9th INTERNATIONAL SCIENTIFIC CONFERENCE
ON DEFENSIVE TECHNOLOGIES
OTEH 2020
Belgrade, Serbia, 15 – 16 October 2020

MULTICHANNEL RADIO-JAMMER DEVELOPMENT CONSIDERATIONS FOR PREVENTION OF ILLICIT DRONE MISSIONS

JOVAN RADIVOJEVIĆ
IRITEL a.d., Belgrade, jovan.radivojevic@iritel.com

ALEKSANDAR LEBL
IRITEL a.d., Belgrade, lebl@iritel.com

MLADEN MILEUSNIĆ
IRITEL a.d., Belgrade, mladenmi@iritel.com

ALEKSANDAR VUJIĆ
IRITEL a.d., Belgrade, aleksandar.vujic@iritel.com

TAMARA ŠEVIĆ
Military Technical Institute, Belgrade, tamara.sevic23@gmail.com

VASILIJA JOKSIMOVIĆ
Military Technical Institute, Belgrade, vasilija.joksimovic@vti.vs.rs

Abstract: *This paper presents development considerations of the multichannel Anti Drone Radio-Jammer (ADRO) system, which is intended for illicit drone mission prevention. The objectives of ADRO implementation are to jam and disable communication signals for command, control, video signals transmission, telemetry and navigation of enemy drone systems and devices. Such multidisciplinary functions are allowed by the generation of optimum jamming signals of drone navigation and wireless radio-frequency communication. Drones require reliable navigation for their autonomous or semi-autonomous operation. That's why one way for successful jamming is to block the Global Navigation Satellite System (GNSS) receiver on the drone. The transmitter unit in ADRO is realized in five frequency bands, thus allowing free selection of different jamming strategies and emission power depending on the required situation. With the help of a compact remote control, it is extremely easy to operate ADRO system by selecting the appropriate tactical jamming scenarios. The performed tests have proved that drone may be effectively disabled and grounded at its current location as the result of ADRO function.*

Keywords: *Anti Drone Radio Jammer, Global Navigation Satellite System, jamming strategy, jamming range.*

1. INTRODUCTION

The overall socio-economic progress and especially the development of information and communication technologies and the creation of global telecommunication networks led to the construction and the expansion of unmanned aerial vehicles (UAVs), better known as drones. The term unmanned aerial system (UAS), which is also used for drones, designates that there is a number of other resources which allow drones application. They are the drone ground control (its pilot) as well as communication between the pilot and the drone and drone navigation.

There are two important phases in the fight against drone illicit application: 1. drones detection and identification and 2. drones jamming [1]. Institute IRITEL has experience both in different illicit systems detection and in their jamming. In this paper we are faced with the problem of drones jamming. Solutions [2]-[11] are only a part of literature related to drone jamming.

The methods for drone jamming pertain to the universal jamming methods such as sweep jamming, barrage jamming, multisweep jamming and so on. IRITEL has long-term results both in theory and practical realizations of such solutions [12]-[23], especially against Remote Controlled Improvised Explosive Devices (RCIEDs). The realized jammer solutions were presented on a number of national and international exhibitions, including Eurosatory 2018 – Defense & Security International Exhibition in Paris. These experiences are used in the realization of drone illicit missions jammer.

Section 2 of this paper deals with the presentation of drone jammer implementation principles and structure of IRITEL jammer solution. Some results dealing with developed anti-drone system testing are presented in the Section 3. At the end, conclusions are in the Section 4.

2. DRONE JAMMER REALIZATION PRINCIPLES AND STRUCTURE

Drones or UASs are multifunctional flying machines. In most situations they use remote control (RC) link for receiving commands from a pilot who manages drone flight, telemetry link for sending flight data and status to RC, video link for sending images to RC and Global Navigation Satellite System (GNSS). In modern UASs the applied frequencies for these functions are 433MHz, 868MHz, 915MHz, 1.2GHz, 2.4GHz, 5.8GHz for video and telemetry links, as well as 1176MHz, 1227MHz and 1.57-1.62GHz for locating by GNSS systems.

