International Journal of Engineering

Journal Homepage: www.ije.ir

Secrecy of Communications in Data Transmission by Impulses with Unknown Moments of Appearance and Disappearance

O. V. Chernoyarov[a,b,c], M. M. Shahmoradian*[c], M. Marcokova[d], Y. E. Korchagin[e]

[a] *International Laboratory of Statistics of Stochastic Processes and Quantitative Finance, National Research Tomsk State University, Tomsk, Russia*
[b] *Department of Higher Mathematics and System Analysis, Faculty of Electrical Engineering and Economics, Maikop State Technological University, Maikop, Russia*
[c] *Department of Electronics and Nanoelectronics, Faculty of Electrical Engineering, National Research University "MPEI", Moscow, Russia*
[d] *Department of Structural Mechanics and Applied Mathematics, Faculty of Civil Engineering, University of Zilina, Slovak Republic*
[e] *Department of Radio Physics, Faculty of Physics, Voronezh State University, Voronezh, Russia*

P A P E R I N F O

Paper history:
Received 07 October 2018
Received in revised form 17 February 2019
Accepted 07 March 2019

Keywords:
Rectangular Impulse
Signal Detection
Authorized Access
Unauthorized Access
Threshold Signal-to Noise Ratio
Error Probabilities

A B S T R A C T

We carried out a comparative analysis of the algorithms for detecting a rectangular impulse against Gaussian white noise under either authorized or unauthorized access to the transmitted data. We presupposed that for data transmission the binary communication system is used and that the useful information in the data is whether the signal is present or absent. The case is that unauthorized access by the outsider takes place in the situation when the signal parameters are completely or partially unknown. We then define the degree of the transmitted data secrecy by the secrecy ratio determining how highly the threshold signal-to-noise ratio increases when there is the unauthorized access instead of the authorized one.

***doi**: 10.5829/ije.2019.32.04a.12*

1. INTRODUCTION

At present, one of the main objectives is to protect transmitted and stored information from the unauthorized access [1-3]. As information signals, the ones are often used that take the form of [4-6]

$$s(t,\kappa_0,\chi_0)=\begin{cases} a\,, & \kappa_0 \le t \le \chi_0\,, \\ 0\,, & t<\kappa_0\,,\ t>\chi_0\,. \end{cases} \quad (1)$$

Here the designations are: a is the signal amplitude, κ_0 and χ_0 are the moments of signal appearance and disappearance which can receive the values from the prior intervals

$$\kappa_0 \in [\kappa_{\min},\kappa_{\max}], \quad \chi_0 \in [\chi_{\min},\chi_{\max}],\ \kappa_{\max} < \chi_{\min}\,. \quad (2)$$

Let the signal (1) is transmitted through the communication channel in which the additive Gaussian white noise $n(t)$ takes place with the one-sided spectral density N_0. In this case, the message addressee knows both the signal parameters and the noise statistical characteristics. The useful information is the presence or the absence of the signal (1) and that the binary data communication system has been used. To implement the unauthorized access to the transmitted data in order to use or to destroy it, the outsider should be positive about the signal presence, that is he needs to detect it. This unauthorized access for the outsider is possible even when he/she is completely or partially unaware of the signal parameters and when these parameters are to be determined by the realization of the observable data.

Further in our paper, we present the comparative analysis of the algorithms for detecting the signal (1) against Gaussian white noise in cases of either the

*Corresponding Author Email: *mehdi_shahmoradian@yahoo.com* (M. M. Shahmoradian)

Please cite this article as: O. V. Chernoyarov, M. M. Shahmoradian, M. Marcokova, Y. E. Korchagin, The Secrecy of Communications in the Data Transmission by the Impulses with the Unknown Moments of Appearance and Disappearance, International Journal of Engineering (IJE), IJE TRANSACTIONS A: Basics Vol. 32, No. 4, (April 2019) ... 548-554

authorized or the unauthorized access to the transmitted data. For the comparison of the threshold values of the signal-to-noise ratio (SNR) under the authorized and the unauthorized access, the secrecy parameter is introduced. This parameter allows us to quantify the degree of the transmitted data secrecy.

