FACTA UNIVERSITATIS
Series: **Electronics and Energetics** Vol. 32, N° 2, June 2019, pp. 211-229
https://doi.org/10.2298/FUEE1902211M

ANALYSIS OF JAMMING SUCCESSFULNESS AGAINST RCIED ACTIVATION WITH THE EMPHASIS ON SWEEP JAMMING*

Mladen Mileusnić, Branislav Pavić, Verica Marinković-Nedelicki, Predrag Petrović, Dragan Mitić, Aleksandar Lebl

IRITEL a.d., Belgrade, Serbia

Abstract. *In this paper we first briefly compare the performances of active jamming remote controlled improvised explosive devices activation using wide-band noise and frequency sweep signal. Frequency sweep is the most widely used technique intended for active jamming and we analyze its characteristics: 1) sweep speed, 2) conditions for certainly successful jamming, 3) successful jamming probability if jamming is not certainly successful, and 4) step of frequency change when frequency sweep is applied. The separate paper section is devoted to the successful jamming probability calculation in general. The attention is also paid to jamming probability determination when starting and ending sweep signal frequencies are varied. The initial research has been upgraded and extended. The presented results refer to jamming equipment development in IRITEL, but it is important to add that they are also applicable to the other similar jamming systems realizations.*

Key words: *Jammer, Remote controlled improvised explosive devices, Frequency sweep, Successful jamming probability, Bit error correction*

1. INTRODUCTION

Today the world is faced with the growing challenges in the fight against terrorism. Methods of terrorist attacks are constantly improved. It is the reason why devices for the fight against these attacks must follow changes in the applied techniques of attack.

Remote Controlled Improvised Explosive Devices (RCIED) are widely used as the equipments intended for terrorism. Such devices are activated by messages, which are transmitted from longer or shorter distances by wireless communications.

The two most widely used jamming techniques against RCIED activation are reactive and active jamming [2]. The advantage of reactive jamming is related to the lower level of emission power, because jamming signal is generated only when RCIED activation message is detected in one intercepted channel. It is necessary to detect activation signal appearance

Received July 19, 2018; received in revised form October 3, 2018
Corresponding author: Aleksandar Lebl
IRITEL a.d., 11080 Belgrade, Batajnički put 23, Serbia
(e-mail: lebl@iritel.com)
*The earlier version of this paper is awarded as the best one in the section Telecommunications at the 5th IcETRAN Conference, Palić, 11-14 June 2018, [1].

and its frequency, i.e. channel which must be jammed. On the contrary, active jamming supposes constant jamming signal transmission independent of activation signal existence.

Reactive jamming technique is more often applied in the last time [3] - [10]. In the existing solutions Fast Fourier Transform (FFT) is usually used as fast and reliable detection algorithm [3], [4]. The pipeline of different operations when FFT is applied to detection algorithm (signal samples collection, these samples processing, decision making) instead of multiplying hardware elements contributes to more reliable and faster RCIED activation message detection even in the case when it is necessary to analyze frequency hopping signal [5]. A survey of problems arising in the realization of reactive jammers is presented in [4]. The greatest attention in [4] is devoted to time synchronization in the case of simultaneous operation of multiple jammers. The characteristics of some other detector types such as energy detector, matched filter detector, feature detector and detector based on the calculation of eigenvalues of the covariance matrix are theoretically compared in [6], [7]. Contribution [8] deals with 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 general, the achieved detection time is less than 1ms in [9], and even about 200μs for the frequency range up to 6GHz in [10].

It is important to emphasize several problems, which may occur when active jamming is applied. The first one is that activation signal power at the RCIED location may be very different, depending on the implemented techniques for message transmission and on the distance between activation message transmitter and receiver. The second one is that the operating frequency for signal transmission may be in very wide frequency range. In such situation the most reliable method for jamming realization is wide-band jamming signal generation. It means that available transmitter power is used in the whole frequency range. This high jamming power is therefore distributed into many available channels and, as a consequence, its level in each channel is relatively low. The jamming signal power in a channel with an activation signal is, perhaps, not enough to prevent RCIED activation signal reception.

The other possible, most often implemented signal generation method for active jamming is linear variation of jamming signal frequency (i.e. frequency sweep) [11]-[13]. In this, second case it is possible to concentrate significantly higher power in one channel where activation message is transmitted comparing to wide-band jamming. But, as jamming signal is not always present in each channel, there is a risk that generated sweep signal would not reach the desired channel in time, while activation signal is yet not finished. Sweep jamming implementation is not limited only to RCIED activation jamming. It may be also used for mobile telephony systems jamming [14]-[16].

The possibility to achieve the higher sweep speed [17] caused that sweep jamming becomes very popular and widely applied. In this way the benefits of sweep jamming in the area of power saving come to the fore. Sweep jamming is today dominant technique of active jamming and this is the reason to devote significant attention in this paper to its analysis.

The relation of necessary jamming signal power for wide-band and sweep jamming depends on several factors: the desired jamming probability, implemented technique (modulation) for RCIED activation message transmission, level of environmental noise, and so on. The results presented in our analysis in [18] prove and explain that in the case of QPSK modulation for small values of bit error rate (*BER*) till ≈2.5% wide-band jamming is more efficient than sweep jamming. The conclusion is based on the fact that under such conditions lower signal power is necessary to be implemented for wide-band jamming to achieve the same *BER*. But, such low values of *BER* are not important for jamming realization and for *BER*>2.5% sweep jamming is more efficient. For other PSK modulation types the limit value of *BER* above which sweep jamming becomes more efficient than wide-band jamming is ≈10% for BPSK and less than 1% for 8PSK and 16PSK. The power save increases with PSK modulation level and it may reach even 11dB for 16PSK. The additional disadvantage of higher necessary power consumption for wide-band jamming is that jammer may be easier detected. As a consequence, there is a greater opportunity that personnel controlling jammer operation are exposed to enemy attack [19].

When comparing efficiency of wide-band jamming and sweep jamming, available literature is mainly concentrated on their qualitative comparison, or, in some cases, approximate quantitative results of such comparison are presented [20]. As for the knowledge of the authors of this paper, there is no such an analysis related to the *BER* value and the applied signal modulation type for RCIED activation.

