# Evaluation of the Interference's Impact of Cooperative Surveillance Systems Signals Processing for Healthcare

https://doi.org/10.3991/ijoe.v18i03.28015

Mohammad K. Abdul-Hussein[1(✉)], Oleksii Strelnytskyi[2], Ivan Obod[2], Iryna Svyd[2], Haider TH. Salim ALRikabi[3]
[1]Al-Ma'moon University College, Department of Communication Engineering, Baghdad, Iraq
[2]Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
[3]Wasit University, Wasit, Iraq
mohammad.k.abdul-hussain@almamonuc.edu.iq

**Abstract—**Patient signals produced from a physical device, such as electrocardiography (ECG), which records the electrical activity of the heart, are vulnerable to keep noise due to various physical constraints of acquisition devices. It is critical for the detection and diagnosis of a variety of diseases. An ECG signal should be displayed as clean and clear as feasible due to its relevance in assisting physicians and doctors in making appropriate judgments. ECG is vulnerable to many types of noise because it is an electrical signal. To improve the quality of assistance for consumers Info a surveillance system by cooperative surveillance systems, high-quality data processing by the observed surveillance systems is required, which predetermines the requirement for high noise immunity of the latter. At the same time, the basics of building cooperative surveillance systems as a network of two-channel asynchronous information communication systems which include numeral of transmitting and receiving process using diverse frequency limits for reception and transmission, failure-prone open single-channel queuing systems, and request signals do not allow to provide the required the noise resistance of the systems under consideration. This paper first gives a characterization of request and interference signal flows in cooperative surveillance systems and briefly examines the features of request signals and their effect on the immunity of cooperative surveillance systems. Then, it calculates the noise resistance of the demand signals of the cooperative surveillance systems for the probabilities of errors: signal skipping; First- and second-degree false alarms in the case of unrelated events, unintended and intra-system impulse interferences in the request channel

**Keywords—**signal for healthcare, surveillance systems, impulse interferences

## 1 Introduction

The recording of the electrical activity of the heart is known as electrocardiography (ECG). It is critical for the detection and diagnosis of a variety of illnesses. An ECG signal should be provided as clean and clear as feasible for physicians and doctors to

make appropriate judgments [1]. In another application for signals, radar surveillance systems are a major element in air traffic control networks (ATS) [2, 3]. Among the radar surveillance systems, cooperative surveillance systems (CSS) [4–6] are one of the important ATS information systems that solve the following information support tasks:

- Determining the coordinates of the air object (AO);
- Nationality identification of the detected AO;
- AO dispatch identification;
- Obtaining flight info from the AO—board and info transmission to the AO board.

CSS is a type of asynchronous data communication system that consists of a numeral of sources and receivers that receive and send data using multiple-frequency bands. The CSS is made up of supplicants and responders who form an asynchronous network. The weakest is the response of aircraft, this is a failure-prone open single-channel queuing system, and consequently, it has major security flaws [7, 8]. This allows us to see that, although the usage of recent CSS technologies despite that a considerable lot of study has previously been done in this area, recognition of the aircraft remains a challenge. Thus, in [9], noise immunity of the aircraft responders of the CSS system was assessed and it was shown that, with a flow rate of the request signals of 5000, the aircraft responder readiness ratio was only 0.3, which confirms the low information security of the system in question. The CSS data communication bandwidth (1030—demand signal communication channel; 1090—info packet communication channel) is severely overcrowded, it must be highlighted, which is noted, in particular [10–15]This affects a considerable intra-system interfering density in-demand channel and response channel and, as a consequence, considerably decreases the noise immunity of the measured CSS [9]. For example, in [10] it is shown that (band 1030/1090 MHz) which is assigned for watching the flow of traffic- air, containing the CSS, prevention of collision system and ADS-B systems, is undergoing weighty overload, and three other approaches are presented for using CSS differ powers of query that consider azimuth subdivisions, and ADS-B tracking info of aircraft to decrease the spectrum overload. It was shown in [9] that since the radio channel of the 1090ES signal concurs with the reply signal of the CSS transponder on-board, in working airspace, two kinds of signals frequently intersection in the temporal field. Because of the significant likelihood of intersection, the signal 1090ES cannot be decoded accurately. In [12], it should be noted that the 1090 MHz aeronautical observation frequency band is increasingly being utilized by a growing numeral of aircraft, requests, and tools kinds and that intra-system intrusion can range to catastrophic levels. Loss of data loss caused by intersecting messages or not coherence to several degrees conventional in all protocols, but there is concern that message density is raised; this performance loss may become intolerable. The study introduces a novel technique for evaluating the intrusion medium at a frequency of 1090 MHz. In [12,13], under the influence interfering of intra-system, the operating features of radio systems flight 1030/1090 MHz were examined. The efficacy of such systems is assessed by interfering metrics such as signals received density, and the results of a study of the signal medium recorded during flight tests with a frequency of 1090 MHz are given. Investigation of the identified works indicates that slightly raise questions of assessing the effect of interference on the processing demand signals quality under the

action of intra-system and intentional related and not related interfering in the demand channel. The work aims to estimate the noise immunity of the CSS under the action of intra-system in addition to intentional related and not related interfering in the demand channel. This document provides a brief description of signal and noise flows and a general mathematical record of the CSS request signals. Then, based on the CSS noise classification, an estimate of the noise immunity of the request signals is given when exposed to extraneous interfering, not related with the signal, under the action of unintentional interference, as well as under the effect of intra-system interfering. This paper provides researchers with the analytical ability to calculate the effect of intentional and unintentional interfering in the CSS demand channel on the processing efficiency of the demand signals of the systems in question. There are many works focused on handling many signal treatments especially in heart sound _signals as in [16], IoT as in the line of Fiber-Optic [17], also in sensors in IoT [18, 19]. The rest of this article is organized as follows: Section 2 presents a brief description of the signal and interference flows in the CSS. Section 3 assesses the noise immunity of the request signals of the cooperative surveillance systems. Section 4 briefly discusses the basic management fundamentals for the new power grid system. Section 4 presents the conclusion.

