Analysis of Jamming Successfulness against RCIED Activation

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

***Abstract*— In this paper we first briefly present main features of active and reactive jamming of remote controlled improvised explosive devices activation. We emphasized main problems in such systems implementation. The characteristics of frequency sweep as the most widely used technique of active jamming are analyzed: 1) sweep speed, 2) condition for certainly successful jamming, 3) successful jamming probability if jamming is not certainly successful, and 4) step of stepwise frequency change in practical frequency sweep realization. The separate paper section is devoted to the successful jamming probability calculation in general. The presented results are the contributions to jamming equipment development in IRITEL, but also are more widely applicable to the analysis of the other similar jamming systems development.**

***Index Terms*— Jammer, remote controlled improvised explosive devices, frequency sweep, successful jamming probability**

I. Introduction

Today the world is faced with the growing challenges in the fight against terrorist attacks. Techniques and methods of terrorist attacks are constantly changed and improved. That's why devices for the fight against these attacks must be also changed and accommodated.

Improvised explosive devices (IED) are implemented more and more as the device intended for terrorism. Today such devices are activated by messages, which are transmitted by wireless communications. In the fight against such activation principles we are faced with very difficult demands. It is necessary to act against IED activation signal, which may appear anywhere in very wide frequency range. The activation signal duration is completely unpredictable, from the time which is not greater than 1μs to the time period of several ms or even tens of ms. The maximum signal power used for IED activation message transmission may be in the range from several mW to several W and even tens of W [1]. That's why signal power at IED receiver input may be very different, due to the variation of distance to the message generation position. This distance may be in the range from several tens of meters to several kilometres, depending on the used radio communication system and strategic goals. Maximum ranges of some radio communication technologies, intended for IED activation are presented in [1]. Already on the base of this brief survey it is obvious what challenges are in front of designer of devices for the fight against remote controlled improvised explosive devices (RCIED).

The two most widely implemented jamming techniques against RCIED activation are reactive and active jamming, [2]. Reactive jamming becomes more and more popular, because less power is necessary for its realization than in the case of active jamming. When reactive jamming is realized, it is necessary to detect activation signal appearance and its frequency and then to generate jamming signal only in the intercepted channel. There is a variety of suggested methods, whose goal is as fast as possible and as reliable as possible activation signal detection [1]-[5]. Among these solutions for activation signal transmission, especially interesting one can be found in [2]. It is related to the case when RCIED activation signal is not sent as a separate independent signal, but timing channel, normally intended for regular function of the protected device, is maliciously used as a covert channel to send an activation signal. Jamming of such a signal is a great threat.

The main problem in reactive jamming implementation is to detect activation message during its duration in order to generate jamming signal before the message end, thus preventing RCIED activation. The detection speed analysis of activation signal for different detection methods implemented in reactive jammers is presented in [6]. In practice, RCIED activation signal should be detected in 1-10ms and should last at least 30% of time used for activation signal transmission [7]. In solution presented in [8] detection speed is less than 1ms. The achieved frequency scanning speed is even greater in the solution presented in [9]: it is 30000GHz/s, meaning that typical frequency range of 6GHz may be scanned in only 200μs. On the contrary, it is not necessary to detect activation signal at active jammers, because jamming signal is always generated irrespective of activation signal existence. In principle, successful jamming probability is greater for active than for reactive jammers, but the necessary transmitter power is significantly greater to realize jamming [2]. When active jamming is implemented, some problems may arise. In fact, the most reliable method for jamming realization is simultaneous, constant wide-band jamming signal generation in the whole predicted frequency range. In that case available transmitter power is used in the whole frequency range. As a consequence, emission power in a channel with an activation signal is relatively small, and, perhaps, not enough to prevent IED activation signal reception. The other possible and most often implemented signal generation method in this case is frequency sweep [10]-[12]. In this case it is possible to concentrate significantly greater power in one channel where activation message is transmitted in

Mladen Mileusnić is with the Institute IRITEL, 23 Batajnički put, 11080 Belgrade, Serbia (e-mail: mladenmi@iritel.com).

