# Design Problems in Implementation and Control of Malicious Drone Missions Jammers

Jovan Radivojević, Aleksandar Vujić, Mladen Mileusnić, Predrag Petrović, Aleksandar Lebl

*Abstract*— Three important problems related to the malicious drone missions jamming are analyzed in this paper. These problems are: 1) selection of drone signals which are going to be jammed and corresponding signal frequencies, 2) selection of optimum jamming strategies and definition of signal characteristics, and 3) design of reliable and user friendly system control mechanisms. The implemented solution allows jamming of a significant number of signals important for drone operation: video, telemetry and navigation signals. Classic sweeping is modified to multisweep jamming with continuous and discrete sub-bands to increase jamming efficiency. Device control is possible from the PC application software by the application of user friendly menus or from a specially designed module for remote control. The implemented jamming system is presented as well as the characteristics of the generated jamming signals.

*Index Terms*—Malicious drone missions jamming; jamming scenario; remote control; user interface.

#### I. INTRODUCTION

DRONES or unmanned aerial vehicle (UAV) are every day becoming more often implemented devices in replacing humans in dangerous and time wasting missions. As they come to the place of accident by air flight, sometimes they may save people and material resources just because they are faster than other technologies. But, drones are also used in various malicious missions. They may carry explosive to cause numerous victims and damages of many important objects and places such as airports, stadiums, residential areas, governmental facilities, commercial and industrial facilities, and so on. They may be applied for spy missions, smuggling illicit materials over borders or into and out of the prisons [1], [2]. Well prepared drone mission at one place may cause enormous economy loss and problems for the whole world [3] when just one concentrated attack disabled for a pretty long time 5% of world crude oil production. When considering data from Civil Aviation Directorate of the Republic of Serbia [4], more than 95% of drones in Serbia in 2017. were used illegally. All these illegal drones may be the reason of intentionally or unintentionally caused problem. Only these last two data from national and international literature and the short survey of places suitable for drone illegal activities are sufficient to approve the importance of drone effective jamming when their flight is not regularly registered.

### II. THE PROBLEMS TO BE SOLVED

The problems which have to be solved to prevent illicit drone mission may be divided to three groups: 1) what drone signals have to be jammed; 2) what jamming strategies and jamming signal levels are the most effective for successful drone disabling; 3) what control scenario should be implemented to allow easy and reliable user handling the drone jammer.

There is a variety of drones available on the world market. All of them in principle operate using three main signal types: 1) communication signals interchange between the drone and its operator; 2) video and telemetry signals transmission to the operator; 3) satellite navigation signals reception (GPS or GLONASS). The frequencies for the third signal type are standardized, but the frequencies for the first two signal groups depend on the applied drone model. The more detailed analysis has shown that frequencies used for video and telemetry links at the greatest majority of drone types are 433 MHz, 868 MHz, 915 MHz, 1.2 GHz, 2.4 GHz and 5.8 GHz [2], [5] - [7]. The standardized frequencies for GPS and GLONASS systems are 1176 MHz, 1227 MHz and 1.57-1.62 GHz. It is hard to find that any drone jammer may effectively disrupt transmission of signals at each of the emphasized frequencies. Nearly all these frequencies are jammed in [6]; in other cases the dominant goal is to jam frequencies of navigation systems [7] or navigation system plus links on 2.4 GHz and 5.8 GHz [8]. The objective of the presented solution is to realize jamming of all emphasized frequencies for video and telemetry signals transmission in modern solutions and the frequencies for navigation. Such solution has the maximum flexibility and the highest possibilities.

Various jamming strategies are defined and developed for remote control improvised explosive devices (RCIED) activation jamming and also for radio and mobile systems surveillance and jamming. Two basic groups of jamming strategies are active and reactive jamming. The first of them supposes that jamming signal is continually generated. In the second case jamming signal is generated only when drone presence is detected. When considering signal characteristics, sweep and barrage jamming are most widely used as well as their variants and combinations. IRITEL has the great experience in both jamming development and implementation and theoretical analysis for all mentioned applications and

Jovan Radivojević is with the Institute IRITEL, Batajnički put 23, 11080 Belgrade, Serbia (e-mail: jovan.radivojevic@iritel.com).

