FACTA UNIVERSITATIS
Series: **Electronics and Energetics** Vol. 35, Nº 3, September 2022, pp. 405-420
https://doi.org/10.2298/FUEE2203405R

Original scientific paper

COMB JAMMING AS A STRATEGY FOR RCIED ACTIVATION PREVENTION

Jovan Radivojević, Mladen Mileusnić, Aleksandar Lebl, Verica Marinković-Nedelicki

IRITEL a.d., Belgrade, Batajnički put 23, Serbia

Abstract. *The main objective of this paper is the analysis of comb jamming as a technique for RCIED activation prevention. Presentation of three strategies for comb signal generation follows after comprehensive survey of various jamming techniques in the introduction. There are two paper original contributions. The first one is quantitative comparison for three signal generation techniques of their emission power in relation to barrage jamming under the condition of equal BER value. The second contribution is determination of exact BER value as a function of emission power in the case of barrage jamming. Until now we have made different analyses and comparisons starting from estimated emission power. The analysis procedure is performed for QPSK modulated RCIED activation signal. Power saving is evident for all three methods of jamming signal generation. It is proved that additional 2.5dB of power saving is achieved by equalization of frequency components level in comb signal. The analysis in this paper shows that comb jamming allows the same effects as barrage jamming, but with lower emission power.*

Key words: *Remote controlled improvised explosive devices jamming, Comb jamming, Emission power, QPSK modulation, Bit error rate*

1. INTRODUCTION

Procedures of fight against Remote Controlled Improvised Explosive Devices (RCIED) today are becoming more and more important. This method of activation allows a significant degree of comfort for an attacker to realize his intentions from a safe distance, where his activities are difficult to be detected. Besides, there are few other reasons why remote control is very attractive to the attacker for explosive devices activation: more effective and precise bombing, absence of wires gives autonomy to the attacker and the possibility that an attacker is arrested or killed is decreased [1]. Different wireless communication techniques are available to the attacker. These techniques are not implemented only in highly specialized, hardly available equipment, but may be found in

Received February 12, 2022; revised March 25, 2022; accepted April 7, 2022
Corresponding author: Aleksandar Lebl
IRITEL a.d., 11080 Belgrade, Batajnički put 23, Serbia
E-mail: lebl@iritel.com

low-cost, commercial devices, such as long range cordless telephones, cell phones, satellite phones, radio controlled toys, car alarms, keyless automobile door openers, wireless doorbell buzzers, and so on [1]. It is this variety of attacking techniques that set high requirements in the development of the jammer of RCIED activation. It is necessary to implement a wide variety of jamming strategies and generate a significant number of jamming signal types, and to change signal parameters within wide limits for each signal type. Not only are various signal types necessary, but it is also important to develop new jamming technology, or signal type in a very short time interval, measured in weeks, not in months or years. That is why it is important to have well organized development and production of RCIED jamming equipment, as the one presented in [2]. Very important element in the organization of such development and production is consolidating data about performed RCIED attacks in a database. Event logs, implemented at the systems from one of the suppliers, presented in [3], may be implemented for such a purpose.

After this introduction, a survey of applied RCIED jamming systems is given in the Section 2. Section 3 of the paper presents the three most important techniques for comb signal generation. Section 4 deals with the characteristics of frequency spectrum of these techniques. The exact Bit Error Rate (*BER*) characteristics of sweep and barrage jamming are compared in the Section 5. The procedure to define parameters of comb jamming is described in the Section 6. The emission power relation between comb and barrage jamming is investigated in the Section 7. Paper Conclusions are in the Section 8.

2. A SURVEY OF APPLIED RCIED JAMMING SYSTEMS

Frequencies implemented in commercial devices used for RCIED activation are, a priori, known and these frequencies should be dominantly jammed to achieve successful jamming. A survey of commercial devices frequencies, usually used for RCIED activation, may be found in [4]. These frequencies include those implemented for mobile communication systems (GSM, UMTS), DECT telephones, remote control toys, wireless doorbells and gate drivers, car alarms, and so on. A survey of frequencies shows the part of wireless device spectra which may be adapted for RCIED activation. The applied signal power in these devices is variable in the range from several tens of milliwatts to several watts [1]. A very detailed presentation of jamming techniques with mathematical analysis may be found in [5]. The main analyzed or just explained jamming techniques in [5] are noise jamming (separately broadband, partial-band, narrowband depending on the number of jammed channels), tone jamming (single tone and multiple tones), sweep jamming and pulse jamming (in fact comb jamming according to this paper).

Contribution [6] emphasizes two specific jamming techniques: following (or follower) jamming and smart jamming. Following jamming is applied against frequency hopping: here a jammer follows carrier frequency changes on the transmitted signal and then performs jamming on each hopped frequency. The jamming probability when follower jamming is applied is calculated in [7]. It is proved in [7] that channels scanning speed increases linearly as the function of the hopping rate for the lower values of jaming probability, but this dependence is hyperbolical for the higher jamming probability values. In smart jamming the knowledge of transmission protocol is the key issue, because jamming is based on the attack towards the places of protocol vulnerabilities, such as error correction checksum, acknowledgement messages, transmitting overloading (false messages),

and so on. The special threat for successful jamming in the group of smart jamming strategies is the case when timing channels normally intended for regular function of the protected device are maliciously used as covert channels to send activation signal [8].

Contributions [9] and [10] present an idea that there is a specific, optimum technique for jamming each kind of modulations. In these contributions jamming of digital amplitude-phase modulated signals is analyzed and it is proved that the same kind of jamming signal modulation as the activation signal modulation is not always the optimum choice. Such an analysis is important only in the case that we a priori know the type of implemented modulation in activation message coding, but this is very rarely fulfilled.