Branislav Pavić is with the Institute IRITEL, 23 Batajnički put, 11080 Belgrade, Serbia (e-mail: bane@iritel.com).

Verica Marinković-Nedelicki is with the Institute IRITEL, 23 Batajnički put, 11080 Belgrade, Serbia (e-mail: verica@iritel.com).

Predrag Petrović is with the Institute IRITEL, 23 Batajnički put, 11080 Belgrade, Serbia (e-mail: presa@iritel.com).

Dragan Mitić is with the Institute IRITEL, 23 Batajnički put, 11080 Belgrade, Serbia (e-mail: mita@iritel.com).

Aleksandar Lebl is with the Institute IRITEL, 23 Batajnički put, 11080 Belgrade, Serbia (e-mail: lebl@iritel.com).

comparison with wide-band jamming strategy, but there is a risk that generated sweep signal would not reach the desired channel in time, while activation signal is yet not finished. Besides this, high constant signal power for active jamming means that jammer may be easier detected, thus endangering personnel who use this jamming system and increasing their vulnerability to enemy attack, [13].

As we have seen from this short introductory presentation, both active and reactive jamming have their advantages and disadvantages. It is not possible to exclude one of them and to give priority to the other. That's why they are often both together implemented in the field solutions [9], [13]. In order to increase jamming efficiency, also often two or more separated jammers are present near one to the other, each one of them jamming its special frequency range. In such a situation synchronization of their mutual function is very important, because jamming signal from one of them may be detected as RCIED activation signal in the other. Special attention should be paid to this problem solving, [7].

The method of frequency sweep realization to jam 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 strategies in sweep signal generation considering jamming reliability are analyzed in section 4. Section 5 deals with the calculation of successful jamming probability, when signal physical characteristics do not guarantee secure jamming. At the end, section 6 is related to conclusions.

II. Sweep Speed at IED Activation Jamming

Let us suppose that it is necessary to jam a signal, which may cause activation of improvised explosive device (IED) and which appears somewhere in a frequency band of total width W (in Hz) [14]. Jamming is realized using linear variation of jamming signal frequency (*sweep*) in the defended frequency band of the width $W=f2-f1$, where $f1$ is minimum and $f2$ is maximum frequency of sweep signal (Figure 1). Jamming signal characteristics in relation to IED activation signal (first of all jamming signal level) are such defined that jamming is completely successful (P_{dist}=1) under the condition that jamming signal appears in the frequency band (channel) where activation signal is transmitted. There are two possibilities at the place of IED receiver: jamming signal and activation signal have similar level (in this case IED receiver detects activation message, but with changed content) or jamming signal level is significantly greater than activation signal level (IED receiver does not detect activation message, but only the jamming signal) [15]. The period of one sweep cycle is T. Then, let us suppose that 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 during IED activation message (time interval T_c in Figure 1), we shall suppose that jamming is successfully realized. In this moment we also suppose that jamming signal appears once during the IED activation message duration.

Sweep speed will be defined as frequency change speed:

$$v_{sw} = \frac{W}{T_{sw}} \tag{1}$$

Jamming will be certainly successful (i.e. jamming probability will be P_{dist}=1) if the one cycle time of frequency change from $f1$ to $f2$ satisfies a condition:

$$T_{sw} \le T_{mess} \tag{2}$$

where T_{mess} is IED activation message duration.

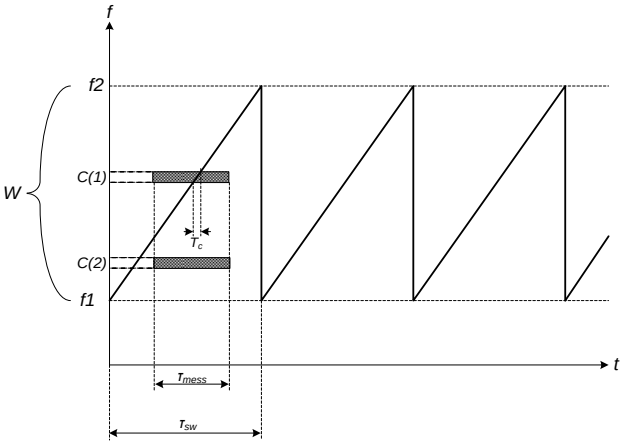

Fig. 1. IED activation jamming when jamming signal frequency is linearly changed.

