double negative property (e < 0 and μ < 0), electromagnetic waves can propagate through the media and satisfy the Maxwell equations, equation (1) - (4),

$$k \times E = \omega \mu H \quad (1)$$

$$k \times E = -\omega \mu H \quad (2)$$

$$k * E = 0 \quad (3)$$

$$k * H = 0 \quad (4)$$

When the permittivity and permittivity are both negative, the three vectors E, H, and K of the double negative materials obey the left-side rule, and the Poynting vector is opposite to the direction of the wave vector that is directed to the source. In this case, it is shown that the energy flux of electromagnetic waves is opposite to the positive direction of the source phase.

The simplest example of the difference between normal materials and a negative refractive index (NRI) is obtained by comparing two materials for the refractive effect. In a normal transparent (dielectric) material, an electromagnetic beam is refracted in the normal direction (blue line) when it passes from air to a material with a higher optical density (positive index), as shown in the figure. In NRI, the beam is refracted to the other side (red line) of the normal, as shown in Figure 2.

The angle of refraction is obtained from Snell's law, which states that the ratio of the sines of the angles of incidence and refraction is equal to the ratio of the velocities in two media or, equivalently, the inverse ratio of the refractive indices n_1 and n_2. Thus,

$$n_1 \sin \theta_1 = n_2 \sin \theta_2 \quad (5)$$

where n_1, n_2, θ_1 and θ_2 – are the refractive index of media 1 and 2, the incident and refractive angles.

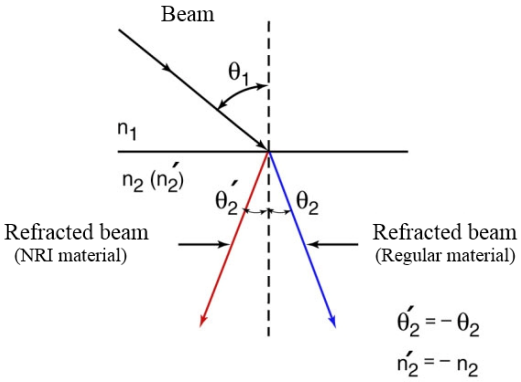


Fig. 2. Refraction in normal material (blue line) and NRI (red line)

Figure 2 shows the practical application of this material with NRI. In this figure, we compare the effects of focusing the light of lenses made from ordinary materials (blue) and NRI (red). Note that NRI has an effect opposite to that of ordinary material: in a convex lens, rays diverge, and in a concave lens, rays converge. In Figure 3, a plate containing normal material (a) deflects the beam (s_1) so that a virtual source is visible inside the material, and a plate containing NRI (b) focuses the beam (s_1) inside the material (f_1) and on the other side of source outside the material (f_2) [1].

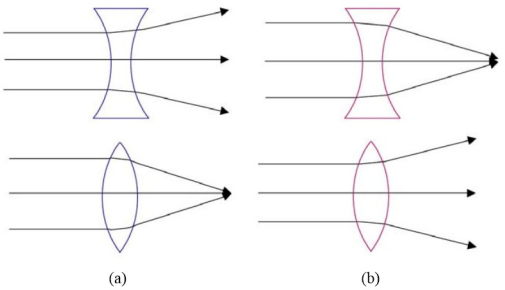


Fig. 3. The effect on the bundles of EM lenses made from (a) normal material and (b) NRI

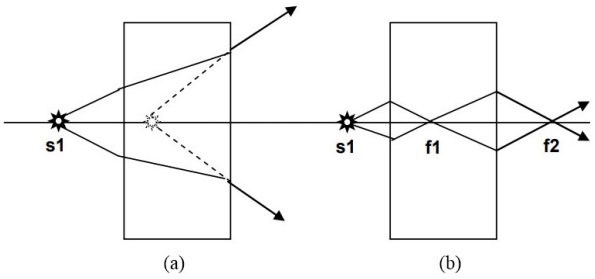


Fig. 4. The effect on electromagnetic beams of flat plates made of (a) normal material and (b) NRI

For metamaterials with negative permittivity and negative permittivity, the incident beam and the refracting beam are on the same side of the normal. This indicates that the refractive index of metamaterials is a negative value, namely $n = -\sqrt{\varepsilon\mu}$.

In addition, metamaterials have other unique properties, including the inverse Doppler effect, Vavilov – Cherenkov back radiation.

The Doppler effect (discovered in 1842 by Christian Doppler) is that with the relative movement of the observer and the wave source, the wave frequency changes. If we are talking about a sound wave, for example, from an approaching train, then its frequency increases as it approaches, when the train moves away, the frequency decreases. The same phenomenon occurs with light. When the object and the observer approach each other, the frequency of the light wave increases (from red to blue), and, conversely, if they move away, the frequency decreases.

To observe this effect, it is necessary to grow a nanostructured silicon crystal, a unique photonic superprism with a negative refractive index. By directing the laser beam to the prism and changing the distance between it and the detector, the scientists managed to register the opposite Doppler effect, when the light "turns red" when objects are approaching, and "turn blue" when removed [2].

We note that the Vavilov – Cherenkov radiation (IVF) of the charge in the "left" medium is "inverse" in nature, that is, it propagates (in the sense of the direction of the energy flux density) at an obtuse angle to the velocity of the charge. In the case when the charge flies into the "left" medium, the ion-frequency generator generated in it falls to the interface, generating radiation, which can be called "reverse Cherenkov-transitional radiation" (RCTR). Radiation exists only in the presence of an interface (as transition radiation) and only in the presence of an inverse IVF in a medium [3].

Metamaterials can be created with various electrical properties. Their classification depending on the values of the relative dielectric and relative magnetic permeabilities is shown in Figure 5.

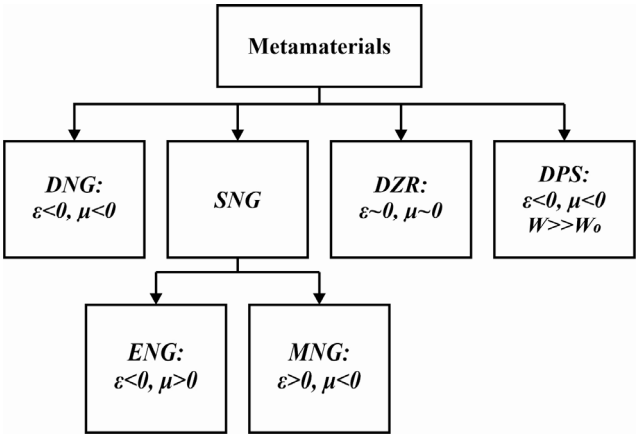


Fig. 5. Classification of metamaterials

An analysis of this figure shows that the names MM determine the relative permeabilities of the material:

– DNG – double negative (both permeabilities are negative);

– DPS – double positive (both permeabilities are positive, the wave resistance of the medium W is much higher than the wave resistance of the free space W_0. Hence the second name - – Hi-Z – high impedance surfaces);

– NG – single negative (one value from the permeabilities is negative: if the relative dielectric constant is negative, then the name ENG is accepted, if the relative magnetic permeability, then MNG). These materials are also called mixed-type metamaterials;

– DZR – double zero (both permeabilities are practically equal to zero, which leads to the fact that the reflection coefficient from these materials is close to zero).

The electrical properties of metamaterials can either vary with frequency, i.e. form dispersing media, or keep their values in a relatively wide frequency band. In the first case, MMs form frequency-selective structures (FSS), as shown in Figure 6.

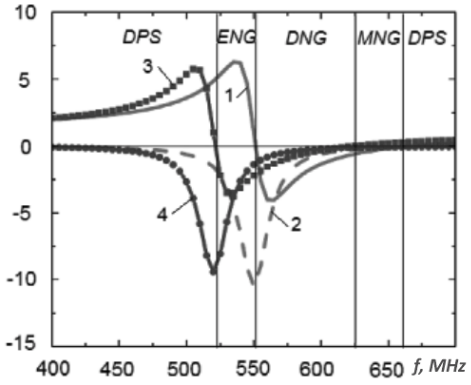


Fig. 6. Frequency dependence of dispersive type metamaterials: 1 –ε_r'; 2 – ε_r''; 3 – μ_r'; 4 – μ_r''

The main feature of the construction of metamaterials is the artificially created periodic structure. Depending on the number of directions the frequency is observed, 1D, 2D and 3D structures are distinguished. The physical implementation of FSS may be different. So, they can be implemented in the form of dielectric materials with fillings in the form of open resonant wire rings (SRR).

The shape of the rings can be deformed from round to square. Examples of designs are shown in Figure 7 a, b. For the physical implementation of metamaterials that retain their electrical properties in a wide frequency band, rings are not closed, but closed. In addition, the rings can be arranged randomly in the material structure. Two options for implementing this design from the work are shown in Figure 8 [4].

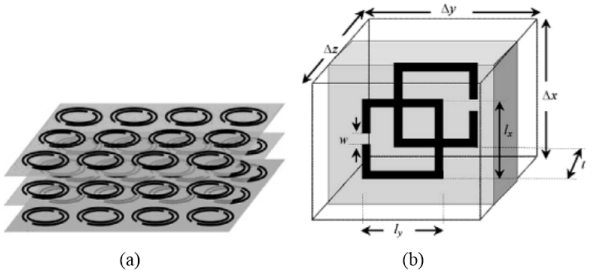


Fig. 7. Examples of the physical implementation of frequency-selective structures: a – with filling from open rings; b – with filling from open squares

In accordance with their specific electromagnetic properties, metamaterials have great potential applications in the development of invisible cloaks, super lenses, absorption of electromagnetic waves and microstrip antennas. In recent years, it is known that negative-permeability metamaterials can improve the resolution of magnetic resonance imaging, due to their ability to focus radio frequency magnetic field lines.

In addition, the unique properties of metamaterials, especially the amplification of damped waves, are of great importance for WPT, since resonant coupling is, in fact, a coupling of damped waves. When the metamaterial is placed between the coils of the transmitter and receiver, the damped wave can be amplified, and the transmission coefficient can also improve, which leads to an increase in the energy transfer efficiency and transmission distance.

B. Principles of operation of metamaterials

We begin the explanation of the metamaterials working principles with the simplest version of their execution - high-impedance structures. These designs are resonant LC circuits tuned to a specific frequency. The elements of these circuits, as shown in Figure 9, are formed as follows: capacitances are created in the gaps between the metal plates of one row or adjacent rows, and the inductance is formed due to the vortex-like leakage of the magnetic field into the internal cavity. High-impedance surfaces are used as shields for controlling the electromagnetic field located near wire antennas.

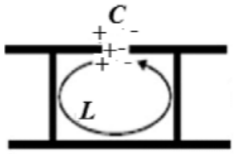


Fig. 8. Representation of a Hi-Z cell as an LC circuit

In the classical construction of an antenna with a metal reflector in the form of a plane (PEC), the emitter is placed at a distance of λ / 4 (λ is the working wavelength) from the metal screen, as shown in Figure 9 a. In this case, the electr agnetic wave incident on the screen from the emitter and reflected from the screen in the region located behind the emitter is added in antiphase, and the diffraction maximum occurs only in the direction of the main lobe of the radiation pattern. When the emitter is placed at a distance less than λ / 4, as shown in Figure 9b, these waves are not in antiphase and a diffraction lobe appears, comparable in level with the main lobe of the antenna pattern.

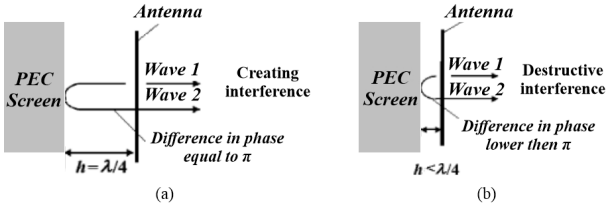


Fig. 10. Placing the emitter near a perfectly conducting electric current screen: a – case of suppression of the diffraction lobe; b – the case of the formation of a diffraction lobe

Near the high-impedance surface, the phase shift between the incident and reflected waves is zero. As a result, when the emitter is placed at distances much shorter than the wavelength, the diffraction lobe does not occur, as shown in Figure 10. This effect is due to the fact that a resonant cavity is formed between the metal base and the emitter, acting as a partially reflecting surface [4].

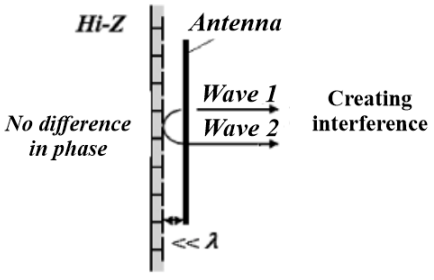


Fig. 11. Placing the emitter near Hi-Z

C. Magnetic field of a flat spiral coil

The magnetic field of a conductor with a current of arbitrary configuration (for example, a coil) can be obtained by the known method of superposition of the fields of elementary linear sections of the conductor.

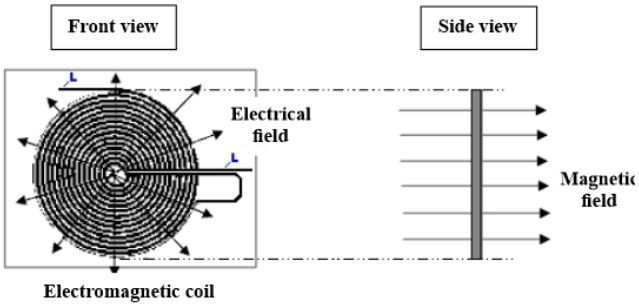


Fig. 12. The structure of the magnetic field lines in the area adjacent to the turns of a flat spiral coil

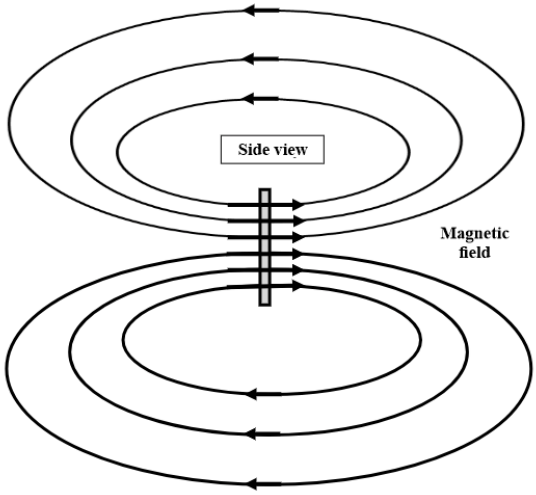


Fig. 13. The generally accepted structure of the magnetic field lines in the near zone (coil zone) of a flat spiral coil outside

The magnetic field of a flat spiral coil can be represented by a superposition of the fields of concentric individual turns, the diameter of which varies in accordance with the pitch of the spiral. The turn consists of infinitely small individual straight-line sections. In this case, the magnetic field of each turn is calculated as a superposition of the fields of its constituent discrete sections (DE). The numerical solution of the mathematical model constructed in this way allows us to obtain the value of the magnetic field induction of a complex configuration of conductors at any point in space.

