Wireless channel noises and data protection

Victor Tsvetov
Samara National Research University
Samara, Russia
tsf-su@mail.ru

***Abstract*—The paper proposes an application of a quadrature amplitude modulation (QAM) scheme using orthogonal frequency division multiplexing (OFDM) transmission for data protection. Our approach bases on the symmetric encryption and uses a natural or induced noise in a wireless channel as a random part of a secret key. The main idea for this is the sensitivity of the signal decoding model to variations of measured values. This kind of protection does not require additional computational costs and does not affect the bit rate of the channel.**

Keywords—QAM OFDM wireless channel, physical layer security, data protection, Ill-conditioned problem

I. Introduction

Contemporary wireless communications are vulnerable to various attacks because of the open nature of radio propagation [1, 2]. One of the main ones is an eavesdropping the content of the transmission [3, 4]. And in consequence, the conventional wireless security mechanisms are cryptographic techniques [5, 6]. Currently, there are a lot of various cryptographic methods to secure the wireless transmissions [7]. Nevertheless, we are trying to design an easy-to-use additional cryptographic tool in this paper. The proposed tool operates at the physical (PHY) layer security of wireless networks [8-11]. PHY layer is the bottom layer of the network and deals with carrier frequency generation, modulation, signal detection etc.

Everyone knows how important it is to generate a truly random encryption key [12-14]. At the same time, everyone knows that natural noises in the wireless channel are random and unpredictable. If we add noises to the encryption protocol, we will improve communication security. To do this, we are taking into account some mathematical features of the digital channel formed using OFDM technology.

OFDM is a promising technique for wideband digital communication. The method it is based on is encoding digital data on multiple carrier frequencies. The basic principle of multicarrier transmission is to translate high rate serial data stream into several slower parallel streams and then modulate it on subcarriers. By reducing the symbol transmission rate in the subcarrier the effect of the delay spread of the multipath channel is also greatly reduced. In addition to that, inter-symbol interference can be also decreased [15-17].

A simple and reliable scheme of modulating subcarriers is provided by QAM. In this case, the amplitudes of two waves of the same frequency, 90° out-of-phase with each other are modulated to represent the multi-leveled digital signal. The number of modulation levels depends on the signal-to-noise ratio (SNR). In practice, it is chosen based on worst-case forecast for each subcarrier.

If we use QAM scheme to modulate subcarriers, the modulation scheme is called QAM OFDM [17, 18].

A mathematical model for generating and decoding QAM OFDM signal is considered, for example, in [19]. It is reduced to the following problem.

At first, we define the set of codes

$$Q_m^N = \{\{Z_N | Z_N^T = \langle z_0, z_1, \dots, z_{N-1}\rangle\} \subset I^N, \qquad (1)$$

where $z_k = x_k + I \cdot y_k$, $(x_k, y_k) \in q_h^m$, $I^2 = -1$, $q_m^h = \{(h \cdot k_1, h \cdot k_2) | k_1, k_2 \in 0, \dots, 2 \cdot m - 1, m \in Z\}$ and the z^T symbol denotes the transpose operation on z.

Then, we map the N-tuple $Z_N \in Q_m^N$ to the signal $s(t) = \sum_{k=0}^{N-1} z_k \cdot e^{\frac{I 2\pi k t}{T}}$ on the interval $[0, T]$, where T is the useful symbol duration. We send $s(t)$ to the channel and we need to extract Z_N from $s(t)$ in the receiver side.