2. SIGNAL DETECTION IN AUTHORIZED ACCESS

We formulate the signal detection problem in terms of the statistical hypotheses testing [5, 6]. Namely, the hypothesis H_0: $x(t)=n(t)$ stating that the signal (1) is absent in the analyzable realization has to be tested against its simple alternative – H_1: $x(t)=s(t,\kappa_0,\chi_0)+n(t)$ claiming that the signal is present in the observations.

In order to synthesize the detector, we apply the statistical-decision theory approach [5, 6]. According to this approach, the algorithm for detecting the signal (1) should form the logarithm of the functional of the likelihood ratio (FLR) having the form of [5, 6]

$$L_0 = L(\kappa_0,\chi_0)=\frac{2a}{N_0}\int_{\kappa_0}^{\chi_0}\left[\,x(t)-a/2\,\right]\mathrm{d}t \tag{3}$$

and then compare it with the threshold c determined by the selected optimality criterion. The decision on the signal presence is made when the threshold is exceeded, that is when $L_0 > c$.

The type I (false alarm) and the type II (signal missing) error probabilities, that are designated as α_0 and β_0 respectively, are found in literature [7]:

$$\begin{aligned}\alpha_0 &= 1-\Phi\left(c/z_{\max}\nu_0 + z_{\max}\nu_0/2\right),\\ \beta_0 &= \Phi\left(c/z_{\max}\nu_0 - z_{\max}\nu_0/2\right).\end{aligned} \tag{4}$$

Here $z_{\max}^2 = 2a^2T_{\max}/N_0$ is the maximum possible SNR; $T_{\max}=\chi_{\max}-\kappa_{\min}$ is the maximum possible signal duration; $\nu_0=\sqrt{\mu_\kappa+\mu_\chi+1/k}$; $\mu_\kappa=(\kappa_{\max}-\kappa_0)/T_{\max}$; $\mu_\chi=(\chi_0-\chi_{\min})/T_{\max}$; $k=T_{\max}/T_{\min}$; $\Phi(x)=\int_{-\infty}^{x}\exp\left(-t^2/2\right)\,\mathrm{d}t\big/\sqrt{2\pi}$ is the probability integral.

We characterize the detection quality by the threshold SNR $z_{0t}(p)$ which provides the set level of the false alarm and the signal missing probabilities: $\alpha_0(c,z_{0t})=\beta_0(c,z_{0t})=p$, that is, $z_{0t}(p)$ is the solution for the combined equations:

$$\begin{cases}\alpha_0(c,z_{0t})=p\,,\\ \beta_0(c,z_{0t})=p\,.\end{cases} \tag{5}$$

By applying the formula (4), we determine the threshold c from the first equation of the system (5):

$$c = z_{0t}\nu_0\,\mathrm{arc}\Phi(1-p) - z_{0t}^2\nu_0/2\,, \tag{6}$$

where $\mathrm{arc}\Phi(x)$ is the inverse function to the probability integral. By substituting the expression (6) into the second equation of the system (5) and then solving it, we get the threshold SNR in the form of

$$z_{0t} = 2\,\mathrm{arc}\Phi(1-p)/\nu_0\,, \tag{7}$$

if $p<1/2$.

3. THE QUASI-LIKELIHOOD DETECTION ALGORITHM UNDER THE UNAUTHORIZED ACCESS

We now consider the signal (1) detection efficiency for the outsider who does not know the moments of appearance and disappearance κ_0 and χ_0. Then hypothesis H_0: $x(t)=n(t)$ should to be tested against the composite alternative H_1: $x(t)=s(t,\kappa_0,\chi_0)+n(t)$. When the moments of signal appearance and disappearance, designated as κ_0 and χ_0, respectively, are unknown, the simplest way of carrying out the unauthorized access to the transmitted data is the application of the quasi-likelihood [8, 9] detection algorithm. In this case, the detector generates the logarithm of FLR (3) for some expected (predictable) moments of κ^* and χ^*:

$$L^* = L\left(\kappa^*,\chi^*\right) \tag{8}$$

and then compares it with the threshold c. The decision on the signal presence is made, if $L^*>c$. In Figure 1, the block diagram of such detector is presented. Here the switch S is closed during the time interval $\left[\kappa^*,\chi^*\right]$ while the rest of the time it is open. The switch S and the integrator I selected by the dashed line we will refer to as the switched integrator (SI). The resolver RS compares the logarithm of FLR L^* formed at the SI output with the threshold c and then makes the decision in favor of one of the hypotheses.