The implementation of this model for a flat coil includes the following steps:

1. Calculation of the magnetic induction of the DE field at any point in space (PiS) according to the Bio-Savard-Laplace law:

$$\Delta\mathbf{B}(\mathbf{r}) = \frac{\mu_0 I}{4\pi}\left(\frac{\Delta\mathbf{L}\times\mathbf{r}}{\mathbf{r}^3}\right) \tag{6}$$

where $\Delta\mathbf{L} = (\Delta L_x; \Delta L_y; \Delta L_z)$ – discrete section; $\mathbf{r} = (r_x; r_y; r_z)$ – research point.

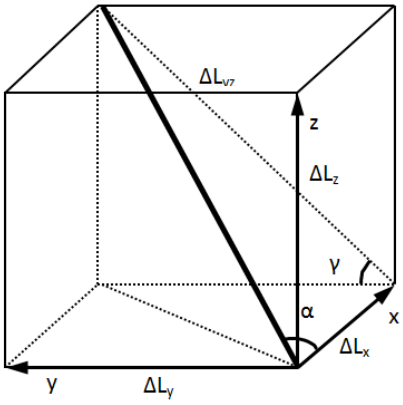


Fig. 14. Determination of orientation DS

If the vector product $\Delta\mathbf{L}\times\mathbf{r}$ is denoted by the auxiliary vector $\mathbf{k}$ ($\mathbf{k} = \Delta\mathbf{L}\times\mathbf{r}$), then, taking into account formulas (7), it follows (8) and (9):

$$\Delta Lx = \Delta L\cos\alpha;\ \Delta L_y = \Delta L\sin\alpha\cos\gamma;\quad \Delta L_z = \Delta L\sin\alpha\sin\gamma \tag{7}$$

$$|\mathbf{k}| = |\Delta\mathbf{L}\times\mathbf{r}| = \sqrt{k_x^2 + k_y^2 + k_z^2};$$

$$\mathrm{k}_x = \begin{vmatrix}\Delta L_y & \Delta L_z\\ r_y & r_z\end{vmatrix} = \Delta L_y r_z - r_y\Delta L_z;$$

$$\mathrm{k}_y = \begin{vmatrix}\Delta L_z & \Delta L_x\\ r_z & r_x\end{vmatrix} = \Delta L_z r_x - r_z\Delta L_x; \tag{8}$$

$$\mathrm{k}_z = \begin{vmatrix}\Delta L_x & \Delta L_y\\ r_x & r_y\end{vmatrix} = \Delta L_x r_y - r_x\Delta L_y;$$

$$|\mathbf{r}| = \sqrt{\mathrm{r}_x^2 + \mathrm{r}_y^2 + \mathrm{r}_z^2};$$

$$\mathrm{r}_x = \mathrm{x}_i - \mathrm{x};\ \mathrm{r}_y = \mathrm{y}_i - \mathrm{y};\ \mathrm{r}_z = \mathrm{z}_i - \mathrm{z}; \tag{9}$$

7

where: (*xi*, *yi*, *zi*) are the coordinates of the remote control; (*x*, *y*, *z*) - coordinates of an arbitrary point in space.

2. Calculation of the magnetic field of a coil:

For this, a consistent calculation of the influence of all sites is necessary, taking into account their spatial location and the linear dimensions of the projections of the sites.

To simplify the calculation, the coil is placed in one of the planes of space (*xy* plane) (see Figure 13). Then the projections of the remote control are defined as:

$$\Delta L_{xi} = \Delta L\cdot\sin\alpha;\ x_i = R\cdot\cos\beta;$$
$$\Delta L_{yi} = \Delta L\cdot\cos\alpha;\ y_i = R\cdot\sin\beta; \tag{10}$$
$$\Delta L_{zi} = 0;\qquad z_i = 0.$$

where: i = 1…N; β = 0…360^{O} in increments of 2π / N; ΔL = 2π R / N; *N* – the number of sections of the coil (determines the accuracy of the calculations); *R* – turn radius.

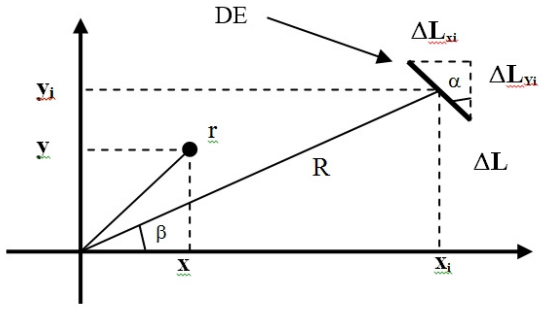


Fig. 14. Straight line discrete section (DS)

3. Calculation of the total magnetic induction in PiS:

It is carried out by the principle of a superposition of induction of turns creating a spiral:

$$B_{full} = B_{R1} + B_{R2} + ... + B_{Rm-1} + B_{Rm} \quad (11)$$

where R_m is the radius of the outer coil (ring) of the spiral.

This simulation by measurement allows you to visualize the structure of the magnetic field using the well-known classical method.

RESEARCH METHODS OF PRODUCING METAMATERIALS

The frequency range of metamaterials extends to the terahertz, infrared and visible frequency ranges. The size of the structure for metamaterials depends on the practical application, as well as on the methods of synthesis and manufacture. In the field of microwave frequencies, metamaterials are mainly manufactured by lithography with a shadow mask; in the terahertz or visible frequency range, metamaterials can be obtained by electron or ion beam lithography.

Figure 15 shows metamaterials with various sizes and structures. The first manufacturing method is the nanofabrication method to obtain metamaterials consisting of nanoscale U-shaped unit cells of gold in Figure 15a. Compared to previous double ring resonators, this single gold ring matrix can generate magnetic resonance and achieve a negative refractive index of about 100 THz, which is the result of the resonance of the inductive-capacitor circuit.

The second method is electron beam lithography for the manufacture of multilayer Ag – MgF2 – Ag structural metamaterials that were located on a glass substrate coated with a thin film of 5 nm thick indium tin oxide to avoid charging effects during lithography. As shown in Figure 15b, the structural unit was a nanoscale grid, and a negative refractive index was observed at a wavelength of almost 780 nm in silver-based metamaterials.

The copper-based metamaterial was prepared by lithography using a shadow mask, and the microdimensional structure nodes were composed of split-cavity ring resonators (SRR) and copper wires in Figure 15 g, which showed negative permittivity and negative permeability in the microwave mode.

Figure 15 e shows the method of surface multilayer galvanic synthesis of non-planar copper-based SRRs on a flexible silicon substrate.

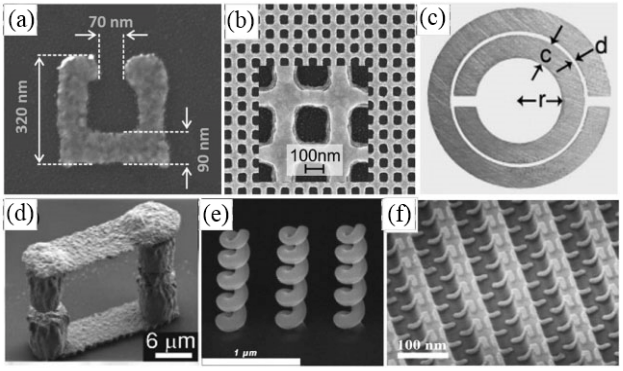


Fig. 15. Metamaterials with various sizes and structures. (a-f) Metamaterials with a nanoscale U-shaped, nanoscale mesh, round, flexible metamaterial with a micronized U-shaped structure, nanoscale spiral and nanoscale L-shaped [1]

EXPERIMENTAL PART

The figures show various geometric forms of structures simulating a metamaterial. In this section, the parameters of the coils and their calculations will be presented.

D. Flat disk inductance (coils)

The flat disk inductance (coil) is found by:

$$L=\frac{\mu_0}{8\pi}\omega^2 d\,\pi \quad (12)$$

where ω is the number of turns of the coil; d = (d1 + d2) / 2 – its average diameter; Ψ is the value whose values are given in table 1 depending on the ratio ρ = r / d, where r is the radial size (width of the winding) of the coil and the magnetic constant μ0 = 4n* 10 $^{-7}$ GN/m.

For small values of ρ, the interpolation according to Table 1 may turn out to be insufficiently accurate, and then to determine Ψ one should use the formula:

$$\pi=4\,\pi[\,(1+\frac{p^2}{24}+\frac{11}{2880}p^4+\ldots)\ln\frac{4}{p}$$

$$-\frac{1}{2}+\frac{43}{288}p^2+\frac{1}{150}p^4+\ldots]. \quad (13)$$

On the contrary, with large ρ (ρ> 0,5):

$$\pi=\frac{(1+p)^3}{p^2}(1{,}7424+3{,}2900\,®^3\ln\pi-2{,}27\,\pi^3+0{,}3702$$

$$\pi^5+0{,}0826\,\pi^7+0{,}0312\,\pi^9+\ldots), \quad (14)$$

Table 1

Values Ψ for flat reel

ρ	Ψ	ρ	Ψ	ρ	Ψ	ρ	Ψ
0,00	—	0,25	28,767	0,50	20,601	0,75	16,360
01	69,008	26	28,290	51	20,381	76	16,235
02	60,299	27	27,832	52	20,165	77	16,112
03	55,206	28	27,392	53	19,955	78	15,992
04	51,595	29	26,968	54	19,750	79	15,874
0,05	48,794	0,30	26,560	0,55	19,550	0,80	15,759
06	46,507	31	26,166	56	19,354	81	15,646
07	44,574	32	25,786	57	19,162	82	15,536
08	42,902	33	25,418	58	18,976	83	15,428
09	41,428	34	25,063	59	18,793	84	15,323
0,10	40,111	0,35	24,719	0,60	18,614	0,85	15,220
11	38,920	36	24,386	61	18,440	86	15,119
12	37,835	37	24,063	62	18,269	87	15,021
13	36,838	38	23,750	63	18,102	88	14,925
14	35,916	39	23,446	64	17,939	89	14,832
0,15	35,058	0,40	23,150	0,65	17,779	0,90	14,740
16	34,258	41	22,863	66	17,623	91	14,650
17	33,507	42	22,584	67	17,470	92	14,563
18	32,800	43	22,313	68	17,320	93	14,478
19	32,132	44	22,049	69	17,174	94	14,394
0,20	31,500	0,45	21,792	0,70	17,032	0,95	14,314
21	30,900	46	21,541	71	16,891	96	14,235
22	30,330	47	21,297	72	16,754	97	14,158
23	29,785	48	21,059	73	16,620	98	14,083
24	29,265	49	20,827	74	16,489	99	14,010
0,25	28,767	0,50	20,601	0,75	16,360	1,00	13,939

E. Inductance of flat polygonal coils

The average diameter *d* of the equivalent planar circular coil is found from the diameter *D* of the circle described around the middle coil of the coil. Having found the average diameter d of the coil, we determine its inductance *L*.

If the radial size *r* is small compared with the diameter *D*, then the inductance of the coil can be determined directly by the following formulas:

For n = 3

$$L=\frac{3}{2\pi}\mu_0\omega^2 c\left(\ln\frac{1}{p}+0{,}0945+0{,}4132\,p+0{,}3194p^2+\ldots\right);$$

For n = 4

$$L=\frac{2}{\pi}\mu_0\omega^2 c\left(\ln\frac{1}{p}+0{,}7260+0{,}1776\,p+0{,}125p^2+\ldots\right); \quad (15)$$

n=6

$$L=\frac{3}{\pi}\mu_0\omega^2 c\left(\ln\frac{1}{p}+1{,}3485+0{,}0678\,p+0{,}0491p^2+\ldots\right);$$

For n=8

$$L=\frac{4}{\pi}\mu_0\omega^2 c\left(\ln\frac{1}{p}+1{,}7120+0{,}0363\,p+0{,}0277p^2+\ldots\right).$$

F. Calculation of the inductance of structures simulating a metamaterial:

1) Square shape flat coil:

c= 8,5 cm; r= 3,5 cm; ω= 5; $D=\frac{c}{\sin\frac{\pi}{n}}$, cm; D= 12 cm;

$\frac{r}{D}=\frac{3,5}{12}=0,3$; d= 0, 8075*12= 10 cm; $\rho=\frac{3,5}{8,5}=0,4$;

$\ln\frac{1}{0,4}=0,9$; 0,1776*p = 0,07; 0,125*p^2 = 0,02

Substituting these values in the formula, we obtain the inductance value:

At n = 4

$$L=\frac{2}{n}\mu_0\omega^2 c\left(\mathrm{Ln}\frac{1}{p}+0{,}726+0{,}1776\,p+0{,}125p^2\right)$$

$$L=\frac{2}{\pi}\times 4\pi\times 10^{-7}\times 25\times 0{,}085\,(0{,}9+0{,}726+0{,}07+0{,}02)$$

L = 3 μH

Sm = 33 cm^2 – coil conductor area

Fig. 16. Square shape flat coil

2) Square shape flat coil:

c= 13 cm; r= 5 cm; ω = 6; $D=\frac{13}{\sin\frac{\pi}{n}}$ = 18 cm;

r/ D= $\frac{5}{18}$= 0,3; d=0,8075×18= 15 cm; p= $\frac{5}{13,5}$ = 0,4;

$\mathrm{Ln}\frac{1}{0,4}$= 0,9; 0,1776*p = 0,07; 0,125*p^2 = 0,02;

$L=\frac{2}{\pi}\times\mu_0\times 36\times 0{,}13\times 1{,}716$ = 6,7 μH;

Sm = 80 cm^2

Fig. 17. Square shape flat coil

3) Rectangular s pe flat coil

c= 14 cm; r= 4,5 cm; ω = 7; $D=\frac{14}{\sin\frac{\pi}{0,4}}$ = 20 cm;

r/ D= $\frac{4,5}{20}$= 0,3; d=0,8075×20= 16 cm; p= $\frac{4,5}{14}$= 0,3;

$\mathrm{Ln}\frac{1}{0,3}$= 1,2; 0,1776*p = 0,05; 0,125*p^2 = 0,01;

$L=\frac{2}{\pi}\times 4\pi\times 10^{-7}\times 49\times 0{,}14\times 1{,}986$ = 9,4 μH;

Sm = 94 cm^2

Fig. 18. The rectangular shape of a flat coil

4) Hexagonal shape flat coil:

c= 7,5 cm; r= 5 cm; ω= 6; n= 6; μ_0= 4 $\pi \times 10^{-7}$;