It follows from equations (1) and (2)

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

Let us further suppose that single jamming is not enough to be successful. Therefore, it is necessary that jamming signal appears m times in a considered channel during message duration to achieve satisfactory IED activation jamming probability. In such a case sweep speed must be increased. Formula (3) is, consequently changed to:

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

Expressions (3) and (4) define lower limit of sweep speed to assure successful jamming. It is, in fact, a time needed to guarantee that jamming signal at least once (in the case of equation (3)) or m-times (in the case of equation (4)) „crosses" the considered channel when it changes its frequency.

III. Successful Jamming Probability for Frequency Sweep Implementation

Let us suppose that the condition from equation (2) is not satisfied. In that case it is P_{dist}<1. 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 by a jamming signal, while the message from the frequency band $C(2)$ will not be blocked, because jamming signal at no time „comes" to the band $C(2)$ during time interval T_{mess}.

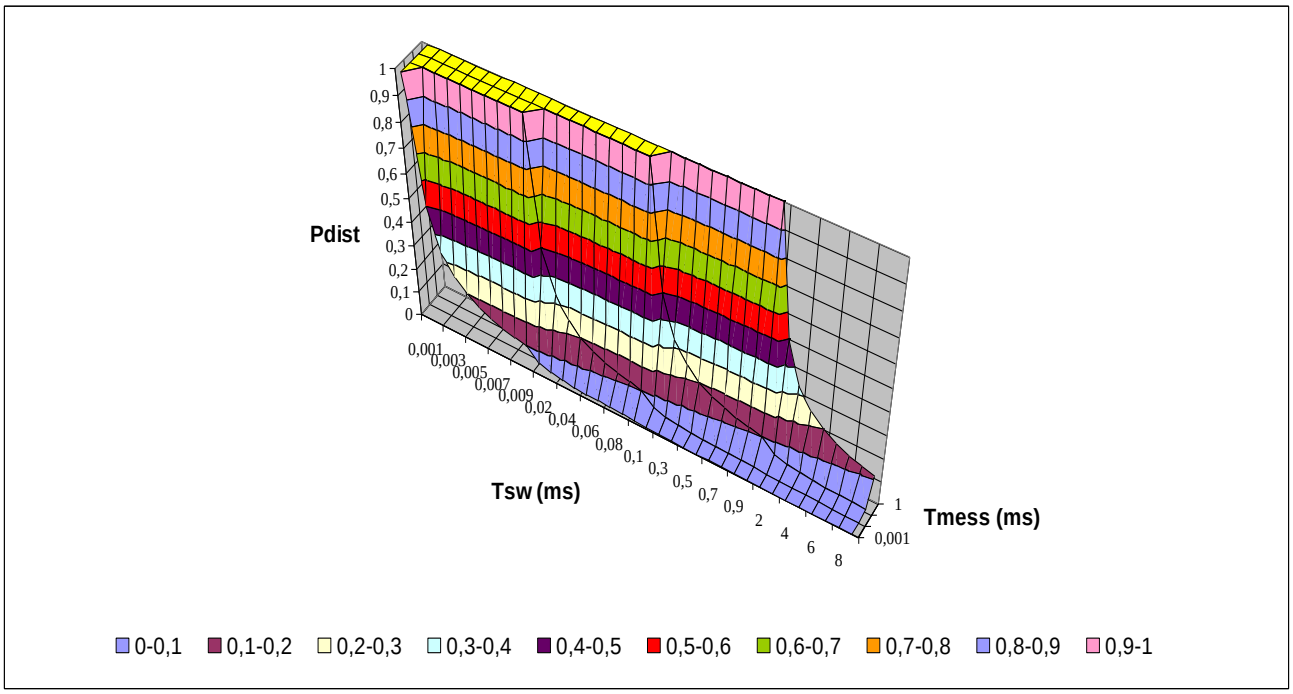

Fig. 2. IED successful jamming probability as a function of sweep time and message duration.