The type I (false alarm) and type II (signal missing) error probabilities α_q and β_q are determined by the following expressions:

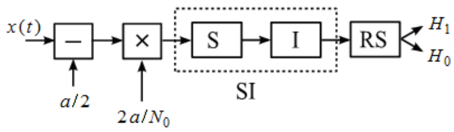

Figure 1. Block diagram of the quasi-likelihood detector

$$\alpha_q = P\left[L^* > c \middle| H_0\right] = 1 - F\left(c \middle| H_0\right), \tag{9}$$

$$\beta_q = P\left[L^* < c \middle| H_1\right] = F\left(c \middle| H_1\right), \tag{10}$$

where $F\left(x \middle| H_j\right) = P\left[L^* < x \middle| H_j\right]$, $j = 0,1$ is the distribution function of the random value L^* under the hypothesis H_j. According to relations (3) and (8), the value L^* is formed as the linear transformation of the Gaussian random process $x(t)$ and therefore it is itself Gaussian. For full statistical description of L^* determined in Equation (8), finding its mathematical expectation and dispersion under both hypotheses will suffice. By averaging Equation (8) over all the observable realizations $x(t)$ under the fixed values κ_0 and χ_0 we get following expressions:

$$m_0 = \left\langle L^* \middle| H_0 \right\rangle = -z_{\max}^2 \left(\mu_k + \mu_\chi + \frac{1}{k}\right) \frac{1 - \delta\kappa + \delta\chi}{2}, \tag{11}$$

$$m_1 = \left\langle L^* \middle| H_1 \right\rangle = z_{\max}^2 \left(\mu_k + \mu_\chi + \frac{1}{k}\right) \frac{1 - |\delta\kappa| - |\delta\chi|}{2}, \tag{12}$$

$$D = \left\langle \left(L^* - \left\langle L^* \right\rangle\right)^2 \middle| H_{0,1} \right\rangle = z_{\max}^2 \left(\mu_k + \mu_\chi + \frac{1}{k}\right) \left(1 - \delta\kappa + \delta\chi\right), \tag{13}$$

where $\delta\kappa = \left(\kappa^* - \kappa_0\right) / \left(\chi_0 - \kappa_0\right)$, $\delta\chi = \left(\chi^* - \chi_0\right) / \left(\chi_0 - \kappa_0\right)$.

The application of Equations (11)-(13) enables us to write the distribution function of the Gaussian random variable L^* in the form of

$$F\left(x \middle| H_j\right) = \Phi\left[\left(x - m_j\right) / \sqrt{D}\right]. \tag{14}$$

We then substitute the function (14) into the expressions (9), (10) and, based on Equations (11)-(13), present the detection error probabilities as follows:

$$\begin{aligned} &\alpha_q = 1 - \Phi\left(c / z_{\max}\nu_q + z_{\max}\nu_q / 2\right), \\ &\beta_q = \Phi\left(c / z_{\max}\nu_q - z_{\max}\nu_q \Delta / 2\right). \end{aligned} \tag{15}$$

where $\nu_q = \sqrt{\left(\mu_\kappa + \mu_\chi + 1/k\right)\left(1 + \delta\chi - \delta\kappa\right)}$, $\Delta = \left(1 - |\delta\chi| - |\delta\kappa|\right) / \left(1 + \delta\chi - \delta\kappa\right)$.

We characterize the quality of detection by the threshold SNR $z_{qt}(p)$ providing the set level of the error probabilities: $\alpha_q\left(c, z_{qt}\right) = \beta_q\left(c, z_{qt}\right) = p$ and therefore serving as a solution of the combined equations:

$$\begin{cases} \alpha_q\left(c, z_{qt}\right) = p, \\ \beta_q\left(c, z_{qt}\right) = p. \end{cases} \tag{16}$$

Through determining the threshold $c = z_{qt}\nu_q \operatorname{arc}\Phi(1-p) - z_{qt}^2 \nu_q / 2$ from the first Equation (16) and substituting it into the second Equation (16), we find the threshold SNR z_{qt} in the form of

$$z_{qt} = \frac{4\left(1 + \delta\chi - \delta\kappa\right) \operatorname{arc}\Phi(1-p)}{\nu_q\left(2 + \delta\chi - \delta\kappa - |\delta\kappa| - |\delta\chi|\right)}. \tag{17}$$