D= $\frac{c}{\sin\frac{\pi}{n}}$; D= $\frac{7,5}{\sin\frac{3,14}{6}}$ = 15 cm; r/ D= $\frac{5}{15}$= 0,3;

d=0,9124×15=14 cm; p= $\frac{r}{c}$ = $\frac{5}{7,5}$= 0,6; Ln$\frac{1}{p}$= 0,51;

0,0678*p = 0,04; 0,0491*p^2 = 0,017;

L=$\frac{3}{\pi}$ μ_0 ω^2 c (Ln$\frac{1}{p}$ + 1,3485+ 0,0678p+0,0451p^2)=

= $\frac{3}{3,14}$ ×4 $\pi \times 10^{-7}$ × 36 × 0,075 (0,51+ 1,349+ 0,04+

+ 0,017)= 6,6 μH; Sm = 80 cm^2

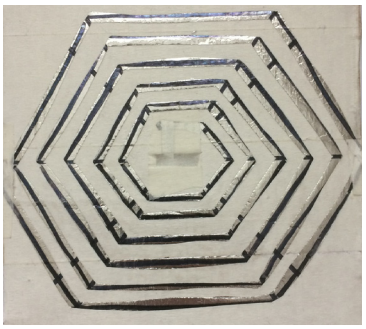


Fig. 19. Hexagonal shape of a flat coil

5) Octagonal flat coil shape:

c= 6 cm; r= 5 cm; ω= 6; n=8; D= $\frac{6}{\sin\frac{3,14}{6}}$ = 16 cm;

r/ D= $\frac{5}{16}$= 0,3; d=0,9501×16=15 cm; p= $\frac{r}{c}$ = $\frac{5}{6}$= 0,8;

Ln$\frac{1}{p}$= 0,2; 0,0363*p = 0,029; 0,0277*p^2 = 0,017;

L=$\frac{4}{n}$ μ_0 ω^2 c (Ln$\frac{1}{8}$ + 1, 712+ 0,0363p+0,0277p^2)=

= $\frac{4}{3,14}$ ×4 $\pi \times 10^{-7}$ × 36 × 0,06 × (0,2+ 1,712+ 0,029+

+ 0,017)= 7 μH; Sm = 86 cm^2

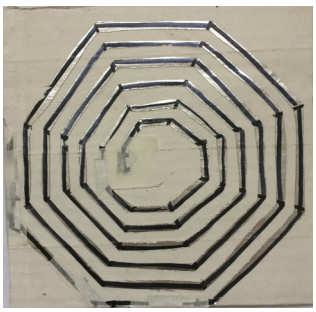


Fig. 20. Octagonal flat reel shape

6) Spiral shape flat coil:

d_1= 13 cm; d_2= 3 cm; r= 5 cm; ω= 6; d=$\frac{d1+d2}{2}$= 8 cm;

p=$\frac{r}{d}$ = $\frac{5}{8}$ =0,6; π= 18,814; π =$\frac{3}{13}$ =0,25;

π=$\frac{(1+0,6)^3}{0,6^2}$(1,7424+ 3,29 × $0,25^3$ Ln 0,2-2,27× $(0,2)^3$ =19;

L=$\frac{4\pi\times10^{-7}}{8\pi}$× 36 × 0,08× 19= 2,7 μH; Sm = 73 cm^2

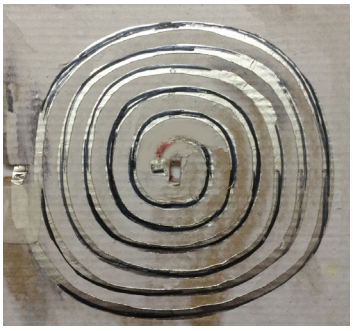


Fig. 21. Spiral shape flat coil

7) Spiral shape flat coil:

d_1= 15 cm; d_2= 3 cm; r= 6 cm; ω= 6; d=$\frac{18}{2}$= 9 cm;

p=$\frac{r}{d}$ = $\frac{6}{9}$ = 0,7; π= 18,814; π=$\frac{1-p}{1+p}$ +$\frac{1-0,7}{1+0,7}$ =0,2;

π= 17,032; π=$\frac{(1+0,7)^3}{0,7^2}$(1,7424+ 3,2900 ×

× $0,2^2$ Ln 0,2-2,27× $(0,2)^3$ = 17; L=$\frac{4\pi\times10^{-7}}{8\pi}$× 36 ×

× 0,09× 17= 2,8 μH; Sm = 110 cm^2

Fig. 22. Spiral shape flat coil

8) Spiral shape flat coil:

d_1= 10 cm; d_2= 1,5 cm; r= 4 cm; ω= 6; d=$\frac{11,5}{2}$= 6 cm;

p=$\frac{r}{d}=\frac{4}{6}$= 0,6; π= 18,814; π =$\frac{1-p}{1+p}+\frac{1-0,6}{1+0,6}$= 0,25;

π = 18,614; π =$\frac{(1+0,6)^3}{0,6^2}$(1,7424+ 3,2900 ×

×$0,25^2$ Ln 0,25-2,27× $(0,25)^3$ = 19; L= $\frac{4\pi\times10^{-7}}{8\pi}$× 36 ×

× 0,06× 19= 2,1 μH; Sm = 41 cm^2

Fig. 23. Spiral shape flat coil

9) Spiral shape flat coil:

d_1= 13 cm; d_2= 3 cm; r= 5 cm; ω= 6; d=$\frac{16}{2}$= 8 cm;

p=$\frac{r}{d}=\frac{5}{8}$=0,6; π= 19; π =$\frac{3}{13}$=0,25; π =19;

L= $\frac{4\pi\times10^{-7}}{8\pi}$× 36 × 0,08× 19= 2,7 μH; Sm = 73 cm^2

Fig. 24. Spiral flat coil shape

10) S iral shape flat coil:

d_1= 12 cm; d_2= 6 cm; r= 3 cm; ω= 7; d=$\frac{18}{2}$= 9 cm;

p=$\frac{r}{d}=\frac{3}{9}$=0,3; □= 26,56; L= $\frac{4\pi\times10^{-7}}{8\pi}$× 49 × 0,09 ×

× 26,56 = 5,8 μH; Sm = 36 cm^2

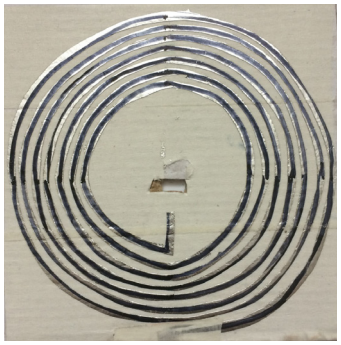


Fig. 25. Spiral shape flat coil

Table 2

Flat coil parameters

	d_1, cm	d_2, cm	r, cm	ω	L, μH
1	9	2,5	3	**5**	3
2	13		5	6	6,4
3	14		4,5	7	9,4
4	12		4,5	6	6,6
5	14		5	7	7
6	12,5	3	5	6	2,7
7	14		5,5	6	2,8
8	10	1	4	6	2,1
9	13		5	6	2,7
10	12		3	7	5,8

ANALYSIS OF DATA RECEIVED

To study these structures, two coils were used, located at a distance of 20 cm from each other, were connected to a network analyzer to determine the resonant frequency of the structure of the modeling metamaterials, and a frequency from 7 MHz to 30 MHz was applied using a pulse generator. The wavelength of 10-43 m.

The shape of the structure modeling the metamaterials was chosen from numerous sets of geometric shapes (square, 6.8-angled, rectangular, and also spiral).

Table 3

Structure transfer factor at their location closer to the receiver

№		1	2	3	4	5	6	7	8	9	10
L, μH		6	13,4	9	12,4	14	5,4	5,6	4,2	5,4	1
Sm, cm^2		33	80	94	80	86	73	110	41	73	36
R, cm		15									
Frequency (MHz)	**7**	1,1	1,2	1,3	1,3	1,2	1,4	1,4	1,2	1,4	1,7
	10	1,1	1,2	1,1	1,4	1,1	1,4	2,1	4,4	1,6	7
	11	1,4	1,3	1,4	1,8	1,4	1,6	5	0	0,3	1,4
	12	1,1	1,2	1,2	2,5	1,5	1,7	2,9	0,4	0,5	0,4
	14	1,2	1,4	1,4	1,8	2,3	4,4	0,2	0,6	0,4	0,3
	16	1,1	1,2	1,2	1,3	1,5	3	0,	1	0,8	0,9
	18	1	1,5	1,8	0,3	4,8	0,8	0,4	0,7	0,5	0,6
	20	1	1,	2,2	2	0,7	0,5	0,5	0,7	0,7	0,7
	30	0,8	0,8	0,8	0,8	0,5	0,8	0,8	0,8	0,8	0,8

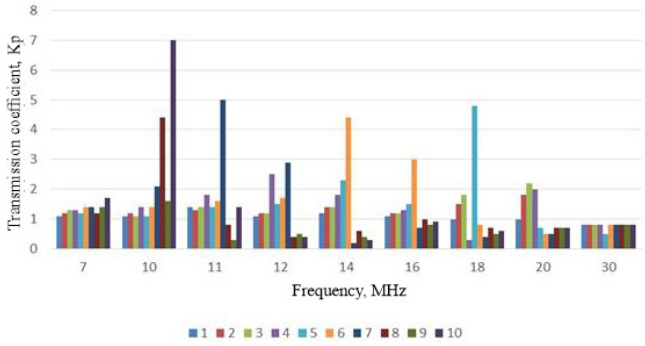


Fig. 26. The dependence of the transmission coefficient on the frequency (closer to the receiver)

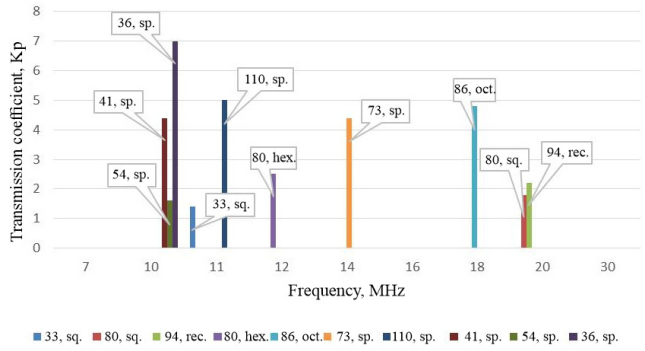


Fig. 27. Dependence of the transmission coefficient on the frequency (closer to the receiver)

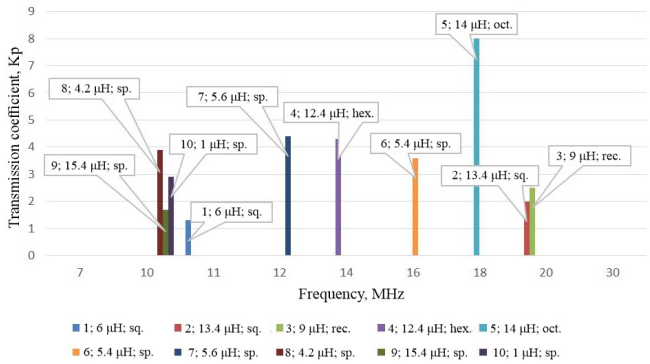


Fig. 28. The dependence of the transmission coefficient on the frequency (closer to the receiver)

Table 3

Structure transfer factor at their location closer to the receiver

№		1	2	3	4	5	6	7	8	9	10
L, μH		6	13,4	9	12,4	14	5,4	5,6	4,2	5,4	1
Sm, cm^2		33	80	94	80	86	73	110	41	73	36
R, cm		15									
Frequency (MHz)	7	1,1	1,2	1,3	1,4	1,3	1,6	1,3	1,3	1,5	1,3
	10	1	1,2	1,2	1,4	1,2	1,5	2	4,2	1,6	3
	11	1,1	1,3	1,3	1,5	1,3	1,4	3,5	0,5	0,3	1
	12	1,1	1	1,2	2	1,3	1,5	2,7	0,5	0,5	0,5
	14	1,2	1,2	1,3	3	1,6	2,7	0,2	0,8	0,6	0,6
	16	1,1	1,2	1,2	0,6	1,9	2,6	0,6	0,9	0,8	0,8
	18	1	1,6	1,9	5,3	6,4	0,4	0,4	0,7	0,6	0,6
	20	1	1,9	2,3	0,6	0,4	0,5	0,6	0,7	0,7	0,7
	30	0,8	0,8	0,8	0,8	0,5	0,8	0,8	0,8	0,8	0,8

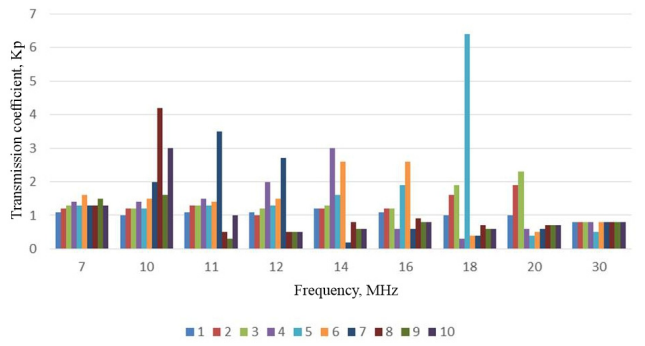


Fig. 29. The dependence of the transmission coefficient on the frequency (in the middle)

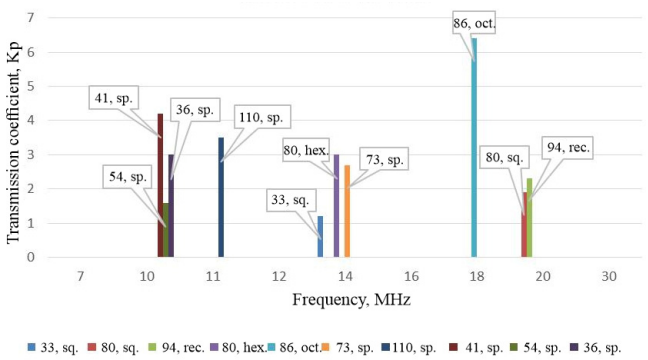


Fig. 30. The dependence of the transmission coefficient on the frequency (in the middle)

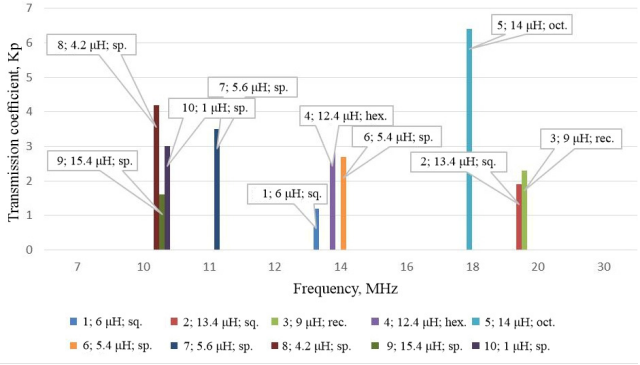


Fig. 31. The graph of the dependence of the transmission coefficient on the frequency (in the middle)

Based on the graph, we can conclude that when the structures are located in the middle between two coils, the coefficient decreases.