Let us suppose that 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 such that it is k>1, i.e. one sweep cycle period is greater than message duration. In this case IED activation signal jamming is not guaranteed. The probability of IED 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}), which is obtained on the basis of equation 6. It is obvious that this probability is equal 1 for T_{mess}>T_{sw}.

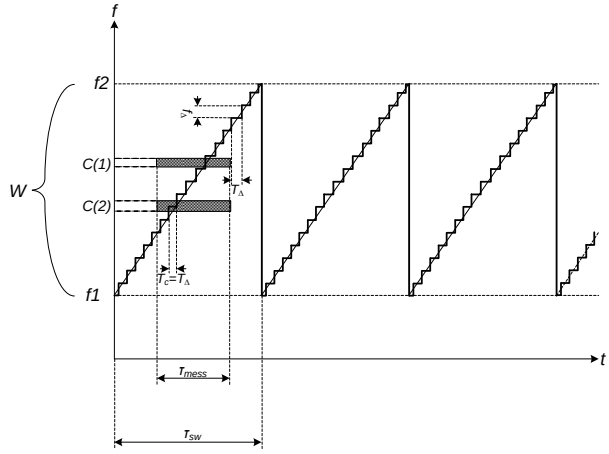

Fig. 3. Practical realization parameters of IED activation jamming.

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 defining the time step of exactly determined signal frequency. This is practically 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 second manner as

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

If it is satisfied the condition

$$f_\Delta \le C \tag{8}$$

jamming will be certainly successful. If not, two situations are possible: 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) or these two frequencies coincide during some time interval (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, we choose the minimum value of T_Δ, which is allowed by applied hardware components [16]. The calculation is performed for such defined T_Δ value.

IV. Comparison of Detection Probability for Two Sweep Signal Generation Methods

Figure 4 presents two methods for sweep signal generation. In the first case a frequency is linearly changed always in the direction from the minimum value to the maximum one (Figure 4a), while in the second case, when a frequency reaches its maximum value, it starts to linearly decrease (Figure 4b). In both cases two IED activation messages are presented together with a sweep signal. IED activation messages are located in two different frequency bands: *C(1)* and *C(2)*. The message length (T_{mess}) is equal to the sweep time (T_{sw}). If a sweep signal is generated

according to Figure 4a, jamming is always successful, independent of the part of frequency range between *f1* and *f2* where IED activation signal appears. However, if sweep signal is generated according to Figure 4b, jamming may be successful (for a signal in a channel *C(2)*, where jamming signal two times „crosses“ over the channel with activation message), but may be also unsuccessful (for a signal in a channel *C(1)*, because jamming signal does not „cross“ channel *C(1)* in a time of message duration). It is important to emphasize that jamming is certainly successful if the little changed condition comparing to formula (2) is satisfied:

$$2 \cdot T_{sw} \leq T_{mess} \tag{9}$$

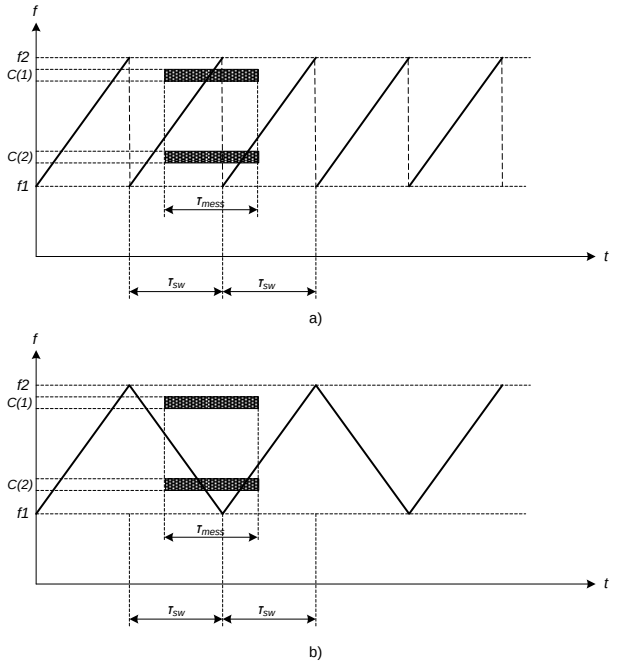

Fig. 4. Detection of IED activation signal for two methods of sweep signal generation.

Successful jamming probability for a jamming signal realization as in Figure 4b is determined starting from formula (9) and is:

$$P_{dist} = \frac{1}{2 \cdot k} = \frac{T_{mess}}{2 \cdot T_{sw}} \tag{10}$$

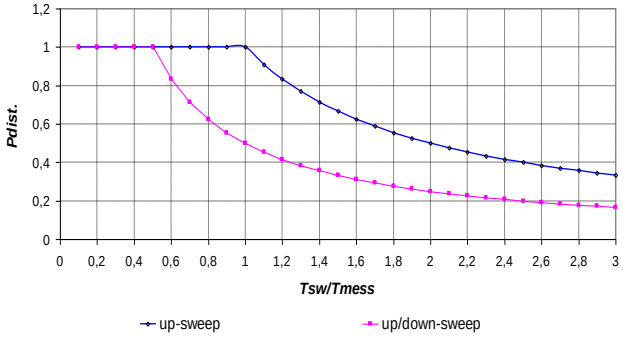

Fig. 5. Successful jamming probability as a function of relation T_{sw}/T_{mess} for two methods of sweep signal generation.

Figure 5 presents probability variation of IED activation signal jamming 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 starting from the smallest frequency for all values $T_{sw}/T_{mess}>0.5$.

V. RCIED Activation Jamming When Jamming Signal Level is too Small

In analysis until now we supposed 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). In such a case each bit in activation message will be changed in relation to its exact value with probability *BER* (*bit error rate*). Let us, further, suppose that total number of bits, forming an activation message is *n*. We suppose that error correction coding is not implemented. In such a case activation message will be successfully transmitted, if all bits in its content are successfully transmitted. Probability of message successful transmission is therefore:

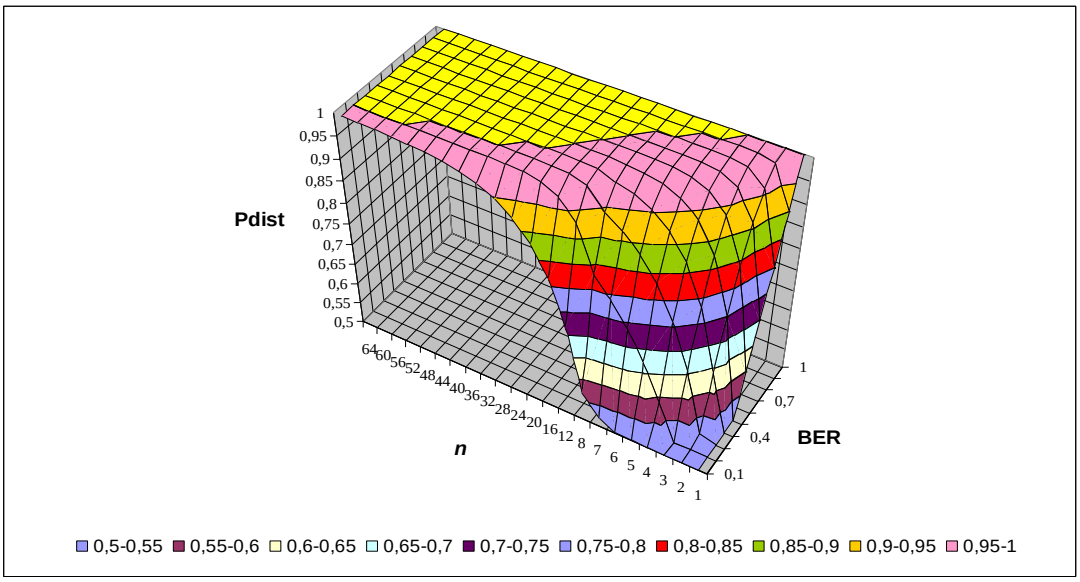

Fig. 6. Successful jamming probability (P_{dist}) as a function of message length (*n*) and bit error rate (*BER*).