Aleksandar Vujić is with the Institute IRITEL, Batajnički put 23, 11080 Belgrade, Serbia (e-mail: <u>aleksandar.vujic@iritel.com</u>).

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

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

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

signal generation strategies. References [9] - [18] represent the small part of IRITEL previous solutions relating to the topic of this paper. The goal of our analysis is to select a set of optimum jamming strategies and signal characteristics for effective jamming.

In the field of jammer control, the aim is to provide flexibility of operator handling. It means that the scenario of the first choice is to allow the parameters of the jamming signal to be easily and instantaneously changeable according to operator plans. In the more rigid situations only a set of jamming signal characteristics is defined and operator should make a decision between a priori specified options. This is the second device control procedure. The additional objective which results from these two scenarios is that reliability of control function practical implementation is significantly improved.

### III. DESIGN CONSIDERATIONS

The frequencies which are jammed cover a wide frequency range 433-5800 MHz. It is important to notice that in the range 1620-2400 MHz there are no important frequencies to be jammed. Sweep and barrage jamming as two dominant jamming strategies have specific problems when jamming is applied to the wide bandwidth. When considering sweep jamming, the problem is to achieve very high sweep rate to reliably disrupt very short messages [13], [14]. In the case of pure barrage jamming implementation, the problem is necessity to have too high emission power which is split to the whole applied frequency band even where this is not necessary [15]. These two limiting factors are the reason to split the whole bandwidth into several sub-bands using separate jammer modules which may operate in parallel. We have decided to have five independent modules. Among these modules, the third module in the range 1164-1620 MHz covers the greatest number of frequencies of interest: all frequencies for navigation and one frequency for video and telemetry link. Only this module is sufficient to achieve performances comparable to the majority drone jammer solutions in the world.

Frequencies of the signals which have to be jammed are a priori mainly known. In such a case efficiency of sweep jamming may be improved. For example, it is not necessary to generate sweep signal in the whole third band 1164-1610 MHz, but only in some its parts where the frequencies of interest are located. It is possible to implement two sweep jamming strategies which decrease necessary sweep rate: 1) multisweep with continuous sub-bands (continuously sweeping over some parts of the total frequency band) and 2) multisweep with discrete sub-bands (sweeping only over discrete frequencies within frequency sub-bands). The second of these two variants is innovative in IRITEL jamming systems and not implemented in other solutions according to the authors' knowledge.

Flexibility of operator's jammer handling is achieved both by hardware and software methods. Hardware solutions allow variable gain adjust, precise jamming signal frequencies definition, more discrete frequencies selection for jamming, several (four) different jamming strategies implementation, precise definition of jamming and non-jamming time intervals and selection of one jamming scenario between several (eight) predefined programmed procedures when system is controlled by special developed remote controller. Dealing with software, user interface is intuitive, easily understandable and clear when control is devoted to a PC to support all wide hardware possibilities.

#### IV. THE JAMMER IMPLEMENTATION

IRITEL previous jammer solutions related to drones are presented in [19], [20]. In [19] it is explained how drones are used in friendly missions to improve RCIED activation jamming efficiency: if drone is carrying jamming device, the jamming signal may reach larger distance in comparison to the ground jamming. On the other hand, the main principles of malicious drone jamming system and the frequency spectrum of all implemented jamming strategies are presented in [20].

The block-scheme of the realized jamming system is now presented in the Fig. 1. The system includes the jamming device and separate module for remote control as also the application software for control and management at the distant PC computer.