The main purpose and the novelty of this paper is that it presents and analyzes different parameters of sweep jamming:

1. sweep speed;
2. the role of practical sweep jamming realization as step function instead of linear frequency change in jamming probability determination;
3. performances comparison of two different sweep jamming strategies;
4. jamming probability calculation when starting and ending jamming frequency are varied;
5. jamming probability calculation when different error detection and correction algorithms are applied.

The method of frequency sweep realization for jamming RCIED activation is presented in Section 2 of this paper. The sweep speed is defined as the most important characteristic of this method. After that, successful jamming probability for frequency sweep signal implementation is determined in Section 3. Two methods of sweep signal generation considering jamming reliability are analyzed in Section 4. Section 5 explains the influence of starting and ending jamming frequency variation on the value of successful jamming probability. Section 6 deals with the calculation of successful jamming probability when signal physical characteristics are such that reliable jamming is not guaranteed. At the end, Section 7 presents conclusions.

2. Sweep Speed of RCIED Activation Jamming Signal

There are two jamming signal characteristics, which must be considered to prevent successful RCIED activation: jamming signal frequency and jamming signal level. Jamming signal frequency must be equal to the activation signal one or in its proximity. The difference between activation and jamming signal frequency depends on several factors such as characteristics of RCIED activation message receiver (its bandwidth and attenuation characteristic) and relation between amplitudes of jamming signal and RCIED activation signal. In general, there are three possibilities in the analysis of jamming and activation signal levels at the place of RCIED activation message receiver. First, if activation message signal level is greater than jamming signal level, jamming is unsuccessful. In other two situations jamming is successful, but the reaction of activation message receiver is different. If jamming and activation signal levels have nearly the same values, RCIED receiver detects activation message of no use due to its changed content. In the case that jamming signal level is significantly greater than the activation signal level, RCIED receiver does not detect activation message, but only the jamming signal [21].

Let us suppose that it is necessary to jam a signal, which may cause activation of RCIED anywhere in a frequency band of total width W (in Hz) [22]. The sweep jamming is applied in the same frequency bandwidth $W=f2-f1$, where $f1$ is the minimum and $f2$ is the maximum sweep signal frequency (Figure 1). It can be supposed that jamming may be successful under the condition that jamming signal appears in the frequency band (channel) where activation signal is transmitted. It is assumed that successful jamming probability is $P_{dist}=1$. The period of one sweep cycle is T_{sw}. One channel width where activation signal is transmitted is C (channels $C(1)$ and $C(2)$ in Figure 1). When jamming signal appears somewhere in this channel while RCIED activation message is present (time interval T_c in Figure 1) and the condition related to level of two considered signals is satisfied, we shall suppose that jamming is successfully realized. In this moment we also suppose that jamming signal appears only once in the frequency band reserved for RCIED activation message transmission in a time of this message duration.

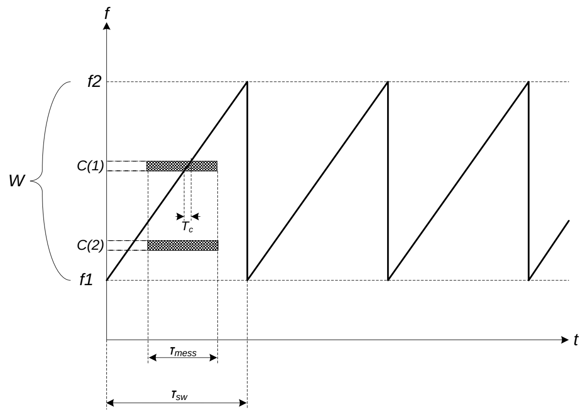

Fig. 1 RCIED activation jamming when jamming signal frequency is linearly changed.

Sweep speed will be defined as frequency change speed:

$$v_{sw} = \frac{W}{T_{sw}}. \quad (1)$$

Jamming probability will be $P_{dist}=1$ if one cycle time of frequency change from $f1$ to $f2$ satisfies a condition:

$$T_{sw} \leq T_{mess}, \quad (2)$$

where T_{mess} is RCIED activation message duration.

It follows from Eq. (1) and Eq. (2)

$$v_{sw} \geq \frac{W}{T_{mess}}. \tag{3}$$

It is possible that jamming is not successful, although jamming signal frequency is in the proximity of activation message frequency and the condition related to signal levels is satisfied. In such a case it is necessary that jamming signal appears more than once (*m* times in our analysis) in a considered channel during message duration to achieve satisfactory RCIED activation jamming probability. In such a case sweep speed must be increased. Expression (3) is, consequently, changed to:

$$v_{sw} \geq \frac{m \cdot W}{T_{mess}}. \tag{4}$$

The value v_{sw} for which it is valid the equating part of (3) and (4) defines lower limit of sweep speed to assure successful jamming. It is a time needed to guarantee that jamming signal at least once (in the case of (3)) or *m*-times (in the case of (4)) „hits“ the considered channel when its frequency sweeps.

3. Successful Jamming Probability for Frequency Sweep Implementation

Let us suppose that the condition from Eq. (2) is not satisfied, i.e. that it is $T_{mess}<T_{sw}$. Such a case is presented in Figure 1: the message, which appears in the frequency band *C(1)* during time interval T_{mess} will be successfully blocked, but the message from the frequency band *C(2)* will not be blocked, because jamming signal at no time „hits“ the band *C(2)* during time interval T_{mess}.

In the considered case when it is $T_{mess}<T_{sw}$, the relation between T_{mess} and T_{sw} may be expressed as:

$$T_{sw} = k \cdot T_{mess}, \tag{5}$$

where *k* is real-valued number whose value is $k>1$. In this case RCIED activation signal jamming is not guaranteed, i.e. $P_{dist}<1$. The probability of RCIED activation jamming is:

$$P_{dist} = \frac{1}{k} = \frac{T_{mess}}{T_{sw}}. \tag{6}$$

Figure 2 presents successful jamming probability (P_{dist}) as a function of one sweep cycle time interval (T_{sw}) and message duration (T_{mess}). The values of P_{dist} are obtained on the basis of Eq. (6) if it is satisfied the condition $T_{mess} \leq T_{sw}$. If it is $T_{mess}>T_{sw}$, jamming signal frequency in any case crosses the frequency of RCIED activation message at least once. That’s why in such situation is $P_{dist}=1$, providing that other conditions for successful jamming are satisfied.

