Intelligent OFDM telecommunication system. Part 1. Model of system

V.G. Labunets[1], E.V. Ostheimer[2]

[1]Ural State Forest Engineering University, Sibirskiy trakt 37, Ekaterinburg, Russia, 620100
[2]Capricat LLC, Pompano Beach, Florida, US

Abstract. In this paper, we aim to investigate the superiority and practicability of many-parameter transforms (MPTs) from the physical layer security (PHY-LS) perspective. We propose novel Intelligent OFDM-telecommunication systems based on MPT. The new systems use Inverse MPT (IMPT) for modulation at the transmitter and Direct MPT (DMPT) for demodulation at the receiver. The purpose of employing the MPT is to improve: 1) the PHY-LS of wireless transmissions against to the wide-band anti-jamming and anti-eavesdropping communication; 2) the bit error rate (BER) performance with respect to the conventional OFDM-TCS; 3) the peak to average power ratio (PAPR). Each MPT depends on finite set of independent parameters (angles), which could be changed independently of one another. When parameters are changed, MPT is also changed taking form of a set known (and unknown) orthogonal (or unitary) transforms. For this reason, the concrete values of parameters are specific "key" for entry into OFDM-TCS. Vector of parameters belong to multi-dimension torus space. Scanning of this space for find out the "key" (the concrete values of parameters) is hard problem. MPT has the form of the product of the sparse Jacobi rotation matrixes and it describes a fast algorithm for MPT. The main advantage of using MPT in OFDM TCS is that it is a very flexible anti-eavesdropping and anti-jamming Intelligent OFDM TCS. To the best of our knowledge, this is the first work that utilizes the MPT theory to facilitate the PHY-LS through parameterization of unitary transforms.

1. Introduction

In today's world, an important aspect of communication and technology is security. Wars are being fought in the virtual world rather than in the real world. There is a rapid increase in cyber warfare. Ensuring information security is of paramount importance for wireless communications. Due to the broadcast nature of radio propagation, any receiver within the cover range can listen and analyze the transmission without being detected, which makes wireless networks vulnerable to eavesdropping and jamming attacks. Orthogonal Frequency-Division Multiplexing (OFDM) has been widely employed in modern wireless communications networks. Unfortunately, conventional OFDM signals are vulnerable to malicious eavesdropping and jamming attacks due to their distinct time and frequency characteristics. The communication that happens between the two legitimate agents needs to be authorized, authentic and secured. Hence, in order to design a secured communication, we need a secret key that can be used to encode the data in order to be prevented from phishing. Therefore, there is a need to generate a secret key with the existing information available. This key should not be shared, as the wireless channel remains vulnerable to attack. So, the key should be generated by communicating legitimate agents. Traditionally, cryptographic algorithms/protocols implemented at

upper layers of the open systems interconnection (OSI) protocol stack, have been widely used to prevent information disclosure to unauthorized users [1]. However, the layered design architecture with transparent physical layer leads to a loss in security functionality [2], especially for wireless communication scenarios where a common physical medium is always shared by legitimate and non-legitimate users. Moreover, the cryptographic protocols can only offer a computational security [3].
As an alternative, exploiting physical layer characteristics for secure transmission has become an emerging hot topic in wireless communications. The pioneering work by Wyner in [4] introduced the concept of "secrecy capacity" as a metric for PHY-layer security (PHY-LS). It is pointed out that perfect security is in fact possible without the aid of an encryption keys when the source-eavesdropper (wire-tap) channel is a degraded version of the source-destination (main) channel [4].
As the physical-layer transmission adversaries can blindly estimate parameters of OFDM signals, traditional upper-layer security mechanisms cannot completely address security threats in wireless OFDM systems. Physical layer security, which targets communications security at the physical layer, is emerging as an effective complement to traditional security strategies in securing wireless OFDM transmission [8]. The physical layer security of OFDM systems over wireless channels was investigated from an information-theoretic perspective in [5].
Based on the theoretical secrecy capacity study, several OFDM security techniques have been proposed. A secure OFDM system was investigated by degrading the eavesdropper's channel condition, where distributed transmitters independently sent out pre-equalized OFDM signals [6]. Power and subcarrier allocation schemes in OFDM systems subject to the power and security constraints were reported in [7]. Moreover, transmit beamforming [8] and artificial noise [9] can be adopted to improve the security of OFDM-based transmission. However, these secretive capacities based security techniques usually require the knowledge of the eavesdropping channel, which is conditioned on a successful detection of eavesdroppers.
These serious drawbacks make OFDM a less than ideal technique for high data rate communications over secret and military channels (SC and MC). These channels are characterized by both deliberate noise and strong impulsive noise. Therefore, alternative MCMs should be considered for SCs (MCs) and compared to conventional OFDM.
In this paper, we propose a simple and effective anti-eavesdropping and anti-jamming Intelligent OFDM system, based on many-parameter transforms (MPTs) [10]-[14]. In this paper, we aim to investigate the superiority and practicability of MPTs from the physical layer security (PHY-LS) perspective. We propose novel Intelligent OFDM-telecommunication systems (Intelligent-OFDM-TCS) based on MPT $\mathrm{U}_N(\boldsymbol{\theta}) = \mathrm{U}_N(\varphi_1, \varphi_2, ..., \varphi_q)$, where $\boldsymbol{\theta} = (\varphi_1, \varphi_2, ..., \varphi_q)$. MPT has the form of the product of the sparse Jacobi rotation matrixes and it describes a fast algorithm for MPT. The main advantage of using MPT in OFDM TCS is that it is a very flexible anti-eavesdropping and anti-jamming Intelligent OFDM TCS. To the best of our knowledge, this is the first work that utilizes the MPT theory to facilitate the PHY-LS through parameterization of unitary transforms. We do study of Intelligent- $\mathrm{U}_N(\boldsymbol{\theta})$ -OFDM-TCS to find out optimal values of parameters optimized PARP, BER, SER, anti-eavesdropping and anti-jamming effects (see Part 3 and Part 4 of our work). The purposes of employing the MPT:

- is studied the influence of parameters $\boldsymbol{\theta} = (\varphi_1, \varphi_2, ..., \varphi_q)$ on the transmission performances of OFDM-TCS,
- Is to improve the PHY-LS of wireless transmissions against to the wide-band anti-jamming and anti- eavesdropping communication.
- is to minimized the peak to average power ratio (PAPR), the bit error rate (BER) and symbol error rate (SER) performances with respect to the conventional OFDM-TCS, based on fast Fourier transform (FFT),
- is to minimize inter-symbol interference (ISI) by chaining of parameters.

Each MPT $\mathrm{U}_N(\boldsymbol{\theta})$ depends on finite set of independent Krylov-Jacobi (or Euler-Jacobi) parameters (angles $\boldsymbol{\theta} = (\varphi_1, \varphi_2, ..., \varphi_q)$), which could be changed independently of one another. When parameters

are changed, sub-carriers, corresponding to multi-parametric transform, are changed too taking form of all known (and unknown) orthogonal sub-carriers that transmit useful information. For this reason, the concrete values of parameters $\varphi_1=\varphi_1^0,\varphi_2=\varphi_2^0,...,\varphi_q=\varphi_q^0$ are specific "key" for entry into OFDM-TCS. Vector $\boldsymbol{\theta}=(\varphi_1,\varphi_2,...,\varphi_q)$ of parameters belong to q-D torus space $[0,2\pi)^q$. For $(N\times N)$-MPT $\mathrm{U}_N(\boldsymbol{\theta})$ q is equals to $\mathrm{O}(N\log_2 N)$. If, for example, $N=2^{10}=1024$, then the torus $[0,2\pi)^q$ will have dimension $10\cdot 2^9=5120$ (it is not 1-D radio frequency axis in the Fourier analyses!). Scanning of the space $[0,2\pi)^{5120}$ for find out the "key" (the concrete values of parameters $\varphi_1=\varphi_1^0,\varphi_2=\varphi_2^0,...,\varphi_q=\varphi_q^0$) is a hard problem. The process of generating a "key" (parameters) of MPT can be more efficient in terms of providing security as compared to RSS based technique. Our implementation contains three agents: two legitimate agents Alice and Bob who want to communicate with each other. An illegitimate agent (stated as Eve) tries to listen to Alice's and Bob's OFDM-TCS and try to find out the "key" so that she can 1) to eavesdrop the confidential information, or 2) break the communication between them by Jamming. Jamming in wireless OFDM-networks is defined as the disruption of existing wireless communications by decreasing the signal-to-noise ratio at receiver sides through the transmission of interfering wireless signals.

The paper is organized as follows. Section 2 of the paper presents a brief introduction to the conventional OFDM system along with various notations used in the paper. Section 3 presents novel Intelligent-OFDM-TCS based on MPTs $\mathrm{U}_N(\boldsymbol{\theta})$. On the next parts of our work we do study of Intelligent $\mathrm{U}_N(\boldsymbol{\theta})$-OFDM-TCS to find out optimal values of parameters optimized **PAR**P, **BER**, **SER**, anti-eavesdropping and anti-jamming effects, where $\mathrm{U}_N(\boldsymbol{\theta})$ is the many parameter wavelet transform, the many-parameter wavelet transform or many-parameter Fourier transform (in particular case, 1-parameter fractional Fourier transform).

2. Intelligent OFDM TCS

Most of the data transmission systems nowadays use orthogonal frequency division multiplexing telecommunication system (OFDM-TCS) based on the discrete Fourier transform (DFT). Some versions of it is: digital audio broadcast (DAB), digital video broadcast (DVB), and wireless local area network (WLAN), standards such as IEEE802.11g and long term evolution (LTE and its extension LTE- Advanced, Wi-Fi (IEEE 802.11), worldwide interoperability for microwave ACCESS (WiMAX IEEE 802.16) or ADSL [15]. The concept of using parallel data broadcast by means of frequency division multiplexing (FDM) was printed in mid 60s [16].

The conventional OFDM is a multi-carrier modulation technique that is basic technology having high-speed transmission capability with bandwidth efficiency and robust performance in multipath fading environments. OFDM divides the available spectrum into a number of parallel orthogonal sub-carriers and each sub-carrier is then modulated by a low rate data stream at different carrier frequency. In OFDM system, the modulation and demodulation can be applied easily by means of inverse and direct discrete Fourier transforms (DFT). The conventional OFDM will be denoted by the symbol F_N-**OFDM**.

Conventional OFDM-TCS makes use of signal orthogonality of the multiple sub-carriers $e^{j2\pi kn/N}$ (discrete complex exponential harmonics). All sub-carriers $\{\mathbf{subc}_k(n)\}_{k=0}^{N-1}=\{e^{j2\pi kn/N}\}_{k=0}^{N-1}$ form matrix of discrete orthogonal Fourier transform $\mathrm{F}_N=[\mathbf{subc}_k(n)]_{k,n=0}^{N-1}\equiv[e^{j2\pi kn/N}]_{k,n=0}^{N-1}$. At the time, the idea of using the fast algorithm of different orthogonal transforms $\mathrm{U}_N=[\mathbf{subc}_k(n)]_{k,n=0}^{N-1}$ for a software-based implementation of the OFDM's modulator and demodulator, transformed this technique from an attractive. OFDM-TCS, based on arbitrary orthogonal (unitary) transform U_N will be denoted as U_N-**OFDM**. The idea which links F_N-**OFDM** and U_N-**OFDM** is that, in the same manner that the

complex exponentials $\left\{e^{j2\pi kn/N}\right\}_{k=0}^{N-1}$ are orthogonal to each-other, the members of a family of U_N -sub-carriers $\left\{\mathbf{subc}_k(n)\right\}_{k=0}^{N-1}$ (rows of the matrix U_N) will satisfy the same property.