Reactive (responsive) jamming technique is lately more and more implemented [4], [11] - [16]. This technique may be treated, in fact, as a kind of smart jamming because jamming is based on successful detection of frequency band implemented for RCIED activation signal transmission. In the existing solutions usually is implemented Fast Fourier Transform (FFT), as a fast and reliable detection algorithm [4], [11]. In [17] it is proved that RCIED activation signal detection on the basis of FFT analysis may be faster and in this way more reliable than frequency sweep in active jammer. In [18] this analysis is further expanded to other reactive detector types. A survey of problems, arising in the realization of reactive jammers, is presented in [11]. Among them, the greatest attention in [11] is devoted to time synchronization in the case of simultaneous function of multiple jammers. In [12], [13] the characteristics of some other detector types (energy detector, matched filter detector, feature detector and detector based on the calculation of eigenvalues of the covariance matrix) are theoretically compared one to the other. Contribution [14] is devoted to activation signals jamming in one specific network (IEEE. 802.15.4), where message packet duration is very short (only about 350μs), thus causing necessity for a very short detection time. In the case of universal jamming (not for specific activation signal type), the achieved detection time is less than 1ms in [15], and even about 200μs for the frequency range of 6GHz in [16].

A survey of implemented techniques for remote activation of improvised explosive devices and the frequency band intended for each technique implementation may be found in [19]. Besides these techniques, SMS message sending is very attractive and in some world regions dominant technique of RCIED activation, because of its realization simplicity [20], [21]. RCIED activation signal sending by SMS messages may be prevented or delayed by various detection algorithms implemented in base stations [21].

Modern solutions of RCIED activation signal jammers should follow development in communication procedures and techniques. One such direction which aims at reliable and hardly detectable communication is implementation of frequency hopping signals. Today hopping speed in realized systems may be significantly higher than it is presented in [7]. Responsive jammers realized on the base of RCIED activation signal detection in some cases have the possibility to follow frequencies changes when frequency hopped signal is applied [22], [23]. According to the achieved detection rate, the solution [22] may block the signal with 300hops/s while the solution [23] is effective even when the hop rate is 10000hops/s. The systems [22], [23] are available now and may be purchased on the market. Our idea is to implement active jamming in a broad frequency range with not too high jamming power and thus to avoid the risk of, perhaps, unsuccessful RCIED activation signal detection. One possible solution with these desired characteristics is comb jamming signal implementation according to the principles presented in this paper.

There are two mutually different accesses to jamming signal generation. The first one is to generate the desired shape of jamming signal at low/lower frequency band and then to shift it by the modulator to the necessary frequency band [24]. It is easier to model the signal at lower frequencies, but modulation is additional complication in the solution practical implementation. The other possibility is to directly generate the signal in the jammed frequency band. Our intention is to consider the first possibility since we want to cover the broad frequency range in one moment and the generated signal may be shifted by several modulators adjusted at different frequency bands in the same time.

A completely new approach to jamming signal generation is presented in [25], [26]. There is no need to take care about the shape of jamming signal or even to have such a generator. The solutions belong to the group of responsive jammers. When this approach is applied, the detected signal which has to be jammed is first delayed by the implementation of optical lines with adjustable, precise delay and then transmitted as the generated jamming signal. The selected value of delay determines the level of RCIED activation signal attenuation. Instead of this approach, we apply a specific jamming signal generation again to avoid the possibility that RCIED activation signal is not detected.

The complexity of the fight against the RCIED activation and development perspectives of remote control of these devices were already noticed in [27]. There were made measurements of the bit error rate in the transmission when several jamming procedures types are implemented, thus presenting the possibilities for the fight against the then existing devices, but also against devices, which would appear in the future. The obtained measurement results led to the development of practical devices for fight against RCIED activation [28] - [30]. In these devices generation of very heterogeneous jamming signal types is applied: Continuous Wave (CW), Amplitude Shift Keying (ASK), Phase Shift Keying (PSK), Frequency Shift Keying (FSK), Comb Signal (Barrage Jamming), Sweep Signal (with different sweep strategies, as, for, example, single sweep, multiple sweep, sweep with frequency gap, where there is no sweep signal and where jamming device management may be realized, etc.), white Gaussian noise (WGN), and so on. Among all these techniques jamming by sweep signal and jamming by WGN are most often applied. The characteristics of sweep jamming are analyzed in detail in [31] - [33]. In [34] there is compared necessary power to realize jamming of MPSK (M-ary PSK) modulated RCIED activation message by sweep signal and by WGN, but without considering simultaneous influence of sweep signal and noise which is normally present in the system environment (environmental noise). Sweep signal and WGN are in some cases combined in one unique signal, as demonstrated in [35]. A method for WGN signal generation is analyzed in [36]. The results presented in these last six papers are based on IRITEL great experience in developing jamming devices of various applications: against RCIED activation [37], for jamming mobile telephony systems [38] and for radio surveillance and jamming [39].

Comb jamming is a special technique for generating a signal for RCIED activation prevention, similar to, but more energy efficient than barrage jamming. IRITEL is one of the pioneers for such jamming implementation [40], [41]. Regarding recent times, the main characteristics of comb jamming are presented in [42].

3. TECHNIQUES FOR COMB JAMMING REALIZATION

The main purpose of comb signal definition for jamming is to achieve similar implementation characteristics as if barrage jamming is applied, but with reduced emission power. Comb signal consists of a number of discrete, usually equidistant components when considering frequency spectrum. In this way continual part of frequency spectrum is replaced by only one frequency component, but with the same jamming effect.

There are three main methods for comb signal generation [43]: rectangular pulse train, filtered pulse train and pseudorandom sequence. The signal with the desired frequency characteristics (number of discrete frequency components, components distance in frequency domain) is usually first generated in a low frequency band. After that such a signal modulates a carrier in order to be shifted to the pre-defined frequency band.