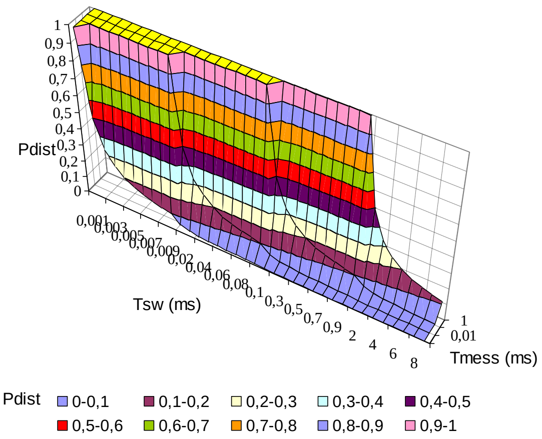

Fig. 2 RCIED successful jamming probability as a function of sweep time and message duration.

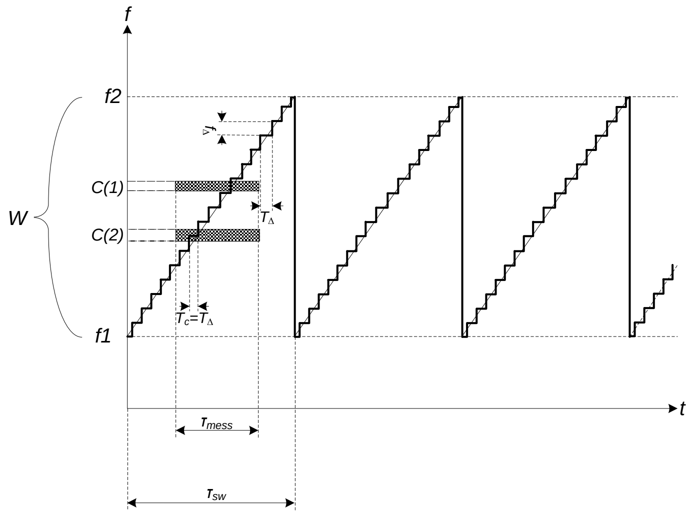

Fig. 3 Practical realization parameters of RCIED activation jamming.

Practical realization of sweep signal generation differs from the presentation in the Figure 1. Instead of generation by linear frequency change, signal is generated as stepwise function. In this way it is realized an approximation of linearly variable signal frequency, as presented in Figure 3. According to this figure, the basic data defined in implementation are time step (T_Δ) and frequency change step (f_Δ). These two values may be used to express sweep speed in the other manner as

$$v_{sw} = \frac{f_\Delta}{T_\Delta}. \tag{7}$$

If it is satisfied the condition

$$f_{\Delta} \leq C, \tag{8}$$

jamming will be certainly successful. If not, there are two possibilities:

1. the value of generated frequency is in no moment in the frequency range dedicated to the considered channel (channel *C(1)* in the Figure 3);
2. generated frequency coincides during some time interval with the frequency of a channel (interval T_c in the Figure 3, when signal in channel *C(2)* is jammed).

In the first case jamming will be unsuccessful, while in the second case it will be successful.

The aim of practical sweep signal generation is to approximate linear frequency change as much as possible. To achieve this, it is chosen the minimum value of T_{Δ} ($T_{\Delta min}$) which is allowed by applied hardware components [17]. The calculation is performed for such defined T_{Δ} value. The details of implemented jammer solution are presented in [13].

Let us suppose that we want to determine whether it is possible to assure successful jamming using the selected hardware component for sinusoidal signal generation. The first step in the analysis is to find the necessary number of frequency steps for linear approximation of frequency change. We have already emphasized in Eq. (2) the necessary condition for such successful jamming. In the limiting case T_{sw}=T_{mess}, the number of frequency steps for linear approximation of frequency change is:

$$n_s = \frac{T_{sw}}{T_{\Delta\min}}. \tag{9}$$

The value of necessary frequency change step to (eventually) achieve successful jamming may be now determined on the base of Eq. (8) and Eq. (9) as:

$$f_{\Delta} = \frac{W}{n_s} = \frac{W \cdot T_{\Delta\min}}{T_{sw}} \leq C. \tag{10}$$

The conclusion of this short analysis expressed by Eq. (9) and Eq. (10) is that fast linear change of jamming frequency does not always lead to successful jamming. The jamming successfulness is also related to the characteristics of applied hardware components for jamming signal synthesis, namely to the possibility to achieve satisfactory short step for linear approximation of frequency change. It is possible that the time of one frequency sweep from the minimum to maximum frequency is satisfactory, but that one step of frequency change is still greater than one channel width (*C*), thus causing unreliable jamming.

4. Comparison of Jamming Successfulness for Two Sweep Signal Generation Methods

There are two methods for sweep signal generation:

1. signal frequency is always generated from its minimum towards the maximum value and after reaching the maximum value, signal frequency immediately drops down to its minimum value;
2. signal frequency starts to linearly increase from its minimum value and when reaches its maximum, starts to linearly decrease towards the minimum usually at the same rate as it was previously in the increasing direction.

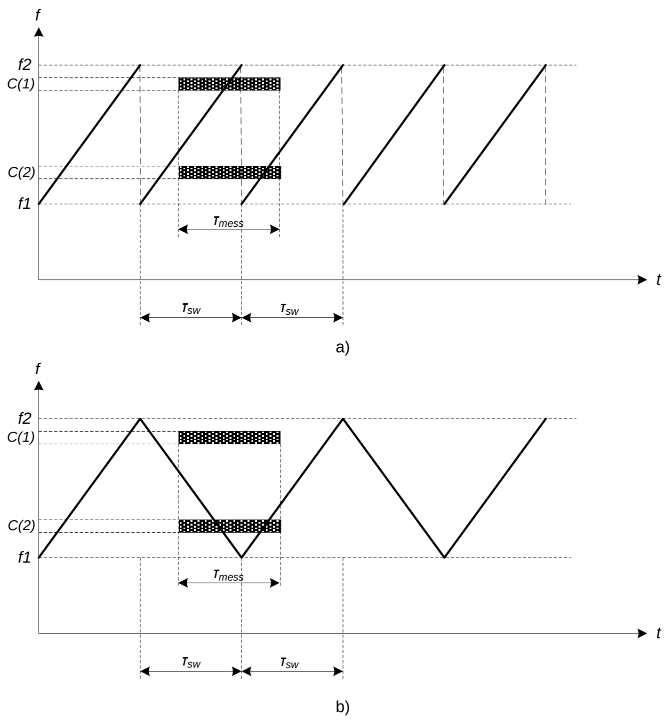

Fig. 4 Jamming possibilities of RCIED activation signal for two methods of sweep signal generation.