The U_N-**OFDM** reshapes the multi-carrier transmission concept, by using carriers $\left\{\mathbf{subc}_k(n)\right\}_{k=0}^{N-1}$ instead of OFDM's complex exponentials $\left\{e^{j2\pi kn/N}\right\}_{k=0}^{N-1}$. There are a number of candidates for orthogonal function sets used in the OFDM-TCS: discrete wavelet sub-carriers [17]-[18], Golay complementary sequences [19]-[23], rectangle pulses [17], Walsh functions [24]-[26], pseudo random sequences [27].

Intelligent-OFDM TCS can be described as a dynamically reconfigurable TCS that can adaptively regulate its internal parameters as a response to changes in the surrounding environment. One of the most important capacities of Intelligent OFDM systems is their capability to optimally adapt their operating parameters based on observations and previous experiences. There are several possible approaches towards realizing such intelligent capabilities. In this work, we aim to investigate the superiority and practicability of MPTs from the physical layer security (PHY-LS) perspective.

In this work, we propose a simple and effective anti-eavesdropping and anti-jamming Intelligent OFDM system, based on many-parameter transform. In our Intelligent-OFDM-TCS we use MPT $\mathrm{U}_N=\mathrm{U}_N(\boldsymbol{\theta})$ instead of DFT F_N. Each MPT depends on finite set of independent Krylov-Jacobi (or Euler-Jacobi) parameters (angles $\boldsymbol{\theta}=(\varphi_1,\varphi_2,...,\varphi_q)$), which could be changed in dependently of one another. When parameters are changed, multi-parametric transform is changed too taking form of known (and unknown) orthogonal transforms. MPT $\mathrm{U}_N(\boldsymbol{\theta})$ has the form of the product of the sparse Jacoby rotation matrixes and which describes a fast algorithm for this transform.

We do study of Intelligent $\mathrm{U}_N(\boldsymbol{\theta})$-OFDM-TCS to find out optimal values of parameters optimized PARP, BER, SER, anti-eavesdropping and anti-jamming effects (see next parts of our work). For simplicity, we consider a single-input single-output OFDM setup with N sub-carriers (see Fig. 1).

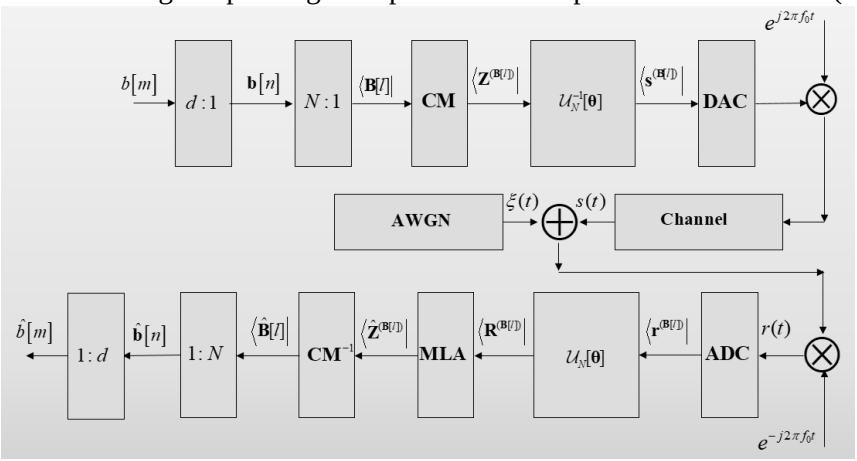

Figure 1. Block diagram of Intelligent OFDM-TCS.

Let 2^d-$\mathbf{CD}=\left\{Z^{(\mathbf{b})}=Z^{(b_0,b_1,...,b_{d-1})}\in\mathbf{C}\middle|\mathbf{b}=(b_0,b_1,...,b_{d-1})\in\{0,1\}^d\right\}$ be a constellation diagram (**CD**) on the complex plane $\mathbf{C}$ consisting of 2^d points (stars) $Z^{(b_0,b_1,...,b_{d-1})}$ and numbered by binary d-digital numbers $\langle\mathbf{b}|=(b_0,b_1,...,b_{d-1})\in\{0,1\}^d$. Here $\{0,1\}^d$ is d-D Boolean cube. In the constellation diagrams, the symbols are indexed using the Grey coding scheme. We interpret $\langle\mathbf{b}|=(b_0,b_1,...,b_{d-1})$ as an address of star $Z^{(b_0,b_1,...,b_{d-1})}$ in computer memory. Let us introduce the following designations

$$\mathbf{CM}(b_0,b_1,...,b_{d-1})=Z^{(b_0,b_1,...,b_{d-1})}\in 2^d\text{-}\mathbf{CD},\quad \langle\mathbf{b}|=\mathbf{CM}^{-1}\left\{Z^{(b_0,b_1,...,b_{d-1})}\right\}=(b_0,b_1,...,b_{d-1})\in\{0,1\}^d,$$

where $\mathbf{CM}$, $\mathbf{CM}^{-1}$ are constellation direct and inverse mappings.