Fig. 1. Block-scheme of the malicious drone jamming system



Fig. 2. Block-scheme of the EXCITER module and the output module RANGE

The jammer control and management is based on the implementation of processor board TS-7250. This module defines the functional characteristics of the EXCITER blocks for each of the five frequency bands. EXCITER blocks are based on the function of direct digital synthesis (DDS). After jamming signal generation and shaping in the exciter, the output signal level is achieved in the blocks designated by RANGE and further sent towards emission antennas. The signal frequencies in the last two ranges are too high for DDS realization and the function of these two segments is based on the lower frequency signal generation in the local oscillator. The signal in the local oscillator is used to shift the signal generated in DDS modules 4 and 5 to the desired frequency band by the implementation of mixers.

The control unit in the jammer exchanges information with the application software in distant PC and with the module for remote control using Ethernet and RS485 interface. Communication with the module for the remote control is realized over two converters: USB2.0/Ethernet and RS232/RS485.

The simplified, general block-scheme of the modules EXCITER and RANGE is presented in the Fig. 2. After generation of the jamming signal in RF GENERATOR, the signal frequency is up-converted (for the modules 4 and 5). Band pass filter (BPF) is used to finally achieve the desired jamming signal frequency. The obtained signal is then amplified by two amplifier stages, one in the block EXCITER and the other in the block RANGE to achieve the desired jamming signal level.

The appearance of the jammer device is presented in the Fig. 3. Its dimensions are 640 mm x 320 mm x 155 mm. The jammer main connectors are designated in the figure as the connectors for five antennas, Ethernet and RS485 port for the connection to the remote control module and the LAN port to connect the remote PC. The last connector is for power supply 24 V. The measured device power supply current is 28.75 A from 24 V, thus obtaining total power consumption of 690 W when generating all five jamming signals. The system operating temperature range is from -20°C till +55°C. The time interval between the device switch-on till the start of jamming signal characteristics definition change in a device menu till the moment of such signal generation start is 2s. Precision of jamming frequency definition is  $\pm 2kHz$ .





Fig. 3. Jammer device and its connections

Fig. 4. Block-scheme of the module for remote control



Fig. 5. Module for the remote control and its interfaces

| Samozaštitni Ometač  |  |               |             |        | Multisweep             |                                      |                            |                 |                  |                   |    |        |         |
|--|--|---------------|-------------|--------|------------------------|--------------------------------------|----------------------------|-----------------|------------------|-------------------|----|--------|---------|
| Programiranje DNU Baza Podešavanje Napajanje Log Kalibracija |  |               |             |        |                        | MODUL 3 (1164-16<br>Centraina F [MHz | i10) PROGF<br>] Span [MHz] | LAM: 1<br>Lista | Broj frekvencija | Interval ometanja |    |        |         |
| Program  1   |  | Modul         | Tip Signala |        | Nivo[%]                | 1                                    | 1300                       | 50              | 0                | 5                 | 50 | Podela | 🖬 Snimi |
|  |  |               |             |        |                        | 2                                    | 1500                       | 50              | 0                | 5                 | 50 | Podela |         |
| 0 4  |  | 1 (400-470)   | SWEEP       | ~      | < >                    | 3                                    | 0                          | 0               | 0                | 0                 | 0  | Podela |         |
| <ul> <li>○ 5</li> <li>○ 6</li> </ul>                         |  | 2 (800-1000)  | SWEEP       | $\sim$ | < >                    | 4                                    | 0                          | 0               | 0                | 0                 | 0  | Podela |         |
| 07   |  | 3 (1164-1610) | MULTISWEEP  | ~      | < >                    | 5                                    | 0                          | 0               | 0                | 0                 | 0  | Podela |         |
|  |  | 4 (2200-2500) | SWEEP       |        | < >                    | 6                                    | 0                          | 0               | 0                | 0                 | 0  | Podela |         |
| Povezan  |  | 5 (4900-5900) | SWEEP       | ~      | < >                    | 7                                    | 0                          | 0               | 0                | 0                 | 0  | Podela |         |
| ALL OFF  |  |               |             | ∕ Ša   | alji Prog.   🍇 Šalji I | 8                                    | 0                          | 0               | 0                | 0                 | 0  | Podela | Zatvori |
|  |  |               |             |        |                        | -                                    |                            |                 | -                |                   | _  |        |         |
| Zatvori  |  | Im            | e Programa: |        |                        |                                      |                            |                 |                  | 25-May-20         |    |        |         |