The degree of the signal (1) secrecy is quantitatively described by means of the ratio

$$\varphi = z_t / z_{0t}, \tag{18}$$

where z_t is the threshold SNR under the unauthorized access to the transmitted data. If the outsider applies the quasi-likelihood detector, then the secrecy parameter (18) will take the form of

$$\varphi_q = \frac{z_{qt}}{z_{0t}} = \frac{2\sqrt{1 + \delta\chi - \delta\kappa}}{2 + \delta\chi - \delta\kappa - |\delta\kappa| - |\delta\chi|}. \tag{19}$$

Now let the true moments of appearance and disappearance are located in the middle of their prior intervals of the possible values (2), that is, $\kappa_0 = \left(\kappa_{\min} + \kappa_{\max}\right)/2$, $\chi_0 = \left(\chi_{\min} + \chi_{\max}\right)/2$. Since the expected moments of appearance and disappearance also belong to the specified intervals, the following conditions are satisfied:

$$|\delta\kappa| \le k\eta_\kappa / (k+1), \quad |\delta\chi| \le k\eta_\chi / (k+1). \tag{20}$$

Here $\eta_\kappa = \left(\kappa_{\max} - \kappa_{\min}\right)/T_{\max}$, $\eta_\chi = \left(\chi_{\max} - \chi_{\min}\right)/T_{\max}$ are the normalized lengths of the prior intervals of the possible values that the moments of appearance and disappearance of the signal (1) may accept. We presuppose that the intervals (2) are of the same length – $\eta_\kappa = \eta_\chi = (k-1)/2k$, and thus we get $|\delta\kappa| \le (k-1)/2(k+1)$, $|\delta\chi| \le (k-1)/2(k+1)$.

In Figures 2 and 3, the dependences are presented of the secrecy parameter φ_q (19) upon $\delta\kappa$ under the fixed $\delta\chi$ and upon $\delta\chi$ under the fixed $\delta\kappa$, correspondingly. All the curves are calculated for $k = 50$ so that $|\delta\kappa| \le 0.5$, $|\delta\chi| \le 0.5$.

As we can see from Figures 2 and 3, the maximum detection efficiency is achieved, if the expected and the true values of the moments of appearance and disappearance coincide. In case they differ and this difference increases, the information transmission secrecy increases too.

It should be noted that the positive values of $\delta\kappa$ and the negative values of $\delta\chi$ result in that the duration of the reference signal is less than the duration of the received signal. Therefore, some part of the received signal energy is lost and it is not involved in the formation of the decision statistics. If the duration of the reference signal is greater than the duration of the received signal, then the excess noise segment is integrated during the decisive statistics forming.

As it follows from Figures 2 and 3, the received signal energy loss is a more important disadvantage in comparison with the entrapping of the excess noise.

Let the expected moments of appearance and disappearance are situated in the middle of the prior intervals (2), that is $\kappa^* = (\kappa_{\min} + \kappa_{\max})/2$, $\chi^* = (\chi_{\min} + \chi_{\max})/2$. Then the detunings $\delta\kappa$ and $\delta\chi$ can be rewritten in the form of

$$\begin{aligned} \delta\kappa &= (2\mu_\kappa - \eta_\kappa)\big/2(\mu_\kappa + \mu_\chi + 1/k), \\ \delta\chi &= -(2\mu_\chi - \eta_\chi)\big/2(\mu_\kappa + \mu_\chi + 1/k). \end{aligned} \tag{21}$$

Assuming that the lengths of the prior intervals (2) are equal $\eta_\kappa = \eta_\chi = (k-1)/2k$, we can get the following expressions for the secrecy parameter (19):

– if the received signal duration is minimum, then $\varphi_q = \sqrt{(k+1)/2}$,

– if the received signal duration is maximum, then $\varphi_q = \sqrt{2k/(k+1)}$,

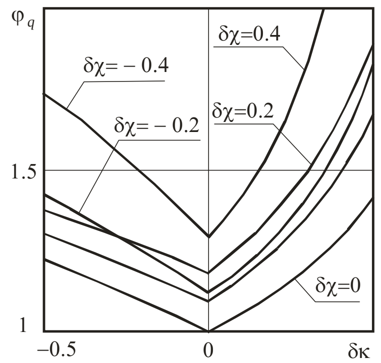

Figure 2. The dependences of the secrecy parameter upon the detuning of the moment of appearance