$$P_{sa} = (1 - BER)^n \tag{11}$$

i.e., successful jamming probability will be:

$$P_{dist} = 1 - P_{sa} = 1 - (1 - BER)^n \tag{12}$$

Figure 6 presents RCIED activation successful jamming probability (P_{dist}) as the function of the number of bits, which form a message (message length – n) and bit error rate (BER). This graph is obtained on the base of equation (12). We shall suppose that satisfactory combinations of n and BER, give as a result P_{dist}>0.95. In a case that activation message consists of only one byte (8 bits), the desired jamming probability is achieved for $BER \approx 0.35$.

A message coded on the base of algorithm, which corrects certain number of incorrectly transmitted message bits, may be implemented for RCIED activation. In this paper we consider possibilities to 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 all message bits are transmitted correctly or if only one bit in a message is faulty. In the first case message successful transmission probability may be determined according to (11), while in the second case, when one bit is faulty, successful message transmission may be calculated from

$$P_{sa1} = \binom{n}{1} \cdot BER \cdot (1 - BER)^{n-1} \tag{13}$$

Successful jamming probability on the base of (11)–(13) is then:

$$\begin{aligned} P_{dist} &= 1 - P_{sa} - P_{sa1} = \\ &= 1 - (1 - BER)^n - \binom{n}{1} \cdot BER \cdot (1 - BER)^{n-1} \end{aligned} \tag{14}$$

If we have a code with a possibility to correct two faulty message bits, a message will be correctly transmitted if all message bits are correctly transmitted or if one or two message bits are incorrectly transmitted. The successful transmission probability when two bits are faulty may be determined according to

$$P_{sa2} = \binom{n}{2} \cdot BER^2 \cdot (1 - BER)^{n-2} \tag{15}$$

i.e., successful jamming probability will be:

$$\begin{aligned} P_{dist} &= 1 - P_{sa} - P_{sa1} - P_{sa2} = \\ &= 1 - (1 - BER)^n - \binom{n}{1} \cdot BER \cdot (1 - BER)^{n-1} - \\ &- \binom{n}{2} \cdot BER^2 \cdot (1 - BER)^{n-2} \end{aligned} \tag{16}$$

The graphs in figures 7 and 8 are obtained using formulas (12), (14) and (16). They present successful jamming probability as the function of the number of activation message bits and the characteristics of implemented error correction coding algorithm (i.e. the number of bits, whose content may be corrected in the RCIED receiver). The graph in Figure 7 is presented for BER=0.4, while the graph in Figure 8 is presented for BER=0.6. A satisfactory jamming probability rate P_{dist}>0.95 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.

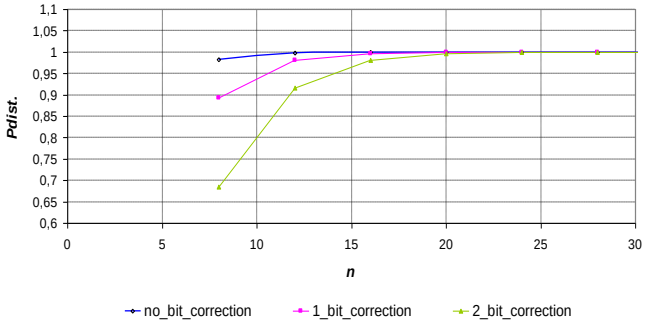

Fig. 7. Successful jamming probability in the case of error correction coding implementation in RCIED activation message for BER=0.4.