The values T, N, m determine the bit rate of the channel as $C_B = \frac{2N(\log(m)+1)}{T}$ bps. We note that the subcarriers $e^{\frac{I 2\pi k t}{T}} \in L^2(0, T)$ are orthogonal to each other on the interval $[0, T]$. This property allows using the discrete Fourier transform (DFT) to demodulate the signal on the receiver side. Indeed, let us define the set $\left\{t_n = \frac{T}{N} \cdot n\right\}_{n=0}^{N-1}$ and the square matrix $F_{NN} = \left(\varepsilon_N^{kn}\right) = \left(e^{\frac{I 2\pi k n}{N}}\right)$, where $k, n \in 0..N-1$. If we denote $S_N^T = \langle s_0, s_1, .., s_{N-1}\rangle = \langle s(t_0), s(t_1), .., s(t_{N-1})\rangle$ and $Z_N^T = \langle z_0, z_1, .., z_{N-1}\rangle$ then

$$F_{NN} Z_N = S_N, \qquad (2)$$

$$Z_N = \frac{1}{N} F_{NN}^* S_N, \qquad (3)$$

where $F_{NN}^* = \left(\varepsilon_N^{-nk}\right) = \left(e^{\frac{-I 2\pi k n}{N}}\right)$ is a Hermitian transpose of F_{NN}.

It is easy to show that

$$F_{MN} Z_N = S_M^M, \; Z_N = \frac{1}{M} F_{NM}^* S_M^M, \qquad (4)$$

where $F_{MN} = \left(\varepsilon_M^{kn}\right) = \left(e^{\frac{I 2\pi k n}{M}}\right)$, $F_{NM}^* = \left(\varepsilon_M^{-nk}\right) = \left(e^{\frac{-I 2\pi k n}{M}}\right)$, $S_M^{MT} = \langle s_0, s_1, .., s_{M-1}\rangle = \langle s(t_0), s(t_1), .., s(t_{M-1})\rangle$, $t_n = \frac{T}{M} \cdot n$, $n \in 0..M-1$, $k \in 0..N-1$, $M \geq N$.

Now we note that we actually send $s(t)$ to the noisy channel and we need to extract $Z_N \in T^N$ from

Copyright © 2020 for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0)

CEUR-WS.org/Vol-2667/paper51.pdf

$\tilde{s}(t) = s(t) + \delta(t)$ in the receiver side. We assume that $\left\|\delta(t)\right\|_{L^2(0,T)} = \sqrt{\int_0^T \delta^2(t)dt} < \delta$.

We denote $\tilde{S}_N^T = S_N^T + \Delta S_N^T = \left\langle \tilde{s}_0, \tilde{s}_1, .., \tilde{s}_{N-1} \right\rangle$ and $\Delta S_N^T = \left\langle \delta_0, \delta_1, .., \delta_{N-1} \right\rangle = \left\langle \delta(t_0), \delta(t_1), .., \delta(t_{N-1}) \right\rangle$. Let $\tilde{Z}_N$ be a solution of matrix equation

$$F_{NN} \tilde{Z}_N = \tilde{S}_N . \quad (5)$$

It is well known that

$$\frac{\left\|\Delta Z_N\right\|_N}{\left\|Z_N\right\|_N} \le \mu\left(F_{NN}\right) \frac{\left\|\Delta S_N\right\|_N}{\left\|S_N\right\|_N}, \quad (6)$$

where we denote $\left\|\Delta Z_N\right\|_N = \left\|Z_N - \tilde{Z}_N\right\|_N = \frac{1}{N} \cdot \left\|F_{NN}^* \Delta S_N\right\|_N$, $\mu\left(F_{NN}\right) = \frac{1}{N} \cdot \left\|F_{NN}\right\|_{NN} \cdot \left\|F_{NN}^*\right\|_{NN}$, $\left\|F_{NN}\right\|_{NN} = \sup_{Z \in \mathbb{C}^N} \frac{\left\|F_{NN} Z_N\right\|_N}{\left\|Z_N\right\|_N}$ and $\left\|Z_N\right\|_N = \sqrt{\sum_{k=0}^{N-1} \left|z_k\right|^2}$.

If the matrix A_{NN} is invertible, then $\mu\left(A_{NN}\right) = \left\|A_{NN}\right\|_{NN} \cdot \left\|A_{NN}^{-1}\right\|_{NN}$ is called the matrix condition number (in Euclidean norm). $\mu\left(A_{NN}\right)$ is used to measure how sensitive a solution X_N of matrix equation $A_{NN} X_N = B_N$ is to changes or errors in the right-hand-side (RHS) of this equation B_N.