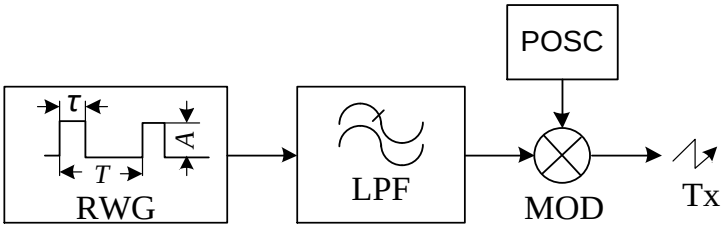

Fig. 1 Principle block-scheme of rectangular pulse train jamming signal generation

Figure 1 presents the principle block-scheme for generating the rectangular pulse train signal. The generation process is initiated in the Rectangular Waveform Generator (RWG), where the pulses of duration τ and period T are formed. The amplitude of pulses is A. The frequency spectrum of the generated pulses is band-limited in the low-pass filter (LPF). The frequency characteristic of this LPF is flat in the pass-band, meaning that only the undesired frequency components are truncated. Amplitudes of frequency components in the pass band are not changed and they remain as generated. Such modified impulses have the frequency spectrum at low frequency band and this spectrum is shifted to the required higher frequency band in the modulator (MOD). Here the generated pulse train signal is multiplied by the signal from the programmable oscillator (POSC). It is possible to produce variable signal frequency band changing the frequency of POSC, i.e. to additionally sweep the generated comb signal in the case that it is necessary to jam wider frequency band (one such application example for jamming mobile communication in GSM systems may be found in [44]). At the end the generated jamming signal is transmitted by a transmit antenna (T_x).

The generation of filtered pulse train signal is a slight modification of the previous method. Its principle block-scheme is equal to the one presented in Figure 1. Difference is in the function of LPF. Besides limiting the pass-band width, this filter also modifies the amplitudes of the generated comb frequency components with the aim to achieve approximately flat frequency characteristic in the pass band. In LPF the higher frequency components are more amplified (or, in other sense, less attenuated) than the lower frequency components. Modifications are also noticeable in the pulse train signal shape in the time domain [43].

Figure 2 presents the principle block-scheme for comb signal generation according to the third method based on pseudorandom sequence implementation. The initial signal is generated in the linear feedback shift register (LFSR). The period of a sequence is T and it consists of N pulses whose duration is τ (i.e. it is $T=N\cdot\tau$). The amplitude of each pulse is $+A$ or $-A$. The remaining algorithm realization phases are the same as for the previous algorithms: the spectrum of the generated comb signal is filtered in LPF and transferred to higher frequencies after signals modulation (implementation of blocks MOD and POSC).

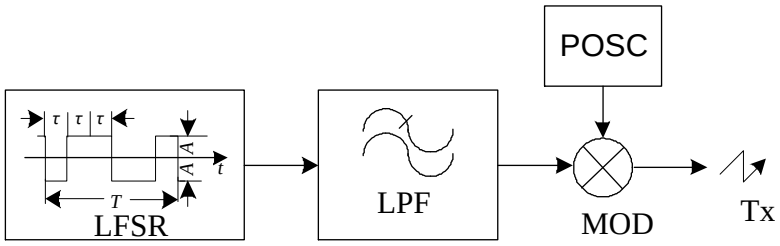

Fig. 2 Principle block-scheme of pseudorandom sequence based jamming signal generation

4. FREQUENCY SPECTRUM CHARACTERISTICS OF THREE METHODS FOR COMB SIGNAL GENERATION

Frequency spectrum of rectangular pulse train signals is well-studied and presented in many references [43]. This spectrum is discrete with equidistant components and may be expressed by the equation

$$P(f)=\sum_{k=-\infty}^{\infty}\frac{A^2\cdot\tau^2}{T^2}\cdot\frac{\sin^2(\frac{k\cdot\pi\cdot\tau}{T})}{(\frac{k\cdot\pi\cdot\tau}{T})^2}\cdot\delta(f-\frac{k}{T}) \tag{1}$$

where $P(f)$ presents signal power spectral density, $\delta(f\text{-}k/T)$ is designation for places where discrete frequency components are situated and the remaining part in the equation presents frequency components power envelope. The meaning of variables A, τ and T is already illustrated in the Fig. 1.

Frequency spectrum of the signal shaped as the rectangular pulse train is presented in the Fig. 3. Such signal is obtained implementing the comb signal generator from the Fig. 1. Spectral components envelope is the function in the form $(\sin(x)/x)^2$ and the number of frequency components in the main lobe is selected by the ratio $K=T/\tau$. The function of the LPF is to pass certain number of components from the main lobe leaving them with unchanged amplitudes. In the example from the Fig. 3 it is $K=6$ and the LPF passes total $2\cdot i+1$ frequency components where $i=3$ is the number of non-attenuated frequency components on both sides related to the central component.

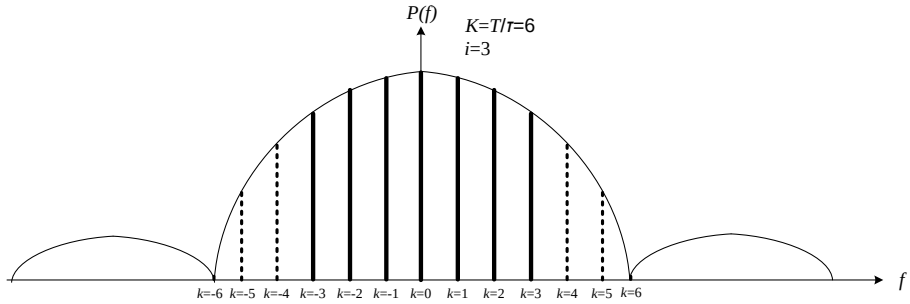

Fig. 3 Frequency spectrum of rectangular pulse train signal

Frequency spectrum of the signal shaped as the filtered rectangular pulse train is presented in Fig. 4. Its initial shape is equal to the one presented in Fig. 3 with the addition that the LPF characteristic (the curve designated by LPF in Figure 4) has to approximate reciprocal function of $(\sin(x)/x)^2$ in the filter pass band. In this way $2 \cdot i+1$ transferred frequency components at the generator output have approximately the same level.