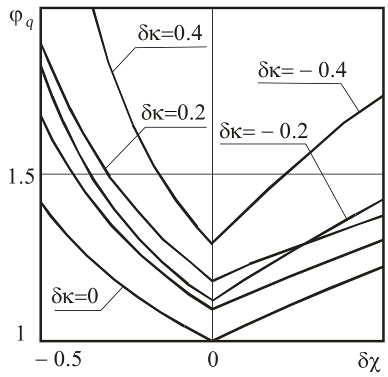

Figure 3. The dependences of the secrecy parameter upon the detuning of the moment of disappearance

– if $\kappa_0 = \kappa_{\min}$, $\chi_0 = \chi_{\min}$ or $\kappa_0 = \kappa_{\max}$, $\chi_0 = \chi_{\max}$, then $\varphi_q = 2(k+1)/(k+3)$.

In Figure 4, by solid lines, the dependences are drawn of the secrecy parameter φ_q (19) upon k. Curve 1 corresponds to the minimum duration of the received signal, curve 2 – to the maximum duration of the received signal, curve 3 – to $\kappa_0 = \kappa_{\min}$, $\chi_0 = \chi_{\min}$ or $\kappa_0 = \kappa_{\max}$, $\chi_0 = \chi_{\max}$.

As it follows from Figures 2-4, when the detunings of the expected moments of appearance and disappearance relative to their true values are great enough, the detection efficiency may be insufficient while the level of the transmission secrecy is rather high.

4. ADAPTIVE DETECTION ALGORITHM UNDER UNAUTHORIZED ACCESS

In order to increase the efficiency of the interception detection, we consider the implementation of the unauthorized access to the transmitted data by applying the adaptive (using the maximum likelihood method) detector [5, 6]. As in the text above, the hypothesis H_0: $x(t) = n(t)$ has to be tested against its more complex alternative H_1: $x(t) = s(t, \kappa_0, \chi_0) + n(t)$. According to the adaptive approach, the receiver generates the logarithm of FLR (3) for all the possible values of the moments of appearance and disappearance (2), then searches its absolute (greatest) maximum $L = \sup L(\kappa, \chi)$ and, finally, compares it with the threshold c. If the threshold is exceeded, then the decision on the signal presence is made.

In order to define the optimal structure of the adaptive detector, we rewrite the logarithm of FLR (3) in the form of [5, 6]

$$\begin{aligned} L(\kappa,\chi) &= \frac{2a}{N_0}\int_{\kappa}^{t_0} \left[\, x(t) - a/2 \,\right] dt + \\ &+ \frac{2a}{N_0}\int_{t_0}^{\kappa} \left[\, x(t) - a/2 \,\right] dt . \end{aligned} \tag{22}$$

where t_0 is the point belonging to the interval $(\kappa_{\max}, \chi_{\min})$. Then the specified detector can be implemented, as it is shown in the block diagram presented in Figure 5. Here the switched integrators SI1 and SI2 operate over the time intervals $[t_0, \chi_{\max}]$ and $[\kappa_{\min}, t_0]$, respectively. The delay line DL delays the input signal at the time interval $(t_0 - \kappa_{\min})$. The switches S are closed at the point $t = \chi_{\max}$. The resolver RS compares the sum of the output signals of the peak detectors with the threshold c and then makes a decision on the information signal presence under the exceeded threshold c.

The probabilities of false alarm and signal missing – α_m and β_m, respectively – that are operating characteristics of the adaptive detector can be calculated by the formulas (9) and (10) where $F(x|H_j)$ refers to the distribution function of the absolute maximum of the random field (22). By applying the results obtained in literature [10, 11], for the specified detection error probabilities we get:

$$\alpha_m = 1 - \frac{1}{\eta\sqrt{2\pi}} \int_0^\infty \int_0^\infty \left[\Phi\left(\frac{z_{\max}\sqrt{\eta_\kappa}}{2} + \frac{\xi_1}{\sqrt{\eta_\kappa}} \right) - \exp(-\xi_1 z_{\max}) \Phi\left(\frac{z_{\max}\sqrt{\eta_\kappa}}{2} - \frac{\xi_1}{\sqrt{\eta_\kappa}} \right) \right] \times \left[\Phi\left(\frac{z_{\max}\sqrt{\eta_\chi}}{2} + \frac{\xi_2}{\sqrt{\eta_\chi}} \right) - \exp(-\xi_2 z_{\max}) \times \Phi\left(\frac{z_{\max}\sqrt{\eta_\chi}}{2} - \frac{\xi_2}{\sqrt{\eta_\chi}} \right) \right] \times \exp\left[-\frac{(\xi_1 + \xi_2 - c/z_{\max} - z_{\max}\eta/2)^2}{2\eta} \right] \times \left(\frac{\xi_1 + \xi_2 - c/z_{\max}}{\sqrt{\eta}} - \frac{z_{\max}\sqrt{\eta}}{2} \right) \mathrm{d}\xi_1 \mathrm{d}\xi_2 \,, \tag{23}$$

$$\beta_m = \frac{\exp\left[-z_{\max}^2 (\mu_\kappa + \mu_\chi)/8 \right]}{2\pi\sqrt{\mu_\kappa \mu_\chi}} \times \int_0^\infty \int_0^\infty \int_0^\infty \int_0^\infty \frac{\xi_1 + \xi_3 - c/z_{\max} + z_{\max}\eta_0/2}{\sqrt{2\pi}\eta_0^{3/2}} \times \left[\Phi\left(\frac{z_{\max}\sqrt{\eta_\kappa - \mu_\kappa}}{2} + \frac{\xi_2}{\sqrt{\eta_\kappa - \mu_\kappa}} \right) - \exp(-\xi_2 z_{\max}) \Phi\left(\frac{z_{\max}\sqrt{\eta_\kappa - \mu_\kappa}}{2} - \frac{\xi_2}{\sqrt{\eta_\kappa - \mu_\kappa}} \right) \right] \times \left[\Phi\left(\frac{z_{\max}\sqrt{\eta_\chi - \mu_\chi}}{2} + \frac{\xi_4}{\sqrt{\eta_\chi - \mu_\chi}} \right) - \exp(-\xi_4 z_{\max}) \Phi\left(\frac{z_{\max}\sqrt{\eta_\chi - \mu_\chi}}{2} - \frac{\xi_4}{\sqrt{\eta_\chi - \mu_\chi}} \right) \right] \times \left\{ \exp\left[-\frac{(\xi_2 - \xi_1)^2}{2\mu_\kappa} \right] - \exp\left[-\frac{(\xi_2 + \xi_1)^2}{2\mu_\kappa} \right] \right\} \times \left\{ \exp\left[-\frac{(\xi_4 - \xi_3)^2}{2\mu_\chi} \right] - \exp\left[-\frac{(\xi_4 + \xi_3)^2}{2\mu_\chi} \right] \right\} \times \exp\left[-\frac{(\xi_1 + \xi_3 - c/z_{\max} + z_{\max}\eta_0/2)^2}{2\eta_0} \right] \times \exp\left[\frac{z_{\max}}{2} (\xi_1 - \xi_2 + \xi_3 - \xi_4) \right] \mathrm{d}\xi_1 \mathrm{d}\xi_2 \mathrm{d}\xi_3 \mathrm{d}\xi_4 \,, \tag{24}$$

where $\eta = 1/k$, $\eta_0 = 1/k - \mu_\kappa - \mu_\chi$.

We will describe the detection quality by the threshold SNR z_{mt} that is determined based on the solution of the combined equations:

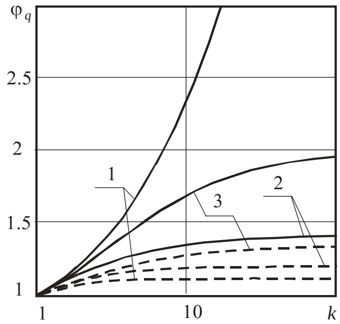

Figure 4. The dependences of the secrecy parameter upon the dynamic range of the signal duration

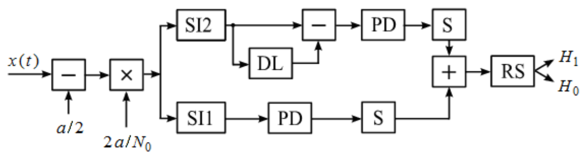

Figure 5. Block diagram of the adaptive detector

$$\begin{cases} \alpha_m(c, z_{mt}) = p \,, \\ \beta_m(c, z_{mt}) = p \,. \end{cases} \tag{25}$$

Then the secrecy parameter of the transmitted data is equal to:

$$\varphi = z_{mt}/z_{0t} \,. \tag{26}$$

The numerical computations by the formulas (7), (23)-(26) show that the secrecy parameter value does not depend upon the set value of the error probabilities p.