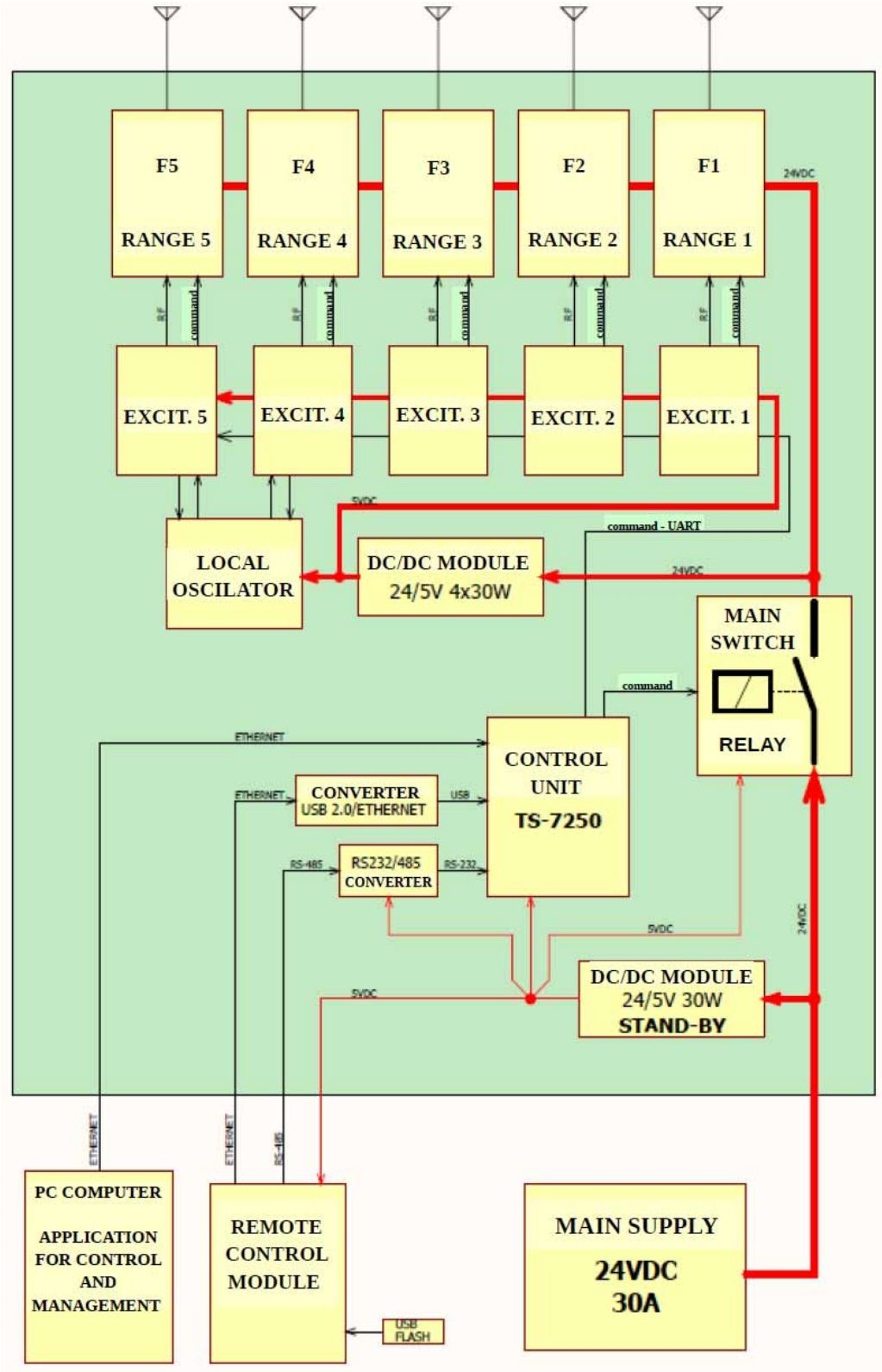


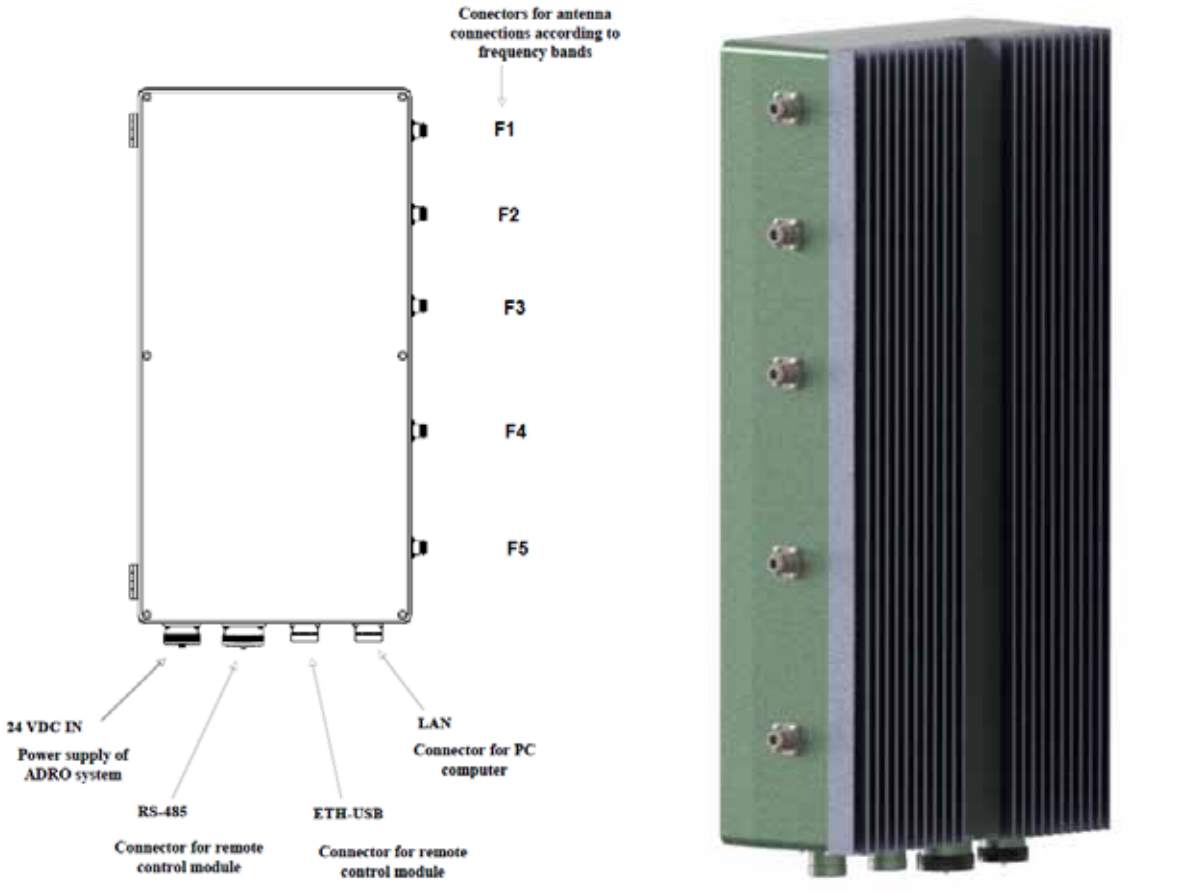
Figure 1 – Block diagram of ADRO system

The complete solution of drone mission prevention would be to jam signals of all these frequencies, but among existing solutions in the world it is hard to find such a realization. Nearly all emphasized frequencies are jammed in [9]. Knowing of applied frequencies leads to significantly simplified jammer realization comparing to RCIED activation jamming. The most effective way to jam drone operation is to prevent reception of GNSS signal [10], because such a situation will cause the drone crash. If GNSS reception is not disabled and other drone systems are disrupted, drone is usually programmed to land itself or to "Return home" to its starting position [3].