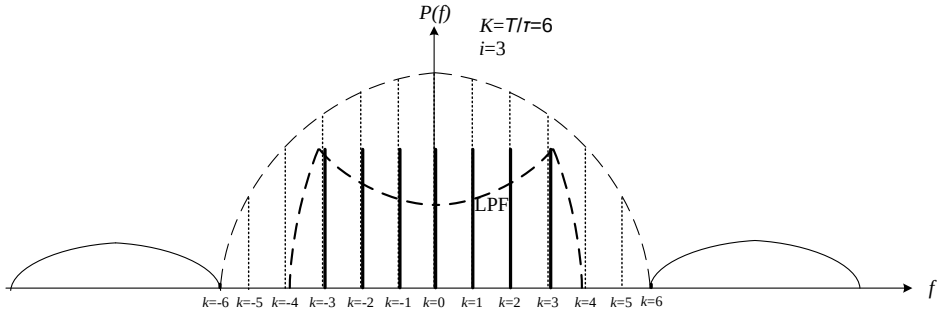

Fig. 4 Frequency spectrum of filtered rectangular pulse train signal

Similar to the case of rectangular pulse train, frequency spectrum of the pseudorandom sequence signal may be presented by the equation

$$P(f) = \sum_{k=-\infty}^{\infty} p_k \cdot \delta(f - \frac{k}{N \cdot \tau}) \tag{2}$$

where coefficients p_k which model the frequency spectrum envelope are

$$p_k = \frac{1}{N^2} \text{ for } k = 0 \tag{3}$$

$$p_k = \frac{N+1}{N^2} \cdot \frac{\sin^2(\frac{k \cdot \pi}{N})}{(\frac{k \cdot \pi}{N})^2} \text{ for } k \neq 0 \tag{4}$$

Variables A, N and τ are already defined in the Fig. 2 and in the explanation dealing with the same figure.

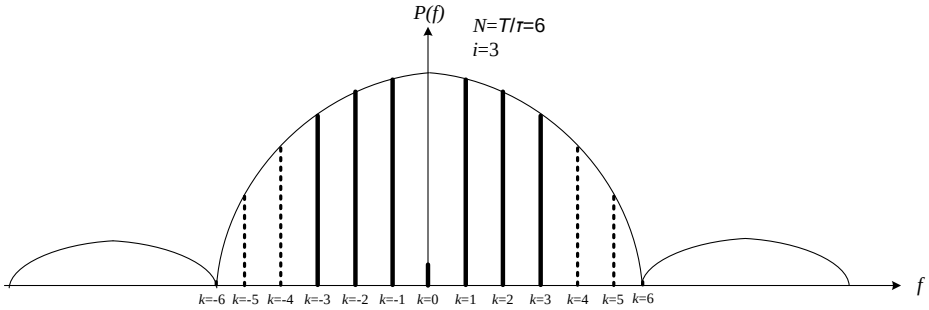

Fig. 5 Frequency spectrum of the pseudorandom sequence signal

Fig. 5 presents the frequency spectrum of the generated pseudorandom sequence signal [43], [45]. Comparing to the frequency spectrum of rectangular pulse train (Fig. 3), difference exists at the component for i=0. This component has very low level (it is nearly eliminated) comparing to other components in the main lobe, because the typical values of N are more than 10. As frequency spectrum of pseudorandom sequence signal is similar to the spectrum of rectangular pulse train, all analysis in the continuation of the paper are performed only for this second type of signal.

Now, when we have explained the main characteristics of comb signal in time and frequency domain, the logical question is: what are the possibilities for this signal generation and practical implementation. If we want to have a wide main frequency lobe, the rectangular pulse duration τ should be very narrow. In a hardware sense it is difficult to generate such an impulse with a significant amplitude level. On the other hand, if we adopt the longer τ, there are fewer frequency components in the main lobe and there is a need for more additional hardware processing to expand the frequency spectrum. This means that we need to have more modulators and programmable oscillators connected as in Fig.1 or Fig. 2 to realize complete solution. Generally, the process of shifting and shaping the frequency spectrum of comb signal which is generated in lower frequency band is also challenging. These are the reasons why comb jamming is not often practically applied.

5. PERFORMANCES COMPARISON OF SWEEP AND BARRAGE JAMMING

The main purpose of comb jamming implementation is to achieve benefits as at barrage jamming, but with lower emission power. Our first step in such an analysis is to compare the performances of pure sweep and pure barrage jamming. Such an analysis is already approximately performed in [34] for MPSK modulated signals. The deviation from the accurate result is mainly caused by the fact that it is supposed that only one error in the symbol is possible regardless of the jamming signal level. In other words, the situation when both bits in QPSK symbol are faulty is replaced by only one faulty bit.

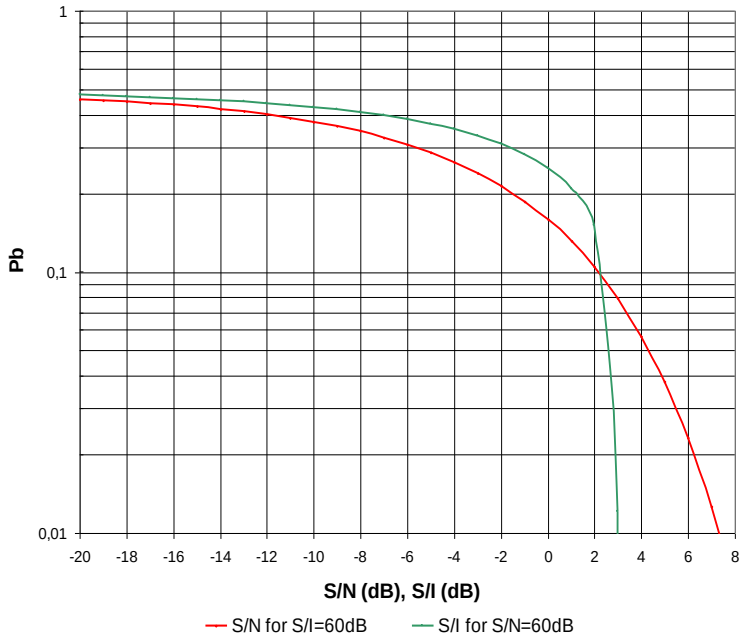

Fig. 6 *BER* (P_b) as a function of the ratio S/N in the case of barrage jamming and as a function of S/I in the case of sweep jamming

In this paper we implemented more accurate comparison in the case of QPSK signal jamming. The exact number of faulty bits in a symbol is supposed in an estimation process. The estimation is based on the implementation of our originally developed simulation program which is already presented in [35]. The purpose of the simulation program is to determine Bit Error Rate (*BER*) when MPSK modulated signal is jammed by the simultaneous influence of sweep and barrage jamming. For the implementation in this paper we select one of the two jamming signals to have very low level. In order to simulate barrage jamming, we have defined the sweep signal level by the expression *S*/*I*=60dB and in order to simulate sweep jamming we have defined noise level by *S*/*N*=60dB, where *S* is reserved for the level of QPSK modulated RCIED activation signal and *I* and *N* are the levels of sinusoidal interference and noise signal, respectively.