## 2 Brief description of signal and interference flow in CSS

As stated above, modern responders and interrogators are united by two-way radio links. The coded request signals are transmitted on the request channel [20, 21]. These signals are received by the responders, decrypted, and thereafter, the responders emit coded response signals. In this case, a response signal is generated for each correctly received demand signal, and the start of servicing the next demand code is possible only after the transmission of the response signal to the previous request is completed, that is, after paralysis time, which is bounded by the CSS operation. This circumstance permits the concerned party an illegal usage of the respondents if there is information about the structure of the request signals. In this situation, it is possible to create deliberately a request signals flow density that significantly exceeds the bandwidth capabilities of the request-response system, which in turn will affect the quality of reception and maintenance of the request signals of their CSS resources. In addition, setting deliberate uncorrelated interference on the request channel on the request channel is possible, which can lead to an even greater decrease in the noise immunity and throughput of the transponders. Simultaneously, the signals produced alongside the lobes of the interrogator pattern of the antenna will also contribute to the total flow of interrogation signals and interferences. Thus, it follows from the foregoing that the CSS system's input can receive demand signal flows produced both alongside the core lobe of the interrogator's pattern of antenna and side lobes, as well as the unauthorized request signal flow and the deliberate uncorrelated interference flow. Thus, the entire flow of demand signals coming to the input of the responder of the CSS system can be inscribed as

$$\lambda_{\Sigma} = \sum_{k=1}^{K} \lambda_{0k} + \sum_{i=1}^{I} \lambda_i + \sum_{j=1}^{J} \lambda_j + \lambda_0,$$

Where $\lambda_j$ is the unauthorized request signal flow; $\lambda_i$ is the demand flow of signals on the side lobes of pattern antenna; $\lambda_{0k}$ is the demand flow of signals on the core lobes of a pattern of the antenna; $\lambda_0$ is the deliberate uncorrelated interfering flow. The flow of response signals arriving at the receiving device of the interrogator will be composed of the flow of response signals of its interrogator, the flow of response signals of other investigators, and intentional uncorrelated interfering flow. Consequently, the total signal flow intensity arriving at the investigators' receiver can be represented as

$$\lambda_{\Sigma} = \sum_{i=1}^{N} \lambda_{pi} + \lambda_0,$$

where $\lambda_0$ is the flow of deliberate uncorrelated interference; $\lambda_{pi}$ is the flow of response signals from $N$ responders. Interval-time codes [22–26] (request signal) and positional code (response signal) are used as informational signals in the CSS. On the one hand, these signals are characterized by simplicity, and on the other, they are l characterized by little noise resistance. The conquest of at least one- the impulse of request (reply) signals by interference or the false appearance of impulses at code intermissions of request (reply) signals instantly cause errors: the transmission of signals, and at first and second kind false alarms are produced, or confusion of requests .Thus, the use of time-interval codes as the CSS request signals significantly affects the characteristics and parameters of all query CSS. Centered on this, we concisely consider the character tics of the CSS request signals. Transmitters emit distinct signals $S_i$(t) that belong to a certain limited set—the collaborative $\vec{S} = \|s_i(t)\|;\ i = 1, 2, ..., N,$ and emit them asynchronously, individually of one another, at the instants of time-limited by themselves. In this instance, the circumstance $t_i \ll T_p$ where $t_i$ is the signal $S_i$(t) period is usually satisfied; $T_p$ is the recurrence of the period of the demand signals. The usage of one channel for transferring demand signals, in addition to the production of the whole surveillance system on the source of an open-queue system with failure-prone, makes it problematic for such systems to work when exposed to extraneous and intra-system interference. Request CSS radio signal can be written with the following Equation $s_i(t) = U_i f_i(t) \cos(\omega_0 t + \phi)$, where $f_i(t)$ is a specific sequence of binary coding, which 1 or 0 value; "Units" $f_i(t)$ resemble pulses, and "zeros"—to hiatuses of the signal $S_i$(t) and of this series itself; $w_0$ frequency of the carrier, $\varphi$ high-frequency filling of the first phase randomly, in the common case for every of the coding sequence pulse it differs; $U_i$ factor of amplitude, which is constant in one complete signal. The group $\overline{S}$ comprises V of various signals (as an instruction, in modes number of operation of the query CSS), which different one to other in the sequence of coding $f_i(t)$, in the circumstance of signals radio, resounding frequency $w_0$. The signal form sufficiency expressed in a period of pulse and the entire pulses necessity remain similar in signals entirely. Pulses number in a code n is named the significance code. Coding sequences $f_i(t)$ are usually given by $\tau_k$ values, the so-called code interval between the leading edges of pulses. Code intervals between two consecutive pulses are called main code intervals, the rest are composite ones. The size of the composite interval is equal to the sum of the values of all the main intervals contained in it. The non-cyclic sequence $f_i(t)$ has m=n(n-1)/2 code intervals, including $m_{osn}=n–1$ the main ones. In applied request, two parameters are limited related to the code period values: the least length of the code period $\tau_0$ and the least variance amid the

two periods values $\Delta\tau_k$ are not equivalent in magnitude. The first parameter is limited by the communicating capability, and the second parameter is limited by the resolve of the receiver. Typically, $2\Delta_{\tau_k} \le \tau_0 \le 4\Delta_{\tau_k}$. The value of the largest composed interval $(\tau_M)_i$ is essential—it determines the duration of the sequence $f_i(t)$. The value of the largest composed interval in all signals of $\bar{S}$ ensemble—$T_s = \max(\tau_M)_i$ is called the time base of this ensemble.