The principle of any OFDM system is to split the input 1-bit stream $b[m]$, $m=0,1,2,...$ into d-bit stream ($\mathbf{B}_2^d$-valued stream): $b[m]=b[nd+r]\to\mathbf{b}[n]=(b_0[n],...,b_r[n],...,b_{d-1}[n])$, where $\mathbf{b}\in\mathbf{B}_2^d=\{0,1\}^d$, $m=nd+r$, $r=0,1,...,d-1$ and $n=0,1,2...$. Here m is the real discrete time, n is the "time" for d-bit stream $\mathbf{b}(n)$ (i.e., the d-decimation "time" with respect to real discrete time). The $\mathbf{B}_2^d$-valued sequence $\mathbf{b}(n)$ is split into N sub-sequences (sub-streams)

$$\mathbf{b}[n]=\mathbf{b}[lN+k]\to\langle\mathbf{B}[l]|=(\mathbf{b}^0[l],...,\mathbf{b}^k[l],...,\mathbf{b}^{N-1}[l]) \tag{1}$$

where $n=lN+k$, $k=0,1,...,N-1$ and $l=0,1,2...$.

The row-vector $\langle\mathbf{B}[l]|=(\mathbf{b}^0[l],\mathbf{b}^1[l],...,\mathbf{b}^k[l],...,\mathbf{b}^{N-1}[l])$ is called the l^{th} $\{0,1\}^d$-valued time-slot. Here l is the "time" for time-slot $\langle\mathbf{B}[l]|$ (i.e., the N-decimation "time" with respect to d-bit stream "time" n and Nd-decimation "time" with respect to real discrete time m).

The data of the l^{th} time-slot $\langle\mathbf{B}[l]|$ is first being processed by a constellation mapping (**CM**). Various CMs could generally be employed. For example, such CM as QPSK, BPSK (also with their differential form) and QAM with several different signal constellations are used to map $\mathbf{B}_2^d$-valued data to appropriate complex-valued symbols $Z_k^{(\mathbf{b}^k[l])}$: $\mathbf{b}^k[l]\to Z_k^{(\mathbf{b}^k[l])}=\mathbf{CM}\{\mathbf{b}^k[l]\}$, $k=0,1,...,N-1$, *i.e.*,

$$\langle\mathbf{Z}^{(\mathbf{B}[l])}|=\mathbf{CM}\{\langle\mathbf{B}[l]|\}=$$
$$=(\mathbf{CM}\{\mathbf{b}^0[l]\},...,\mathbf{CM}\{\mathbf{b}^k[l]\},...,\mathbf{CM}\{\mathbf{b}^{N-1}[l]\})=(Z_0^{(\mathbf{b}^0[l])},...,Z_k^{(\mathbf{b}^k[l])},...,Z_{N-1}^{(\mathbf{b}^{N-1}[l])}). \tag{2}$$

Complex numbers $Z_k^{(\mathbf{b}^k[l])}$ $(k=0,1,...,N-1)$ are called data symbols. These symbols are then input into the inverse MPT ($\mathrm{U}_N^{-1}(\boldsymbol{\theta})$-block). The output of MPT is the sum of the information signals in the discrete time domain as follows:

$$\langle\mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta})|=(s_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}),...,s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}),...,s_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta}))=$$
$$=\langle\mathbf{Z}^{(\mathbf{B}[l])}|\cdot\mathrm{U}_N^{-1}(\boldsymbol{\theta})=(Z_0^{(\mathbf{b}^0[l])},...,Z_k^{(\mathbf{b}^k[l])},...,Z_{N-1}^{(\mathbf{b}^{N-1}[l])})\ \mathrm{U}_N^{-1}(\boldsymbol{\theta}), \tag{3}$$

where $s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta})=\sum_{k=0}^{N-1}Z_k^{(\mathbf{b}^k[l])}\cdot\mathbf{subc}_k(v|\boldsymbol{\theta})$, and $\langle\mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta})|=(s_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}),...,s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}),...,s_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta}))$ is a sequence in the discrete time domain, N is the number of sub-carriers $\{\mathbf{subc}_k(v|\boldsymbol{\theta})\}_{k=0}^{N-1}$. All sub-carriers $\{\mathbf{subc}_k(v|\boldsymbol{\theta})\}_{k=0}^{N-1}$ transmit dN data bits. As we see in digital Intillegent OFDM TCS, *many-parameter sub-carriers* $\{\mathbf{subc}_k(v|\boldsymbol{\theta})\}_{k=0}^{N-1}$ are used to carry the digital data $\{Z_k^{(\mathbf{b}^k[l])}\}_{k=0}^{N-1}$. By this reason, all coefficients $s_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}),...,s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}),...,s_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta})$ depend on parameters $\boldsymbol{\theta}=(\varphi_1,...,\varphi_q)$. This dependence can be used for multiple purposes such as, anti-eavesdropping and anti-jamming in order to increase the system secrecy. Digital data $\langle\mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta})|$ is interpolated by digital-to-analog converter (DAC): $\langle\mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta})|\xrightarrow{\mathrm{DAC}}s^{(\mathbf{B}[l])}(t|\boldsymbol{\theta})$, $(t\in[0,T])$ in generating the analog signal $s^{(\mathbf{B}[l])}(t|\boldsymbol{\theta})$.