Fig. 6 presents the *BER* values as a function of the ratio *S*/*N* when barrage jamming is implemented and as a function of *S*/*I* when sweep jamming is implemented. For the *BER* values greater than 0.1 (which are of interest in jamming applications) it is necessary to apply higher interference signal level in the case of barrage jamming to achieve the same *BER* as if sweep jamming is implemented. Difference in interference level is about 3dB when it is *BER*=0.2, 4dB when it is *BER*=0.3 and 4.8dB when it is *BER*=0.4.

6. COMB JAMMER PARAMETERS DEFINITION

Jammed bandwidth is usually the initial condition which has to be defined in each jammer realization. This bandwidth is then transferred to the bandwidth important for comb jammer design.

Let us suppose that $2 \cdot i+1$ is the number of discrete frequency components which is expected to effectively cause jamming. This number of frequency components is odd, but the generality of results is not lost because we may always select one component more than it is necessary. The second parameter which has to be satisfied at the beginning is the desired *BER* value.

The first problem in jammer design is to determine the optimum number of frequency components in the main lobe of a comb signal before LPF when the number of generated jamming frequencies is known. Optimum number of frequency components is selected so that jamming signal emission power is minimized for the pre-defined *BER*. When rectangular pulse train or filtered rectangular pulse train is designed, the problem is manifested as the selection of the ratio τ/T.

The comb jamming signal is presented as the sum of a number of frequency components. According to the shape of frequency spectrum in Figure 3 for the rectangular pulse train, the minimum level has the highest frequency component in the main lobe which is passed through the LPF (i.e. the component of the order *i*). Comb jammer has to be designed so that this component satisfies the desired *BER* value. As a consequence, all other frequency components after the LPF have the higher level than the component of the order *i* and thus cause the higher *BER* value.

The fact that comb signal has the minimum power means that its amplitude *A* is minimum. There are two opposite effects, which have the influence on the value of *A*. First, if we select the lower value of ratio τ/T, there will be more frequency components in the main lobe and the frequency components after the LPF will tend to be equal. The effect of this modification is lower value of *A*. But, according to the equation (1), lower value of τ/T means that multiplication factor in this equation in front of the part in the shape $(\sin(x)/x)^2$ is decreased and it is necessary to compensate this effect by the higher value of *A*. That is why there is the ratio τ/T where signal amplitude *A* is minimum. This is illustrated in Figure 7. There are three presented characteristics. Each of them is for the same width of filter pass-band, i.e. equal signal period *T*, but for different pulse width τ.

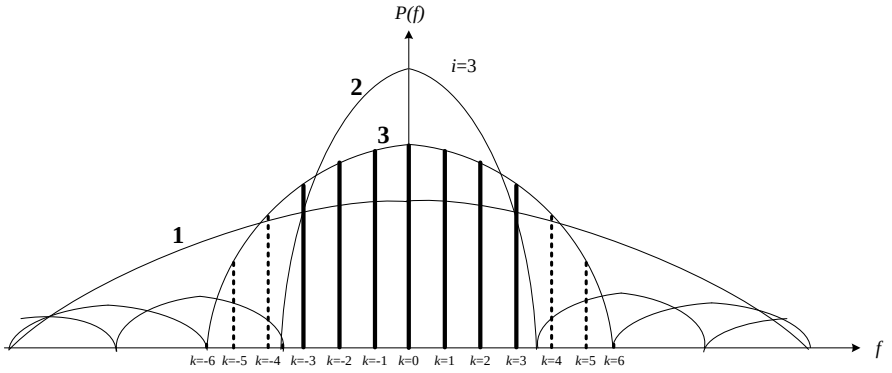

Fig. 7 Frequency spectrum of rectangular pulse for i=3 and three different values of τ

The curve 1 in Figure 7 corresponds to the case when the number of frequencies in the main lobe is significantly higher than the number of frequencies which have to cause jamming. Signal energy in the main lobe is distributed on relatively high number of frequency components which have relatively low level each. The curve 2 is opposite case, when a low number of frequencies are in the pass-band. These frequencies have higher level than in the previous case. The curve 3 is in the middle when considering signal level at f=0, but its level at the frequency f=i is maximal.

Our problem to determine the optimum ratio τ/T is now solved after finding the first and the second derivative of the expression (1) at the point i, because it is necessary to find when the power in this point is maximal. The first derivative when considering only spectrum envelope in the (1) is expressed as

$$\frac{dP}{dx} = \sum_{k=-i}^{i} A^2 \cdot \frac{\sin(2 \cdot k \cdot \pi \cdot x)}{k \cdot \pi} \tag{5}$$

while the second derivative is

$$\frac{d^2P}{dx^2} = 2 \cdot A^2 \cdot \sum_{k=-i}^{i} \cos(2 \cdot k \cdot \pi \cdot x) \tag{6}$$

where it is $x=\tau/T$ and components between k=-i and k=i are passed through the LPF. According to the real conditions from the Figure 3, it must be $i<(1/x)$.

In the point i the expressions (5) and (6) become

$$\left(\frac{dP}{dx}\right)_i = A^2 \cdot \frac{\sin(2 \cdot i \cdot \pi \cdot x)}{i \cdot \pi} \tag{7}$$

and

$$\left(\frac{d^2P}{dx^2}\right)_i = A^2 \cdot \frac{\cos(2 \cdot i \cdot \pi \cdot x)}{i \cdot \pi} \tag{8}$$

The equation (7) is equal 0 if it is satisfied the condition

$$x = \frac{1}{2 \cdot i} \tag{9}$$

meaning that it is the function extreme. For this x the value of the second derivative according to (8) is less than 0, which proves that emission power in the point defined by (9) is really the maximum. It further means that system gain should have minimum value to reach the desired power level and that emission power should be minimal in that case.