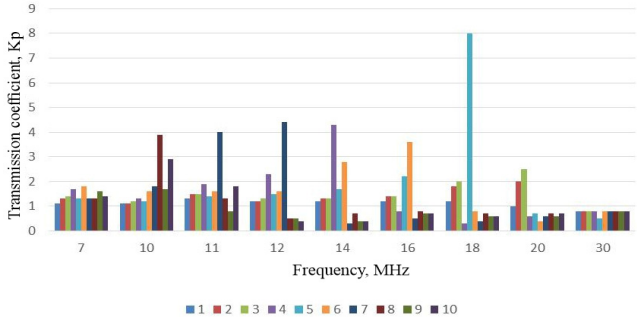


Fig. 32. The dependence of the transmission coefficient on the frequency (closer to the transmitter)

Table 4

Structural transmission factor at their location closer to the transmitter

№		1	2	3	4	5	6	7	8	9	10
L, μH		6	13,	9	12,4	14	5,4	5,6	4,2	5,4	1
Sm, cm^2		33	80	94	80	86	73	110	41	73	36
R, cm		15									
Frequency (MHz)	7	1,1	1,3	1,4	1,7	1,3	1,8	1,3	1,3	1,6	1,4
	10	1,1	1,1	1,2	1,3	1,2	1,6	1,8	3,9	1,7	2,9
	11	1,3	1,5	1,5	1,9	1,4	1,6	4	1,3	0,8	1,8
	12	1,2	1,2	1,3	2,3	1,5	1,6	4,4	0,5	0,5	0,4
	14	1,2	1,3	1,3	4,3	1,7	2,8	0,3	0,7	0,4	0,4
	16	1,2	1,4	1,4	0,8	2,2	3,6	0,5	0,8	0,7	0,7
	18	1,2	1,8	2	0,3	8	0,8	0,4	0,7	0,6	0,6
	20	1	2	2,5	0,6	0,7	0,4	0,6	0,7	0,6	0,7
	30	0,8	0,8	0,8	0,8	0,5	0,8	0,8	0,8	0,8	0,8

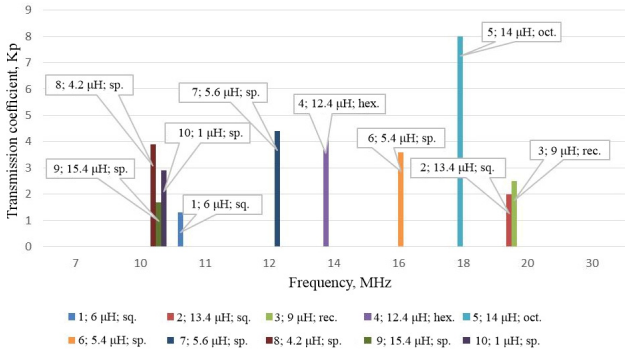


Fig. 33. The dependence of the transmission coefficient on the frequency (closer to the transmitter)

Based on the graph, we can conclude that each structure has its own resonant frequency. At a frequency of 18 MHz, the octagonal structure at No. 5 has the highest transmission coefficient (Kp = 8) with an inductance of 14 μH when located closer to the receiving coil. The structure No. 1 of a square shape has the smallest transmission coefficient (Kp = 1.3), since it has the smallest diameter and width of the conductor, unlike other structures. And for the rest of the structures modeling the metamaterial, the transmission coefficient is in the range from 1.5 to 4.5.

Table 5

Structure transfer coefficient depending on their distance

Frequency	№	Number of structures m.m.	Distance R (cm)	Gear ratio, Kp
11		1	10	5
			15	2
			20	1
			25	1
			30	
11		2	10	
			15	11
			20	6
			25	3
			30	2

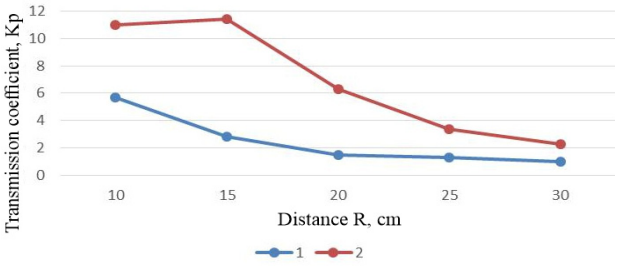


Fig. 34. The dependence of the gear ratio from R

On this graph, you can see that Kp increases by 2 times, 1 line (blue) characterizes Kp values without a structure, 2 line (red) with a structure modeling a metamaterial.

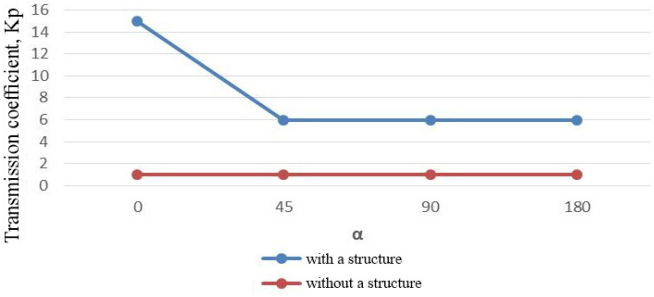


Fig. 35. The dependence of the gear ratio from the angle

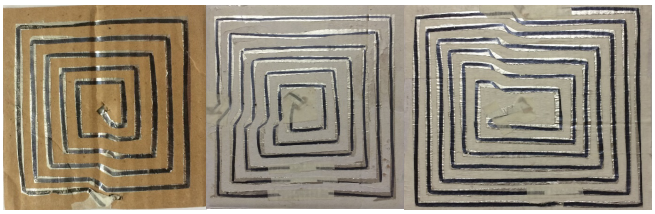
Based on the graph, we can conclude that when the structures are rotated by a certain angle, the transmission coefficient slightly decreases, but not lower than the value of Kp = 1, but equal to 6.

Table 6

Structure transfer coefficient depending on their angle

Frequency	№	Number of structures m. m.	Distance R (cm)	α	Gear ratio, Kp	
					without	with
11		2	20	0	1	15
				45		6
				90		6
				180		6

The following are tables comparing structures modeling a metamaterial with various parameters.



	1	2	3
Ext. diameter d_1, cm	9	13	14
Int. diameter d_2, cm	2,5	3	4
Conductor width r, cm	3	5	4,5
Number of turns, ω	5	6	7
Inductance L, μH	3	6,	9,4
Frequency, MHz	18	1	18
Coef. transmission Kp	1	1,	1,9

Fig. 36. Parameters of structures modeling the metamaterial No. 1,2,3

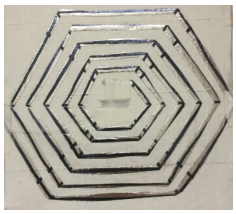
	4	5
		
Ext. diameter d_1, cm	12	
Int. diameter d_2, cm	3	
Conductor width r, cm	4,5	5
Number of turns, ω	6	
Inductance L, μH	6,6	6,8
Frequency, MHz	18	
Coef. transmission Kp	5,3	6,4

Fig. 37. The parameters of the structures modeling the metamaterial, the hexagonal shape on the left (No. 4), and the octagonal on the left (No. 5)

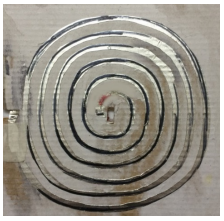
	5	6
		
Ext. diameter d_1, cm	14	12
Int. diameter d_2, cm	5	
Conductor width r, cm	5	
Number of turns, ω	7	
Inductance L, μH	6,8	2,7
Frequency, MHz	18	
Coef. transmission Kp	6,4	0,4

Fig. 38. The parameters of structures modeling the metamaterial, on the left is an octagonal shape (No. 5), and spiral on the left (No. 6)

	5	9
		
Ext. diameter d_1, cm	14	
Int. diameter d_2, cm	5	
Conductor width r, cm	5	
Number of turns, ω	7	
Inductance L, μH	6,8	2,7
Frequency, MHz	18	
Coef. transmission Kp	6,4	0,6

Fig. 39. The parameters of the structures modeling the metamaterial, the hexagonal shape on the left (No. 5) and the spiral on the left (No. 9)

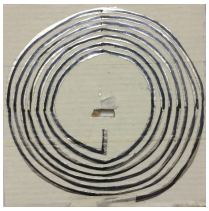
	8	10
		 
	8	**9** **10**
Ext. diameter d_1, cm	10	1 12
Int. diameter d_2, cm	1,5	3 6
Conductor width r, cm	4	5 3
Number of turns, ω	6	6 7
Inductance L, μH	2,1	2,7 4,5
Frequency, MHz	18	1 18
Coef. transmission Kp	0,7	0,6 0,6

Fig. 40. Parameters of structures simulating a spiral-shaped metamaterial (No. 8, 9, 10)

Table 7

Parameters of structures modeling metamaterial

L, μH	Sm cm^2	R, cm	№	Frequency (GHz)
				15
6	33	15	1	-8
13,4	80		2	-5
9	9		3	-3
12,4	80		4	-7
14	8		5	-4
5,4	73		6	-6
5,6	110		7	-13
4,2	41		8	-12
5,4	54		9	-9
1	3		10	-2

This table shows the CR values of various structures at a frequency of 15 GHz. Based on the table, we can conclude that at this frequency the signal is attenuated, where the maximum attenuation value of structure 7 is -13 dB.

CONCLUSION

In the framework of this paper, we present the results of a study of the structures modeling metamaterials, as well as the features of the properties of the structure of metamaterials based on flat spiral coils.

The analysis of literary sources is carried out, the unique properties of metamaterials are studied, on the basis of which, modeling of structures modeling metamaterial is carried out.

The possibility of modeling the properties of metamaterials using structures from a cascade of flat coils placed in a magnetic field is considered. The possibility of such an approach proceeds from the assumption that for atoms of the crystal lattice charged particles moving in orbits form a magnetic field that interacts with the magnetic field of a neighboring atom.

Thus, the transfer of electromagnetic energy with frequencies having wavelengths is much greater than the step of the crystal lattice. This approach allows the use of flat coils as an element of the model of the structure of matter.

By placing the coils in a certain sequence, one can achieve both the usual electromagnetic properties of the substance and the anomalous ones that we observe with metamaterials. It was found that short-circuited passive flat coils located in a certain order not only weaken the transmitted signal, but increase it under certain conditions, namely when they are closer to the transmitter and when the internal conductors are open.

Based on the experiments, it can be concluded that when the metamaterial is placed between these two coils, the transmission distance can be significantly increased by controlling and manipulating the near-field wave, which usually decays quickly from the source. This indicates that transmission efficiency and distance range can be improved by increasing the amount of structure of modeling metamaterials.

A study of the obtained structures revealed that resonant coupling can be realized when the transmitter and receiver are tuned to the same or similar resonant frequency.

REFERENCES

[1] J. Franklin. Double Negative Materials (DNM), Phenomena and Applications. Science. 2009.

[2] O. Baklickaya. Obratnyj effekt Doplera stal vidimym. Nauka i zhizn'. 2005-2019.

[3] S.N. Galyamin, A.V. Tyuhti. Obratnoe cherenkovsko – perekhodn e izluchenie zaryada, vletayushchego v anizotropnuyu sredu. *Pis'ma v "ZHurnal tekhnicheskoj fiziki"*. 2011. Vol. 37 (7). P. 54-63.

[4] M.Yu. Zvezdina. Primenenie innovacij pri razrabotke radiotekhnicheskih sistem. Kollektivnaya monografiya. Izd. dom Akademii Estestvoznaniya, 2015. 224 p.

INCREASING THE THROUGHPUT OF LTE USING DEVICE-TO-DEVICE COMMUNICATION BY REDUCING INTRA-SYSTEM INTERFERENCE FLOW

Adel F. Rakhimov,
Dept. of Radioelectronic and Telecommunication Systems,
Kazan National Research Technical University named after A. N. Tupolev-KAI, City of Kazan, Russia;
German-Russian Institute of Advanced Technologies (GRIAT), Rakhimov2897@yandex.ru

Anna A. Bukharina,
Dept. of Radioelectronic and Telecommunication Systems,
Kazan National Research Technical University named after A. N. Tupolev-KAI, City of Kazan, Russia;
German-Russian Institute of Advanced Technologies (GRIAT), AABukharina@kai.ru

DOI: 10.36724/2664-066X-2020-6-4-31-35

ABSTRACT

This article focuses on the using collective dynamic route method for D2D LTE networks. It provides algorithms for the analysis stage, taking into account the availability of D2D users and the routing stage, as well as their implementation. The dependencies of the D2D communication routes quantity fraction for various cases of user location are shown.

KEYWORDS: *collective dynamic routing, one-dimensional routes, multidimensional routes, Bounded Recurrent Algorithm.*

INTRODUCTION

To increase the throughput of broadband radio access networks by reducing intra-system interference flow in [1], a collective dynamic routing method was developed. It includes two stages:

1) The analysis stage includes following steps:

- Constructing set of routes;
- Calculating signal power for each route;
- Calculating signal-to-interference ratio (SINR) for each route for each channel;
- Calculating data rate with a given error probability for each route and each channel.

2) Routing stage that includes defining the optimal set of routes that provides data transmission with minimal delivery time.

As described in [3], this method allows increase the IEEE 802.11 networks throughput.

However, the researches did not consider the applying possibility this method for LTE networks using D2D communication. Features of D2D communication require a change in the algorithm for searching acceptable route set.

So, this article is devoted to the development of the algorithm for searching acceptable route set for LTE networks with D2D communication and its effectiveness analysis.

PROBLEM STATEMENT

Consider LTE network example consisting of one base station (BS) and three users (Figure 1).

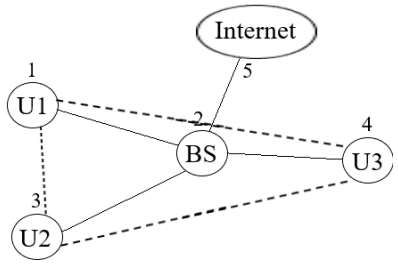


Fig. 1. The LTE network example

The task of this network is to deliver data between users U1 – U3, as well as between them and the Internet, i.e. deliver data in volumes specified by the matrix $\mathbf{I}$ accumulated in the interval T^I using acceptable route set $\{\mathbf{w}\}$.