Problems with a low condition numbers are called well-conditioned, while problems with a high condition numbers are called ill-conditioned. An ill-conditioned problem is one where, for a small change in the RHS of an equation there is a large change in the solution.

It is easy to show that $\mu\left(F_{NN}\right) = 1$. If we choose h (see (1)) to correspond with SNR, we can use nearest neighbor search (NNS) to define Z_N from (5) as $Z_N = \arg\min_{Z_N \in Q_m^N} \left\|Z_N - \tilde{Z}_N\right\|_N$.

In the following sections, the QAM OFDM scheme in the wireless noisy channel will be used to protect transmitted data from unauthorized access.

II. Ill-conditioned problem for the QAM OFDM scheme

Let us fix values T, N, m and restrict the signal $s(t) = \sum_{k=0}^{N-1} z_k \cdot e^{\frac{I 2\pi k t}{T}}$ to the interval $[0, T_{MN}] \subseteq [0, T]$, where $T_{MN} = \frac{T \cdot N}{M}$ and $M \ge N$.

Technically, we have constructed a new channel with the useful symbol duration T_{MN} and the bit rate $C_M = \frac{2N\left(\log(m)+1\right)}{T_{MN}} = \frac{2M\left(\log(m)+1\right)}{T} \ge \frac{2N\left(\log(m)+1\right)}{T} = C_B$ bps.

Similar to the previous one, we can define the set $\left\{ t_n = \frac{T}{M} \cdot n \right\}_{n=0}^{N-1}$ and square matrix $F_{NN}^M = \left(\varepsilon_M^{kn}\right) = \left(e^{\frac{I 2\pi kn}{M}}\right)$, where $k, n \in 0..N-1$. If we put $Z_N^T = \left\langle z_0, z_1, .., z_{N-1} \right\rangle$ and $S_N^{MT} = \left\langle s_0^M, s_1^M, .., s_{N-1}^M \right\rangle = \left\langle s(t_0), s(t_1), .., s(t_{N-1}) \right\rangle$ then

$$F_{NN}^M Z_N = S_N^M . \quad (7)$$

Note that $\det\left(F_{NN}^M\right) \ne 0$ for all $M \ge N$ and hence there exists unique solution $Z_N = \left(F_{NN}^M\right)^{-1} S_N^M$ of matrix equation (7) for all RHS.

As before, we are dealing with the noisy channel and we need to extract Z_N from $\tilde{s}(t) = s(t) + \delta(t)$ in the receiver side.

We set $\tilde{S}_N^{MT} = \left\langle \tilde{s}_0^M, \tilde{s}_1^M, .., \tilde{s}_{N-1}^M \right\rangle = \left\langle \tilde{s}(t_0), \tilde{s}(t_1), .., \tilde{s}(t_{N-1}) \right\rangle$ and try to find Z_N by solution of the matrix equation

$$F_{NN}^M \tilde{Z}_N = \tilde{S}_N^M . \quad (8)$$

This problem is complicated by the fact that, if $M \in N$ it becomes ill-conditioned. Calculations have shown that the condition number $\mu\left(F_{NN}^M\right)$ depends exponentially on M. For example, if $N = 16$ then $\mu\left(F_{NN}^{N+s}\right) \approx e^{5.4 \cdot s + 7.8}$, and if $N = 32$ then $\mu\left(F_{NN}^{N+s}\right) \approx e^{11.1 \cdot s + 16.6}$, were $s \in 1..2 \cdot N$. Because of this, small values of $\left\|\delta(t)\right\|_{L^2(0,T_{MN})} < \delta$ leads to large differences between the solutions of (7) and (8), and so we cannot use NNS to define Z_N by $\tilde{Z}_N$.