7. Emission Power Relation of Comb and Barrage Jamming

We have already emphasized that the intention of comb jamming implementation is to produce the same effect as with barrage jamming, but with the reduced jammer emission power. That is why we are now going to compare the necessary jamming power for these two jamming strategies.

Let us suppose that our wish is to cause jamming in total $2 \cdot i+1$ channels. The classical solution is to implement noise signal for jamming which covers continually frequency

band of these channels. The improved possibility is to implement only one jamming frequency in each channel.

The characteristics presented in Figure 6 correspond to each one of $2 \cdot i+1$ considered channels, i.e. frequency components. As a consequence, benefits of filtered rectangular pulse train are directly obvious from Figure 6. Namely, the power of each frequency component in the filtered pulse train signal is equal and for the same extent lower than uniform noise jamming power to cause the same *BER*. In this way the total effect of jamming in all channels is also equal to the one presented in Figure 6. The necessary emission power decreases when comb jamming is implemented is ΔP_{1fp}=3dB when it is *BER*=0.2, ΔP_{2fp}=4dB when it is *BER*=0.3 and ΔP_{3fp}=4.8dB when it is *BER*=0.4.

The benefits are decreased when rectangular pulse train or pseudorandom sequence signal is implemented. To determine the improvement in emission power in this case, we start from the calculation of total emission power related to the case of uniform spectrum emission power. Our estimation is illustrated by the example when it is i=3, meaning that total 7 frequency components are passed through the LPF. According to the problem which is earlier defined to be solved, components at i=3 need to have equal power.

Table 1 illustrates procedure to determine the ratio of comb signal power to the barrage signal power when the sinusoidal component level at i=3 is equal to the value of the power at the same frequency in the case of filtered pulse train or also to the level of barrage (noise) signal. The column with the designation P_{rel} presents ratio of considered sinusoidal component power with the order k to the unity power. The last two rows in the table present the power ratio of total 7 frequency components after the LPF to the uniform power in the same frequency band. The data in the last column of the Table 1 is graphically presented by Fig. 8. It illustrates the power level ratio of frequency components of rectangular pulse train signal to barrage signal where rectangular pulse train signal has (at least) the same jamming effect as barrage signal. The calculated power difference of 2.5dB has to be subtracted from the power save when filtered rectangular pulse train signal is implemented to obtain the equivalent power save when rectangular pulse train is considered. Therefore, in the case of rectangular pulse train implementation, power save is ΔP_{1p}=0.5dB when it is *BER*=0.2, ΔP_{2p}=1.5dB when it is *BER*=0.3 and ΔP_{3p}=2.3dB when it is *BER*=0.4. These values are significantly lower than the values for filtered pulse train, thus approving the benefits of power spectrum equalization.

Table 1 Power ratio of comb signal for rectangular pulse train to barrage jamming

k	τ/T	P_{rel}	$P_{comb}/P_{barrage}$
-3	0.167	0.011258	1
-2	0.167	0.019044	1.692
-1	0.167	0.025422	2.258
0	0.167	0.027889	2.398
1	0.167	0.025422	2.258
2	0.167	0.019044	1.692
3	0.167	0.011258	1
Total			1.768
Total (dB)			≈2.5

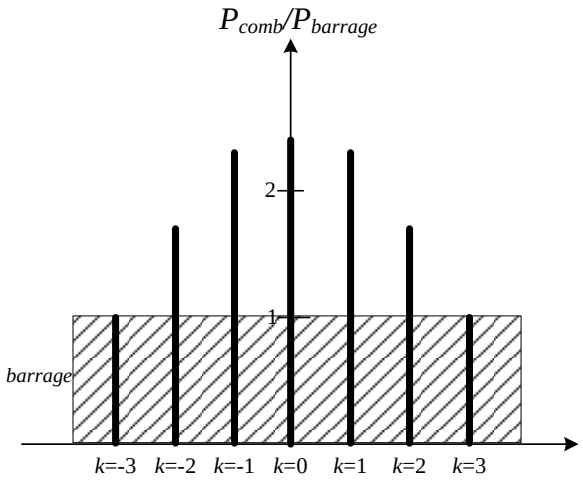

Fig. 8 Power spectrum ratio graphical presentation for rectangular pulse train to barrage signal

8. CONCLUSIONS

This paper starts with the comprehensive presentation of IRITEL contributions in the area of RCIED activation jamming. After that analysis is directed towards comb jamming. Comb jamming is a wide-band jamming strategy. It efficiently replaces more often implemented barrage jamming strategy. The available literature only emphasizes the fact that comb jamming signal power is lower than barrage jamming power, but without any attempt to quantitatively support this statement [5], [46]. The main paper contribution is quantitative estimation of emission power difference between comb and barrage jamming under the criterion of the same achieved *BER* value in both cases. The analysis in the paper considers all three most often implemented strategies for comb jamming signal generation: rectangular pulse train, filtered pulse train and pseudorandom sequence. It is proved that power equalization for all generated frequency components when filtered pulse train signal is considered additionally achieves 2.5dB improvement of power saving possibilities. In this way power saving is more than doubled comparing to the pulse train signal.

The second paper contribution is determination of exact *BER* value when barrage jamming of RCIED activation message is applied. In our previous contributions we have used only approximate calculation of this value [34]. The exact value of this variable is obtained by the implementation of our original simulation program.

Our other direction of jammers development is related to malicious drones' missions prevention. Modern drone communication channels are often realized using some broadband techniques [47]: Frequency Hopping Spread Spectrum (FHSS) [48] or Direct Sequence Spread Spectrum (DSSS) [49]. Comb jamming is highly suitable for jamming these two signal types due to its ability to cover great bandwidth with not too high emission power. The solutions presented in this paper are the first step for the future development to allow broadband jamming of drone communication signals.

REFERENCES

[1] G. Kumaraswamy Rao and K. V. Ranga Rao, "Intelligent Jamming Solution to Defeat the Growing Menance of Remotely Controlled Improvised Devices (Rcieds) Using Electronic Counter Measures", *Int. J. Electron. Commun. Comput. Eng*., vol. 4, no. 5, pp. 1479–1488, 2013.