In Figure 4, by dashed lines, the dependences are plotted of the parameter (26) upon k under the minimum signal duration (curve 1), under the maximum signal duration (curve 2) and in case when $\kappa_0 = \kappa_{\min}$, $\chi_0 = \chi_{\min}$ or $\kappa_0 = \kappa_{\max}$, $\chi_0 = \chi_{\max}$ (curve 3). While calculating these curves, we presuppose that the lengths of the prior intervals of the moments of appearance and disappearance are the same, so that $\eta_\kappa = \eta_\chi = (k-1)/2k$. From Figure 4, it follows that when the outsider applies the adaptive detector instead of the quasi-likelihood one, it results in the secrecy parameter decreasing, meaning that the information transmission secrecy is getting lower. However, under the same signal-to-noise ratios, the error probabilities during the signal detection are significantly greater for the intercepting outsider than for the signal addressee. Besides, the resolver of the adaptive detector presented in Fig. 5 makes the decision with a delay, namely, at the time moment $t = \chi_{\max} + t_0 - \kappa_{\min}$.

In order to evaluate the error range of the theoretical results obtained, statistical computer simulation has been carried out of the adaptive algorithm for detecting the signal with unknown moments of appearance and disappearance based on the decision statistics (22).

In Figure 6, there are drawn the analytical dependences (24) of the missing probability upon the maximum SNR under the fixed false alarm probability (23) and $k = 4$. Solid curve corresponds to $\alpha_m = 10^{-1}$, dashed curve – to $\alpha_m = 10^{-2}$, dash-dotted curve – to $\alpha_m = 10^{-3}$. By circles, squares and triangles the corresponding simulation data are shown for $\alpha_m = 10^{-1}$, 10^{-2}, 10^{-3}.

As it follows from Figure 6, the specified formulas for the detection characteristics well describe the simulation data for any SNR values. All this attests to the validity of the proposed techniques for calculating the secrecy of information transfer while using the signals with the unknown moments of appearance and disappearance.

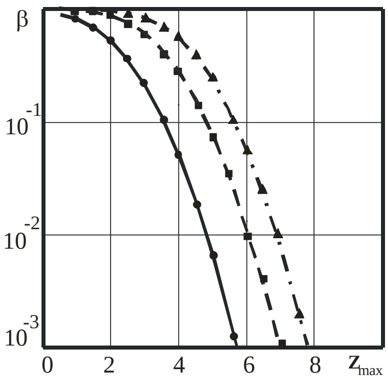

Figure 6. The dependences of the missing probability upon the signal-to-noise ratio

5. CONCLUSION

The outsiders have to carry out the detection of the signal with the unknown moments of appearance and disappearance in the conditions of prior parametrical uncertainty. In order to overcome this uncertainty, there can be applied a number of methods. In the simpler quasi-likelihood detector, some expected values of the moments of appearance and disappearance are used instead of the unknown time parameters. This inevitably leads to a low detection quality. The adaptive detection algorithm implements the adaptation by the moments of appearance and disappearance. Thus, the detection quality improves while the information transmission secrecy decreases. In order to characterize the secrecy, we have offered to use the threshold signal-to-noise ratio as it provides the required error probabilities. The obtained results allow us to determine the information transmission secrecy quantitatively in cases when the signals with the unknown moments of appearance and disappearance are intercepted.

6. ACKNOWLEDGEMENT

This study was financially supported by the Russian Science Foundation (research project no. 14-49-00079) and the Ministry of Education and Science of the Russian Federation (research project no. 2.3208.2017/4.6).