For example, $\frac{\left\|\left(F_{16,16}^{32}\right)^{-1} \Delta S_{16}^{32}\right\|_{16}}{\left\|\Delta S_{16}^{32}\right\|_{16}} \approx 10^6$, where $\Delta S_{16}^{32} = \left\langle \delta_0^{32}, \delta_1^{32}, .., \delta_{15}^{32} \right\rangle = \left\langle \delta(t_0), \delta(t_1), .., \delta(t_{15}) \right\rangle$ and the norm value $\left\|\Delta S_{16}^{32}\right\|_{16}$ is less then $\frac{h}{2}$.

We should apply regularization in case we want to extract Z_N from noisy signal $\tilde{s}(t) \in L^2(0, T_{MN})$, but on the other hand, we can use a noise to disguise the transmission of Z_N.

If $M > N$ then the subcarriers $e^{\frac{I 2\pi k t}{T}} \in L^2(0, T_{MN})$ are not orthogonal to each other on the interval $[0, T_{MN}]$, so the QAM OFDM scheme becomes the QAM FDM scheme.

III. Well-conditioned problem for a QAM FDM scheme and a secret key

Let us set $N = 2 \cdot N_0$ and $M = 2 \cdot N$. Note that now the bit rate of the QAM FDM channel is $C_M = \frac{2N\left(\log(m)+1\right)}{T_{MN}} = \frac{4N\left(\log(m)+1\right)}{T} = 2 \cdot C_B$ bps.

In this section we are going to reduce the ill-conditioned problem (7), (8) with matrix F_{NN}^M to the well-conditioned one in the subspace $M^{N_0} \subset N^N$.

First of all we define a submatrix $F^1_{N_0N_0}$ of the matrix F^M_{NN}, which is obtained by deleting all odd rows and all odd columns. In this case $F^1_{N_0N_0} = \left(\varepsilon_{4N_0}^{(2k)\cdot(2n)}\right) = \left(\varepsilon_{N_0}^{kn}\right) = \left(e^{\frac{I2\pi kn}{N_0}}\right)$, $\det\left(F^1_{N_0N_0}\right) \neq 0$, $\left(F^1_{N_0N_0}\right)^{-1} = \frac{1}{N_0}\left(\varepsilon_{N_0}^{-nk}\right)$ and $\mu\left(F^1_{N_0N_0}\right) = 1$, where $k,n \in 0..N_0-1$.

Then we define a submatrix $F^2_{N_0N_0}$ of the matrix F^M_{NN}, which is obtained by deleting all odd rows and all even columns. It is obvious that $F^2_{N_0N_0} = \left(\varepsilon_{4N_0}^{(2k+1)\cdot(2n)}\right) = \left(\varepsilon_{N_0}^{kn}\cdot\varepsilon_{2N_0}^{n}\right)$, because $e^{\frac{I2\pi(2k+1)n}{2N_0}} = e^{\frac{I2\pi kn}{N_0}}\cdot e^{\frac{I2\pi n}{2N_0}}$. Note that $\det\left(F^2_{N_0N_0}\right) \neq 0$, $\left(F^2_{N_0N_0}\right)^{-1} = \frac{1}{N_0}\left(\varepsilon_{N_0}^{-nk}\cdot\varepsilon_{2N_0}^{-k}\right)$ and $\mu\left(F^2_{N_0N_0}\right) = 1$, where $k,n \in 0..N_0-1$.

And at last we can set a secret key $\Gamma_N^0 = \langle 0,\gamma_0,0,\gamma_1,\ldots,0,\gamma_{N_0-1}\rangle \in Z^N = Z^{2N_0}$ for the sender and receiver sides, and a code $Z_N^0 = \left\langle z_0,0,z_1,0,\ldots,z_{N_0-1},0\right\rangle$.

Now we are ready to define a combination $Z_N^+ = Z_N^0 + \Gamma_N^0 = \left\langle z_0,\gamma_0,z_1,\gamma_1,\ldots,z_{N_0-1},\gamma_{N_0-1}\right\rangle$ and rewrite (8) in the form

$$F^M_{NN}Z_N^+ + \Delta S_N^M = F^M_{NN}Z_N^0 + F^M_{NN}\Gamma_N^0 + \Delta S_N^M = \tilde{S}_N^M, \quad (9)$$

where $\Delta S_N^M = \left\langle \delta_0^M,\delta_1^M,\ldots,\delta_{N-1}^M\right\rangle$.