The collective dynamic routing method allows to find the optimal route set $\vec{N}^{opt}$, as the number of using frames for each of the route in the set $\{\mathbf{w}\}$, which deliveries data with the volumes $\mathbf{I}$ for the minimum time according to:

$$\begin{cases} \vec{N}^{opt} = \arg\min\limits_{\vec{N}} \left(\sum\limits_{g=1}^{G} N_g \right) \\ \sum\limits_{g=1}^{G} N_g \cdot \tilde{I}_{gn^R n^T} \geq I_{n^R n^T}, \quad n^R = \overline{1,N}, n^T = \overline{1,N}, \\ N_g \geq 0, \qquad g = \overline{1,G} \\ N_g \in Z, \end{cases} \quad (1)$$

where $\vec{N} = \left(N_1, \ldots, N_g, \ldots, N_G\right)$ is the used route set; G is the total routes quantity; n^R is the receiving node in route w_g; n^T is the transmitting node in route w_g; N is the total transmitting or receiving nodes quantity.

Thus, depending on the volumes matrix $\mathbf{I}$, the optimal routing set will be different.

ANALYSIS STAGE

According to collective dynamic routing method, the acceptable route set consists of certain amounts of end-to-end routes that can be divided into one-dimensional and multidimensional routes.

One-dimensional route is set of serially connected communication channels in order to connect desirable users. All one-dimensional routes can be divided into three groups: routes that allow users to access the Internet and routes connecting different users which are into routes connecting users through the BS and directly (D2D). For the considering LTE network example the first group contains routes: (1-2-5), (3-2-5) and (4-2-5), the second group – routes: (1-2-3), (1-2-4), (3-2-1), (3-2-4), (4-2-1), (4-2-3) and third group – routes: (1-3), (1-4), (3-1), (3-4), (4-1), (4-3).

Multidimensional routes are obtained by unification of one-dimensional routes that use different communication channels. Two dimensional routes includes two one-dimensional routes, e.g. {(1-2-3), (3-4)}. Three dimensional routes includes three one-dimensional routes, e.g. {(1-2-3), (3-2-4), (4-3)}.

The implementation was done in Matlab. After routes construction and removing redundant routes, such as (1-2-5) and (1-5), for the example shown in figure 1 215 routes were obtained.

The signal powers $P_{gn^R n^T}$ were calculated depends on the propagation loss described by ITU-R 1411 [4] for each route in set $\{\mathbf{w}\}$ and each user pairs. The transmitter powers of BS and user equipment were determined based on the standard for LTE and LTE-Advanced dated October 29, 2018 [5].

According to [6] SINR $\rho^{R^S}_{gin^R n^T}$ is calculated such way:

$$\rho^{R^S}_{gin^R n^T} = \frac{P_{gn^R n^T}}{P_n \cdot \left(1 + K^{NR^S}_{gin^R}\right) + \sum\limits_{n'^T=1}^{N^T} P_{gn^R n'^T} \cdot \sum\limits_{i'=1}^{I^u} K^{PR^S}_{gii'n^R n'^T}}, \quad (2)$$

where $\rho_{gn^R n^T}$ is a SNR at n^R-th user receiver from n^T-th user transmitter; $K^{NR^S}_{gin^R}$ and $K^{PR^S}_{gii'n^R n'^T}$ are noise and intra-system an interference influence coefficients with calculated with program OFDM Receiver [7].

In order to reduce interference, we should think about resource blocks distribution between routes. The algorithm for resource blocks distribution in one-dimensional routes is shown in figure 2.

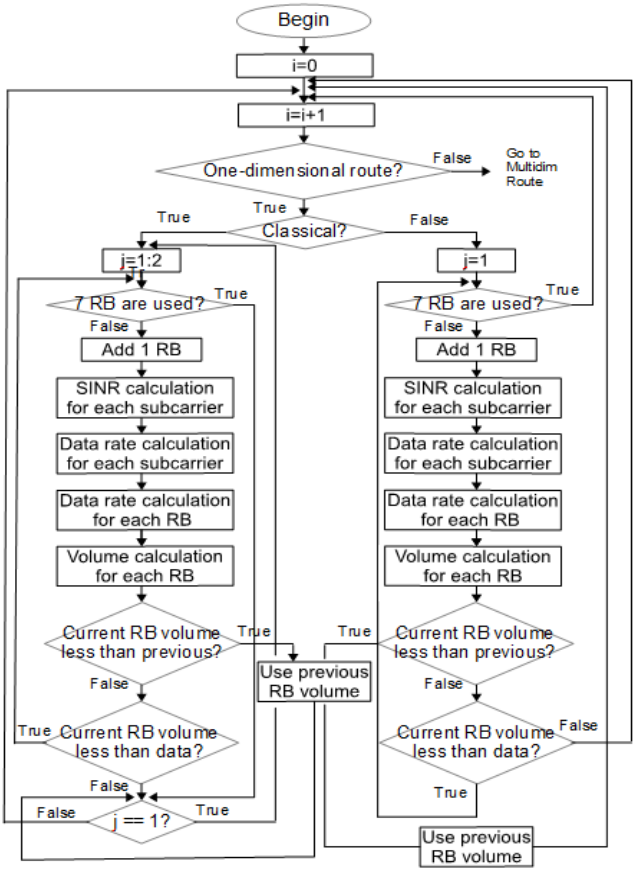


Fig. 2. Algorithm of one-dimensional routes analysis stage

As can be seen, the distribution is done based on the total number of resource blocks and the comparison of current and previous values of volume that is delivered by the total used resources per route. If current value of volume is less than previous, it denotes that interference level when we use current distribution is much higher in comparison with interference level when we use previous distribution and, as a result, previous distribution gives more efficient results in data rate terms.

The same approach used for two and three multidimensional routes but algorithm will be more complicated because in this case we should remember about finite number of resource blocks, namely 7, and the variety of the variants of data delivery. In two dimensional routes there are 3 variants, e.g. only classical approach: {(1-2-3), (3-2-4)}; classical approach and D2D: {(1-3), (3-2-4)} or {(1-2-3), (3-4)} and D2D only {(1-3), (3-4)}. In three dimensional routes case we have such variants: only classical approach; two routes with classical approach and one route with D2D; one route with classical approach and two routes with D2D; D2D only.

SINR $\rho^{R^S}_{gin^R n^T}$ for each subcarrier is different. Therefore data rate for each subcarrier will be different too. In this case the channel's data rate from n^T-th to n^R-th user is calculated by following expression:

$$V_{gn^R n^T}\left(R^s\right) \le 2 \cdot V^{tec} \cdot \sum_{i=1}^{I^u} \log_2 \left(\frac{\sqrt{\rho^{R^S}_{gin^R n^T}}}{2 \cdot Q^{-1}\left(P^{Er}_{\max}/2\right)} + 1 \right) \quad (3)$$

where V^{tec} is an amount of transmitted OFDM-symbols per second; $P^{Er}_{\max}$ is transmitting symbol error probability; I^u is an amount of subcarriers that are used for data delivery.

The volume $\widetilde{I}_{gn^R n^T}$ that can be delivered by one resource block from n^T-th to n^R-th user along the route w_g can be found as production of the channel's data rate by the resource block delivery time T^F:

$$\widetilde{I}_{gn^R n^T} = V_{gn^R n^T} \cdot T^F . \quad (4)$$

The choice of routes used for the data delivery is carried out at the routing stage based on data volumes $I_{n^R n^T}$ at matrix $\mathbf{I}$, and volumes $\widetilde{I}_{gn^R n^T}$ delivered by one resource block.

ROUTING STAGE

The aim of this stage is finding optimal route set $\vec{N}^{opt}$. In the general, $\vec{N}^{opt}$ can be obtained by solving system (1), which is the task of integer linear programming (ILP). However, due to the high complexity of the exact solution ILP task, recurrent algorithm can be used.

Based on the algorithms comparison that can be used in the collective dynamic routing method described in [8], given the complexity of the calculations and the obtained data delivery time, the Bound Recurrent Algorithm (BRA) was been choose. This recursive algorithm at each step determines the number of the best route, which can be determined as follows:

$$g^* = \arg\max_{g=\overline{1,G}} \sum_{n^R=1}^{N} \sum_{n^T=1}^{N} I_{n^R n^T} \times \begin{cases} \widetilde{I}_{gn^R n^T}, & I_{n^R n^T} > \widetilde{I}_{gn^R n^T} \\ I_{n^R n^T}, & I_{n^R n^T} \le \widetilde{I}_{gn^R n^T} \end{cases} \quad (5)$$

where w_{g^*} is the best route with number g^*; N is the user quantity; $I_{n^R n^T}$ is amount of data, which needed to transmitted by user n^T to user n^R; $\widetilde{I}_{gn^R n^T}$ is amount of data transmitted by user n^T to user n^R at the resource block delivery time T^F using route w_g.

So, w_{g^*} computes in T^F=0.5mc every time until all data is transmitted. The sequence of w_{g^*} give us the vector of optimal route set $\vec{N}^{opt}$.

RESULTS

Four cases were considered eo evaluate the effectiveness of using D2D communications.

The first case considers all users are placed close to BS and at equal distances from each other. It is shown in Figure 3.

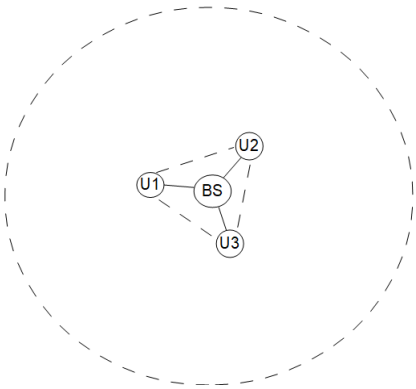


Fig. 3. Case 1

The second case is depicted in figure 4. In this case all users are placed far from BS and at equal distances far from each other.

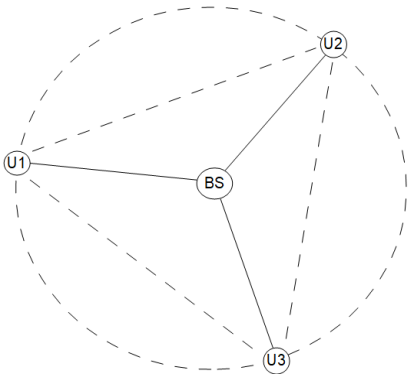


Fig. 4. Case 2

The third case considers two users that are placed close to each other but third user is far from them. All users are far from BS (Figure 5).

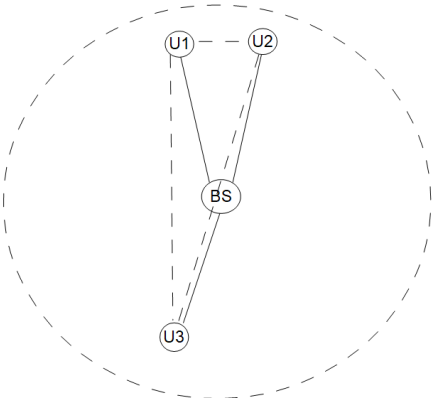


Fig. 5. Case 3

The location of users in fourth case is far from BS but they are close to each other. It is shown in Figure 6.

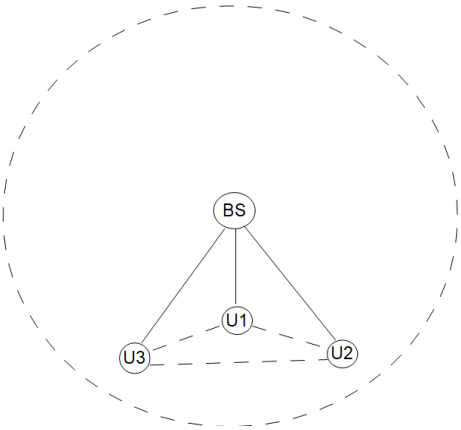


Fig. 6. Case 4

In each case 100 random matrix **I** realizations were generated. For example, first matrix **I** realization can be U1 transmits to U2, U2 transmits to U3, and U3 transmits to Internet. Second realization can be U2 transmits to U1, U1 transmits to U3. Base on these realizations it can be estimated used D2D routes percentage. This percentage for each case of user location is shown in Figure 7.

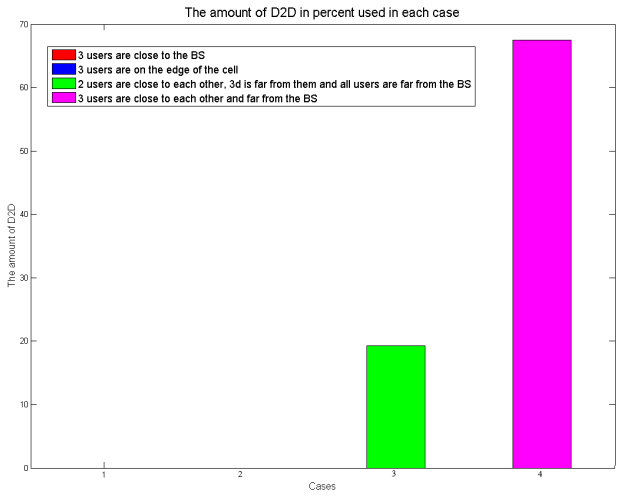


Fig. 7. D2D utilization versus case

According to this dependent, first and second cases use only routes transmitted data through BS (classical approach). Third case use about 19 percent of the maximum number of D2D routes that can be used. In fourth case roughly 67 percent are used. So, the most beneficial case for D2D communication usage is fourth case. Of course, numbers in each case can be varied. It depends on users' location and matrix **I** realizations.

The next question is how does the data delivery time change when using D2D communications compared to using only the classical approach? To answer it, it will be considered two models: with the using only classical approach and the classical approach and D2D communications. Using these models, the D2D utilization gain as the ratio of the delivery time of the classical approach and D2D for the delivery time of only the classical approach is calculated. It's gain was calculated in each combination and then it was averaged.The average D2D utilization gain for the same cases of placed users and matrix **I** realizations are shown in Figure 8 for the transmitted data size of which is medium, i.e. less or equal to 1 Mb and in Figure 9 for the transmitted data size of which is large, i.e. between 8 and 12 Mb.