7. REFERENCES

1. Asadi Saeed Abad, F., and Hamidi, H., "An architecture for security and protection of big data", ***International Journal of Engineering, Transactions A: Basics***, Vol. 30, No. 10, (2017), 1479-1486.
2. Mohammadi, A., and Hamidi, H., "Analysis and evaluation of privacy protection behavior and information disclosure concerns in online social networks", ***International Journal of Engineering, Transactions B: Applications***, Vol. 31, No. 8, (2018), 1234-1239.
3. Mohammadi, A., and Hamidi, H., "Analyzing tools and algorithms for privacy protection and data security in social networks", ***International Journal of Engineering, Transactions B: Applications***, Vol. 31, No. 8, (2018), 1267-1273.
4. Middleton, D., "An Introduction to Statistical Communication Theory", New Jersey, Wiley-IEEE Press, (1996).
5. Kay, S. M., "Fundamentals of Statistical Signal Processing, Volume II: Detection Theory", New Jersey, Prentice Hall, (1998).
6. Van Trees, H. L., Bell, K. L., and Tian, Z., "Detection, Estimation, and Modulation Theory, Part I, Detection, Estimation, and Filtering Theory", New York, Wiley, (2013).
7. Barton, D. K., "Radar System Analysis and Modeling", Norwood, Artech House, (2005).
8. Heyde, C. C. "Quasi-Likelihood And Its Application: A General Approach to Optimal Parameter Estimation (Springer Series in Statistics)", New York, Springer-Verlag, (1997).
9. Korchagin, Y. E., Chernoyarov, O. V., Salnikova A. V., and Shakhtarin, B. I., "Algorithms for the detection of a signal with unknown amplitude and duration against white noise", ***2015 International Conference on Modeling, Simulation and Applied Mathematics (MSAM2015)***, Phuket, Thailand, (2015), 23-24.
10. Trifonov, A. P., and Korchagin, Y. E., "Optimal reception of a rectangular pulse with unknown appearance and disappearance times", ***Radiophysics and Quantum Electronics***, Vol. 43, No. 4, (2000), 245-255.
11. Chernoyarov, O. V., Salnikova, A. V., Rozanov, A. E., and Marcokova, M., "Statistical characteristics of the magnitude and location of the greatest maximum of Markov random process with piecewise constant drift and diffusion coefficients", ***Applied Mathematical Sciences***, Vol. 8, No. 147, (2014), 7341-7357.

Secrecy of Communications in Data Transmission by Impulses with Unknown Moments of Appearance and Disappearance

O. V. Chernoyarov[a,b,c], M. M. Shahmoradian[c], M. Marcokova[d], Y. E. Korchagin[e]

[a] *International Laboratory of Statistics of Stochastic Processes and Quantitative Finance, National Research Tomsk State University, Tomsk, Russia*
[b] *Department of Higher Mathematics and System Analysis, Faculty of Electrical Engineering, Maikop State Technological University, Maikop, Russia*
[c] *Department of Electronics and Nanoelectronics, Faculty of Electrical Engineering, National Research University "MPEI", Moscow, Russia*
[d] *Department of Structural Mechanics and Applied Mathematics, Faculty of Civil Engineering, University of Zilina, Slovak Republic*
[e] *Department of Radio Physics, Faculty of Physics, Voronezh State University, Voronezh, Russia*

P A P E R I N F O

Paper history:
Received 07 October 2018
Received in revised form 17 February 2019
Accepted 07 March 2019

Keywords:
Rectangular Impulse
Signal Detection
Authorized Access
Unauthorized Access
Threshold Signal-to Noise Ratio
Error Probabilities

چکیده

در این کار تجزیه و تحلیل مقایسه ای از الگوریتم های تشخیص پالس مستطیلی در پس زمینه نویز سفید گاوسی در زمان اجرای دسترسی مجاز و غیر مجاز به اطلاعات منتقل شده انجام شده است. فرض بر این است که در واقع اطلاعات منتقل شده در وجود یا عدم وجود سیگنال خلاصه میشود. مساله این است که دسترسی غیرمجاز بوسیله بیگانه، در شرایطی اتفاق می افتد که پارامترهای سیگنال به طور کامل یا جزئی ناشناخته هستند. سپس درجه پوشیدگی اطلاعات منتقل شده، بوسیله نرخ پوشانندگی تعریف میشود که مشخص میکند آستانه نسبت سیگنال به نویز وقتی که به جای دسترسی مجاز، دسترسی غیر مجاز وجود دارد افزایش پیدا میکند.

***doi**: 10.5829/ije.2019.32.04a.12*