We denote $\tilde{S}_N^0 = \left\langle s_0^0,s_1^0,\ldots,s_{N-1}^0\right\rangle = \tilde{S}_N^M - F^M_{NN}\Gamma_N^0$ and obtain

$$F^M_{NN}Z_N^0 + \Delta S_N^M = \tilde{S}_N^0. \quad (10)$$

Seeing that $Z_N^0 = \left\langle z_0,0,z_1,0,\ldots,z_{N_0-1},0\right\rangle$, we can write

$$F^M_{NN_0}Z_{N_0}^0 + \Delta S_N^M = \tilde{S}_N^0, \quad (11)$$

where $F^M_{NN_0}$ is a submatrix of the matrix F^M_{NN}, which is obtained by deleting all odd rows, and $Z_{N_0}^0 = \langle z_0,z_1,\ldots,z_{N_0-1}\rangle \in K^{N_0}$. Note that for all $K \in 1..N$ the following matrix equalities take place

$$F^M_{KN_0}Z_{N_0}^0 + \Delta S_K^M = \tilde{S}_K^0, \quad (12)$$

where $\Delta S_K^M = \left\langle \delta_0^M,\delta_1^M,\ldots,\delta_{K-1}^M\right\rangle$ and $S_K^0 = \left\langle s_0^0,s_1^0,\ldots,s_{K-1}^0\right\rangle$. If we set $K = N_0$ in (12) and take into account that $F^1_{N_0N_0} = \left(e^{\frac{I2\pi kn}{N_0}}\right)$, we obtain

$$F^1_{N_0N_0}Z_{N_0}^0 + \Delta S_{N_0}^M = \tilde{S}_{N_0}^0, \quad (13)$$

where $\tilde{S}_{N_0}^0 = \tilde{S}_{N_0}^M - F^2_{N_0N_0}\Gamma_{N_0}^0$, $\Gamma_{N_0}^0 = \langle\gamma_0,\gamma_1,\ldots,\gamma_{N_0-1}\rangle \in \check{Z}^{N_0}$.

Let $\tilde{Z}_{N_0}^0$ be a unique solution of the matrix equation

$$F^1_{N_0N_0}\tilde{Z}_{N_0}^0 = \tilde{S}_{N_0}^0, \quad (14)$$

therefore,

$$\frac{\left\|Z_{N_0}^0 - \tilde{Z}_{N_0}^0\right\|_{N_0}}{\left\|Z_{N_0}^0\right\|_{N_0}} \le \mu\left(F^1_{N_0N_0}\right)\frac{\left\|\Delta S_{N_0}^M\right\|_{N_0}}{\left\|S_{N_0}^M\right\|_{N_0}} = \frac{\left\|\Delta S_{N_0}^M\right\|_{N_0}}{\left\|S_{N_0}^M\right\|_{N_0}}, \quad (15)$$

where $\left\|\Delta S_{N_0}^M\right\|_{N_0} \le \left\|\Delta S_N^M\right\|_N$.

And now we are ready to use NNS to define $Z_{N_0}^0$, and therefore, Z_N, as $Z_{N_0}^0 = \underset{Z_{N_0}^0 \oplus \Gamma_{N_0}^0 \in Q_m^N}{\arg\min}\left\|Z_{N_0}^0 - \tilde{Z}_{N_0}^0\right\|_{N_0}$, where $Z_{N_0}^0 \oplus \Gamma_{N_0}^0 = Z_N^+ = Z_N^0 + \Gamma_N^0$.

Let us call the scheme discussed above the QAM FDM NSK (noisy secret key) scheme.

Note that now the bit rate of this QAM FDM NSK channel is equal to the bit rate of QAM OFDM channel, i.e. $C_M^0 = \frac{2N_0(\log(m)+1)}{T_{MN}} = \frac{4N_0(\log(m)+1)}{T} = \frac{2N(\log(m)+1)}{T} = C_B$ bps. At the same time, it is very difficult to extract $Z_{N_0}^0$ from a high SNR channel without the secret key $\Gamma_{N_0}^0$, even with regularization.