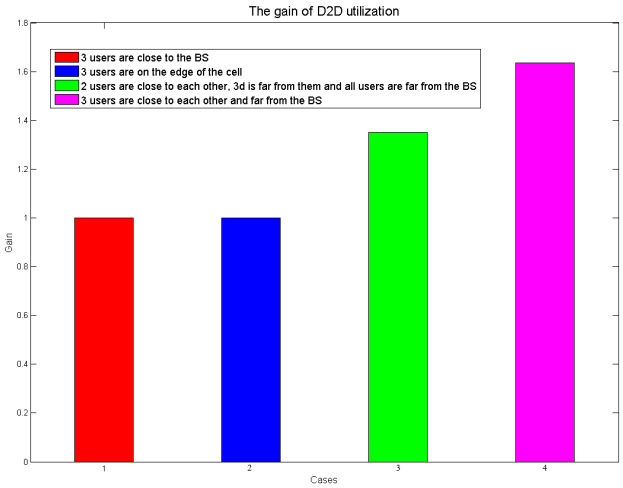


Fig. 8. D2D utilization gain when the transmitted data size is medium

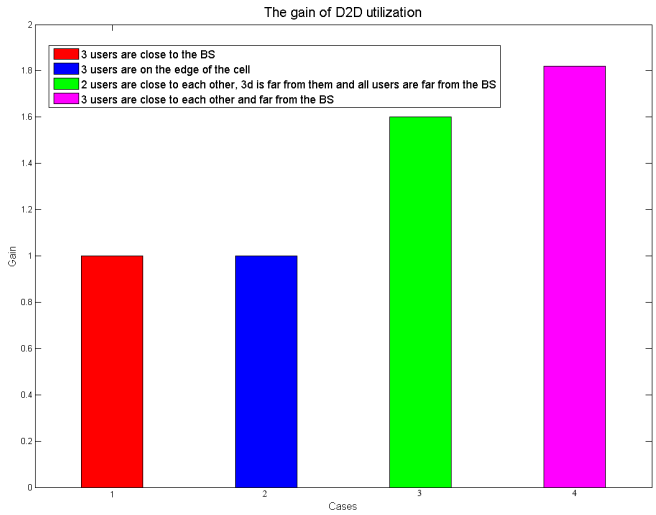


Fig. 9. D2D utilization gain when the transmitted data size is large

So, if gain equal to 1, there is no benefit to use D2D as it can be seen in case 1 and case 2. Gain shows how much on average the using one combination of the classical approach and D2D in comparison with the classical approach only gives a benefit.

Since $\widetilde{I}_{gn^R n^T}$ is constant, the data delivery time depends on their size, which also affects the D2D utilization gain. The figures' 8 and 9 analysis shows that D2D utilization gain increases with an increase in the transmitted data size.

CONCLUSION

According to the results, there is no need to use the D2D connection when the distance between all users and the BS, as well as the distance between all users are approximately the same, which corresponds to cases 1 and 2. D2D gives a benefit when users are far from the BS and close to each other. In the 3rd case, when 2 users were close to each other, the D2D utilization gain is 1.35 when the transmitted data size is medium, and 1.6 when the transmitted data size is large, whereas in the 4th case, when 3 users are located close to each other, the gain is 1.63 if the transmitted data size is medium, and 1.82 if the transmitted data size is large.

Moreover, the idea of using the collective dynamic routing method for allocating resource blocks was presented and implemented with using Bounded Recurrent Algorithm in Routing Stage. It allowed increasing data rates by reducing the intra-system interference flow in real systems due to its low computational complexity.

References

[1] E.A. Spirina Optimizacija raspredelenija informacii v fiksirovannyh setjah shirokopolosnogo radiodostupa s uchetom vnutrisistemnyh pomeh. *Zhurnal radiojelektroniki* [jelektronnyj zhurnal]. 2015. No 9. at http://jre.cplire.ru/jre/sep15/5/text.pdf. (in Russian)

[2] E.A. Spirina, S.V. Kozlov. A routing method providing throughput increase in IP networks with intrasystem interference. *Zhurnal radiojelektroniki* [jelektronnyj zhurnal]. 2015. No 12. Ava http://jre.cplire.ru/jre/dec15/3/text.pdf. (in Russian)

[3] Ju.S. Vintenkova, S.V. Kozlov, E. A. Spirina. Analiz jeffektivnosti metoda sovmestnoj dinamicheskoj marshrutizacii v setjah shirokopolosnogo radiodostupa s trafikom protokolov TCP, HTTP, FTP. *Zhurnal radiojelektroniki* [jelektronnyj zhurnal]. 2016. No 1. at http://jre.cplire.ru/jre/jan16/5/text.pdf. (In Russian)

[4] Recommendation ITU-R P.1411-10. Propagation data and prediction methods for the planning of short-range outdoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 100 GHz. Electronic Publication, Geneva, 2019, p. 52.

[5] Ministry of digital development, communications and mass communications of the russian federation, order № 572 on approval of the rules for application of basic stations and relays of networks of mobile radiotelephone communications. Part VI. Rules for application of basic stations and relays of networks of mobile radiotelephone communications of LTE standard and its modification LTE-advanced. Link: https://rulaws.ru/acts/Prikaz-Minkomsvyazi-Rossii-ot-29.10.2018-N-572/. (in Russian)

[6] S.V. Kozlov, E.A. Spirina, "Application efficiency analysis of the optimal measurement algorithm for method OFDM communication networks integrated optimization", *2019 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2019*. DOI: 10.1109/SYNCHROINFO.2019.8813911

[7] S.V. Kozlov, E.A. Spirina, L.I. Fazylova, "Svidetel'stvo o gosudarstvennoj registrac i programmy dlja JeVM №2016663494. Programma OFDM Receiver" – Zajavka №2016661064; Registered: 18.12.2016. (In Russian)

[8] Y.S. Vintenkova, S.V. Kozlov, E.A. Spirina. Bran collective dynamic routing optimal routes evaluation algorithm. *2018 Systems of Signals Generating and Processing in the Field of on Board Communications*, 2018-January, 2018, pp. 1-3. DOI: 10.1109/SOSG.2018.8350578

SECURITY ANALYSIS THREATS, ATTACKS, MITIGATIONS AND ITS IMPACT ON THE INTERNET OF THINGS (IOT)

Alireza Nik Aein Koupaei,
Moscow Institute of Physics and Technology -MIPT (State University), Moscow region, Dolgoprudny, Russia;
Asia Pacific University (APU), Kuala Lumpur, Malaysia; Staffordshire University (SU), United Kingdom;
University of Applied Science and Technology (UAST), Isfahan, Iran,
anikaeinkoupaei@phystech.edu

Alexey N. Nazarov,
Federal Research Center Computer Science and Control of Russian Academy of Sciences, Moscow, Russia,
a.nazarov06@bk.ru

DOI: 10.36724/2664-066X-2020-6-4-36-41

ABSTRACT

In the past, only mobiles and computers were connected to the internet but in the new era with the advent of new technologies other things like security cameras, microwaves, cars and industrial equipment's are now connected to internet. Internet of things (IoT), there are over several billion electronic equipment de- vices already on the internet, and within a decade these number is expected to scale above 20 billion devices. Smartphones and computers have various software security solutions to defend and protect them from most of threats and attacks, although there are indiscernible security solutions to take care of the rest of the IoT [1]. Lately, as a strong example, several thousands of security cameras were breached to proceed DOS and DDOS attacks that caused the Twitter down. Solutions in the IoT are not exclusively software but the entire physical environment of hardware, World Wide Web (WWW), Software, Cloud and mobile interfaces involved. The IoT ecosystem services are young and not very fully developed yet for these reasons there are main primarily concerns fact around IoT adoption due to security threats/attacks. IoT Top Security Concerns: Secure constrained devices, Secure communication, Keeping IoT hardware updated, Distributed Denial of Service (DDoS), Authorize and authenticate devices, Ensure data privacy and integrity. This research reviews the achievements of mitigation IoT security challenges and the key viewpoint is for authors to clearly dene adversary goals, assumptions and dependencies.

KEYWORDS: *Internet of Things (IoT), Cybersecurity threats and attacks, DDoS, Authorize and authenticate devices, Secure constrained devices, Ensure data privacy and integrity.*

INTRODUCTION

Internet of Things (IoT) is a comprehensive and detailed framework for the information society. Various applications and programs are using in IoT which affect smart devices installed in different environments specifically in workfellow optimization, health and energy deficiency [2]. The formatter will need to create these components, incorporating the applicable criteria that follow. These equipment's consist of integrating sensors and devices, limited processing power and energy recourses that are connected to the internet with different internet protocols and computational components. These restrictions rule communication technologies that require provide efficient performance under different conditions, limited energy overheads and reliance larger address space. A certain number of communication technologies have moved out to facilitate and help these requirements.

These contain as part of a whole Wireless Sensor Networks (WSN) [3], Radio Frequency Identification (RFID) [4], Bluetooth and IPv6 over Low power Wireless Personal Area Networks (6LoWPAN)[5], Zig Bee [6], and have shaped M2M communication as well as dedicated communication technologies for emerging paradigms such as Light Fidelity (LiFi), IoT and Internet of Vehicles (IoV). Unlikely, the majority of these equipment's and applications are not addressed to handle the security and privacy attacks, such a reason brings up security and privacy challenges in the IoT networks such as confidentiality, authentication, data integrity, access control, secrecy, etc. [7]. On every day, the IoT devices are targeted by attackers and intruders. An appraisal discloses that 70 per of the IoT devices are very easy to attack. Therefore, an efficient mechanism is extremely needed to secure the devices connected to the internet against hackers and intruders [8].

Nevertheless, the lack of IoT network architecture also attracted attackers to use this network of dozen devices for penetrating malicious content such as the Active content, Scareware and recent IoT Botnets [9,10]. Furthermore, recent study by Howard [11] has addressed and predicted IoT based attacks to the all enterprise vulnerabilities highlighting the need for preferable mitigation methods. Due to security enhancements not interactively devices in almost every aspect of our life, the threats constituted due to their inadequate and incomplete security are unique with unsecured devices exposing the software programs to the serious security and privacy threats. For example, if the attacker having considerable skill to penetrate vehicular ad-hoc networks (VANETs), the data could be at risk. As long as the attacker is inside the network car's data can spoof with a connection to outside data sources and steal the owner's personal data including the credit card information [12].

Due to the emerging threats, the need to respond to security challenges for the IoT system is very important. There are numbers of effort to address different dimensions of security for IoT such as secure applications [11] [12], privacy of information [13], and authentication [14]. However, the challenges in the embedding security into applications is divided into the 3 different categories: firstly, a user-centered threat model which is an analysis of what tasks the user is trying to achieve, and the concepts which user has to work with, before beginning the design of a traditional threat model. Secondly, inferring security action form (user intention) injecting effective human-computer-interaction (HCI) design toward the security-related components of applications is implied security real – to conclude what essential changes in security state are implicated by the user's actions. The last, reflecting security state back to the user - provide the user visibility into their security state, and in that context, make it possible to provide interface principle that control and change that state without requiring them to understand arbitrary security technology science [15]. Intrusion detection systems (IDS) are normally used as monitors network or systems for preventing malicious activity or policy violations. During the past decade, IDS for the IoT system according to a various number of IDS purposed methods such as [16-18]. Diverse research dimensions focus on broadcast authentication in resource-constrained devices for different applications for concurrency, network management, and software updates [19-22].

In the secure constrained devices, the attackers proved that resource-constrained has limited storage capabilities and computational analysis are defenseless because they have not been purposefully designed to have successful security measures. Keeping protect IoT devices might be sophisticated for the IoT scientist designer and developer because it needs an experiment with embedded system security. Providing encryption and authentication in the chip and firmware has its own complexity which is challenging for the companies without appropriate experiment in cryptography with new threats and technologies. Five of the key challenges in securing these resource-constrained devices are detailed as:

a. Limited CPU and Memory,

b. b. Vulnerable Networking Options,

c. c. High Performance, Lightweight Cryptography,

d. d. Strong Passwords Are Not Enough,

e. Enabling Secure Updates.

According to the [23] a new authentication approach based on the state-of-the-art protocol TESLA, that helps to decrease the delay of forged packets in the buffer of the receiver, by efficiently computing the key disclosure delay. In addition, TESLA addressed to prevent the DDoS Attack by integrating the LEAP and LEAP++ protocols.

Blockchain technologies are able to enable decentralized and reliable features for IoT. However, existing blockchain based solutions to make adequate preparation for data integrity verification for semi-trusted data storages (e.g. cloud providers) cannot qualify as time determinism required by Cyber-Physical Systems (CPS). Additionally, they cannot handle resource-constrained IoT devices as well. According to the [24] architecture can take benefit of blockchain features to make sure data integrity verification of data produced by IoT devices both in the area of CPS.

I. Corporate and Personal Data

Today, the most common threats to corporate information security are crime as a service, the risks associated with the Internet of things and the work of companies with suppliers.

The use of the crime-as-service model by non-professional hackers is becoming increasingly widespread.

Cybercrime today has become available for almost every novice hacker because of the penetration of inexpensive criminal services from mature hacker communities to the darknet market. This in turn significantly increases the number of cyber-attacks in the world and creates new threats for corporations. Potential risks include the use of the Internet of things in various companies. IoT devices today, as a rule, are characterized by weak protection, which opens up additional opportunities for their attack. According to Kaspersky Lab, in 2017 the number of malicious programs that attack the Internet of things devices has more than doubled. In addition, companies using the Internet of Things cannot always track which of the data collected by smart devices is transmitted to external organizations.

Supply chains threaten companies to lose control over valuable and confidential information that they pass on to their suppliers. Such organizations are faced with all three types of threats: risks of breach of confidentiality, integrity and availability of information. Meanwhile, almost every one of us faces information security threats in every-day life. For individuals, significant risks are represented by malware (viruses, worms, Trojans, ransomware), phishing (gaining access to user logins and passwords) and identity theft (using someone else's personal data to enrich). In this case, the attackers of social networks and applications, passport data and data of users' credit cards become the subject of hunt for intruders.

Particularly relevant now is also the issue of selling personal data of customers of large companies to third parties. One of the most notorious cases of illegal use of a large amount of personal data is the scandal involving the consulting company Cambridge Analytica and the social networking site Facebook, which broke out in March 2018. According to journalists, the British company used data from about 50 million Facebook users to influence the course of elections in different countries of the world.

II. ADVENCED DATA PROTECTION TECHNOLOGIES

A. Cryptography

Security experts are paying special attention today to cryptographic encryption of information. Cryptographic encryption methods are divided into symmetric and asymmetric[12]. In the first case, the same key is used to encrypt and decrypt data. In the second case, two different keys are used: one for encryption, the other for decryption. In this case, the choice of a decision depends on the goals that the specialist has set himself. Data encryption using cryptography remains protected by itself, and access to encrypted information may not be limited to any other technology.

Today far from all developed countries can afford really strong means of cryptographic protection. Only individual states, including Russia, possess the necessary knowledge and tools for this. An example of cryptographic data protection methods is a digital (electronic) signature. When developing it, algorithms of hash functions can be used - this is the third type of crypto algorithms, except for the other two, which were discussed above. The digital signature allows you to authenticate electronic documents and has all the main advantages of a regular handwritten signature.