Figure 4 presents these two methods for sweep signal generation. The first method is shown in Figure 4a and the second one in Figure 4b. Two RCIED activation messages are taken into account together with a sweep signal in both cases. RCIED activation messages are located in two different frequency bands: *C(1)* and *C(2)*. In this example message length (T_{mess}) is equal to the sweep time (T_{sw}). If a sweep signal is generated according to the first method, jamming is always successful, irrespective of the part of frequency range between *f1* and *f2* where RCIED activation signal appears. However, if sweep signal is generated according to the second method, jamming may be successful for a signal in a channel *C(2)*, where jamming signal two times „hits“ the channel with activation message. In addition, it may be also unsuccessful for a signal in a channel *C(1)*, because jamming signal does not „hit“ channel *C(1)* in a time of message duration. It is important to emphasize that jamming is certainly successful for the second method of sweep signal generation if a bit changed condition comparing to Eq. (2) is satisfied:

$$2 \cdot T_{sw} \leq T_{mess}. \tag{11}$$

Successful jamming probability for the second method of jamming signal generation is determined starting from formula (11) and is:

$$P_{dist} = \frac{1}{2 \cdot k} = \frac{T_{mess}}{2 \cdot T_{sw}}. \quad (12)$$

Figure 5 presents variation of RCIED activation signal jamming probability as the function of the relation T_{sw}/T_{mess} for two presented methods of sweep signal generation. The graph in this figure illustrates that successful jamming probability is always greater if sweep signal is generated according to the first method for all values $T_{sw}/T_{mess}>0.5$. For $T_{sw}/T_{mess}\leq 0.5$ both methods have $P_{dist}=1$.

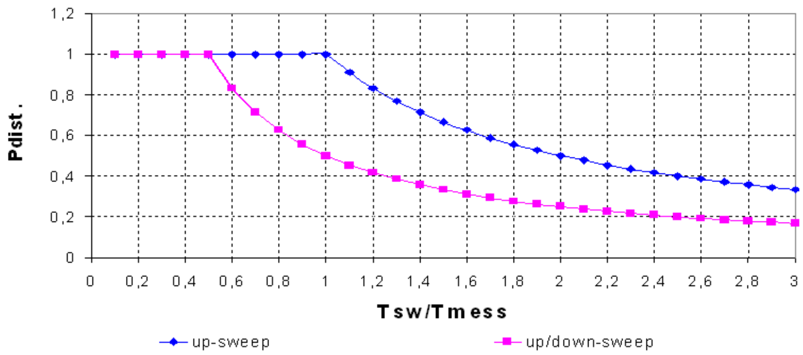

Fig. 5 Successful jamming probability as a function of relation T_{sw}/T_{mess} for two methods of sweep signal generation.

5. The Role of Starting and Ending Jamming Frequency Selection

The analysis from previous sections and graphs in Figure 2 and Figure 5 demonstrate that successful jamming probability decreases very fast when T_{sw} is greater than T_{mess}, i.e. when activation message is short. There is a limit of sweep speed increase due to the characteristics of used hardware components for signal generation. Also too great sweep speed decreases the time of jamming signal frequency existence enough close to activation message frequency and thus message content is not changed to cause successful jamming. These problems may be overcome if sweep cycle does not cover the whole predicted frequency band in the jammer, but the smaller range of frequencies, that is estimated to contain the activation message frequency. In such a case T_{sw} is no more significantly greater than T_{mess}. It is necessary to know in advance the nearer frequency limits of expected activation signal, thus allowing possibility to define smaller distance between the lowest and the highest sweep frequency. It is demonstrated in [23] that the implemented operating frequencies for RCIED activation are specific for different war areas. These frequencies depend on devices, which may be easily purchased in that area and then simply adjusted for the application. Thus it is possible to predict a priori the expected activation frequencies. In any case, it is necessary to satisfy the condition

$$f_{down} \leq f_{mess} \leq f_{up}, \quad (13)$$

to realize jamming successfully. In this expression f_{mess} is the frequency used for activation message transmission and f_{down} and f_{up} are the minimum and maximum sweep frequency, respectively.

Figures 6, 7 and 8 present P_{dist} as a function of f_{down} and f_{up}. Frequencies f_{down} and f_{up} are presented as shifted values. The value 0 on these figures corresponds to minimum possible sweep frequency (f_{minsw}), which may be implemented in the jammer when sweep signal is realized, while the value 1 corresponds to maximum sweep frequency (f_{maxsw}). The value of activation signal frequency is also shifted. The correct relation of the frequencies for the graphs in figures 6, 7 and 8 is $f_{down} \leq f_{up}$. That's why $P_{dist}=0$ if this condition is not satisfied.

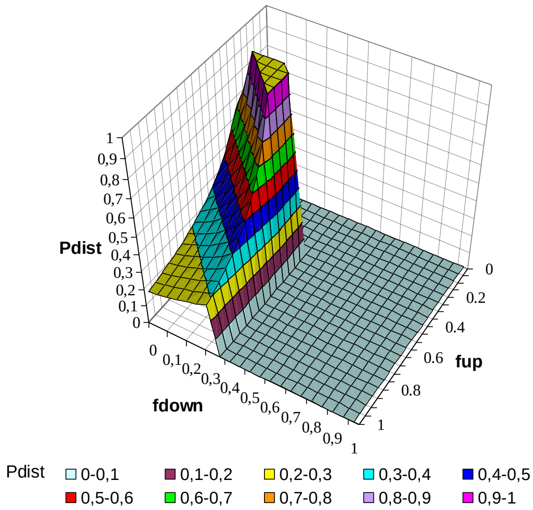

Fig. 6 Successful jamming probability as a function of minimum (f_{down}) and maximum (f_{up}) shifted sweep frequency, T_{mess}/T_{sw}=0.2, shifted f_{mess}=0.3.