The peak to average power ratio (PAPR) for l^{th} time-slot is defined as

$$\mathbf{PARP}_{\mathrm{U}}[l|\boldsymbol{\theta}]=20\log\frac{\max\limits_{t\in\{0,T\}}|s^{(\mathbf{B}[l])}(t|\boldsymbol{\theta})|}{\sqrt{\frac{1}{T}\int_0^T|s^{(\mathbf{B}[l])}(t|\boldsymbol{\theta})|^2\,dt}}. \tag{4}$$

It is interesting to minimize the peak to average power ratio $\mathbf{PARP}_{\mathrm{U}}[l|\boldsymbol{\theta}]$, the bit error rate $\mathbf{BER}_{\mathrm{U}}[l|\boldsymbol{\theta}]$, symbol error rate $\mathbf{SER}_{\mathrm{U}}[l|\boldsymbol{\theta}]$, inter-symbol interference $\mathbf{ISI}_{\mathrm{U}}[l|\boldsymbol{\theta}]$ and is to improve the PHY-LS of

wireless transmissions against to the wide-band anti-jamming and anti- eavesdropping communication by chaining of parameters $\boldsymbol{\theta}$. In practice the $\mathbf{PARP}_{\mathrm{U}}$ is defined in terms of the discrete signal $\left\langle \mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right| = \left(s_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}),..., s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}),..., s_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right)$ as

$$\mathbf{PARP}_{\mathrm{U}}[l \mid \boldsymbol{\theta}] = 20 \log \frac{\max\limits_{v \in [0,N-1]} \left| s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right|}{\sqrt{\frac{1}{N} \sum\limits_{v \in [0,N-1]} \left| s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right|^2}}. \tag{5}$$

The signal $s^{(\mathbf{B}[l])}(t \mid \boldsymbol{\theta})$ is then AM-modulated $\left[1 + m \cdot s^{(\mathbf{B}[l])}(t \mid \boldsymbol{\theta}) \right] \cdot e^{j 2\pi f_0 t}$ to the carrier frequency f_0 and radiated to a wireless medium, the so-called radio channel (RF), before it is picked up at the receiver side. Here m is the AM-modulation index.

At the receiver side, after AM-demodulation and discretization by analog-to-digital converter (ADC) from received signal $r(t \mid \boldsymbol{\theta})$ we obtain the received symbols

$$\left\langle \mathbf{r}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right| = \left(r_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}),..., r_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}_q),..., r_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right).$$

They are the transmitted symbols $\left\langle \mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right| = \left(s_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}),..., s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}),..., s_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right)$ plus the additive complex-valued Gaussian noise samples:

$$\left\langle \mathbf{r}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right| = \left(r_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}),..., r_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}_q),..., r_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right) =$$

$$= \left\langle \mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right| + \left\langle \boldsymbol{\xi} \right| = \left(s_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}) + \xi_0(l),..., s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}) + \xi_v(l),..., s_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) + \xi_{N-1}(l) \right),$$

where $\xi_v(l)$ is a discrete–time additive complex Gaussian process (ACWGNP) $\left\langle \boldsymbol{\xi} \right| = \left(\xi_0(l),..., \xi_v(l),..., \xi_{N-1}(l) \right)$, $\xi_k \in \mathbb{CN}\left(\dot{m}, \sigma^2 \right)$, $k = 0,1,..., N-1$ with a complex-valued mean $\dot{m} = \Re(\dot{m}) + i\Im(\dot{m})$, variance σ_{jam}^2 and with autocorrelation function $\mathrm{E}\left(\xi_i \overline{\xi}_k \right) = \sigma^2 \delta_{i,k}$, where $\delta_{i,k}$ is the Dirac delta (*i.e.*, Gaussian process is white). From one hand, noise can be considered as a natural passive thermal noise. From the other hand, noise can be considered as an active jamming noise (for example, in military or police special force operations this type of noise appears).

At the receiver side, the process is reversed to obtain the data. The signal $\left\langle \mathbf{r}^{(\mathbf{B}[l])} \right| = \left(r_0^{(\mathbf{B}[l])},..., r_v^{(\mathbf{B}[l])},..., r_{N-1}^{(\mathbf{B}[l])} \right)$ is demodulated by direct N-tap MPT. The output of direct MPT is represented as follow:

$$\left\langle \mathbf{R}^{(\mathbf{b}^k[l])}(\boldsymbol{\theta}) \right| = \left(R_0^{(\mathbf{b}^0[l])}(\boldsymbol{\theta}),..., R_k^{(\mathbf{b}^k[l])}(\boldsymbol{\theta}),..., R_{N-1}^{(\mathbf{b}^{N-1}[l])}(\boldsymbol{\theta}) \right) = \left\langle \mathbf{r}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right| \cdot \mathrm{U}_N(\boldsymbol{\theta}) =$$

$$= \left(s_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}) + \xi_0(l),..., s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}) + \xi_v(l),..., s_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) + \xi_{N-1}(l) \right) \cdot \mathrm{U}_N(\boldsymbol{\theta}) =$$

$$= \left(Z_0^{(\mathbf{b}^0[l])} + \Xi_0(l \mid \boldsymbol{\theta}),..., Z_k^{(\mathbf{b}^k[l])} + \Xi_k(l \mid \boldsymbol{\theta}),..., Z_{N-1}^{(\mathbf{b}^{N-1}[l])} + \Xi_{N-1}(l \mid \boldsymbol{\theta}) \right) =$$

$$= \left(Z_0^{(\mathbf{b}^0[l])},..., Z_k^{(\mathbf{b}^k[l])},..., Z_{N-1}^{(\mathbf{b}^{N-1}[l])} \right) + \left(\Xi_0(l \mid \boldsymbol{\theta}),..., \Xi_k(l \mid \boldsymbol{\theta}),..., \Xi_{N-1}(l \mid \boldsymbol{\theta}) \right) = \left\langle \mathbf{Z}^{(\mathbf{B}[l])} \right| + \left\langle \boldsymbol{\Xi}(l \mid \boldsymbol{\theta}) \right|,$$

where

$$R_k^{(\mathbf{b}^k[l])}(\boldsymbol{\theta}) = \frac{1}{\sqrt{N}} \sum_{v=0}^{N-1} r_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \cdot \mathbf{subc}_k(v \mid \boldsymbol{\theta}) =$$