B. EDS

To date, not all e-signatures are used (therefore, for example, the possibility of identifying a mobile phone number as an identity is being discussed - this is expected to be a more affordable option. - Rusbase note), however, numerous enthusiasts among private individuals and companies. In addition, an electronic digital signature is an indispensable element when carrying out certain operations in Russia, such as filing financial statements, participating in procurement, maintaining legally relevant document flow and filing arbitration claims in courts.

C. Quantum Cryptography

One of the most promising data protection technologies today analysts call quantum cryptography. This technology allows you to provide almost absolute protection of encrypted data from hacking.

The basis of the quantum network is the principle of quantum key distribution. The key is generated and transmitted through photons brought into the quantum state. You cannot copy such a key. When trying to break in, the photons that transmit information, according to the laws of physics, change their state, introducing errors in the transmitted data. In this case, you can only pick up and send a new key - until the transmission reaches an acceptable level of errors.

Quantum cryptography is not yet used in practice, but the technology is already close to this. IBM, GAP-Optique, Mitsubishi, Toshiba, the National Laboratory in Los Alamos, California Institute of Technology, as well as the QinetiQ holding, supported by the British Department of Defense, are conducting active research in this area today.

D. Blockchain

The development of information security technologies is also closely related to the blockchain and smart contract capabilities. When researchers realized that not only data from cryptocurrency transactions but also various meta-data could be entered into the register, the blockchain began to actively expand to the area of information security. This technology can guarantee not only the safety, but also the immutability and authenticity of the data, and also makes it almost impossible to deceive identification systems. Today, experts call the blockchain one of the most secure, transparent and unchanging information storage systems.

The possibilities of using distributed registry technology for credit card verification are already being studied at Mastercard. The payment company says that the integration of the new solution into POS terminals will reliably protect transactions and save users from having to carry payment cards with them.

E. Tokenization

One of the most reliable ways to protect payment information is tokenization technology. Its essence lies in the substitution of real confidential data with other values, or tokens. As a result, trading companies may no longer need to store user billing information, and attackers who will have access to information on the cards of companies 'clients will not be able to use it.

Tokenization is especially actively used in e-commerce. At present, the technology is supported by the VISA and MasterCard payment systems, however, with the development of contactless payments and financial technologies, the use of tokenization may spread to the entire trading market in the near future.

F. Moving Target Protection Technology

The protection technology of a moving target can also make a significant contribution to cybersecurity in the future. Now this technology is only being tested and is not widely used in practice.

The new protection system was first introduced in 2016 by scientists from the University of Pennsylvania. Using the technology of protecting a moving target, developers intend to solve one of the main problems of data protection - to deprive the authors of cyber-attacks of access to the code that is used for encryption. Experts say that having one fact of encryption today is not enough. To protect data, you need to continuously change the system, and then the attacker will not be able to obtain relevant information about its state, which can be used

at the next moment in time. As a result, it will be extremely difficult to plan an attack.

G. Biometric Authentication

Among the promising areas of information security, experts also include biometric authentication technologies that allow users to be authenticated by measuring the physiological parameters and characteristics of a person and his behavior.

Voice biometrics and face recognition technologies are developing the fastest in this segment. These solutions are already actively used in the field of forensic science and social control and are gradually becoming a standard feature in smartphones. However, analysts believe that the future of biometrics is due to the use of \closed data", such as heart pulse, drawing of intraocular vessels, the shape of earlobes, and more. In addition, biometric data can be protected by implanted under the skin chips, tablet computers, as well as DNA testing and analysis of human neural connections.

H. Artificial Inteligence

New opportunities for information security professionals open artificial intelligence. Machine learning technologies are already helping to protect corporate data in the Gmail mail service. In June 2017, Google introduced a new system for detecting Phishing attacks for companies using machine learning technologies that send instant warnings about clicking on suspicious links, sending messages about sending an unwanted response to recipients outside the domain and offering built-in protection against new threats.

Artificial intelligence is actively applied by Kaspersky Lab to protect data. Technology Machine Learning for Anomaly Detection, presented by the company in January 2018, allows you to prevent cyber-attacks aimed at sensors and controllers installed in industrial facilities. The new solution analyzes all changes in production processes and informs enterprises about potential attacks.

III. Forinet Framework For Prtotection Against Advanced Threats

One of the greatest solutions for protection against modern threats, the so-called Fortinet ATP (Advanced Threat Protection) Framework, which is positioned as a complete modular solution for cybersecurity. Below is an overview of the solution for automated identification, prevention, suppression of malware and the protection of the entire ecosystem.

Advanced malware can cause huge damage to organizations, from data theft through compromised individuals to the termination of important operations. The attacks of cyber criminals are complex, constantly evolving developments aimed at creating new and cunning methods of penetration and attack.

Partly due to the ever-increasing frequency of public attacks, most organizations have realized the need to improve the IT security infrastructure. According to ESG research, 37 Organizations must evaluate both the ability to identify threats to their IT infrastructure and their ability to counter them. Most of the advanced malware is hidden or zero-day software. Hidden threats are built to penetrate the system undetected, sometimes stored in the system in an inactive state for a certain period of time. Zero-day threats are attacks that exploit previously unknown vulnerabilities of a network, operating system, or application, making it difficult to control them.

Traditionally, security has been implemented on the basis of a perimeter firewall in conjunction with endpoint scanners (workstations). Perimeter firewalls blocked simple types of attacks, preventing unauthorized access to internal systems at the time when antivirus on endpoints scanned user devices according to the signatures of previously known or suspected malware. Firewalls of the new generation and endpoint protection software increase the depth of inspection both at the perimeter and at the end device, but they still rely on the search for already known attacks. They are simply not designed to detect the latest, previously unknown attacks. Too often, organizations are not aware of such threats until the moment of significant damage.

A. Fortinet Framework For Preventing Advanced Threat

Fortinet has developed its own protection framework for advanced threats to provide comprehensive visibility of all activities on the network using existing and new methods using a modular approach to integrating its security products for the network, applications, endpoints and cloud services.

The Advanced Threat Protection Framework includes:

1) FortiGate is a next-generation firewall that provides in-depth inspection of packets and the definition of network security and threat protection applications.

2) FortiWeb - Web Application Firewall is designed to protect applications available from the Internet. Two-way protection against advanced threats including denial of service, SQL injection, XSS, buffer overfllow, cookie poisoning and a large number of other attacks.

3) FortiMail - a security gateway for mail, protects email users from incoming threats using anti-spam, anti-phishing, and malware prevention techniques. Outgoing mail protection includes information leakage prevention (DLP), identification-based encryption (IBE), and message archiving.

4) FortiClient - protection for Windows, Mac, IOS, and Android endpoints, including, but not limited to, malware protection, application control, web filter, vulnerability management, two-factor authentication, and remote access.

5) FortiSandbox - centralized analysis and detection of potential threats using code emulation and execution of this code in a virtual protected environment. Checks activity in addition to attributes to determine unwanted behavior. Dynamically takes steps to respond to incidents and update security.

6) FortiGuard - Fortinet researchers use information from global sources to research threats and attacks, and also

maintain a cloud-based knowledge base about the study of threats and how to prevent them.

FortiGate, FortiWeb and FortiMail are the most common solutions, presented in both hardware and software form, in conjunction with the FortiClient application that is used on end devices that meet the needs of organizations of all sizes. Each product ATP Framework can act as a separate solution or can be combined with other products for enhanced protection due to compatibility. In a fully integrated Framework, protection against network threats and endpoints send potentially dangerous data to FortiSandbox for analysis, which in turn returns instructions for handling data to these products, as well as to FortiGuard's laboratory for distribution to Fortinet products.
Fortinet describes the three phases of its products to ensure coordinated protection: prevention, detection and mitigation.

- Prevention - prevent attacks from many known and highly suspicious threats.
- Detection - identify previously unknown threats and spread information about the threat for an accelerated response.
- Mitigation - research and analyze new data; create a signature and turn the unknown into the known for prevention in the future.

B) Revealing
Fortinet's main approach to identifying advanced threats is to identify unknown threats and redirect them to FortiSandbox to reveal the behavior, tactics, techniques, and procedures used in cyber-attacks. FortiSandbox uses virtual machines as tools for assessing potential threats from executable files, compressed files (zip files), application data such as Adobe Flash, Adobe PDF, and JavaScript, etc. However, the execution of each suspicious file on a virtual machine can be resource intensive and take some time. This can limit the total number of suspicious files that can be evaluated, with a significant impact on performance.
Fortinet uses many different techniques to increase efficiency. Prior to sand-boxing, suspicious files can be pre-filtered, including screening by the antivirus engine, requests to the FortiGuard cloud service, OS-independent simulation, which is possible thanks to the Compact-Net patented recognition language (CPRL). CPRL is a system for deep code inspection and pattern recognition, which allows you to significantly expand the capabilities of protection methods against advanced threats (APT) and recognition of advanced circumvention techniques (AET) that are possible with traditional signature-based analysis.

CONCLUSION

Any corporate infrastructure computing device, from smartphones and tablets to laptops, desktops, and application services, is subject to security breaches. Attacks affect organizations of any size indiscriminately, the consequences can be devastating for operations, company reputation and bank accounts. Costs arising from successful attacks can include not only the resumption of operations and the resolution of security problems but also legal liability and regulatory fines.

The Fortinet framework for protection against advanced threats is easy to understand and manage. Fortinet's modular approach with stand-alone products that can be combined to implement prevention, detection, and mitigation can improve detection and protection against advanced attacks in comparison with individual security systems from other manufacturers. Integration of Fortinet products into an entire ecosystem is quite simple in terms of configuration, thanks to an intuitive interface and many publicly available documentations. After configuration, the analysis of unknown files, no matter how they got into the ecosystem, occurs automatically. The FortiSandbox graphical user interface provides intuitive access to understandable and clear information. FortiSandbox makes understanding current security levels clear and easy to understand.

The Fortinet solution offers the functionality, features, and connectivity that solve the entire spectrum of an organization's security requirements, giving security teams the ability to detect, prevent, and mitigate threats. The ability to work as standalone products or unite into a full framework provides the flexibility to integrate into almost any system. Companies that are looking for more flexible, effective solutions to improve security will be satisfied with the Fortinet Framework for protection against advanced threats.

REFERENCES

[1] S. Naik and V. Maral. 2017. "Cyber security | IoT," *2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, Bangalore, 2017, pp. 764-767. doi:10.1109/RTEICT.

[2] Pacheco J., Hariri S. 2016. IoT security framework for smart cyber infrastructures. *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W).* https://doi.org/10.1109/FAS-W.2016.58.

[3] Z. C. L. V. Sheng Z, Mahapatra C. 2015. Recent advances in industrial wireless sensor networks toward efficient management in IoT, *IEEE Access*, vol. 3, pp. 622-37.

[4] C. S. Chen, M. 2017. RFID Technologies for Internet of Things. Springer Cham.

[5] J. Hui and P. Thubert. 2011. Compression format for ipv6 datagrams over ieee 802.15.4-based networks," IETF, Tech. Rep.

[6] C. V. C. S. G. A. H. Y. Baronti P, Pillai P. 2007. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and zigbee standards," *Computer Communications*, vol. 30, p. 16551695.

[7] M. M. Hossain, M. Fotouhi, and R. Hasan. 2015. Towards an analysis of security issues, challenges, and open problems in the internet of things," in Services (SERVICES), *2015 IEEE World Congress on. IEEE*, 2015, pp. 21-28.

[8] Ragupathy, Somasundaram Thirugnanam, Mythili. 2017. IoT in Health-care: Breaching Security Issues.

[9] M Antonakakis, T April, Akamai, M Bailey, M Bernhard, A Arbor, E Bursztein, J Cochran, Cloud are, Z Durumeric and J. Alex Halderman, L Invernizzi, M Kallitsis, D Kumar, C Lever, Z Ma and Joshua Mason, D Menscher, C Seaman, Akamai, N Sullivan, K Thomas, Yi Zhou. 2016. "Un- derstanding the Mirai Botnet", 26th USENIX Security Symposium ,Vancouver, BC, Canada ISBN 978-1-931971-40-9

[10] K. Townsend. 2018. Financial services ddos attacks tied to reaper botnet," in available at: https://www.securityweek.com/ nancial-servicesddos-attacks-tied-reaper-botnet.

[11] Howard Solomon. 2018. Top 10 IoT vulnerabilities," in https://www.itworldcanada.com/article/top-10-iot-vulnerabilities-of-2018/413433.

[12] A. N. Nazarov and A. N. A. Koupaei. 2019. "An Architecture Model for Active Cyber Attacks on Intelligence Info-communication Systems:Application Based on Advance System Encryption (AES-512) Using Pre-Encrypted Search Table and Pseudo-Random Functions(PRFs)," *2019 International Conference on Engineering and Telecommunication (EnT),* Dolgoprudny, Russia, 2019, pp. 1- 10.1109/EnT47717.2019.9030541.

[13] Mahmoud Ammar, Giovanni Russello, Bruno Crispo,, 2018. Internet of Things: A survey on the security of IoT frameworks, Jour- nal of Information Security and Applications. Vol. 38. P. 8-27, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2017.11.002. (http://www.sciencedirect.com/science/article/pii/S2214212617302934)

[14] A. N. Nazarov and A. Nik Aein Koupaei. 2019. "Models of Risk of Attack of university Infocommunication System," *2019 Systems of Signals Generating and Processing in the Field of on Board Communications,* Moscow, Russia, pp. 1-8, doi: 10.1109/SOSG.2019.8706780.

[15] Angen, Gaute, Hallstensen, Christo er, nekkenes, Einar. 2018. A frame-work for estimating information security risk assessment method completeness," *International Journal of Information Security,* vol. 17, no 6, p681-699.

[16] D. X. Z. Xuanxia Yao, Xiaoguang Han,, 2013. A lightweight multicast authentication mechanism for small scale iot applications," IEEE Sensors, vol. 13, pp. 3693-3701.

[17] Rebecca E. Grinter and D. K. Smetters., 2018. "Three Challenges for Em-bedding Security into Applications", Palo Alto Research Center (PARC) 3333 Coyote Hill Road Palo Alto, CA 94304 USA.

[18] H. Haddad Pajouh, R. Javidan, R. Khayami, D. Ali, and K. Choo. 2016. A two-layer dimension reduction and two-tier classi cation model for anomaly-based intrusion detection in iot backbone networks," *in IEEE Transactions on Emerging Topics in Computing.*

[19] Arbia Riahi, Yacine Challal, Enrico Natalizio, Zied Chtourou, Abdelmad-jid Bouabdallah. 2013. "A Systemic Approach for IoT Security." *IEEE. DCOSS*, 2013, Boston, United States, pp. 351-355.

