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

O. V. Chernoyarov, M. M. Shahmoradian*, M. Marcokova, Y. E. Korchagin

*International Laboratory of Statistics of Stochastic Processes and Quantitative Finance, National Research Tomsk State University, Tomsk, Russia
†Department of Higher Mathematics and System Analysis, Faculty of Electrical Engineering and Economics, Maikop State Technological University, Maikop, Russia
‡Department of Electronics and Nanoelectronics, Faculty of Electrical Engineering, National Research University "MPEI", Moscow, Russia
§Department of Structural Mechanics and Applied Mathematics, Faculty of Civil Engineering, University of Zilina, Slovak Republic

PAPER INFO

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

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

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

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

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]

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

(1)

Here the designations are: $a$ is the signal amplitude, $\kappa_0$ and $\chi_0$ are the moments of signal appearance and disappearance which can receive the values from the prior intervals

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

(2)


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

\[
L_0 = L(\kappa_0, \chi_0) = \frac{2a}{N_0} \int_{-\infty}^{\infty} \left[ x(t) - a/2 \right] \, dt
\]

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 \( \alpha_0 \) and \( \beta_0 \) respectively, are found in literature [7]:

\[
\alpha_0 = 1 - \Phi(c/\sqrt{\text{max} N_0}) + \Phi(z_{\alpha}v_0/2),
\]

\[
\beta_0 = \Phi(c/\sqrt{\text{max} N_0}) + \Phi(z_{\beta}v_0/2).
\]

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

\[
c = z_{\alpha}v_0 \arcsin(1 - p) - z_{\beta}v_0/2. \tag{6}
\]

where \( \arcsin(x) \) 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

\[
z_{\alpha} = 2 \arcsin(1 - p)/v_0. \tag{7}
\]

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 \( \kappa_0 \) and \( \chi_0 \). Then hypothesis \( H_0 \): \( x(t) = n(t) \) should 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 \( \kappa_0 \) and \( \chi_0 \), 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 \( \kappa^* \) and \( \chi^* \):

\[
L^* = L(\kappa^*, \chi^*) \tag{8}
\]

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 \( [\kappa^*, \chi^*] \) 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 \( \alpha_q \) and \( \beta_q \) are determined by the following expressions:

\[
\begin{cases}
\alpha_0(c, z_0) = p, \\
\beta_0(c, z_0) = p.
\end{cases}
\]
\[ \alpha_0 = P\left[L^* > c \big| H_0 \right] = 1 - F(c \big| H_0) , \]  
\[ \beta_0 = P\left[L^* < c \big| H_1 \right] = F(c \big| H_1) , \]  
where \( F(\lambda H_j) = P\left[L^* < c \big| H_j \right] , j = 0,1 \) 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 \( \kappa_0 \) and \( \chi_0 \) we get following expressions:

\[ m_0 = \left( L^* \big| H_0 \right) = -c_2 \max \left( \mu_k + \mu_x + \frac{1}{k} \right) \frac{1 - \delta \kappa + \delta \chi}{2} , \]  
\[ m_1 = \left( L^* \big| H_1 \right) = c_2 \max \left( \mu_k + \mu_x + \frac{1}{k} \right) \frac{1 - \delta \kappa - \delta \chi}{2} , \]  
\[ D = \left( \left| L^* - L_0 \right| \big| H_0 \right) = c_2 \max \left( \mu_k + \mu_x + \frac{1}{k} \right) \frac{1 - \delta \kappa + \delta \chi}{2} , \]  
where \( \delta \kappa = (\kappa^* - \kappa_0) / (\chi_0 - \kappa_0) \), \( \delta \chi = (\chi^* - \chi_0) / (\chi_0 - \kappa_0) \).

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

\[ F(\lambda \big| H_j) = \Phi \left( \frac{x - m_j}{\sqrt{D}} \right) . \]  
We then substitute the function (14) into the expressions (9), (10) and, based on Equations (11)-(13), present the detection error probabilities as follows:

\[ \alpha = 1 - \Phi \left( c_2 \max \nu + \max \nu \right) / 2 \right) , \]  
\[ \beta = \Phi \left( c_2 \max \nu - \max \nu \right) / 2 \right) , \]

where \( \nu = \sqrt{(\mu_k + \mu_x + 1/k) \left( 1 + \delta \chi - \delta \kappa \right)} \), \( \Delta = \left( 1 - \left| \delta \kappa \right| \right) / (1 + \delta \chi - \delta \kappa) \).