## 3 Evaluation of signal immunity of cooperative surveillance systems

As mentioned above, the CSS immunity of noise is largely determined by the noise immunity of the user demand signals. Consider the immunity of noise requested by signals, consider the diverse nature of intrusion that might be existent in the CSS. The general classification of interferences in the existing CSS is given in Figure 1. According to the degree of occurrence, the CSS radio interference will be divided into unintentional (intra-system) and intentional. According to the degree of coincidence with the actual request signals, interference is divided into correlated, i.e. fully consistent with the valid request signals and uncorrelated. By type, interference is divided into fluctuation interference and chaotic impulse noise. As follows from the presented classification, the most dangerous interference, which significantly reduces the immunity of noise of the demand signals, and, as a result, the CSS is related and not related with the present interrogation signals set. It must be well-known that such intrusion happens both in the CSS itself and can be intentionally generated. Such a possibility exists and, as a result, once again shows the complexity of the CSS functioning in the formulation of intentional interference. There are three kinds of errors that can occur when asynchronously receiving request signals: signal skipping, as well as first and second false alarms. Therefore, the noise resistance of the CSS request signals can be characterized by three error probabilities $P_p$, $F_1$, and $F_2$. It is of interest to determine the resistance of noise of the demand signals relatively uncorrelated interference. Such a situation may arise if for some reason it is impossible to avoid the interaction of a useful and interfering signal that is not similar in structure. This particular case is also interesting because it allows you to outline a general approach to solving the problem of calculating the probability of these errors.

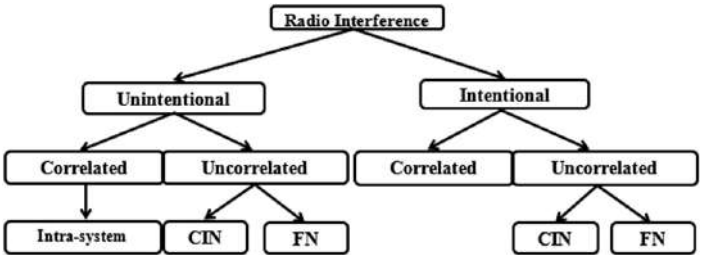


**Fig. 1.** Classification of interference cooperative surveillance systems

### 3.1 Probability of detecting interrogation signals from CSS when exposed to extraneous interfering not related with the signal

Assume that intrusion is stand, has no repercussion, and it's architecturally and statistically self-governing of the signal. The signal comprises n basic pulses and its uncertainty function of *R* and *k* is detection threshold.

The miss of probability occurs when receipt a signal, no a lesser of than *n–k + 1* impulses will be repressed by an intrusion determined from the succeeding equation:

$$P_p = \sum_{i=n-k+1}^{n} C_n^i P_{10}^i (1 - P_{10})^{n-i} \tag{1}$$

Where $P_{10}$ is suppressing a single probability of signal pulse by an intrusion, which is influenced by precise kind of intrusion and intrusion intensity. It is somewhat more complicated to define the probabilities of false alarms. False alarm goes to the first type, it is essential to note that first, a false arrangement with *k* or additional intrusion pulses (an essential rule) is essential to the decoder's input, and secondly, this wrong arrangement essential to be decoded by a decoder (an adequate rule). For such an event the probability can be calculated as follows:

$$F_1 = \sum_{i=k}^{n} C_n^i P_{01}^i (1 - P_{01})^{n-i} P_d(i), \tag{2}$$

Where $P_{01}$ is false pulse probability occurrence at the input decoder in the period $\delta\tau$ which relays on the intensity and kind of the intrusion; $P_d$ is a decode of an erroneous probability *i* pulse arrangement by the decoder. In the second kind, defining the falsealarm probability will kind the probability through the signal passes time over and done with the decoder, in the second type one falsealarm of the occurs at least. In this circumstance, the return value will limit the restricted event probability, which consists in the time of signal arrival, they will be firm individually (of course, with accurateness within the duration of pulse). Thus, the false alarm probability of the second type is given by

$$F_2 = 1 - \prod_{s=1}^{R} [1 - F_2(s)]^{M(s)}, \tag{3}$$

Where $F_2(S)$ is the creation and decoding probability of a false arrangement of the second kind, comprising of *s* pulses of the signal which one lobe is produced by function of uncertainty, equivalent to *s*, and *i* pulses of interfering $(k - s < i < n - s)$

$$F_2(s) = \sum_{i=k-s}^{n-s} C_{n-s}^i P_{01}^i (1 - P_{01})^{n-s-i} P_d(i+1) \tag{4}$$

and *M(S)* is the side numeral of lobes of the function of uncertainty equivalent to *s*. Relation (1)—(4) for the $P_{10}$, $P_{01}$ values and the established high bounds of

probabilities of error $P_p$, $F_1$, and $F_2$ configure the system of three inequalities having three unknowns—n, k, R, which are resolved which, it is possible to evaluate values of rational parameters, such a least n, highest R and k, $R < k < n$, corresponding to them, error of probabilities do not remain surpassed the definite higher limits. The joint solution of irregularities molded by Equations (1) and (2) regarding $n$ and $k$ is like to the statistical problem of bounding the least energy of the signal and ideal threshold by the Neumann-Pearson criterion, this threshold is necessary to find a particular signal in the interference of certain intensity. Here the numeral of pulses $n$ seems as the parameter of equal energy, the threshold used from the sense of the decoder k hold. The variance is found in the false alarm probability, which in ordinary statistical difficulties rest on the only value of the threshold and interference intensity, in this circumstance, also rests on incomplete pulses number. In practical applications, one usually has to deal with two kinds of extraneous uncorrelated interference: chaotic impulse_noise (CIN) and fluctuation_noise (FN). Thus, based on the feasibility and practicality, the main type of CSS intentional interference will be CIN. Let us define probabilities $P_{10}$, and $P_{01}$ in this case as well.