[2] M. E. Pesci, "Systems Engineering in Counter Radio-Controlled Improvised Explosive Device Electronic Warfare", *John HopkinsAPL Technical Digest*, vol. 31, no. 1, pp. 58–65, 2012.

[3] J. Haystead, "Defeat IED Mission Expands to Defensive Electronic Attack (DEA)", *The J. Electron. Defense*, pp. 28–40, 2015.

[4] K. Wilgucki, R. Urban, G. Baranowski, P. Grądzki and P. Skarżyński, *Automated Protection System Against RCIED, Military Communications and Information Technology*. Chapter 7: Cognitive Radio and Spectrum Management Techniques, 2012, pp. 593–601.

[5] R. Poisel, *Modern Communications Jamming Principles and Techniques*. Boston/London, Second Edition, Artech House, 2011.

[6] K. Wilgucki, R. Urban, G. Baranowski, P. Grądzki and P. Skarżyński, "Selected Aspects of Effective RCIED Jamming", In Proceedings of the Military Communications and Information Systems Conference, Warsaw, 2012, pp. 1–5.

[7] K. Burda, "The Performance of Follower Jammer with a Wideband Scanning Receiver", *J. Electr. Eng.*, vol. 55, no. 1–2, pp. 36–38, 2004.

[8] S. D'Oro, L. Gallucio, G. Morabito and S. Palazzo, "Efficiency Analysis of Jamming-based Countermeasures against Malicious Timing Channel in Tactical Communications", In Proceedings of the IEEE International Conference on Communications ICC, Budapest, 2013, pp. 4020–4024.

[9] S. Amuru and R. M. Buehrer, "Optimal jamming strategies in digital communications / Impact of modulation", In Proceedings of the IEEE Global Communications Conference (GLOBECOM), 2014, pp. 1619–1624.

[10] S. Amuru and R. M. Buehrer, "Optimal Jamming Against Digital Modulation", *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 10, pp. 2212–2224, 2015.

[11] J. Mietzner, P. Nickel, A. Meusling, P. Loos and G. Bauch, "Responsive communications jamming against radio-controlled improvised explosive devices", *IEEE Commun. Mag.*, vol. 50, no. 10, pp. 38–46, 2012.

[12] M. Tanatwy, "Responsive Communication Jamming Detector with Noise Power Fluctuation using Cognitive Radio", *Int. J. Innovative Res. Comput. Commun. Eng*., vol. 2, no. 10, pp. 5967–5973, 2014.

[13] T. Trump and I. Müürsepp, "Detection Speed of Responsive Communication Jamming Detectors, Recent Advances in Telecommunications and Circuits", In Proceedings of the 2nd International Conference on Circuits, Systems, Communications, Computers and Applications, Dubrovnik, 2013, pp. 149–154.

[14] M. Wilhelm, I. Martinović, J. Schmitt and V. Lenders, "Reactive Jamming in Wireless Networks: How Realistic is the Threat?", In Proceedings of the 4th ACM Conference on Wireless Network Security (WiSec '11), ACM, Hamburg, 2011, pp. 47–52.

[15] G. Evans, "A new weapon in the fight against RCIEDs, Army Technology", August 2015, https://www.army-technology.com/features/featurea-new-weapon-in-the-fight-against-rcieds-4647155/.

[16] Selena Electronics, *RSS intelligent reactive stationary jammer and RSV vehicle reactive jammer*. In *Electronics Warfare Systems: Jamming Solution*, 2015.

[17] M. Mileusnić, P. Petrović, A. Lebl and B. Pavić, "Comparison of RCIED Activation Responsive and Active Jamming Reliability", In Proceedings of the 6th International Conference IcETRAN 2019. Srebrno Jezero, 2019, pp. 988–993, awarded as the best paper in the Section of Telecommunications.

[18] M. Mileusnić, P. Petrović, V. Kosjer, A. Lebl and B. Pavić, "Reliability Analysis of Different RCIED Activation Signal Responsive Jamming Techniques and Their Comparison to Active Jamming", *FU Electr. Energ.*, vol. 33, no. 3, pp. 459–476, 2020.

[19] A. GulyÁs, "The Radio Controlled Improvised Explosive Device (RCIED) threat in Afghanistan", *AARMS*, vol. 12, no. 1, pp. 1–11, 2013.

[20] OSS Net, *Survey of RCIEDs - Southeast Asia – Feb 2003-Oct 2005*. OSS Southeast Asia Division, 2005.

[21] F. E. Idachaba, "Algorithm for source mobile identification and deactivation in SMS triggered improvised explosive devices", *Procedia Eng.*, vol. 78, pp. 96-101, 2014.

[22] Stratign, "Radio Jammers", https://www.stratign.com/radio-jammers/.

[23] Security & Counterintelligence Group LLC, "LIGHTNING: RCIED Jamming System – Vehicle Installed", https://scgroup-ltd.com/lightning/.

[24] J. Magiera, "Wideband Signal Generation for Jamming Radio-Controlled Improvised Explosive Devices", In Proceedings of the 41st International Conference on Telecommunications and Signal Processing (TSP). Athens, 2018, pp. 1–4.

[25] M. E. Belkin, A. Alyoshin, D. Fofanov and A. S. Sigov, "Studying microwave-photonics design principle of a responsive jammer for radio-controlled explosive devices", *Tech. Phys. Lett.*, vol. 46, no. 11, pp. 1132–1135, 2020.

[26] M. E. Belkin, L. Zhukov and N. Smirnov, "Devising an Optimal Time-Delay Circuit Configuration for a Microwave-Photonics-Based Radio Communication Jammer", In Proceedings of the 29th Telecommunications Forum (TELFOR), Belgrade, 2021, pp. 440–443.

[27] P. Petrović and M. Šunjevarić, "Radio Surveillance and Jamming Systems and Techniques", *Trends in Telecommunications*, pp. 17.1.-17.22., Belgrade, November 1988, (P. Petrović, M. Šunjevarić, "Savremeni sistemi i tehnike za radio-izviđanje i ometanje", Pravci razvoja telekomunikacija, str. 17.1-17.22, Beograd, Novembar 1988).