The block diagram of the IRITEL Anti Drone Radio-Jammer (ADRO) system is presented in the Figure 1. Jamming is realized in the five frequency bands (F1 to F5) to cover all frequencies important for drones operation according to remarks in the Introduction. Comparing to other existent solutions IRITEL jammer disrupts wider or at least equal palette of drone functions.

ADRO implementation is universal: it may be used in a system ensemble for the fight against drones or independently. Operational conditions include mobile implementation when it is remotely controlled (remote control module in the Figure 1) or on the dwell in stationary conditions when it is controlled by the software for control and management (application for control and management in the Figure 1). In the case of remote control, ADRO is placed on the platform and connected by two interfaces with the remote control module (as presented in the Figure 2). The first one is RS485 for communication between remote control module and control unit. Implementation of RS485 standard and corresponding RS232/RS485 converter allows remote control from a larger distance than if RS232 has been used for this purpose. The second one is Ethernet (designation ETH-USB in the Figure 2) whose function is to load configuration file to the control unit. The programming file for ADRO function is easily changeable as it is envisaged first to load it to module for remote control from an USB flash (Figure 1).

ADRO system may be also controlled in stationary conditions as it is already emphasized. For such implementation ADRO is connected to PC computer over Ethernet interface (designation LAN in the Figure 2). The parameters for ADRO operation are generated in the software for control and management, which is installed at the PC. These parameters are adjusted on the base of operator definition from the PC.



a) b)

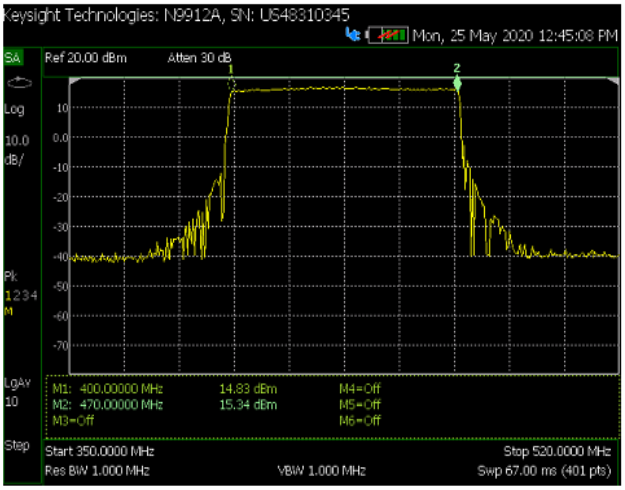
Figure 2 – ADRO interfaces (a) and external appearance (b)

Each of five envisaged jamming signals are generated in the separate autonomous exciter block according to the Figure 1. The generated signal is amplified in two stages: in the exciter block and then, finally, in the block designated by “Range 1” till “Range 5”. At the end, there are five antenna connectors at the system output (F1 to F5 in the figures 1 and 2).

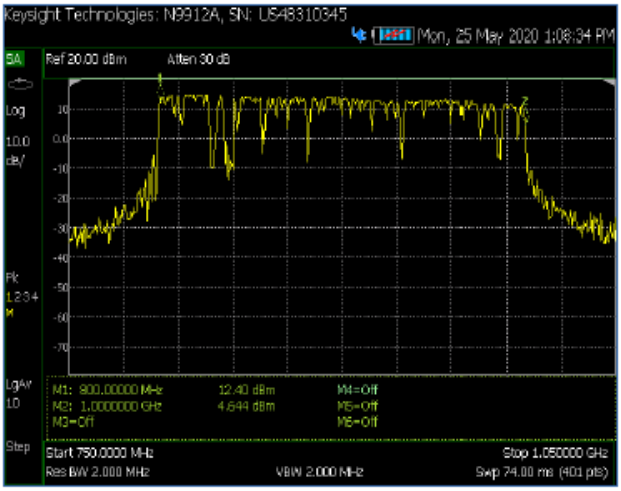
The significant flexibility of jamming strategy is allowed based on various signal types implementation. ADRO may generate sweep, multisweep and barrage (FM modulated) jamming signal. Sweeping in multisweep signal may be realized as a continual sweep or in discrete steps. The jamming strategy selection is independent for each of five applied frequency bands. The results from [24] prove that the jamming signal whose power is 20mW causes disruption of all GNSS receivers in the range of 2km. ADRO signal emission power is adjustable with the maximum level higher then this limit except for the band F5 which reaches nearly 6GHz. It means that ADRO may prevent drone flight and mission in a wide range around its position.