This results can be generalized to the cases where $N = m\cdot N_0$ and $M = m\cdot N$. If $N_0 = 2^k$ then we can use radix-2 fast Fourier transform (FFT) to demodulate the signal on the receiver side.

IV. Conclusion

In this paper we have configured a QAM OFDM modulation scheme for data protection in wireless noisy channel. Our approach is based on symmetric cryptography and uses composite secret key. The regular part of the key is used to modulate odd subcarriers. Natural or induced noise in the wireless channel is used as a random part of the key. This scheme is very sensitive to signal variations without knowing the regular part of the secret key. We called this scheme QAM FDM NSK.

Note that after syncing the QAM FDM NSK session, similar secret keys can be generated along with encoding and decoding in the sender and receiver sides.

The QAM FDM NSK scheme does not affect the bit rate of the channel and does not require extra computations to decode the transmitted data. It can be customized for using radix-2 FFT algorithm in its calculations.

Following by [20], we could adapt the QAM FDM NSK scheme to discrete orthogonal transforms associated with some recursive self-similar processes, regardless of the transmission medium. For example, we could customize this tool for visible light communications (VLC) [21-25] or underwater wireless communications (UWC) [26-28].

References

[1] R.K. Nichols and P.C. Lekkas, “Wireless Security: Models, Threats, and Solutions,” New York, NY: McGraw-Hill, 2002.

[2] H.K. Kalita and A. Kar, “Wireless sensor network security analysis,” International Journal of Next-Generation Networks (IJNGN), vol. 1, pp. 1-10, 2009.

[3] V. Aggarwal, L. Sankar, A. Calderbank and H. Poor, “Secrecy capacity of a class of orthogonal relay eavesdropper channels,” Information Theory and Applications Workshop, pp. 295-300, 2009.

[4] J. Vilela, J.B.M. Bloch and S. McLaughlin, “Wireless secrecy regions with friendly jamming,” IEEE Transactions on Information Forensics and Security, vol. 1.6, no. 2, pp. 256-266, 2011.

[5] M. Hell, T. Johansson and W. Meier, “Grain: a stream cipher for constrained environments,” International Journal of Wireless and Mobile Computing (IJWMC), vol. 2, no. 1, pp. 86-93, 2007.

[6] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J.B. Robshaw, Y. Seurin and C. Vikkelsoe, “An ultra-lightweight block cipher,” Proc. 9th International Workshop on Cryptographic Hardware and Embedded Systems, Vienna, Austria, LNCS 4727, pp. 450-466, 2007.

[7] N. Sklavos and X. Zhang, “Wireless Security and Cryptography: Specifications and Implementations,” Taylor & Francis, 2007.

[8] F. Meucci, S.A. Wardana and N.R. Prasad, “Secure physical layer using dynamic permutations in cognitive OFDMA systems,” Proceedings of the IEEE 69th Vehicular Technology Conference, Barcelona, Spain, pp. 1-5, 2009.

[9] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang and H.-H. Chen, “Physical layer security in wireless networks: a tutorial,” IEEE Wireless Communications, vol. 18, no. 2, pp. 66-74, 2011.

[10] R. Bassily, E. Ekrem, X. He, “Cooperative security at the physical layer: a summary of recent advances,” IEEE Signal Processing Magazine, vol. 30, no. 5, pp. 16-28, 2013.

[11] O. Cepheli and G.K. Kurt, “Efficient PHY layer security in MIMO-OFDM: spatiotemporal selective artificial noise,” Proceedings of the IEEE 14th International Symposium on a World of Wireless, Mobile and Multimedia Networks, Madrid, Spain, pp. 1-6, 2013.

[12] D. May, H. Muller and N. Smart, “Random register renaming to foil DPA,” Proceedings of the 3rd International Workshop on Cryptographic Hardware and Embedded Systems of Lecture Notes in Computer Science, vol. 2162 pp. 28-38, 2001.