The single pulses Poisson flow is most often accepted as a CIN flow model. The probability of

Poisson flow existence of at minimum single pulse in the period $\tau_0$ is:

$P = 1 - exp(-\lambda_0 t_0),$

Where $\lambda_j$ is the CIN intensity.

We are interested in $P_{01}$ probability, defined as

$$P_{01} = 1 - exp(-\lambda_0 \tau_0). \tag{5}$$

The suppressing a single pulse probability of a useful signal by the Poisson interfering can be defined as:

$$P_{10} = 1 - exp(-\lambda_0 \tau_p)[1 - \gamma(1 - exp(1 - \lambda_0 \tau_0))], \tag{6}$$

Where $\tau_p$ is the paralysis receiver time afterward passing the interference pulse over it; $\gamma$ is the coefficient which bounded the interferential suppression probability of pulse signal at the receiver, whenever it occurs at the same time as the interference pulse. Equation (6) takes both forms of suppression into consideration encountered in the systems using pulsed signals: (inertial, interferential suppressions), the first is caused by existing of elements through a non-zero time of recovery for sensitivity in receiving device, the second suppression is caused by the contact and interference of signal with high-frequency pulses whenever they occur at the same time. The coefficient $\gamma$ rest of the oscillations interfering ratio (amplitudes, phases, and the level of the threshold at receiver). With a uniform phase distribution in the interval [0;2π]

$$\gamma = (1/\pi) arccos(h_1^2 + h_2^2 - 1)/2h_1h_2;\ |h_2 - h_1| < 1,$$

Where $h_1 = U_c/z_0, h_2 = U_p/z_0$; $U_c, U_p$ are the amplitudes of signal pulses and interference, respectively. When the condition $h_1$ const is met, the coefficient $\gamma$ reaches a maximum when $h_2$=$h_1$=$h$, $\gamma_m = (1/\pi)arccos(1-1/2h^2) = (2/\pi)arcsin(1/2h)$.

In cases where the value $h_1$ can vary widely, it is usually accepted $\gamma = 0.2$ which gives an adequate margin of reliability for the calculations. The probability of the smallest suppressed of $n$ – pulses of a signal with the Poisson interference is defined as $P_{10p}(n) = 1-[1-P_{10}(1)]^n$.

In general, real-life flow in practice, the total flow set of periodic or quasi-periodic, allowing this set to be classed as regular. Conducting a comparative examination of the effect is intriguing of interference construction for a receiver that has a decoder, with a chance circuit on n code pulses. The chance of a signal skip in such a decoder is equivalent to the suppressing probability of at least a single pulse n, and the probability of the false alarm is equivalent to the creating and decoding probability of a false n-pulse arrangement. Assume intrusive signals generate a steady intrusion flow that is not related with the usable signal by the periods among pulses with a period of the channel of signals T in each of the fractional streams of steady intrusion surpasses the valuable time of the signal. If the interfering flow is obtained by summing a specific number of steady periodic or quasi-periodic flows equipped within interval time equal to the period moments of appearance of pulses for each flow, then the suppressing probability for one signal pulse can be estimated as

$$P_{10r}(n) = 1-[1-(n\tau_f/T)]^{nN}[1-(n\gamma\tau_0/T)]^{nN},$$

Where $N$ is the regular source number of interference, with the $\tau/T$ ratio corresponds to the single pulse hitting probability of interference in the period $\tau$.

To see how the impulse noise structure affects the likelihood of silencing a demand signal, consider the following relationship

$$\mu = P_{10r}/P_{10p} \tag{7}$$

The requirements found in accord with Equation (7) are presented in Figure 2. It can be realized from the dependencies, the suppressing probability of the request signals rests slightly on the regularity degree of the flow of interference.

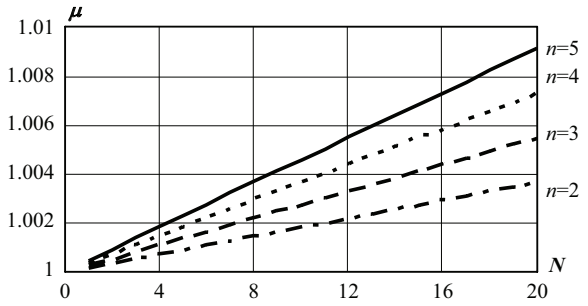


**Fig. 2.** Error value μ when suppressing request signals

The state is diverse with the probability of formation for false n-impulse arrangements by interference. For the Poisson flow of interfering, the probability of formation for false arrangements can be strong-minded from the following Equation:

$$F(n) = n(\lambda_0 \tau_0)^n. \tag{8}$$

For interference flow, the generating false probability of combinations is stated as:

$$F_r(n) = A_N^n n(\lambda_j \tau_0)^n, \tag{9}$$

Where $\lambda_j$ is the average pulses flow intensity in each of N flow interfering; $A_N^n$ is the numeral of placements from $N$ to $n$.

In relations (8) and (9) it is assumed that the observation interval when determining a false alarm is equivalent to $\tau_0$. If the value $\tau_i$ is different $\tau_0$, and the actual values of $F$ will be $\tau_i/\tau_0$ times. From Equation (9), it can be shown the strength of false combinations flow produced by actual impulse noise is influenced by the total intensity and by sources of interference number produced by different self-governing sources. The value of the total flow of interfering intensity $\lambda_0 = N\lambda_j$, the false combination probability rises with raised $N$ and a conforming reduction in $\lambda_j$.