$$= \frac{1}{\sqrt{N}} \sum_{v=0}^{N-1} \left(s_v^{(\mathbf{B}[l])}(\boldsymbol{\theta}) + \xi_v(l) \right) \cdot \mathbf{subc}_k(v \mid \boldsymbol{\theta}) = Z_k^{(\mathbf{b}^k[l])} + \Xi_k(l \mid \boldsymbol{\theta}),$$

and $\Xi_k(l \mid \boldsymbol{\theta}) = \sum\limits_{v=0}^{N-1} \xi_v(l) \cdot \mathbf{subc}_k(v \mid \boldsymbol{\theta})$. After that the maximum-likelihood algorithm (**MLA**) gives the optimal estimation of the signal $\left| \mathbf{Z}^{(\mathbf{B}[l])} \right\rangle$:

$$\left\langle \hat{\mathbf{Z}}_{opt}^{(\mathbf{B}[l])} \right| = \left(\hat{Z}_0^{(\mathbf{b}^0[l])},..., \hat{Z}_k^{(\mathbf{b}^k[l])},..., \hat{Z}_{N-1}^{(\mathbf{b}^{N-1}[l])} \right) = \mathbf{MLA}\left[\left\langle \mathbf{Z}^{(\mathbf{B}[l])} \right| + \left\langle \boldsymbol{\Xi}(l \mid \boldsymbol{\theta}) \right| \right] =$$

$$= \left(\mathbf{MLA}\left[Z_0^{(\mathbf{b}^0[l])} + \Xi_0(l \mid \boldsymbol{\theta}) \right],..., \mathbf{MLA}\left[Z_k^{(\mathbf{b}^k[l])} + \Xi_k(l \mid \boldsymbol{\theta}) \right],..., \mathbf{MLA}\left[Z_{N-1}^{(\mathbf{b}^{N-1}[l])} + \Xi_{N-1}(l \mid \boldsymbol{\theta}) \right] \right) =$$

$$= \left(\min_{Z \in 2^d\text{-}\mathbf{CD}} \rho\left\{ Z_0^{(\mathbf{b}^0[l])} + \Xi_0(l \mid \boldsymbol{\theta}), Z \right\},..., \min_{Z \in 2^d\text{-}\mathbf{CD}} \rho\left\{ Z_k^{(\mathbf{b}^k[l])} + \Xi_k(l \mid \boldsymbol{\theta}), Z \right\},..., \min_{Z \in 2^m\text{-}\mathbf{CD}} \rho\left\{ Z_{N-1}^{(\mathbf{b}^{N-1}[l])} + \Xi_{N-1}(l \mid \boldsymbol{\theta}), Z \right\} \right), \tag{6}$$

where ρ is the Euclidean distance on the complex plane $\mathbf{C}$ and the symbol "^" over $\hat{\mathbf{Z}}_{opt}^{(\mathbf{B}[l])}$ means estimated value $\mathbf{Z}^{(\mathbf{B}[l])}$. Finally, estimation of bit stream is given as

$$\left\langle \hat{\mathbf{B}}[l\,|\,\boldsymbol{\theta}] \right| = \left(\hat{\mathbf{b}}^0[l\,|\,\boldsymbol{\theta}],...,\hat{\mathbf{b}}^k[l\,|\,\boldsymbol{\theta}],...,\hat{\mathbf{b}}^{N-1}[l\,|\,\boldsymbol{\theta}] \right) =$$

$$= \mathbf{CM}^{-1}\left\{ \left\langle \hat{\mathbf{Z}}_{opt}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right| \right\} = \left(\mathbf{CM}^{-1}\left\{ \hat{Z}_0^{(\mathbf{b}^0[l])}(\boldsymbol{\theta}) \right\},...,\mathbf{CM}^{-1}\left\{ \hat{Z}_k^{(\mathbf{b}^k[l])}(\boldsymbol{\theta}) \right\},...,\mathbf{CM}^{-1}\left\{ \hat{Z}_{N-1}^{(\mathbf{b}^{N-1}[l])}(\boldsymbol{\theta}) \right\} \right), \tag{7}$$

where $\hat{\mathbf{b}}^k[l\,|\,\boldsymbol{\theta})] \to \hat{\mathbf{b}}[lN+k\,|\,\boldsymbol{\theta})] \to \hat{b}\left[(lN+k)d+r\,|\,\boldsymbol{\theta}\right] = \hat{b}\left[m\,|\,\boldsymbol{\theta}\right]$ is an estimation of initial bit stream. Here, $m = \left[(lN+k)d+r\right] = lNd+kd+r$ and $l = 0,1,...$, $k = 0,1,...,N-1$, $r = 0,1,...,d-1$.

The **BER** and **SER** for l^{th} time slot are defined as

$$\mathbf{BER}_{\mathrm{U}}[l\,|\,\boldsymbol{\theta}] = \frac{1}{Nd}\sum_{k=0}^{N-1}\sum_{r=0}^{d-1}\left(b\left[(lN+k)d+r\,|\boldsymbol{\theta}\right] \oplus \hat{b}\left[(lN+k)d+r\,|\boldsymbol{\theta}\right]\right) =$$

$$= \frac{1}{Nd}\sum_{m=0}^{Nd-1}\left(b\left[m|\boldsymbol{\theta}\right] \oplus \hat{b}\left[m|\boldsymbol{\theta}\right]\right), \tag{8}$$

$$\mathbf{SER}_{\mathrm{U}}[l\,|\,\boldsymbol{\theta}] = \sum_{k=0}^{N-1}\bigcup_{r=0}^{d-1}\left(b\left[(lN+k)d+r\,|\boldsymbol{\theta}\right] \oplus \hat{b}\left[(lN+k)d+r\,|\boldsymbol{\theta}\right]\right) =$$

$$= \frac{1}{N}\sum_{k=0}^{N-1}\left(\hat{\mathbf{b}}^k\left[l|\boldsymbol{\theta}\right] \neq \hat{\mathbf{b}}^k\left[l|\boldsymbol{\theta}\right]\right). \tag{9}$$

All transmitted $\left\langle \mathbf{s}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right| = \left(s_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}),...,s_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right)$ and received $\left\langle \mathbf{r}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right| = \left(r_0^{(\mathbf{B}[l])}(\boldsymbol{\theta}),...,r_{N-1}^{(\mathbf{B}[l])}(\boldsymbol{\theta}) \right)$ symbols depend on parameters $\boldsymbol{\theta} = (\varphi_1,...,\varphi_q)$. This dependence can be used for multiple purposes such as, anti-eavesdropping and anti-jamming in order to increase the system secrecy, and for PAPR reduction (see the next parts of our work).