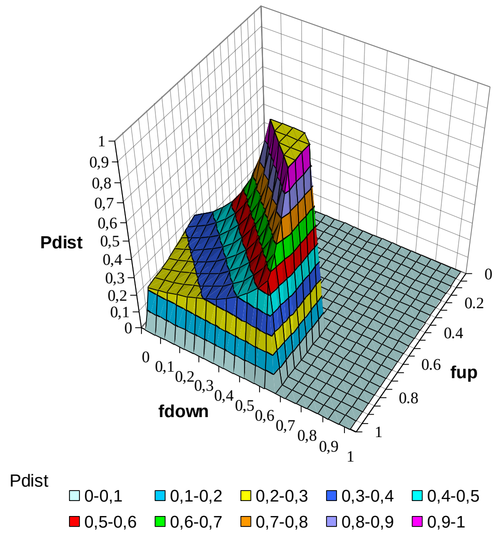

Fig. 7 Successful jamming probability as a function of minimum (f_{down}) and maximum (f_{up}) shifted sweep frequency, T_{mess}/T_{sw}=0.2, shifted f_{mess}=0.6.

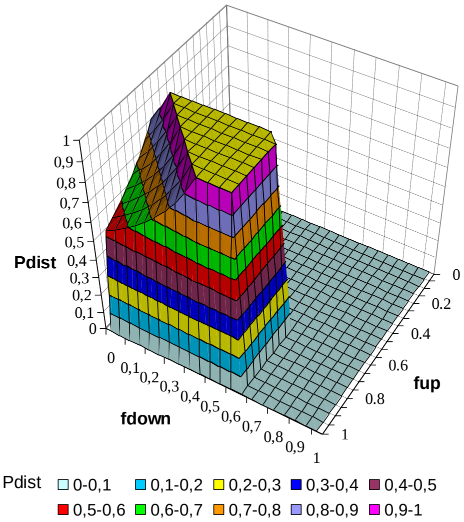

Fig. 8 Successful jamming probability as a function of minimum (f_{down}) and maximum (f_{up}) shifted sweep frequency, T_{mess}/T_{sw}=0.5, shifted f_{mess}=0.6.

Figures 6 and 7 are plotted for the case when the complete sweep cycle from the minimum to the maximum frequency has the duration five times greater than the activation message (T_{mess}/T_{sw}=0.2), while Figure 8 is plotted for T_{mess}/T_{sw}=0.5. Figure 6 corresponds to the shifted value of activation signal frequency 0.3 (i.e., the real value of this frequency is $f_{minsw}+(f_{maxsw}-f_{minsw})\cdot 0.3$), while the value of shifted frequency for the figures 7 and 8 is 0.6.

The main conclusion from the graphs in figures 6, 7 and 8 is that P_{dist} may reach the value equal to 1, which is not possible if the whole range of frequencies is swept. But, it is also possible that activation frequency is never in the range of jammed frequencies, when it is P_{dist}=0. That's why the good estimation of the frequency range used for activation signal transmission is very important.

The second possibility to increase probability of successful jamming is simultaneous implementation of sweep signal generation in several frequency bands (the whole available frequency range is swept in each such formed frequency band). In this way, multisweep signal generation is implemented at the same speed in *m* bands in the same time. That's why P_{dist} is also increased *m* times until the value P_{dist}=1 is reached. In the solution presented in [13], the value of *m* is 7.

6. The Influence of RCIED Activation Message Characteristics on Successful Jamming Probability

Until now we supposed in the analysis that jamming signal characteristics guarantee successful jamming if a signal appears in a channel where RCIED activation message is transmitted. However, it is possible that this condition is not satisfied (first of all, because of a low jamming signal level, as already expressed in Section 3). Even in the case that jamming signal level is satisfactory (i.e. greater than the level of RCIED activation message), it is possible that BER<1. It means that each bit in activation message will be changed in relation to its exact value with probability equal to BER. The total number of bits forming an activation message is n. It is supposed that error correction coding is not applied which means that activation message will be successfully transmitted, if all bits in its content are correctly transmitted. Probability of message successful transmission is therefore:

$$P_{sa} = (1 - BER)^n, \tag{14}$$

and successful jamming probability will be:

$$P_{dist} = 1 - P_{sa} = 1 - (1 - BER)^n. \tag{15}$$

Figure 9 presents probability of successful RCIED activation jamming (P_{dist}) as the function of the number of bits n, which form a message and BER. This graph is obtained on the base of Eq. (15). The importance of this graph is that it presents the dependence of P_{dist} on two independent variables. We shall suppose that satisfactory combinations of n and BER give as a result P_{dist}>0.95. In the case that activation message consists of only one byte (8 bits) the desired jamming probability is achieved for BER≈0.35.

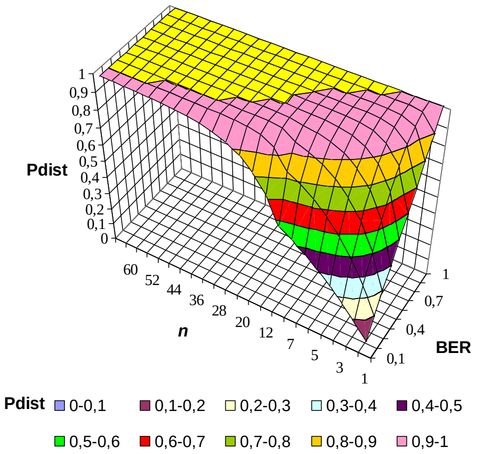

Fig. 9 Successful jamming probability (P_{dist}) as a function of message length (n) and bit error rate (BER).