If we transform the Equation (9), by replacing $\lambda_j = \lambda_0/N$, then we get $F_r = A_N^n n(\lambda_0/N)^n \tau_0^n$. In this case, we have the minimum value of $F_r$ with $N = n$

$$F_r(min) = (n!/n^{n-1})(\lambda_0 \tau_0)^n,$$

and maximum one with $N \to 0$

$$F_r(max) = n(\lambda_0 \tau_0)^n, \tag{10}$$

Equation (10) corresponds exactly to Equation (8), therefore, the maximum formation of false impulse combinations probability will be with the Poisson interference.

Comparison of relations (8) and (10) allows us to estimate the magnitude of the error that is allowed when replacing the real flow of interference with a Poisson model with the same intensity $\lambda_0$ Consider the following dependency.

$$\mu = F_r(n)/F(n). \tag{11}$$

Figure 3 presents the dependences obtained by Equation (11). As follows from the presented dependencies, with a large $n$ and a small number of interrogators, the error can be significant and should be taken into account.

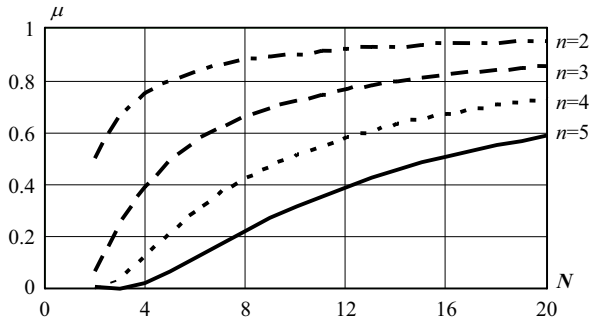


**Fig. 3.** The magnitude of the error $\mu$ in the formation of false combinations.

When determining the disturbing effect of impulse noise on a receiver of impulse signals with interval-time coding, the degree of regularity of the real noise flow should be taken into account, since as the number of impulses of the signal from regular sources increases, it differs more and more from the Poisson flow by the number of generating false combinations. For example, when $N = 8$ this difference is 13% at $n = 2$, and at $n = 3$ this difference is 35%. Normal noise is usually considered as a fluctuation noise. In the receiver of the CSS request signals, false pulses at the input of the decoder will appear when the noise exceeds the quantization threshold. The suppression of the impulses of such a signal will occur in two cases: if the sum of the signal and noise is less than the threshold, or if the noise exceeds the threshold in the time interval $\tau_p$ before the arrival of the impulse of the signal (inertial suppression). The probabilities n and $\beta$ of both the noise exceeding the threshold and not exceeding the sum of the signal and noise of this threshold with non-coherent detection are determined by the well-known Equations:

$$\alpha = exp(-u^2/2),\ \ \beta = \int_0^u \rho exp[-(v^2+\rho^2)/2] I_0(v\rho) d\rho = 1 - Q(u,v),$$

Where = $z_0/\sigma$ and $v = z_0/\sigma$ are threshold/noise and signal/interference ratios; $Q(u, v)$ is an addition of the integral generalized Rayleigh distribution.

The probability $\alpha$ here refers to the observation interval $t_0$ equal to twice the correlation time $\tau_r$ of the normal random process at the output of the linear filter. In most real situations the correlation time lies within

$$\frac{1}{2\sqrt{2}\Delta f} < \tau_r < \frac{1}{2\Delta f},$$

where $\Delta f$ is the filter operating band. The lower boundary is valid for a filter with the Gaussian frequency response, and the upper one is valid for a filter with rectangular frequency response. If the filter is band aligned with the duration of the elementary pulse, then $\tau_r = 0{,}5\tau_0$; $t_0\ 2\tau_r = \tau_0$.

The probabilities that we are interested in $P_{10}$ and $P_{01}$ are determined from the following Equations

$$P_{10} = \beta + \alpha(\tau_p/2\tau_r); \quad P_{01} = \alpha(\tau_p/2\tau_r).$$

In some cases, it is convenient to present the noise interference in the form of an equivalent pulse flow with an average intensity $\lambda = \alpha / 2\tau_r$ and a parameter $\tau_{pIII} = \tau_p + (\beta/\alpha)2\tau_r$, where the ratio $\beta/\alpha$ is equivalent to a coefficient $\gamma$. Figures 4–6 show the dependences of the probabilities of signal skipping and alarms of false of the 1st and 2nd type on the intensity of the flow of uncorrelated impulse noise under the condition that the logic for detecting request signals is an integer and the side lobe value of the signal uncertainty function is equal to one.