[20] A. N. Nazarov, A. N. A. Koupaei, A. Dhoot, A. Azlan and S. M. R. Siadat. 2020. "Mathematical Modelling of Infrastructure as a Service," *2020 Systems of Signals Generating and Processing in the Field of on Board Communications,* Moscow, Russia, pp. 1-6, doi: 10.1109/IEEECONF48371.2020.9078629.

[21] M. K. Khan, S.-K. Kim, and K. Alghathbar. 2011. Cryptanalysis and security enhancement of a more efficient secure dynamic id-based remote user authentication scheme," *Computer Communications*, vol. 34, no. 3, pp. 305-309.

[22] A. Nazarov, A. Sychev, A. N. A. Koupaei, S. K. Ojha and H. Rai. 2019. "Statistical compaction of a monitoring cloud cluster resource when processing streaming services," *2019 International Conference on Engineering and Telecommunication (EnT),* Dolgoprudny, Russia, pp. 1-5, doi: 10.1109/EnT47717.2019.9030598.

[23] Liu and P. Ning. 2004. Multilevel tesla: Broadcast authentication for distributed sensor networks," *ACM Transactions on Embedded Computing Systems (TECS),* vol. 3, no. 4, pp. 800-836.

[24] W. Ben Jaballah, M. Mosbah, and H. Youssef. 2013. Performance evaluation of key disclosure delay-based schemes in wireless sensor networks," *in Pervasive Computing and Communications Workshops (PERCOM Workshops), International Conference on Pervasive Computing and Communications Workshops, PERCOM*. IEEE, 2013, pp. 566-571.

[25] B. Mbarek, A. Meddeb, W. B. Jaballah and M. Mosbah. 2015. A secure authentication mechanism for resource constrained devices, *IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA),* Marrakech, pp. 1-7. Doi: 10.1109/AICCSA.2015.7507270.

[26] Achado, Caciano. 2018. IoT Data Integrity Verication for Cyber-Physical Systems Using Blockchain. 10.1109/ISORC.2018.00019.17.

20th EDITION OF GLOBAL SYMPOSIUM FOR REGULATORS RESPONDS TO CHALLENGES OF DIGITAL TRANSFORMATION IN THE WAKE OF GLOBAL CRISES AND BEYOND

NEW GSR-20 BEST PRACTICE GUIDELINES HIGHLIGHT KEY ROLE OF REGULATORS AND POLICY-MAKERS IN "BUILDING BACK BETTER"

Promoting an adaptive, resilient and collaborative regulatory system is key to "building back better" and advancing digital transformation for all, according to participants at ITU's 20th edition of the Global Symposium for Regulators (GSR-20), held virtually from 1 to 3 September.

Regulatory authorities that gathered at GSR-20 agree that in the wake of COVID-19 digital regulation can boost the readiness of digital markets to face unexpected events and emergencies and deliver up to the expectations despite the odds. Accordingly, they have adopted GSR-20 Best Practice Guidelines: The gold standard for regulation to respond to the challenges of digital transformation in the aftermath of global crises and beyond.

"This crisis has demonstrated that information and communication technology is a unifying thread that runs through all aspects of our societies and economies, and our approach to ICT investments must recognize and embrace this reality," said ITU Secretary-General Houlin Zhao. "At stake is the ability of regulators and policy-makers everywhere to unlock investment to support growth, jobs and innovation – but also to save lives and demonstrate their value added in this increasingly connected world."

National economies and citizens have been relying increasingly on digital infrastructure during COVID-19. The current crisis and the probability of new global emergencies means that regulators will need to switch to regulatory frameworks that are adaptive, collaborative, outcomes-based and technology neutral.

The GSR-20 Best Practice Guidelines emphasize the need for coordination among all stakeholders, integrating sustainability into regulatory frameworks, maximizing benefits while reducing harms of digital technologies, striving for transparency and trust throughout the regulatory process, an evidence-based approach, and frequent revision of regulatory frameworks to ensure they remain fit for purpose.

"The GSR-20 Best Practice Guidelines cast a framework for progressive regulatory patterns and policy while charting the way ahead for industry and regulators. We have identified concrete steps to pursue regulatory reform towards achieving thriving, inclusive digital markets," said GSR-20 Chair Dan Sjoblom. "As the pace of digital transformation accelerates, developing an effective regulatory approach is more vital than ever. In the face of new global emergencies, governments and regulators need to consider holistic, cross-sectoral, and, to the extent possible, multi-national regulatory and policy approaches."

The GSR-20 Best Practice Guidelines propose the following reforms:

Agile framework for competition in digital markets: Regulators should support innovation and new business and licensing models that facilitate affordable access to and investment in health, enterprise, and educational services on digital platforms.

Codes of conduct (voluntary or enforceable): Regulators should guide digital platforms and support them throughout the process of creating codes, their implementation and enforcement in important areas, such as online content moderation on digital platforms, addressing misinformation and online news quality, and child online protection. Media and digital literacy and awareness efforts should likewise be central to navigating the challenges around services that are enabled by the digital transformation.

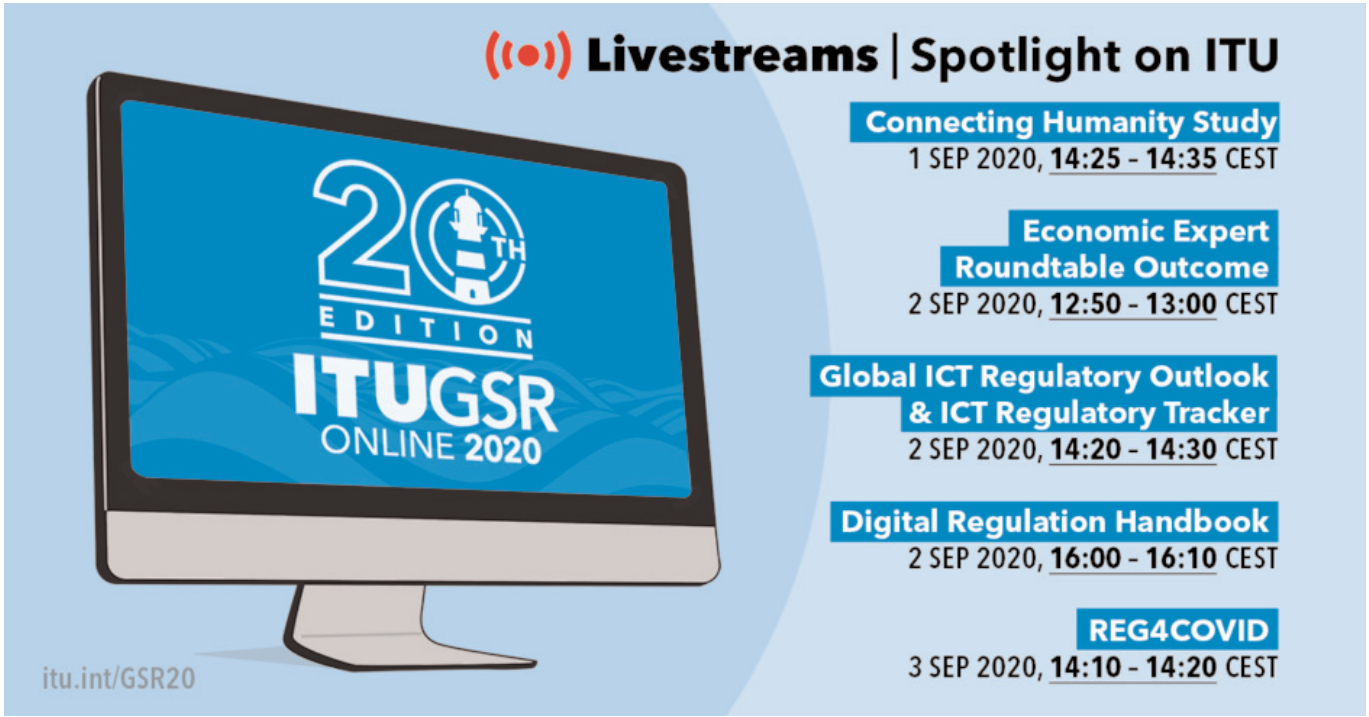
Upgrading national emergency plans: Creation and implementation of effective emergency plans enables better preparedness and decision-making during crises. Such plans are key to anticipating future unexpected events and their negative impacts and they should focus on both urban and rural areas through a multi-technology approach. Bilateral, regional and international cooperation should ensure business and public service continuity and underpin national recovery efforts.

Spectrum reform: Spectrum managers need to be able to respond timely, making spectrum available for wireless applications when and where they are needed, and as easily as possible, giving spectrum users and innovators flexibility to provide services that will deliver the greatest benefits. Ensuring that sufficient unlicensed spectrum is available drives innovation and investment in a range of technologies that can complement and support networks and expand broadband access at low cost. Spectrum reform should also be focused on ensuring that access to broadband service is provided affordably to those areas and populations that have been traditionally unserved or underserved.

At the same time, regulators recognize that there is no single, comprehensive blueprint for best practice and that regulatory patterns for the connected digital economy will be rooted in local circumstances while addressing regional and global challenges, especially now while the world is striving to build back better with digital technologies across the board.

"In the wake of the COVID-19 crisis, the work of regulators and policy-makers is critical," said Doreen Bogdan-Martin, Director of ITU's Telecommunication Development Bureau. "Our ICT policy and regulatory frameworks will need to be fit-for-purpose. They will need to be up-to-date, flexible, incentive-based and market-driven to support digital transformation across sectors, and across geographical regions. In short, they will need to leverage the power of digital platforms and infrastructures to build the resilience we need to protect us against future global emergencies."

This year's GSR programme kicked off on 30 June 2020 with a leadership debate "Resilient and secure digital connectivity for all: COVID-19 Recovery and lessons learned for better preparedness and response". The event was followed by Regional Regulatory Roundtable Discussions for the Europe, CIS, Arab States, Africa and Asia-Pacific regions.



Ahead of the 20th Edition of the ITU's Global Symposium for Regulators (GSR-20) the USTTI and ITU will team up to provide regulatory officials with a behind the scenes look at the work taking place to prepare for the deployment and usage of emerging technologies. During the webinar sessions on August 27 and August 28, subject matter experts will provide regulators with information on the Technological Underpinnings of Emerging Technologies and the Spectrum planning that is taking place to enable these new services.

August 27

Spectrum Planning for Emerging Technologies

As the competing demands for spectrum access intensify, Ronald Repasi, the Acting Chief of the United States Federal Communications Commission's (FCC), Office of Engineering and Technology will talk about work the FCC has been doing in pursuing both exclusive use and shared spectrum allocations among various services and technologies. The training will also walk through several examples to highlight the FCC's continued pursuit of greater spectrum access for all types of services and technologies.

Additionally, information will be shared on Dynamic Spectrum Sharing technology and how it opens the door for operators to seamlessly transition from 4G to 5G networks. Speakers will discuss how this technology functions and how it can speed the path for operators to move from 4G to 5G.

August 28

Technological Underpinnings of Emerging Technologies

Get a "behind the scenes" view of emerging technologies such as artificial intelligence (AI), Internet of Things (IoT), and the Edge. This session will discuss artificial intelligence from hardware to software capabilities and real-world applications across multiple usage scenarios, as well as provide an overview of IoT and the Edge. We will explore the latest technologies and standards underpinning this landscape and how they interact with key policy and regulatory trends.

GSR-20 also featured the Regional Regulatory Associations meeting and the Industry Advisory Group for Development Issues and Private Sector Chief Regulatory Officer's meeting (IAGDI-CRO) on 31 August, and the Heads of Regulators Executive Roundtable on 1 September.

The core sessions in September included a series of lightning sessions presenting the Global Network Resiliency Platform (REG4COVID); the new Digital Regulation Handbook and online platform, a collaborative effort between ITU and the World Bank; the outcome report of the Economic Experts Roundtable; and the Global ICT Regulatory Outlook and ICT Regulatory Tracker.

Global ICT Regulatory Outlook. The flood of digital change continues full spate – and digital transformation, while a reality for some, remains distant for many. A period of hope and aspiration buoyed by smartphones and increasingly accessible broadband has now darkened somewhat as misuse of profiling, data commercialization and harmful online behaviours have increasingly come to light, sparking considerable public debate. While markets are still driven by optimism about all that is digital, key players right across society are increasingly perceiving the role of regulation as central in restoring the full potential of ICT to deliver fully on its promise.

In the first edition of the Global ICT Regulatory Outlook in 2017, we explored the evolution of ICT regulatory trends over the preceding decade. We set out the ITU concept of five 'generations' of ICT regulation – now widely shared – analysing prime evidence and charting possible ways forward.

The second edition (2018) dived deep into the current trends defining regulation in the transition to the digital economy, and also focused on the strong correlation between ICT regulation and the take-up of ICT. It provided insight, inspiration and informed analysis designed to help address the challenges ahead – and paved the way for the first Benchmark for collaborative, fifth generation regulation presented in detail in Chapter 1 of this 2020 edition.

In this year's 2020 edition, we share unique, focused research and offer both evidence and practical advice to support regulators embarked on their journey to fifth generation collaborative regulation. The Benchmark of Fifth Generation Collaborative Regulation (G5 Benchmark), based on GSR19 Best Practice Guidelines together with the ICT Regulatory Tracker, serves as a compass for regulators on their journey of digital transformation, helping establish roadmaps towards regulatory excellence and a thriving digital economy.

Importantly, this year we revisit golden rules for inclusive digital markets based on a wealth of ITU data from 193 countries over more than a decade. Our research and analysis confirm that good regulation makes a difference – and provides the key to unlocking meaningful, inclusive connectivity across countries at different levels of development and national income. Working with those updated golden rules, we offer a regulatory recipe for accelerated take-up of fixed and mobile broadband markets.

Regulatory Associations Meeting 2020: The role of Regional and International Organizations and collaboration at regional level in a post-COVID World to address the challenges of Building Back Better

This year the Regulatory Associations (RA) Meeting will take place virtually on 31 August 2020 from 13h00 PM until 16h00 PM CEST during the 20th Global Symposium for Regulators (GSR-20). The RA meeting will be chaired by Mr Michel van Bellinghen, incoming BEREC Chairman. The Regulatory Associations Meeting at GSR-20 provides a unique platform for Regulatory Associations to share experiences and knowledge, to discuss how they can collaborate, and to identify means to build back better in a post-COVID digital ecosystem, and bring affordable, safe, secure and trusted connectivity and online access and use to people in their respective regions.

The topic for discussion this year will focus on the role of regional and international organizations and collaboration at regional level in a post-COVID World to address the challenges of Building Back Better. In addition, regional regulatory associations will also be able to share on their activities since last GSR-19.