Fig. 6. User interface for jammer control when multisweep signal with discrete sub-bands is generated

The block-scheme of the module for the remote control is presented in the Fig. 4. The control board on the base of processor LPC2148 performs information transmission between the remote module and the device over RS485 and Ethernet interface. Dimensions of this module are 170 mm x 120 mm x 55 mm and its appearance is presented in the Fig. 5 with the designated main module parts.

The module for remote jammer control replaces control from the PC. Eight press buttons with the designation 1...8 for activating one of eight predefined scenarios are obvious at the nearer lateral side of this module. Ethernet and RS485 connector for connecting the remote control module and the jammer are the lower connector at the front side and the connector at the distant lateral side, respectively. The upper connector on the front side is intended for flash placement to read predefined jamming scenarios.

Fig. 6 presents user interface (menu) in the PC to generate multisweep signal with discrete sub-bands. In the presented example the signal is generated in the third band. The parameters of the signal may be very flexibly defined. There are two sub-bands (about 1300 MHz and about 1500 MHz and five frequencies in each sub-band). The span between two discrete frequencies is 50 MHz. Jamming for other frequency bands as well as for other jamming scenarios is also applicable.

## V. MEASUREMENT RESULTS

The measurement results for the third frequency band where there is a majority of jammed frequencies are presented in the Table I and in the Fig. 7. Table I presents the achieved maximum jamming signal power for all four jamming strategies. It is possible to define lower and even significantly lower emission signal level. This is especially important when considering GPS and GLONASS signal jamming. Navigation signals have very low level and it is enough to apply lower jamming signal levels. Too high jamming signal levels in this case could disrupt navigation signals at undesirably high distance outside the protected area [19], [21], where it is not necessary.

The Table II presents the maximum power of generated jamming signal for five signal sub-bands (F1 till F5) when sweep jamming strategy is applied. The similar results are obtained also for other three jamming strategies. F1 is the lowest frequency sub-band and F5 is the highest frequency sub-band. F3 covers the majority of applied frequencies for links of different type drones and these five sub-bands cover all drone frequencies mentioned in this paper.

TABLE I THE POWER OF GENERATED JAMMING SIGNAL FOR VARIOUS JAMMING SCENARIOS

| Jamming strategy                  | Generated signal power (dBm) | Generated signal power (W) |  |  |
|-----------------------------------|------------------------------|----------------------------|--|--|
| Sweep                             | 46.4                         | 43.7                       |  |  |
| Multisweep, continual sub-bands   | 46.4                         | 43.7                       |  |  |
| Multisweep,<br>discrete sub-bands | 46.4                         | 43.7                       |  |  |
| Barrage                           | 46.2                         | 41.7                       |  |  |

 TABLE II

 The maximum power of generated jamming sweep signal for various

 FREQUENCY BANDS

| Frequency band | Generated signal power (dBm) | Generated signal power (W) |  |  |  |
|----------------|------------------------------|----------------------------|--|--|--|
| F1             | 47.4                         | 54.9                       |  |  |  |
| F2             | 46.2                         | 41.7                       |  |  |  |
| F3             | 46.4                         | 43.7                       |  |  |  |
| F4             | 44.6                         | 28.8                       |  |  |  |
| F5             | 43                           | 20                         |  |  |  |