[28] *IRITEL High Frequency (HF) radio surveillance and jamming system*, chapter in the book M. Streetly, *Jane's Radar And Electronic Warfare Systems*. IHS Global Limited, 2011.

[29] *IRITEL Very/Ultra High Frequency (V/UHF) radio surveillance and jamming system*, chapter in the book M. Streetly, *Jane's Radar And Electronic Warfare Systems*. IHS Global Limited, 2011.

[30] M. Mileusnić, P. Petrović, B. Pavić, V. Marinković-Nedelicki, J. Glišović, A. Lebl and I. Marjanović, "The Radio Jammer Against Remote Controlled Improvised Explosive Devices", In Proceedings of the 25th Telecommunications Forum (TELFOR), Belgrade, 2017, pp. 151–154.

[31] M. Mileusnić, B. Pavić, V. Marinković-Nedelicki, P. Petrović, D. Mitić and A. Lebl, "Analysis of Jamming Successfulness against RCIED Activation", In Proceedings of the 5th International Conference IcETRAN 2018. Palić, 2018, pp. 1206–1211, paper awarded as the best one in the section of Telecommunications.

[32] M. Mileusnić, B. Pavić, V. Marinković-Nedelicki, P. Petrović, D. Mitić and A. Lebl, "Analysis of Jamming Successfulness against RCIED Activation with the Emphasis on Sweep Jamming", *FU Electron. Energ.*, vol. 32, no. 2, pp. 211–229, 2019.

[33] V. Marinković-Nedelicki, A. Lebl, M. Mileusnić, P. Petrović and B. Pavić, "BER Calculation for Sweep Jamming of MPSK Modulated RCIED Activation Message Signals", In Proceedings of the 18th International Symposium "INFOTEH Jahorina 2019". Jahorina, 2019, pp. 1–6.

[34] M. Mileusnić, P. Petrović, B. Pavić, V. Marinković-Nedelicki, V. Matić and A. Lebl, "Jamming of MPSK Modulated Messages for RCIED Activation", In Proceedings of the 8th International Scientific Conference on Defensive Technologies OTEH, Belgrade, 2018.

[35] V. Marinković-Nedelicki, A. Lebl, M. Mileusnić and P. Petrović, "Combined Jamming in RCIED Activation Prevention", In Proceedings of the 19th International Symposium "INFOTEH Jahorina 2020". Jahorina, 2020, pp. 1–6.

[36] A. Lebl, M. Mileusnić, B. Pavić, V. Marinković-Nedelicki and P. Petrović, "Programmable Generator of Pseudo-White Noise for Jamming Applications", In Proceedings of the 27th Telecommunications Forum (TELFOR). Belgrade, 2019, pp. 1–4.

[37] P. Petrović, N. Remenski, P. Jovanović, V. Tadić, B. Pavić, M. Mileusnić and B. Mišković, *WRJ 2004 Wideband Radio Jammer against RCIEDs*. Tehničko rešenje – novi proizvod na projektu tehnološkog razvoja TR32051 pod nazivom Razvoj i realizacija naredne generacije sistema, uređaja i softvera na bazi softverskog radija za radio i radarske mreže, http://www.iritel.com/images/pdf/wrj2004-e.pdf, 2011.

[38] N. Remenski, B. Pavić, P. Petrović, M. Mileusnić and V. Marinković-Nedelicki, *Integrisana radio-oprema za zaštitu prostora od mobilnih veza (Treća generacija radio-opreme)*. Tehničko rešenje – novi proizvod s oznakom CJ-1P na projektu tehnološkog razvoja TR-11030 Razvoj i realizacija nove generacije softvera, hardvera i usluga na bazi softverskog radija za namenske aplikacije, http://www.iritel.com/images/pdf/cj-1p-e.pdf,, 2010 (also published in the book M. Streetly, *Jane's Radar And Electronic Warfare Systems*.. IHS Global Limited, 2011). Prva generacija radio-opreme s oznakom CJ-1 je realizovana na projektu tehnološkog razvoja TR6149B, 2006.

[39] P. Petrović, M. Mileusnić, B. Pavić, V. Tadić and V. Marinković-Nedelicki, *Razvoj nove generacije sistema za radio-izviđanje i ometanje u VF i VVF/UVF opsegu*. Tehničko rešenje u okviru projekta 10 M 06, Ministarstvo za nauku i tehnologiju Srbije, Fond za naučni razvoj, 1997-2000.

[40] P. Petrović, *Generator of jamming signals GEMOS.* Technical solution, 1990.

[41] P. Petrović, *Development of new generation of GEMOS devices and signal classifier based on DSP Technology*. Technical solution, 1999.

[42] A. Lebl, M. Mileusnić and J. Radivojević, "Combined and Comb RCIED Activation Messages Jamming – Two Different Strategies with Similar Names", *Sci. Tech. Rev.*, vol. 70, no. 1, pp. 21–28, 2020.

[43] B. A. Black, *On the Generation of Waveforms Having Comb-Shaped Spectra*. NRL Memorandum Report 619, Naval research Laboratory, May 1988.

[44] R. E. Stoddard, *Multi-band Jammer*. Patent No. US7697885 B2, 2010, pp. 1–7.

[45] X. Song, X. Wang, Z. Dong, X. Zhao and X. Feng, "Pseudo-Random Sequence Correlation Identification Parameters and Anti-Noise Performance", *Energies*, vol. 2018, no. 11, pp. 1–18, 2018.
[46] M. R. Frater and M. Ryan, *Electronic Warfare for the Digitized Battlefield*. Artech House Inc., 2001.
[47] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta and M. Guizani, "A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques", *Ad Hoc Networks*, vol. 111, p. 102324, 2021,
[48] H.-B. Kil, J.-S. Lee and E.-R. Jeong, "Analysis of Frequency Hopping Signals in Commercial Drones", *Int. J. Pure Appl. Math.*, vol. 118, no. 19, pp. 2015–2024, 2018.
[49] B. M. Todorović and V. D. Orlić, "Direct sequence spread spectrum scheme for an unmanned aerial vehicle PPM control signal protection", *IEEE Commun. Lett.*, vol 13, no. 10, pp. 727–729, 2009.