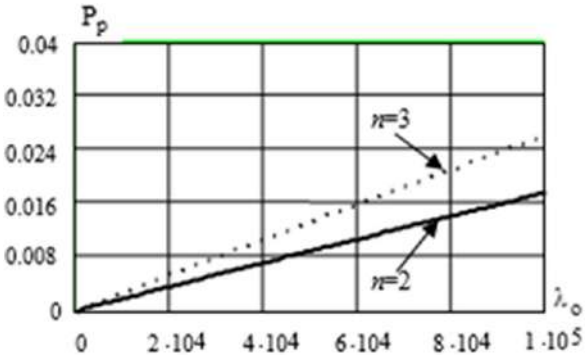


**Fig. 4.** Signal skip probability

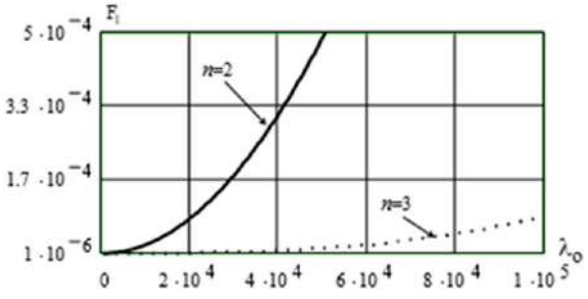


**Fig. 5.** False—alarm probability of the first type

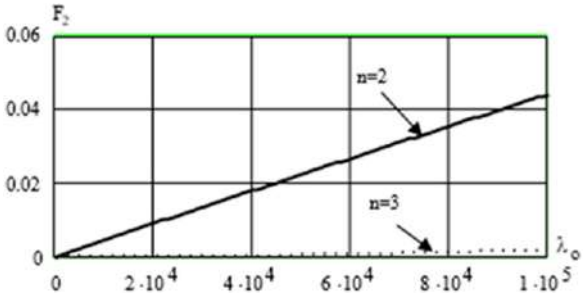


**Fig. 6.** False—alarm probability of the second type

These dependencies show that. the false-alarm probability of the second type has the maximum absolute value n=2. $F_2$ is reduced to an insignificant value with a rise in the value of the demand signals code to n=3; the signal probability skipping combined with a probability of false alarm at n=2 is a maximum one and it decreases with a decrease in the value of the request signals code. The false alarm probability of the first type is insignificant compared to $P_p$ and increases with a reduction in the value of the demand signal code. These results allow us to analyze the immunity noise of the query signals in present CSS. We can assume that the digit of the request signal code equal to 3 is selected successfully. Indeed, a slight loss in the probability of skipping request signals (by the value of $0.5*10^{-2}$ when $\lambda_0 = 10^5$) makes it possible to attain an important decrease in the false alarm probability of the second type (the value of 0.042 when $\lambda_0 = 10^5$)). The use of interrogation signals as request signals of the existing request CSS imposes significant limitations on the bandwidth of the receiving devices of the responder and the interrogator. These limitations are due to the time coding of signals and, as a result, the requirement of a short duration of the rising edges of signals at the output of processing devices. Indeed, the code sequence of the request signals is usually specified by the values of the code intervals between the leading edges of the pulses. In practice, the values of the code intervals are limited by two parameters: the minimum duration of the code interval and the minimum step of changing the duration of the code interval. The first of them is determined by the transmission capacity of the transferring (coding) device, and the second duration is determined by the resolution of the receipting (decoding) device. These limitations significantly reduce the immunity noise of systems when uncovered to fluctuating noise.

### 3.2 Immunity interfering of interrogation signals from CSS systems under the influence of unintentional interference

Regular impulse noise, which is formed by the superposition of several periodic (quasi-periodic) flows of single or multi-pulse signals, has the greatest interest in practical applications. In real conditions, this interference from signals from other radio systems of similar purpose and frequency range is the main type of natural pulse interference. The total flow of regular impulse noise is characterized by the number of sources N of interfering signals, the number of pulses $n_p$ in the signal of one flow, and the intensity $\lambda_p$ in each of the partial flows. The distribution of the moments of

occurrence of signals from different sources within the interval $T_p = 1/\lambda_p$ is usually assumed to be uniform. Assume also that the mutual correlation of the received and each of the interfering signals do not exceed 1 (otherwise the flow of regular impulse noise is identical to the intra-system interference). Thus, this type of interference is correlated not only with the signal but also with the flow, due to the same (or close to that) repetition rate of signals in the partial flows. The occurrence probability at one pulse of regular impulse noise in a small time interval $t_0 \ll T_p$ will be:

$$P = 1 - (1 - n_p t_0 / T_p)^N = n_p N f_p t_0 = \lambda_p t_0,$$

Where $\lambda_p = n_p N f_p$ is the intensity in the entire flow of regular impulse noise, it practically does not differ from the similar probability for the Poisson flow of the same intensity. Therefore, it turns out that it is possible to use the same general method laid out above for chaotic impulse noise for determining the errors probability under the action of regular impulse noise. Hence, however, it should not be claimed that the error probabilities, in either case, will be the same, since regular impulse noise differs from the chaotic impulse noise flow by two significant factors: unconventionality and limited aftereffect. Impositions of pulses from different sources on each other are possible due to the unconventionality in the flow of regular impulse noise, which ultimately leads to a reduction in the intensity of the total flow compared to the ordinary one and, consequently, to a reduction in the probabilities of $P_{10}$ and $P_{01}$ When calculating the noise immunity of signals, this can be taken into account with the help of correction factors

$$g_N = \ln(1 + \lambda_p \Delta t)/\lambda_p \Delta t < 1 \tag{14}$$

to probabilities $P_{10}$ and $P_{01}$ calculated from Equations (5) and (6).

The limited after effect of the regular impulse noise flow manifests itself in the fact that if $i$ signals appear over a certain period of time $T < T_p$, then in the next interval $T_p - T$ with a probability close to unity, exactly $N$ signals appear. The probability of formation of a false multipulse configuration in such a flow differs from the similar probability for the Poisson flow. This difference can be accounted for by using a correction factor

$$g_T = A_N^m / N^m = exp[-m(m-1)/2N] < 1, \tag{15}$$

where $A$ is the number of allocations from $N$ to m the probability of errors calculated for chaotic impulse noise.

### 3.3 Interference immunity of interrogation signals of CSS when exposed to intra-system interference

As follows from the presented classification of interference, intra-system interference should include unintentional and intentional correlated interference. The interfering effect of intra-system interference, created by other signals of the given CSS, depends significantly on the cross-correlation of signals used in the system. And since the number of request signals in the CSS systems is insignificant and all of them are

serviced by responders, it can be argued that intra-system interference significantly affects the immunity noise of the CSS systems. When uncovered to such interfering, it is necessary to take into account that mainly $R_b > 1$ When $R_b = 1$ the interfering effect of the signal flow does not differ from the interfering action of regular impulse noise with the intensity of the flow $\lambda_p = \lambda_b = n_c N_c f_c$. It is most convenient to describe the total interfering effect of intra-system and extraneous interference by joint probabilities:

$$P_{10c}=1-(1-P_{10b})(1-P_{10x})(1-P_{10Ш})$$

$$P_{01c}=1-(1-P_{01b})(1-P_{01x})(1-P_{01Ш})$$

To determine the error probabilities, Equations (1)–(3) are used with a correction factor $g_c$ considering the signal regularity part of the interference flow: $g_c = 1-\mu^2[1-g_r g_N^m]$,

Where μ is the coefficient determining the proportion of the signal part in the total interference flow; $\mu = \lambda_b/\lambda_c$; $\lambda_c = \lambda_b + \lambda_x + \lambda_{Ш}$.