There is a great variety of transmission techniques, which may be used for RCIED activation message sending. It is possible to use an algorithm, which corrects certain number of incorrectly transmitted message bits. In this paper we consider algorithms, which correct one or two message bits. In the case of a code able to correct one message bit, a message will be successfully transmitted if no more than one bit is faulty. When there are no faulty bits, message successful transmission probability may be determined according to (14). In the other possible case, when one bit is faulty, successful message transmission may be calculated from

$$P_{sa1} = \binom{n}{1} \cdot BER \cdot (1 - BER)^{n-1}. \tag{16}$$

Successful jamming probability on the base of (14)–(16) is then:

$$P_{dist} = 1 - P_{sa} - P_{sa1} = \\ = 1 - (1-BER)^n - \binom{n}{1} \cdot BER \cdot (1-BER)^{n-1}. \qquad (17)$$

If we have a code with a possibility to correct two faulty message bits, a message will be correctly transmitted if there are not more than two faulty message bits. The successful transmission probability when two bits are faulty may be determined as

$$P_{sa2} = \binom{n}{2} \cdot BER^2 \cdot (1-BER)^{n-2}, \qquad (18)$$

i. e., total successful jamming probability in this case will be:

$$P_{dist} = 1 - P_{sa} - P_{sa1} - P_{sa2} = \\ = 1 - (1-BER)^n - \binom{n}{1} \cdot BER \cdot (1-BER)^{n-1} - \binom{n}{2} \cdot BER^2 \cdot (1-BER)^{n-2}. \qquad (19)$$

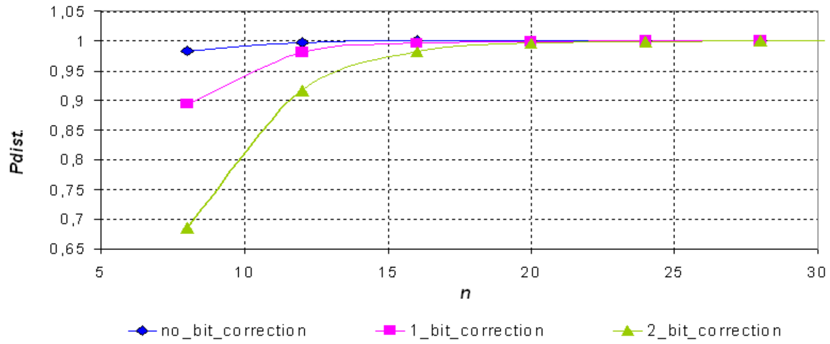

Fig. 10 Successful jamming probability in the case of error correction coding application to RCIED activation message for *BER*=0.4.

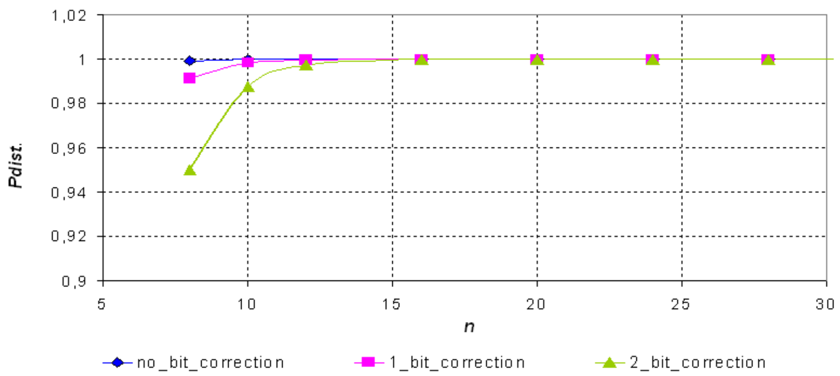

Fig. 11 Successful jamming probability in the case of error correction coding application to RCIED activation message for *BER*=0.6.

The graphs in figures 10 and 11 present successful jamming probability as the function of the number of bits, which form activation message. These graphs are obtained using formulas (15), (17) and (19). The parameter in the figures is the number of bits, whose content may be corrected in the RCIED receiver on the basis of implemented algorithm for error correction. The graphs in Figure 10 and Figure 11 are presented for *BER*=0.4 and *BER*=0.6, respectively. The aim is to achieve as greater as possible value of P_{dist} and for practical considerations satisfactory jamming probability is supposed to be P_{dist}=0.95, as already pointed out. This target value is achieved for *BER*=0.6 in the case of very robust error correction coding algorithm, which may correct two bit errors in a message even in the case of very short messages, whose length is only 8 bits. Such short messages are not real to exist in practice.

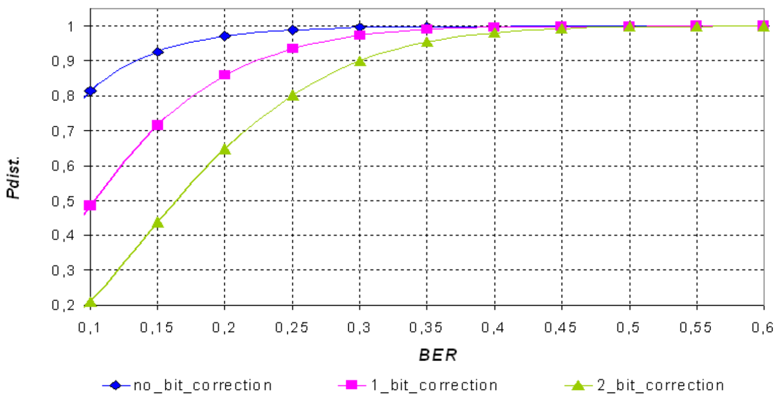

Fig. 12 Successful jamming probability in the case of error correction coding application to RCIED activation message for *n*=16 bits.

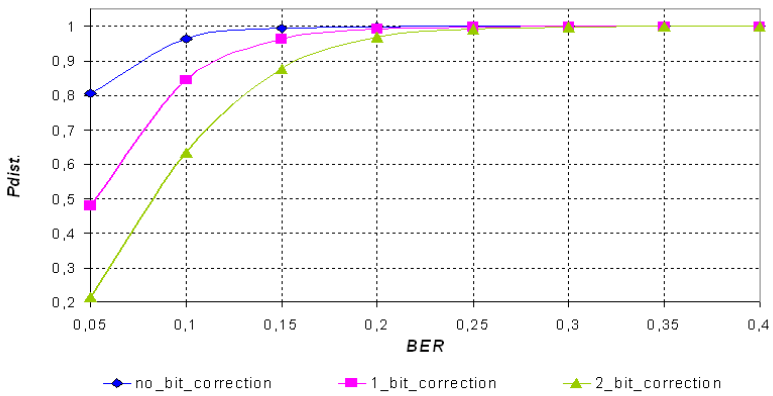

Fig. 13 Successful jamming probability in the case of error correction coding application to RCIED activation message for *n*=32 bits.