We characterize the quality of detection by the threshold SNR \( z_{eq} (p) \) providing the set level of the error probabilities: \( \alpha_0 (c, z_{eq}) = \beta_0 (c, z_{eq}) = p \) and therefore serving as a solution of the combined equations:

\[ \left\{ \begin{array}{l} \alpha_0 (c, z_{eq}) = p , \\
\beta_0 (c, z_{eq}) = p \end{array} \right. \]  

Through determining the threshold \( c = z_{eq} \nu_0 \) for the first Equation (16) and substituting it into the second Equation (16), we find the threshold SNR \( z_{eq} \) in the form of

\[ z_{eq} = \frac{4 (1 + \delta \chi - \delta \kappa) \arcsin (1 - p)}{\nu_0 (2 + \delta \chi - \delta \kappa - 2 \delta \kappa)} . \]  
The degree of the signal (1) secrecy is quantitatively described by means of the ratio

\[ \phi = z_{eq} / z_{eq} . \]  
where \( z_{eq} \) 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

\[ \phi = \frac{2 \sqrt{1 + \delta \chi - \delta \kappa}}{2 + \delta \chi - \delta \kappa - 2 \delta \kappa} . \]  
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, \( \kappa_0 = (\kappa_{min} + \kappa_{max}) / 2 \) , \( \chi_0 = (\chi_{min} + \chi_{max}) / 2 \). Since the expected moments of appearance and disappearance also belong to the specified intervals, the following conditions are satisfied:

\[ |\delta \kappa| \leq k \eta_x / (k + 1) , \quad |\delta \chi| \leq k \eta_x / (k + 1) . \]  
Here \( \eta_k = (\kappa_{max} - \kappa_{min}) / T_{max} \), \( \eta_x = (\chi_{max} - \chi_{min}) / T_{max} \) 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 – \( \eta_k = \eta_x = (k - 1) / 2k \), and thus we get

\[ |\delta \kappa| \leq (k - 1) / (2(k + 1)) , \quad |\delta \chi| \leq (k - 1) / (2(k + 1)) . \]  
In Figures 2 and 3, the dependences are presented of the secrecy parameter \( \phi_1 (19) \) under \( \delta \kappa \) 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 \( |\delta \kappa| \leq 0.5 , \quad |\delta \chi| \leq 0.5 \).

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

\[
\delta\kappa = (2\mu_x - \eta_k)/2(\mu_x + \mu_x + 1/k), \\
\delta\chi = -(2\mu_x - \eta_k)/2(\mu_x + \mu_x + 1/k).
\]

Assuming that the lengths of the prior intervals (2) are equal \( \eta_k = \eta_x = (k-1)/2k \), 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 \( \varphi_q = 2\sqrt{k/(k+1)} \).

![Figure 2. The dependences of the secrecy parameter upon the detuning of the moment of appearance](image)

![Figure 3. The dependences of the secrecy parameter upon the detuning of the moment of disappearance](image)

In Figure 4, by solid lines, the dependences are drawn of the secrecy parameter \( \varphi_q \) (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]

\[
L(\kappa, \chi) = 2 \int_0^{t_0} \left[ s(t) - a/2 \right] \, dt + \\
+ 2\int_{t_0}^{t} \left[ s(t) - a/2 \right] \, dt
\]

where \( t_0 \) is the point belonging to the interval \( \left( \kappa_{\max}, \chi_{\min} \right) \). 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 \( \left[ t_0, \chi_{\max} \right) \) and \( \left[ \kappa_{\min}, t_0 \right) \), respectively. The delay line DL delays the input signal at the time interval \( (t_0 - \kappa_{\max}) \). 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 – $\alpha_m$ and $\beta_m$, respectively – that are operating characteristics of the adaptive detector can be calculated by the formulas (9) and (10) where $F(\text{H}_0)$ 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:

$$\alpha_m = 1 - \frac{1}{\eta \sqrt{2 \pi}} \int_0^\infty \left[ \phi \left( \frac{\tau_{\text{max}} \sqrt{\eta_0} + \xi_1}{\sqrt{\eta}} \right) - \exp(-\xi_2 \tau_{\text{max}}) \phi \left( \frac{\tau_{\text{max}} \sqrt{\eta_0} - \xi_1}{\sqrt{\eta}} \right) \right] \times$$

$$\phi \left( \frac{\tau_{\text{max}} \sqrt{\eta_0} - \xi_1}{\sqrt{\eta}} \right) - \exp(-\xi_2 \tau_{\text{max}}) \phi \left( \frac{\tau_{\text{max}} \sqrt{\eta_0} + \xi_1}{\sqrt{\eta}} \right) \right] \times$$

$$\exp \left[ \frac{(\xi_2 + \xi_2 - c/\tau_{\text{max}} - \tau_{\text{max}} \eta/2)^2}{2\eta} \right] \times$$

$$\exp \left[ \frac{(\xi_2 + \xi_2 - c/\tau_{\text{max}} - \tau_{\text{max}} \eta/2)^2}{2\eta} \right] \times$$

$$\exp \left[ \frac{(\xi_2 + \xi_2 - c/\tau_{\text{max}} - \tau_{\text{max}} \eta/2)^2}{2\eta} \right] \times$$

$$\exp \left[ \frac{(\xi_2 - \xi_2)^2}{2\mu_e} \right] - \exp \left[ \frac{(\xi_2 + \xi_2)^2}{2\mu_e} \right] \right] \times$$

$$\exp \left[ \frac{(\xi_2 - \xi_2)^2}{2\mu_e} \right] - \exp \left[ \frac{(\xi_2 + \xi_2)^2}{2\mu_e} \right] \right] \times$$

$$\exp \left[ \frac{(\xi_2 - \xi_2)^2}{2\mu_e} \right] - \exp \left[ \frac{(\xi_2 + \xi_2)^2}{2\mu_e} \right] \right] \times$$

$$\exp \left[ \frac{(\xi_2 - \xi_2 - c/\tau_{\text{max}} + \tau_{\text{max}} \eta/2)^2}{2\eta_0} \right] d\xi_2^2 d\xi_2^2 d\xi_2^2 ,$$

where $\eta = 1/k \cdot \eta_0 = 1/k \cdot \mu_e - \mu_e$.

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

$$\alpha_m(c, z_{\text{nl}}) = p$$,  
$$\beta_m(c, z_{\text{nl}}) = p$$  

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

$$\varphi = z_{\text{nl}}/z_{\text{nl}}$$.

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 $\kappa_0 = \kappa_{\text{min}}$, $\chi_0 = \chi_{\text{min}}$ or $\kappa_0 = \kappa_{\text{max}}$, $\chi_0 = \chi_{\text{max}}$ (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 $\eta_1 = \eta_2 = (k - 1)/2k$. 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 $t = \chi_{\text{max}} + t_0 - \kappa_{\text{min}}$.

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](image)

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

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

O. V. Chernoyarov\textsuperscript{a,b,c}, M. M. Shahmoradian\textsuperscript{c}, M. Marcokova\textsuperscript{d}, Y. E. Korchagin\textsuperscript{e}

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

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

\textit{چکیده}
در این کار تجزیه و تحلیل مقایسه‌ای از الگوریتم‌های تشخیص پالس مستطیلی در پس زمینه نویز سفید گاوسی در زمان اجرا دسترسی مجاز و غیر مجاز به اطلاعات منتقل شده انجام شده است. فرض بر این است که در واقع اطلاعات منتقل شده در واقع یا عدم وجود سیگنال خلاصه می‌شود. مسئله این است که دسترسی غیرمجاز به سیگنال بی‌پهنایی، در شرایطی اتفاق می‌افتد که پارامترهای سیگنال به طور کامل یا جزئی ناشناخته هستند. سپس درجه پوشانندگی اطلاعات منتقل شده، نرخ پوشانندگی موسسه واحده می‌شود که مشخص می‌شود آستانه نسبت سیگنال به نویز و حالتی که به جای دسترسی مجاز، دسترسی غیر مجاز وجود دارد افزایش یافته.

\textit{دی. ۱۰.۵۸۲۹/ije.۲۰۱۹.۳۲.0۴a.۱۲}