3. Conclusion

In this paper, we proposed a novel Intelligent OFDM-telecommunication systems based on many-parameter transforms (MPTs). The purpose of employing the MPT is to improve: 1) the PHY-LS of wireless transmissions against to the wide-band anti-jamming and anti-eavesdropping communication; 2) the bit error rate (BER) performance with respect to the conventional OFDM-TCS; 3) the peak to average power ratio (PAPR). The new systems use Inverse MPT (IMPT) for modulation at the transmitter and MPT for demodulation at the receiver. Each MPT depends on finite set of independent parameters (angles), which could be changed in dependently of one another. When parameters are changed, multi-parametric transform is changed too taking form of a set known (and unknown) orthogonal (or unitary) transforms. The main advantage of using MPT in OFDM TCS is that it is a very flexible system allowing to construct Intelligent OFDM TCS for electronic warfare (EW). EW is a type of armed struggle using electronic means against enemy to "change the quality of information". EW includes (consists) of suppressor (in our case Eve or Jamie) and protector (Alice and Bob). Suppressor aims to "reduce the effectiveness" of enemy forces, including command and control and their use of weapons systems, and targets enemy communications and reconnaissance by changing the "quality and speed" of information processes. In reverse, EW in defense (Alice&Bob) protects such assets and those of friendly forces. The general suppressor's goal is interception of Alice's and Bob's private communications means the same OFDM-TCS. In order to protect corporate privacy and sensitive client information against the threat of electronic eavesdropping and jamming Alice and Bob use intelligent OFDM-TCS, based on MPTs. The system model that is going to be used in this work is know as the wiretap channel model, which was introduced in 1975 by Wyner [4]. This model is composed of two legitimate users, named Alice and Bob.

A legitimate user (Alice) transmits her confidential messages to a legitimate receiver (Bob), while Eve is trying to eavesdrop Alice's information. An active jammer, named Jamie, attempts to jam up this information. Alice transmits her data using OFDM with N sub-carriers $\left\{ Subc_k(n\,|\,\varphi_1^0,...,\varphi_q^0) \right\}_{k=0}^{N-1}$, i.e. she

use the unitary transform $\mathrm{U}_N^0 = \mathrm{U}_N(\boldsymbol{\theta}^0)$ with fixed parameters $\boldsymbol{\theta}^0 = (\varphi_1^0,...,\varphi_q^0)$. When sub-carriers $\left\{Subc_k(n \mid \varphi_1^0,...,\varphi_q^0)\right\}_{k=0}^{N-1}$ (i.e. unitary transform $\mathrm{U}_N(\boldsymbol{\theta}^0)$) of Alice's and Bob's Intelligent-OFDM-TCS are identified by Eve (or Jammi) this TCS can be eavesdropped (or jammed) by means of Radio-Electronic Eavesdropping Attack (REEA). As an anti-eavesdropping and anti-jamming measures, Alice and Bob can use the following strategy: they can select new sub-carriers by changing parameters in $\mathrm{U}_N(\boldsymbol{\theta})$ in the periodical (or in pseudo random) manner

$$\left(\varphi_1^0, \varphi_2^0,..., \varphi_q^0\right) \to \left(\varphi_1^{rT}, \varphi_2^{rT},..., \varphi_q^{rT}\right) = \left(\varphi_1^0 + \Delta\varphi_1^{rT}, \varphi_2^0 + \Delta\varphi_2^{rT},..., \varphi_q^0 + \Delta\varphi_q^{rT}\right),\ r = 0,1,2,...\ ,$$

where $\boldsymbol{\theta}^0 = (\varphi_1^0,...,\varphi_q^0)$ are initial values of parameters at the initial time t_0, T is the period of changing parameters. Theoretical analysis and simulation results prove that the proposed new system has better anti-eavesdropping and anti-jamming performances than the conventional system.

4. References

[1] Liang, X. Security and privacy in mobile social networks: challenges and solutions / X. Liang, K. Zhang, X. Shen, X. Lin // IEEE Wireless Commun. – 2014. – Vol. 21(1). – P. 33-41.

[2] Jorswieck, E. Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing / E. Jorswieck, S. Tomasin, A. Sezgin // Proc. IEEE. – 2015. – Vol. 103(10). – P. 1702-1724.

[3] Zhang, N. Cooperative spectrum access towards secure information transfer for CRNS / N. Zhang, N. Lu, N. Cheng, J.W. Mark, X.S. Shen // IEEE J. Sel. Areas Commun. – 2013. – Vol. 31(11). – P. 2453-2464.

[4] Wyner, A.D. The wiretap channel // Bell Sys. Tech. J. – 1975. – 54(8). – P. 1355-1387.

[5] Renna, F. Physical-layer secrecy for OFDM transmissions over fading channels / F. Renna, N. Laurenti, H.V. Poor // IEEE Trans. Inf. Forens. Security. – 2012. – Vol. 7(4). – P. 1354-1367.