Figures 12 and 13 present successful jamming probability as a function of *BER* in the case that activation message consists of only 16 bits (Figure 12) or 32 bits (Figure 13).

The results are also obtained on the base of expressions (15), (17) and (19). A satisfactory jamming probability P_{dist}>0.95 is now reached for *BER*=0.35 if the message consists of 16 bits, or for *BER*=0.19 if the message consists of 32 bits when algorithm with two bits correction is applied.

Figures 14 and 15 present successful jamming probability as a function of *n* and *BER* for the case when one bit error in RCIED activation message may be corrected (Figure 14) and when two bit errors may be corrected (Figure 15). Graph in Figure 14 is obtained using (17) and graph in Figure 15 using (19). The results from these two figures make a complete with the graph in Figure 9.

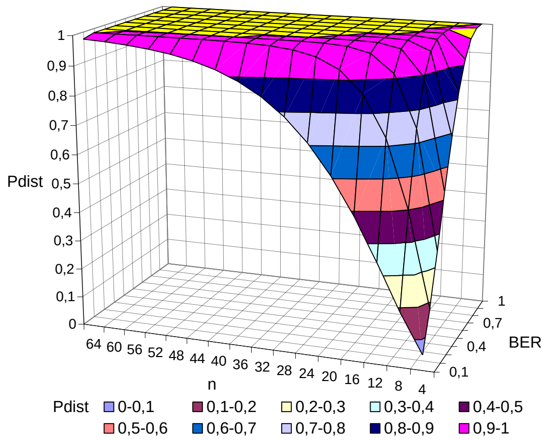

Fig. 14 Successful jamming probability as the function of *n* and *BER* when it is possible to correct one bit error.

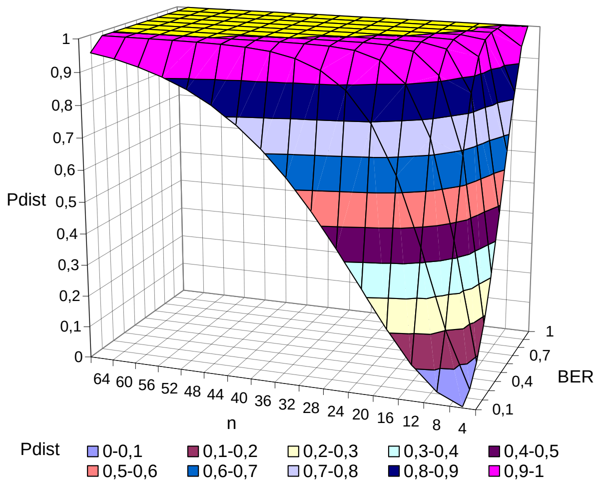

Fig. 15 Successful jamming probability as the function of *n* and *BER* when it is possible to correct two bit errors.

The results from [18] may be used to estimate the necessary jamming signal power relative to activation message level in order to achieve desired *BER* values. Graphs in [18] are presented for often applied MPSK (*M*-ary Phase Shift Keying) activation signal, where the values of *M* are 2 (BPSK – Binary PSK), 4 (QPSK – Quaternary PSK), 8 and 16. When the message consists of relatively small number of bits (16 in Figure 12 or 32 in Figure 13), it is expected that BPSK or QPSK is applied.

It is very interesting to make additional comparison between the sweep speed when active jamming is implemented and the necessary signal detection time when reactive jamming is realized by FFT analysis. The application of very fast, modern digital signal processors (DSP) presented in [24], [25] allows the achievement of very short detection times [10], which are even significantly smaller than the time necessary to realize one sweep cycle. It can be often found in literature that active jamming is more reliable than reactive jamming. We may point out as the conclusion that this statement is certainly valid only if wide-band noise jamming is used as a method of active jamming. When sweep signal is used for active jamming, it is possible to find the frequency of RCIED activation signal by FFT analysis and to start jamming signal generation in a shorter time than to complete one sweep cycle over all envisaged frequencies. The FFT analysis rate depends on the applied DSP clock frequency, the number of activated DSP cores and the application of additional hardware accelerator in DSP. The clock for DSP core is obtained by PLL components, which may generate very fast clock signals [26]. As there are even three factors, which may increase FFT calculation speed, the analysis flow rate is several tens of times greater when these factors have maximum values than if they have minimum ones. The consequence is that for some combinations of considered factors, active sweep jamming is more reliable and for some others reactive jamming is better solution. The more detailed quantitative comparison of these two jamming scenarios, which may be realized by components presented in [17], [24] and [25] will be the subject of our future analysis.

7. Conclusions

There are two techniques applied to RCIED activation jamming: active and reactive jamming. Frequency sweep as the most widely used technique for active jamming is analyzed in this paper. In the introductory section it is explained why sweep jamming is important for application and what are its advantages and disadvantages. We emphasized the condition for certainly successful jamming and presented the method for jamming probability calculation in the case that jamming is not certainly successful. In the analysis two methods for sweep signal generation are compared considering successful jamming probability and all formulas are developed for both methods. The attention is devoted to practical sweep hardware implementation, where linearly variable sweep frequency is approximated by stepwise change of signal frequency. It is proved that the cause of unsuccessful jamming may be not only too slow signal frequency sweep comparing to the RCIED message duration, but also excessively great frequency step change in stepwise jamming signal realization. The particular paper section is devoted to successful jamming probability determination when starting and ending sweep jamming frequencies are varied. At the end we presented the method for successful jamming probability calculation in general. We analyzed the influence of transmission *BER*, RCIED activation message length and applied algorithm for error correction coding of activation messages on the calculated jamming probability value.