It is hardly possible to give exact presentation of jamming successfulness rate as a function of emitted jamming signal power, because it highly depends on the distance between the jammer and the drone. As a consequence, it is difficult to compare the jamming successfulness for various jammers from different suppliers. Two important factors which have great influence on the jamming successfulness, besides generated signal power in a jammer, are signal attenuation coefficient  $\gamma$  and existence/nonexistence of obstacles between the jammer and the drone. The influence of these two factors is even significantly higher than the influence of jamming power. For example, the signal power at a distance *d* from a jammer may be expressed as

$$P(d) = a \cdot d^{-\gamma} \tag{1}$$

where *a* is the constant for adjusting values and dimensions of variables and  $\gamma$  has typical values between 2 and 5 [22]. It means that influence of propagation environment may cause signal attenuation in the ratio of even 8:1. Further, navigation signals should not be jammed by a too high level signal because navigation signals are also disrupted on other systems and devices where it is not desirable. As a brief illustration, according to [21] signal of the power 20mW (13dBm) is enough to block navigation signals in the range of 2km and this is significantly lower than the signal which our system may generate (Tables I and II). The jammer in [8] may cause successful jamming at 2km distance for directional jamming or 500m for omni-directional jamming. It means that our system may be effective at higher distance than solution [8].

Comparison in this case may be made when considering just signal levels at the place of signal reception. There is a number of papers whose authors include the authors of this paper where successful jamming rate (or bit error rate - BER) is determined as the level ratio RCIED activation signal/jamming signal [13]-[15], [18], [23]-[25]. Although the analysis in these papers is performed for RCIED jamming, the results may be also applied for drone jamming as the principles are the same. The results from these references prove that jamming successfulness depends on the applied jamming strategy (we have analysed the jamming strategies sweep, multisweep with continual sweeping and barrage in the mentioned papers) as well as on the jammed signal modulation type. The frequency spectrum of the generated jamming signal is presented in the Fig. 7. for all four implemented jamming scenarios: sweep signal, multisweep signal with continuous and discrete sub-bands and barrage jamming. The signal spectrum is also related to the third frequency sub-band.

The applied jamming strategy mainly depends on the fact what data we have about the malicious drone and what drone signals we want to jam. In the case when a drone jammer is applied as a sole device, there is even no data whether a drone is present or not. It is necessary to jam a wide frequency spectrum in such a situation, perhaps by the jamming activation in all five sub-bands. The advantage of barrage jamming over sweep jamming when jamming is performed without any knowledge of drone presence is that all frequencies are jammed in the same time, but the necessary emitted power is higher than for sweep jamming [13], [14]. It means that, if jamming signal power is enough, jamming successful probability is 1 for barrage jamming and the sweep speed for sweep jamming must be determined in such a way that the probability of successful jamming is higher than some value, usually 0.95 [13], [14]. When the jammer is applied together with some system for drone detection and identification, we obtain some data about the malicious drone before jamming. Then it is possible to jam just on the frequencies where video, telemetry and drone communication signals are detected. It is possible to select to jam only one or two of these three signal groups, or only navigation signals. Thus emitted jamming signal power is significantly reduced.



Fig. 7. Jamming signals in the frequency range 1164-1610MHz: a) sweep; b) multisweep with continual sweeping; c) multisweep with (five) discrete sweep steps; d) barrage

#### VI. CONCLUSION

The malicious drone missions jamming system presented in this paper completes IRITEL's palette of various implementation jammers [9] - [18]. With its wide flexibility in jamming strategies definition, different implementable jamming scenarios and suggestive handling menus, the presented jammer has comparable or even better characteristics than other internationally available solutions [7], [8], [26] - [30]. In the future the realized jamming system will be supplemented by the system for drones detection, identification, classification and localization to construct one comprehensive solution for the fight against malicious drones.