If $R_b > 1$, then the probabilities of errors, caused by intra-system interference, can be significantly greater, since in this case, for the formation of *i*-impulse combination, it entails an error in reception, the participation of $i' < i$ interfering signals from the ensemble is sufficient. By analogy with the above types of correlated interference, when determining the interfering effect of intra-system interference, the mutual correlation of signals is taken into account by coefficients to the error probabilities defined by Equations (1)–(3). Thus, the use of ensembles of signals with a mutual correlation equal to two or more has practical meaning only with minimum repeatability. Ensembles with complete repeatability (as observed in the existing CSS) can find application in a limited number of cases when relatively low requirements are imposed on noise immunity.

## 4 Conclusion

ECG signal data generated is typically significant, as a result, the process of denoising signal and interpretation becomes a difficult undertaking. This emphasizes the importance of autonomous signal analysis and denoising for these monitoring systems to provide relevant notifications for patients and caregivers. The studies performed on the noise immunity of the CSS query signals show a significant dependence of the processing efficiency of these signals on intentional and unintentional (intra-system) interference. It is shown that when determining the interfering effect of impulse noise, the degree of regularity of the real noise flow should be taken into account since as the number of impulses of the signal from regular sources increases, it differs more and more from the Poisson flow by the number of generating false combinations. Estimates of the probabilities of skipping a request signal and alarms of false for the 1st and 2nd from the intensity of the flow of uncorrelated impulse noise showed that: The probability of skipping a request signal total with the false alarm probability at n=2 is maximum and it decreases with decreasing of the request signals value; The false alarm probability of the first type is insignificant compared to the missing demand signal probability

and it increases with decreasing value of request signals; The false-alarm probability of the second kind has a maximum absolute value when the value of the request signal code is 2. With an increase in the value of the demand signal code to 3, the probability of a false alarm is reduced to an insignificant value. It is shown that the evaluation of the immunity noise of the CSS inquiry signals under the effect of unintended and intra-system interference can be taken into account by the correction factors to the error probabilities for missing the request signal and alarms false of for the 1st and 2nd type from the uncorrelated pulse interfering flow intensity.

## 5 References

[1] M. AlMahamdy and H. B. Riley, "Performance study of different denoising methods for ECG signals," *Procedia Computer Science,* vol. 37, pp. 325–332, 2014. https://doi.org/10.1016/j.procs.2014.08.048

[2] B. L. Stevens, F. L. Lewis, and E. N. Johnson, *Aircraft control and simulation: dynamics, controls design, and autonomous systems*. John Wiley & Sons, 2015. https://doi.org/10.1002/9781119174882

[3] A. S. Farina, "Digital radar data processing," *Radio I svyaz, Mosco,* p. 319, 1993.

[4] S. M.C., "Secondary Surveillance Radar," *Artech House,* p. 403, 1988.

[5] I. I. Obod, O. O. Strelnitskyi, and V. A. Andrusevich, Informational network of aerospace surveillance systems, *KhNURE, Kharkov* 2015.

[6] E. Kim and K. Sivits, "Blended secondary surveillance radar solutions to improve air traffic surveillance," *Aerospace Science Technology,* vol. 45, pp. 203–208, 2015. https://doi.org/10.1016/j.ast.2015.05.018

[7] J. Pollack and P. Ranganathan, "Aviation navigation systems security: Ads-b, gps, iff," in *Proceedings of the International Conference on Security and Management (SAM)*, 2018, pp. 129–135: The Steering Committee of The World Congress in Computer Science, Computer.

[8] H. Alrikabi, and H. Tauma, "Enhanced data security of communication system using combined encryption and steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[9] I. Svyd, I. Obod, G. Zavolodko, and O. Maltsev, "Interference immunity of aircraft responders in secondary surveillance radars," in *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, 2018, pp. 1174–1178: IEEE. https://doi.org/10.1109/TCSET.2018.8336404

[10] E. G. Piracci, G. Galati, N. Petrochilos, and F. Fiori, "1090 MHz channel capacity improvement in the air traffic control context," *International Journal of Microwave Wireless Technologies,* vol. 1, no. 3, pp. 193–199, 2009. https://doi.org/10.1017/S1759078709000191

[11] E. M. Valovage, "A method to measure the 1090 MHz interference environment," in *2009 Integrated Communications, Navigation and Surveillance Conference*, 2009, pp. 1–8: IEEE. https://doi.org/10.1109/ICNSURV.2009.5172866

[12] W. Harman, J. Gertz, and A. Kaminsky, "Techniques for improved reception of 1090 MHz ADS-B signals," in *17th DASC. AIAA/IEEE/SAE. Digital Avionics Systems Conference. Proceedings (Cat. No. 98CH36267)*, 1998, vol. 2, pp. G25/1-G25/9 vol. 2: IEEE.