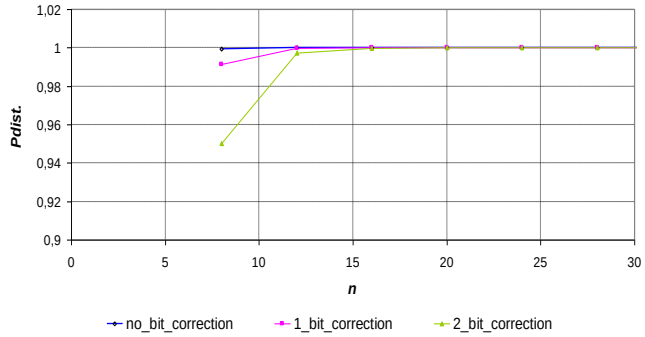

Fig. 8. Successful jamming probability in the case of error correction coding implementation in RCIED activation message for BER=0.6.

VI. Conclusion

In this paper we presented the system performances for active RCIED activation jamming. Frequency sweep as the most widely used technique in this case is analyzed. We emphasized the condition for certainly successful jamming and presented the method for jamming probability calculation when jamming is not certainly successful. In the analysis flow two methods for sweep signal generation are compared and all formulas are developed for both methods. The attention is also devoted to practical sweep hardware implementation, where linearly variable sweep frequency is approximated by stepwise change of signal frequency. At the end we presented the method for successful jamming probability calculation in general. We analyzed the influence of transmission BER, message duration and applied algorithm for error correction on the calculated jamming probability value.

The presented analysis is based on long standing IRITEL experience in the systems development for RCIED activation jamming [10]-[12], and the obtained results are related to the last one [12]. The advantages, but also the shortcomings of active jamming in relation to reactive jamming are emphasized in the paper.

Acknowledgment

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

[2] S. D'Oro, L. Gallucio, G. Morabito, S. Palazzo: „Efficiency Analysis of Jamming-based Countermeasures against Malicious Timing Channel in Tactical Communications“, 2013 IEEE International Conference on Communications ICC, Budapest, June 2013.

[3] J. Mietzner, P. Nickel, A. Meusling, P. Loos, G. Bauch: „Responsive communications jamming against radio-controlled improvised explosive devices,“ *IEEE Communications Magazine*, Vol. 50, Issue 10, pp. 38-46, October 2012.

[4] 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, Issue 10, pp. 5967-5973, October 2014.

[5] M. Wilhelm, I. Martinović, J. Schmitt, V. Lenders: „Reactive Jamming in Wireless Networks: How Realistic is the Threat?“, 4th ACM Conference on Wireless Network Security (WiSec '11), ACM, Hamburg, pp. 47-52, June 2011.

[6] T. Trump, I. Müürsepp: „Detection Speed of Responsive Communication Jamming Detectors“, Recent Advances in Telecommunications and Circuits“, 2nd International Conference on Circuits, Systems, Communications, Computers and Applications, Dubrovnik, June 2013, pp. 149-154.

[7] G. Kumaraswamy Rao, K. V. Ranga Rao: „Intelligent Jamming Solution to Defeat the Growing Menance of Remotely Controlled Improvised Devices (Rcieds) Using Electronic Counter Measures", International Journal of Electronics Communication and Computer Engineering", Volume 4, Issue 5, 2013., pp. 1479-1488.

[8] 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/

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

[10] "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.

[11] "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.

[12] M. Mileusnić, P. Petrović, B. Pavić, V. Marinković-Nedelicki, J. Glišović, A. Lebl, I. Marjanović: „The Radio Jammer Against Remote Controlled Improvised Explosive Devices“, 25th Telecommunications Forum (TELFOR), November 2017, pp. 151-154.

[13] Elbit Systems EW and Signit – Elisra: „MRJ Family – Miniature Reactive Jammer Family“ - for Eurosatory 2016 exhibition, http://elbitsystems.com/media/MRJ.pdf.

[14] 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.

[15] M. Strasser, C. Pöpper, S. Čapkun, M. Čagalj: „Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping“, IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 2008.

[16] 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.