#### REFERENCES

- N. Eriksson, "Conceptual study of a future drone detection system Countering a threat posed by a disruptive technology," Master thesis in Product Development, Chalmers University of Technology, Goethenburg, Sweden, 2018.
- X. Shi, C. Yang, C. Liang, Z. Shi, and J. Chen, "Anti-Drone System [2] Multiple Surveillance with Technologies: Architecture. Implementation, and Challenges," IEEE Communications Magazine, Vol. 56. Issue 4, April 2018., pp. 68-74.. DOF 10.1109/MCOM.2018.1700430.
- [3] N. Razzouk, J. Blas, J. Thornhill, "Speed of Saudi Oil Recovery in Focus After Record Supply Loss," Bloomberg, 15. September 2019., <u>https://www.bloomberg.com/news/articles/2019-09-15/saudis-race-torestore-oil-output-after-crippling-aramco-attack.</u>
- [4] S. Milošević, "Nad Srbijom 4000 dronova, oni ilegalni biće obarani," ("Over Serbia 4000 drones, the illegal ones will be destroyed"), *Novosti*, 15. October 2017., <u>https://www.novosti.rs/vesti/</u>naslovna/drustvo/aktuelno.290.html:690699-Nad-Srbijom-4000dronova-oni-ilegalni-bice-obarani, in Serbian.
   [5] A. L. Drozd, "Spectrum-secure Communications for Autonomous
- [5] A. L. Drozd, "Spectrum-secure Communications for Autonomous UAS/UAV Platforms," MILCOM 2015 - IEEE Military Communications Conference, Tampa, Florida, 26-28. October 2015.
- [6] Drone Killer 6 powerful UAV (GPS WIFI5GHz) Jammer 120W, https://www.jammer-store.com/drone-killer-6.html.
- [7] I. Pokrajac, N. Kozić, A. Čančarević, and R. Brusin, "Jamming of GNSS Signals," *Scientific Technical Review*, Vol. 68, No. 3, UDK: 621.396.96(047)=861, pp. 18-24, September 2018.
- [8] Optix Anti-drone System, Product Information, Specification & Scope of Supply, Company Confidential.
- [9] 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.
- [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, B. Pavić, V. Marinković-Nedelicki, P. Petrović, A. Lebl, "Development, realization and testing the variant of the device for VIP persons protection in the extended frequency range (20MHz-6GHz) with the reduced total power (300W)," tehničko rešenje novi proizvod na projektu tehnološkog razvoja TR32051 "Razvoj i realizacija naredne generacije sistema, uređaja i softvera na bazi softverskog radija za radio i radarske mreže", 2017.
- [13] M. Mileusnić, B. Pavić, V. Marinković-Nedelicki, P. Petrović, D. Mitić, A. Lebl, "Analysis of jamming successfulness against RCIED

activation," 5<sup>th</sup> International Conference IcETRAN 2018, Palić, June 11-14, 2018., Proceedings of Papers, pp. 1206-1211, ISBN 978-86-7466-752-1, the best paper award in the Section of telecommunications.