[13] T. Otsuyama, J. Honda, J. Naganawa, and H. Miyazaki, "Analysis of signal environment on 1030/1090MHz aeronautical surveillance systems," in *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*, 2018, pp. 71–71: IEEE. https://doi.org/10.1109/ISEMC.2018.8394048

[14] T. Otsuyama, J. Naganawa, J. Honda, and H. Miyazaki, "An analysis of signal environment on 1030/1090MHz aeronautical L-band systems," in *2017 International Symposium on Antennas and Propagation (ISAP)*, 2017, pp. 1–2: IEEE. https://doi.org/10.1109/ISANP.2017.8228911

[15] H. T. S. AlRikabi, A. H. M. Alaidi, A. S. Abdalrada, and F. T. Abed, "Analysis of the efficient energy prediction for 5G wireless communication technologies," *International Journal of Emerging Technologies in Learning,* Article vol. 14, no. 8, pp. 23–37, 2019. https://doi.org/10.3991/ijet.v14i08.10485

[16] A. Bourouhou, A. Jilbab, C. Nacir, and A. Hammouch, "Heart sound signals segmentation and multiclass classification," *International Journal of Online and Biomedical Engineering (iJOE),* vol. 16, no. 15, 2020. https://doi.org/10.3991/ijoe.v16i15.16817

[17] P. Beňo, F. Schauer, S. Šprinková, and T. Komenda, "Monitoring and security of fiber optic lines in cloud computing within the operation of remote laboratories," *International Journal of Online Biomedical Engineering,* vol. 17, no. 9, 2021. https://doi.org/10.3991/ijoe.v17i09.20157

[18] Y. Irawan, R. Wahyuni, H. Fonda, M. L. Hamzah, and R. Muzawi, "Real time system monitoring and analysis-based internet of things (IoT) technology in measuring outdoor air quality," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 10, 2021. https://doi.org/10.3991/ijim.v15i10.20707

[19] H. TH. , N. A. Jassim, "Design and implementation of smart city applications based on the internet of things," *International Journal of Interactive Mobile Technologies (iJIM),* vol. 15, no. 13, pp. 4–15, 2021. https://doi.org/10.3991/ijim.v15i13.22331

[20] B. Mohammed, R. Chisab, and H. Alrikabi, "Efficient RTS and CTS mechanism which save time and system resources," *international Journal of Interactive Mobile Technologies,* vol. 14, no. 4, pp. 204–211, 2020. https://doi.org/10.3991/ijim.v14i04.13243

[21] H. T. S. Al-Rikabi, *Enhancement of the MIMO-OFDM Technologies*. California State University, Fullerton, 2013.

[22] K. S. V. Belov A.S., Korobkov A.A., Chabdarov Sh.M., "Multi signal allocation of address flows in asynchronous pulse radio systems," *Bulletin of Kazan State Technical University,* vol. 74, no. 4, pp. 164–171, 2018.

[23] I. Globus, "Binary coding in asynchronous systems," *Svyaz, Moscow,* 1972.

[24] N. F. AL-Bakri, A. F. Al-zubidi, A. B. Alnajjar, and E. Qahtan, "Multi label restaurant classification using support vector machine," *Periodicals of Engineering Natural Sciences,* vol. 9, no. 2, pp. 774–783, 2021.

[25] N. F. AL-Bakri and S. H. Hashim, "A study on the accuracy of prediction in recommendation system based on similarity measures," *Baghdad Science Journal,* vol. 16, no. 1 Supplement, 2019. https://doi.org/10.21123/bsj.16.1.(suppl.).0263

[26] O. H. Yahya, H. Alrikabi, and I. Aljazaery, "Reducing the data rate in internet of things applications by using wireless sensor network," *International Journal of Online and Biomedical Engineering (iJOE),* vol. 16, no. 03, pp. 107–116, 2020. https://doi.org/10.3991/ijoe.v16i03.13021

## 6 Authors

**Dr. Mohammad K. Abdul-Hussein** is received the MSc. degree in 1983 and was specified in automatic electric and instrument equipment of aircraft from Kiev Air Force Engineer institute of Higher Military Education from USSR. The PhD degree in

2014 and specified in communication of engineering from Kharkov National University of Radio Electronics in UKR. Interest areas of study are network communication, electrical circuits, and electronics.

**Oleksii Strelnytskyi** is received MSc from Kharkiv National University of Radio Electronics, specialty—radio engineering. Theme of master's work—Budget of the radio channel of the subscriber radio access system. In 2010—candidate of technical sciences (Ph.D.), Kharkov National University of Radio Electronics, Radiotechnical and TV systems. 2006–2019—worked as an assistant, senior lecturer, associate professor of the department of radio engineering KNURE.

**Ivan Obod** graduated from the Kiev Higher Engineering Radio Engineering School in 1978 with a degree in Automated Control Systems, 1978–1999—Engineer, Junior Researcher, Senior Researcher, Head of Laboratory in the Military Radiotechnical Academy, Kharkov, 1999–2004—Associate Professor KNAFU, 2004–2006—Professor KNAFU, 2005—Doctor of Technical Sciences in specialty 05.12.17—radio engineering and television systems. 2006–2018—Professor, Department of Radar Systems Engineering and Automation, NTU "KPI".

**Iryna Svyd** graduated with honors in 1993 from Kharkov Electromechanical College of transport construction, specialty—telecommunications on the transport. 1998—the techniques of the educational process of the department of communication networks Kharkov Technical University of Radio Electronics. 2000—graduated with honors from the Kharkiv State Technical University of Radio Electronics (KTURE), specializing in multi-channel telecommunications. 2000—Engineer of the educational process; 2012—defended her thesis on the specialty 05.12.17—radio and television systems.

**Haider Th. Salim ALRikabi** He is presently Asst. Prof and one of the faculty College of Engineering, Electrical Engineering Department, Wasit University in Al Kut, Wasit, Iraq. The number of articles in national databases—10, and the number of articles in international databases—40.

Article submitted 2021-11-05. Resubmitted 2021-12-17. Final acceptance 2021-12-18. Final version published as submitted by the authors.