[6] Chorti, A. Faster than Nyquist interference assisted secret communication for OFDM systems / A. Chorti, H.V. Poor // Proceedings of the IEEE Asilomar Conf. Signals, Systems and Comput. – 2011. – P. 183-187.

[7] Wang, X. Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks // IEEE Trans. Inf. Forens. Security. – 2011. – Vol. 6(3). – P. 693-702.

[8] Wang, H.M. Distributed beamforming for physical-layer security of two-way relay networks / H.M. Wang, Q. Yin, X.G. Xia // IEEE Trans. Signal Process. – 2012. – Vol. 60(7). – P. 3532-3545.

[9] Goel, S. Guaranteeing secrecy using artificial noise / S. Goel, R. Negi // IEEE Trans. Wireless Commun. – 2008. – Vol. **7**(6). – P 2180-2189.

[10] Labunets, V. Many-parametric cyclic wavelet transforms. Part 1. The first and second canonical forms / V. Labunets, J. Astola, E. Ostheimer // Proceedings of the 2007 International TICSP Workshop on Spectral Methods and Multirate Signal Processing. – 2007. – P. 111-120.

[11] Labunets, V. Many-parametric cyclic wavelet transforms. Part 2. The third and fourth canonical forms / V. Labunets, J. Astola, E. Ostheimer // Proceedings of the 2007 International TICSP Workshop on Spectral Methods and Multirate Signal Processing. – 2007. – P. 121-132.

[12] Labunets, V. Fast multi-parametric wavelet transforms and packets for image processing / V. Labunets, D. Komarov, E. Ostheimer // CEUR Workshop Proceedings. – 2016. – Vol. 1710. – P.134-145.

[13] Labunets, V.G. Multiparameter Golay, 2-complementary sequences and transforms / V.G. Labunets, V.P. Chasovskikh, E. Ostheimer // Proceedings of the 4th International Youth Conference on Information Technologies and Nanotechnologies. – 2018. – P. 1013-1022.

[14] Labunets, V.G. Multiparameter Golay, m-complementary sequences and transforms / V.G. Labunets, V.P. Chasovskikh, E. Ostheimer // Proceedings of the 4th International Youth Conference on Information Technologies and Nanotechnologies. – 2018. – P. 1005-1012.

[15] Baig, S. Performance comparison of DFT, discrete wavelet packet and wavelet transforms, in an OFDM transceiver for multipath fading channel / S. Baig, F. Rehman, M.J. Mughal // IEEE Communication Magazine. – 2004. – P. 27-35.
[16] Chang, R.W. Synthesis of band limited orthogonal signals for multichannel data transmission // Bell Syst. Tech. J. – 1966. – Vol.45. – P. 1775–1796.
[17] Wornell, G. Emerging applications of multirate signal processing and wavelets in digital communications // Proc. IEEE. – 1966. – Vol. 84. – P. 586-603.
[18] Sandberg, S.D. Overlapped discrete multitone modulation for high-speed copper wire communi-cations / S.D. Sandberg, M.A. Tzannes // IEEE Journal on Sel. Areas in Commun. – 1985. – Vol. 13. – P. 1571-1585.
[19] Halford, K. Complementary code keying for rake-based indoor wireless communication / K. Halford, S. Halford, M. Webster, C. Andren // Proceedings of IEEE International Symposium on Circuits and Systems. – 1999. – P. 427-430.
[20] Golay, M.J.E. Multisplit spectroscopy // J. Opt. Soc. Amer. – 1949. – Vol. 39. – P. 437-444.
[21] Golay, M.J.E. Complementary series // IEEE Trans. Inform. Theory. – 1961. – Vol. 7. – P. 82-87.
[22] Davis J.A. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes / J.A. Davis, J. Jedwab // IEEE Trans. Inform. Theory. – 1999. – Vol. 45. – P. 2397-2417.
[23] Fiedler, F. A framework for the construction of Golay sequences / F. Fiedler, J. Jedwab, M.G. Parker // IEEE Trans. Inform. Theory. – 2008. – Vol. 54. – P. 3114-3129.
[24] Michailow, N. WHT-GFDM for the next generation of wireless networks / N. Michailow, L. Mendes, M. Matthe, I. Festag, A. Fettweis, G. Robust // IEEE Communications Letters. – 2015. – Vol. 19. – P. 106-109.
[25] Xiao, J. Hadamard transform combined with companding transform technique for PAPR reduction in an optical direct-detection OFDM system / J. Xiao, J. Yu, X. Li, Q. Tang, H. Chen, F. Li, Z. Cao, L. Chen // IEEE J. Opt. Commun. Netw. – 2012. – Vol. 4(10). – P. 709-714.
[26] Wang, S. A Walsh-Hadamard coded spectral efficient full frequency diversity OFDM system / S. Wang, S. Zhu, G. Zhang // IEEE Trans. Commun. – 2010. – Vol. 58(1). – P. 28-34.
[27] Wilkinson T.A. Minimization of the peak to mean envelope power ratio of multicarrier transmission schemes by block coding / T.A. Wilkinson, A.E. Jones // Proceedings of the IEEE 45th Vehicular Technology Conf. – 1995. – P. 825-829.
[28] Wilkinson T.A. Combined coding for error control and in creased robustness to system nonlinearities in OFDM / T.A. Wilkinson, A.E. Jones // Proceedings of the IEEE 46th Vehicular Technology Conf. – 1996. – P. 904-908.
[29] Wulich, D. Reduction of peak to mean ratio of multicarrier modulation using cyclic coding // Electron. Lett. – 1996. – Vol. 32. – P. 432-433.

Acknowledgments
This work was supported by the RFBR grant 17-07-00886 and by the Ural State Forest Engineering's Center of Excellence in «Quantum and Classical Information Technologies for Remote Sensing Systems.