[13] E. Oswald and M. Aigner, “Randomized addition–subtraction chains as a countermeasure against power attacks,” Proceedings of the 3rd International Workshop on Cryptograpic Hardware and Embedded Systems of Lecture Notes in Computer Science, vol. 2162, pp. 39-50, 2001.

[14] J.C. Ha and S.J. Moon,. “Randomized signed-scalar multiplication of ECC to resist power attacks,” Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems of LectureNotes in Computer Science, vol. 2523, pp. 129-143, 2002.

[15] A. Bahai, B. Saltzberg and M. Ergen, “Multi-Carrier Digital Communications: Theory and Publications of OFDM,” New York, NY, USA: Springer, 2004.

[16] A. Goldsmith, “Wireless Communications,” Cambridge, MA, USA: Cambridge University Press, 2005.

[17] L. Hanzo, W. Webb and T. Keller, “Single- and Multi-carrier Quadrature Amplitude Modulation,” New York, NY, USA: Wiley, 2000.

[18] G.I. Leonovich, A.I. Danilin, V.V. Sergeev, V.P. Tsvetov and S.V. Kupriyanov, “Promising areas for the development of wireless sensor networks,” Proc. Actual Problems of Radioelectronics and Telecommun. Nat. Rus. Conf., Samara, Russia, pp. 8-11, 2019.

[19] V.P. Tsvetov, “On a problem of decoding symbols from incomplete data set transmitted via radio channel,” Proc. 3rd ITNT Int. Conf., Samara, Russia, pp. 954-957, 2017.

[20] V.M.Chernov, “Discrete orthogonal transforms with bases generated by self-similar sequences,” Computer Optics, vol. 42, no. 5, pp. 904-911, 2018. DOI: 10.18287/2412-6179-2018-42-5-904-911.

[21] J. Kim and H. Park, “A coding scheme for visible light communication with wide dimming range,” IEEE Photon. Technol. Lett., vol. 26, no. 5, pp. 465-468, 2014.

[22] R.X.G. Ferreira, E. Xie, J.J.D. McKendry, S. Rajbhandari, H. Chun, G. Faulkner, S. Watson, A.E. Kelly, E. Gu, R.V. Penty, I.H. White, D.C. O’Brien and M.D. Dawson, “High bandwidth gan-based microleds for multi-gb/s visible light communications,” IEEE Photon. Technol. Lett., vol. 28, no. 19, pp. 2023-2026, 2016.

[23] H. Marshoud, P.C. Sofotasios, S. Muhaidat and G.K. Karagiannidis, “Multi-user techniques in visible light communications: A survey,” Int. Conf. on Adv. Commun. Sys. and Info. Sec., (ACOSIS), pp. 1-6, 2016.

[24] H. Haas, L. Yin, Y. Wang and C. Chen, “What is LiFi?” J. Lightwave Technol., vol. 34, no. 6, pp. 1533-1544, 2016.

[25] H. Sifaou, A. Kammoun, K.H. Park and M.S. Alouini, “Robust transceivers design for multi-stream multi-user mimo visible light communication,” IEEE Access, vol. 5, pp. 387-399, 2017.

[26] J. Heidemann, W. Ye, J. Wills, A. Syed and Y. Li, “Research challenges and applications for underwater sensor networking,” IEEE Wireless Commun. and Netw. Conf., (WCNC), vol. 1, no. 1, pp. 228-235, 2006.

[27] N. Chirdchoo, W.S. Soh and K.C. Chua, “Sector-based routing with destination location prediction for underwater mobile networks,” Int. Conf. on Adv. Info. Netw. and App. Workshops, pp. 1148-1153, 2009.

[28] A. Vavoulas, H.G. Sandalidis and D. Varoutas, “Underwater optical wireless networks: A k-connectivity analysis,” IEEE J. Ocean. Eng., vol. 39, no. 4, pp. 801-809, 2014.