- [14] M. Mileusnić, B. Pavić, V. Marinković-Nedelicki, P. Petrović, D. Mitić, A. Lebl, "Analysis of Jamming Successfulness against RCIED Activation with the Emphasis on Sweep Jamming," *Facta Universitatis, Series: Electronics and Energetics*, Vol. 32, No. 2, June 2019., pp. 211-229., <u>https://doi.org/10.2298/FUEE1902211M</u>, extended and improved version of the paper awarded at 5<sup>th</sup> International Conference IcETRAN 2018, Palić, June 11-14. 2018.
- [15] A. Lebl, M. Mileusnić, B. Pavić, V. Marinković-Nedelicki, P. Petrović, "Programmable Generator of Pseudo-White Noise for Jamming Applications," 27<sup>th</sup> Telecommunications Forum (TELFOR), Belgrade, November 26-27, 2019., Proceedings of Papers, pp. 1-4, ISBN 978-1-7281-4790-1, DOI: 10.1109/TELFOR48224.2019.8971203.
- [16] M. Mileusnić, P. Petrović, A. Lebl, B. Pavić, "Comparison of RCIED Activation Responsive and Active Jamming Reliability," 6<sup>th</sup> International Conference IcETRAN 2019, Srebrno Jezero, June 3-5. 2019., Proceedings of Papers, pp. 988-993, ISBN 978-86-7466-785-9, the best paper in the Section of telecommunications.
- [17] M. Mileusnić, P. Petrović, V. Kosjer, A. Lebl, B. Pavić, "Reliability Analysis of Different RCIED Activation Signal Responsive Jamming Techniques and Their Comparison to Active Jamming," *Facta Universitatis, Series: Electronics and Energetics*, Vol. 33, No. 3, September 2020., pp. 459-476., DOI: <u>https://doi.org/10.2298/FUEE2003459M</u>, extended and improved version of the paper awarded at 6<sup>th</sup> International Conference ICETRAN 2019, Srebrno jezero, June 3-5. 2019.
- [18] A. Lebl, V. Kosjer, J. Radivojević, M. Mileusnić, "Performances of RCIED Activation Signal Multisweep Jamming," 7<sup>th</sup> International Conference IcETRAN 2020, Niš, September 28-29. 2020., Proceedings of Papers, pp. 740-745, ISBN 978-86-7466-852-8.
- [19] V. Matić, V. Kosjer, A. Lebl, B. Pavić, J. Radivojević, "Methods for Drone Detection and Jamming," 10<sup>th</sup> International Conference on Information Society and Technology (ICIST), Kopaonik, March 8-11, 2020, In: Zdravković, M., Konjović, Z., Trajanović, M. (Eds.) ICIST 2020 Proceedings Vol.1, pp.16-21, 2020.
- [20] J. Radivojević, A. Lebl, M. Mileusnić, A. Vujić, T. Šević, V. Joksimović, "Multichannel Radio-jammer Development Considerations for prevention of Illicit Drone Missions," 9<sup>th</sup> International Scientific Conference on Defensive Technologies OTEH 2020., Belgrade, October 15-16. 2020., pp. 270-275, ISBN 978-86-81123-83-6.
- [21] D. A. M. da Silva, "GPS Jamming and Spoofing using Software Defined Radio," A Dissertation for the Degree of Master in Telecommunications and Computer Engineering, University Institute of Lisbon, 2017.
- [22] J. Ebersprächer, H.–J. Vögel, C. Bettstetter, "GSM, Switching, Services and Protocols," (section 5), John Wiley & Sons, 1999.
- [23] A. Lebl, B. Pavić, J. Radivojević, M. Mileusnić, P. Petrović, "Sweep Jamming Successfulness of DMPSK Modulated RCIED Activation Message," 28<sup>th</sup> Telecommunications Forum (TELFOR), Belgrade, November 24-25, 2020., Proceedings of Papers, pp. 21-24, ISBN 978-0-7381-4242-5, DOI: <u>10.1109/TELFOR51502.2020.9306587</u>.
- [24] M. Mileusnić, P. Petrović, B. Pavić, V. Marinković-Nedelicki, V. Matić, A. Lebl, "Jamming of MPSK Modulated Messages for RCIED Activation," 8<sup>th</sup> International Scientific Conference on Defensive Technologies OTEH 2018., Belgrade, October 11-12. 2018., pp. 380-385, ISBN 978-8681123-88-1.
- [25] V. Marinković-Nedelicki, A. Lebl, M. Mileusnić, P. Petrović, B. Pavić, "BER Calculation for Sweep Jamming of MPSK Modulated RCIED Activation Message Signals," 18<sup>th</sup> International Symposium "INFOTEH Jahorina 2019", Jahorina, 20-22. March 2019., ISBN: 978-1-5386-7073-6, pp. 1-6, DOI: <u>10.1109/INFOTEH.2019.8717747</u>.
- [26] Optix: "Anti-Drone System Compact".
- [27] https://www.perfectjammer.com/drone-signal-jammers.html.
- [28] <u>http://jammers4u.com/drones-jammer.</u>[29] https://www.thesignaljammer.com/blog/everything-you-ne
- [29] <u>https://www.thesignaljammer.com/blog/everything-you-need-to-know-about-drone-jammers/</u>
- [30] Drone Killer 6 powerful UAV (GPS WIFI5GHz) Jammer 120W, https://www.jammer-store.com/drone-killer-6.html.