Fig. 16 RCIED jammer at Defense & Security International Exhibition Eurosatory 2018 in Paris

This paper is the enhanced version of the contribution [1]. Comparing to [1], the new Section 5 explains how changes of starting and ending sweep frequency influence the successful jamming probability. The conclusions from the new, finishing part of Section 3 (Eq. (9) and Eq. (10)) are important for the jamming practical realization. It is proved in this part of the paper that jamming may be unsuccessful, although sweep speed satisfies the condition $T_{mess}>T_{sw}$. The results in Section 6 are completed by new graphs in Figure 12 and Figure 13, which present successful jamming probability as the function of *BER* when activation message length is fixed. This is the other way to present the results from Figure 10 and Figure 11, where message duration was variable and *BER* was fixed. The graphs in Figure 14 and Figure 15 are also new in comparison to [1]. They present the value of successful jamming probability as a function of, together, number of bits forming a RCIED activation message (n) and *BER*. When we compare these two graphs to the graph in Figure 9, we can conclude how bit error correction algorithm in RCIED activation message contributes to successful jamming probability decreasing. The importance of the additional, last paragraph in Section 6 is that it emphasizes the fact that reactive jamming may be in some cases more reliable than active jamming, realized by sweep signal generation. Having in mind our study of existing published papers, such statement is not proved in the available literature. We plan to proceed with more detailed quantitative analysis of this problem in our future developmental work. And, last but not least, in the Section 1 we have added the main results from [18], which are related to quantitative comparison of necessary signal power in the case of sweep jamming and wide-band jamming for several modulation techniques. The results are presented without detailed mathematical proof, which is presented in [18].

The presented analysis is based on long standing IRITEL experience in the systems development for RCIED activation jamming [13], [18], [27] and for jammers intended for other applications [11], [12], [16]. The analysis procedures and RCIED jamming implementation are mainly related to [13]. The realized jammer was presented with the great success at the Eurosatory 2018 – Defense & Security International Exhibition in Paris, Figure 16. Having in mind the applications of new technologies in our RCIED jammer implementations, such as absorptive filter at power amplifiers outputs, new theoretical approaches and papers related to this topic are of interest like [28].

Acknowledgement: *The paper is realized in the framework of the project TR32051, which is cofinanced by Ministry of Education, Science and Technological Development of the Republic of Serbia.*

REFERENCES

[1] 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, June 11-14, 2018.

[2] 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 2013 IEEE International Conference on Communications ICC, Budapest, June 2013.

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

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

[5] L. Karlsson, "Method, System and Apparatus for maximizing a Jammer's Time-on-Target and Power-on-Target", United States Patent Application, Publication No. US 2006/0164283 A1, 27. July 2006.

[6] M. Tanatwy, "Responsive Communication Jamming Detector with Noise Power Fluctuation using Cognitive Radio", *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 10, pp. 5967–5973, October 2014.

[7] 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, June 2013, pp. 149-154.

[8] 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, June 2011, pp. 47-52.

[9] 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/.

[10] Selena Electronics, "RSS intelligent reactive stationary jammer and RSV vehicle reactive jammer", in "Electronics Warfare Systems: Jamming Solution", 2015.

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

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

[13] 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, November 2017, pp. 151–154.
[14] Phantom Technologies LTD., TSecNet s.r.l., SGS, "Selective Cellular Jammer", http://www.tsecnet.com/assets/docs/TSECNET%20Cellular_Selective_Jammer.pdf.
[15] "GBPPR 800MHz Cellular Phone Jammer", http://67.225.133.110/~gbpprorg/mil/celljam1/.
[16] N. Remenski, B. Pavić, P. Petrović, M. Mileusnić, 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", 2010., http://www.iritel.com/images/pdf/cj-1p-e.pdf, (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.
[17] Analog Devices, *1 GSPS, 14-Bit, 3.3V CMOS Direct Digital Synthesizer AD9910*, Data Sheet, 2017, http://www.analog.com/media/en/technical-documentation/data-sheets/AD9910.pdf.
[18] M. Mileusnić, P. Petrović, B. Pavić, V. Marinković-Nedelicki, V. Matić and A. Lebl, "Jamming of MPSK Modulated Messages for RCIED Activation", paper accepted for 8th International Scientific Conference on Defensive Technologies OTEH 2018, Belgrade, 11-12th October 2018.
[19] Elbit Systems EW and Signit – Elisra: MRJ Family – Miniature Reactive Jammer Family - for Eurosatory 2016 exhibition, http://elbitsystems.com/media/MRJ.pdf.
[20] Elaman German Security Solutions, "Jammer – Principle of Operation", https://ht.transparencytoolkit.org/rcs-dev%5Cshare/Documentation/Gamma/ELAMAN/elamancat/Jammer/Jammer%20Principles%20of%20Operation.pdf.
[21] M. Strasser, C. Pöpper, S. Čapkun and M. Čagalj, "Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping", IEEE Symposium on Security and Privacy. Oakland, CA, USA, May 2008.
[22] K. Burda, "The Performance of Follower Jammer with a Wideband Scanning Receiver", *Journal of Electrical Engineering*, vol. 55, no. 1-2, pp. 36–38, 2004.
[23] A. GuLyÁS, "The Radio Controlled Improvised Explosive Device (RCIED) threat in Afghanistan", *AARMS*, vol. 12, no. 1, pp. 1–11, 2013.
[24] X. Li and E. Blinka, "Very large FFT for TMS320C6678 processors", Texas Instruments, 2015, pp. 1–6.
[25] Texas Instruments, "Multicore Fixed and Floating-Point Digital Signal Processor", SPRS691 – November 2010 – Revised March 2014, pp. 1–242.
[26] W. Wang, X. Chen, H. Wong, "A System-on-Chip 1.5GHz Phase Locked Loop Realized Using 40nm CMOS Technology", *Facta Universitatis, Series: Electronics and Energetics*, vol. 31, no. 1, pp. 101–113, March 2018.
[27] P. Petrović, N. Remenski, P. Jovanović, V. Tadić, B. Pavić, M. Mileusnić, 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", 2011., http://www.iritel.com/images/pdf/wrj2004-e.pdf.
[28] S. C. Dutty Roy, "A New Lumped Element Bridged-T Absorptive Band-Stop Filter", Facta Universitatis, Series: Electronics and Energetics, vol. 30, no. 2, pp. 179–185, June 2017.