3. GENERATED JAMMING SIGNALS

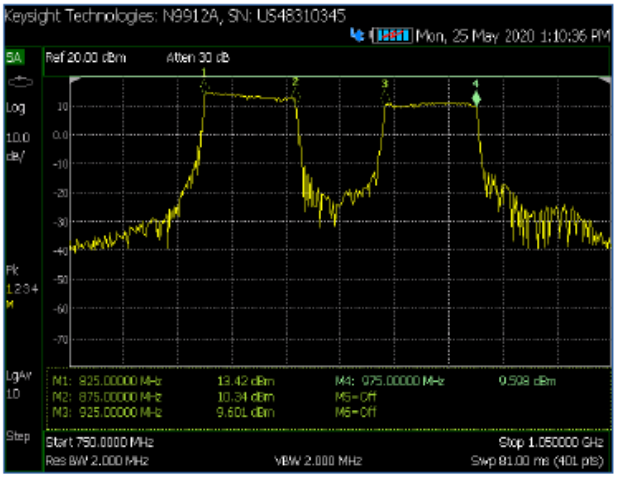
Figure 3 presents the frequency spectrum of the generated jamming signals in ADRO system. They are a spectrum of sweep signal (Figure 3a), FM modulated barrage signal (Figure 3b), multisweep signal with continually changeable frequencies (Figure 3c) and multisweep signal with frequencies changed in discrete steps (Figure 3d).



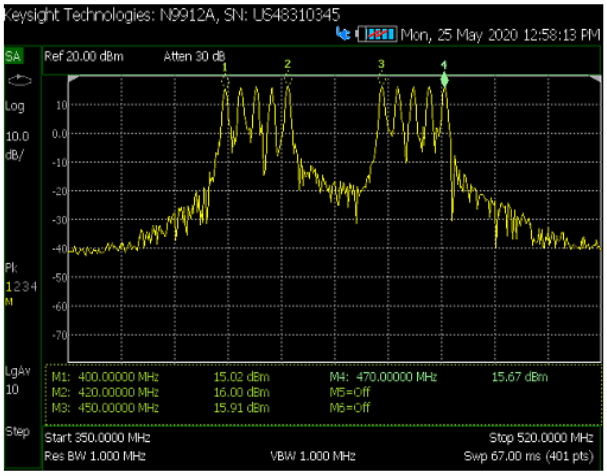
a)



b)



c)



d)

Figure 3 – ADRO jamming signals: a) sweep; b) barrage; c) multisweep with continual sweeping; d) multisweep with discrete sweep steps

Figure 4 presents together drone signal spectrum and the jamming signal spectrum. Drone communication over RC link with a pilot as well as drone video communication are realized in two frequency bands: 2.4GHz (Figures 4a and 4b) and 5.8GHz (Figures 4c and 4d), taking about 60MHz bandwidth for these functions at both frequency bands. There are two records for each jammed frequency. The first one in both situations comprises only drone signals (Figure 4a and Figure 4c), while the second one includes together drone signals and sweep jamming signal (Figure 4b and Figure 4d). The records are made by activating the

function of time hold at the applied real time spectrum analyzer, so it was possible to get the signal spectrum during some time interval.

The frequency of drone communication is changed during time. Random frequency hopping inside each of two applied frequency bands is used as well as alteration from one to the other frequency band if the communication over the first band is not reliable. The tests have been performed in two trials: in the first one we considered drone behaviour when only one frequency band is jammed. The tested drone has successfully overcome such a jamming by continuing communication only over the second not jammed band. In the second trial both frequency bands have been jammed simultaneously. In this situation ADRO has succeeded to prevent drone communication and as a consequence its flight. The drone has safely landed at the place just under the place in the air where it has lost its communication with the pilot.

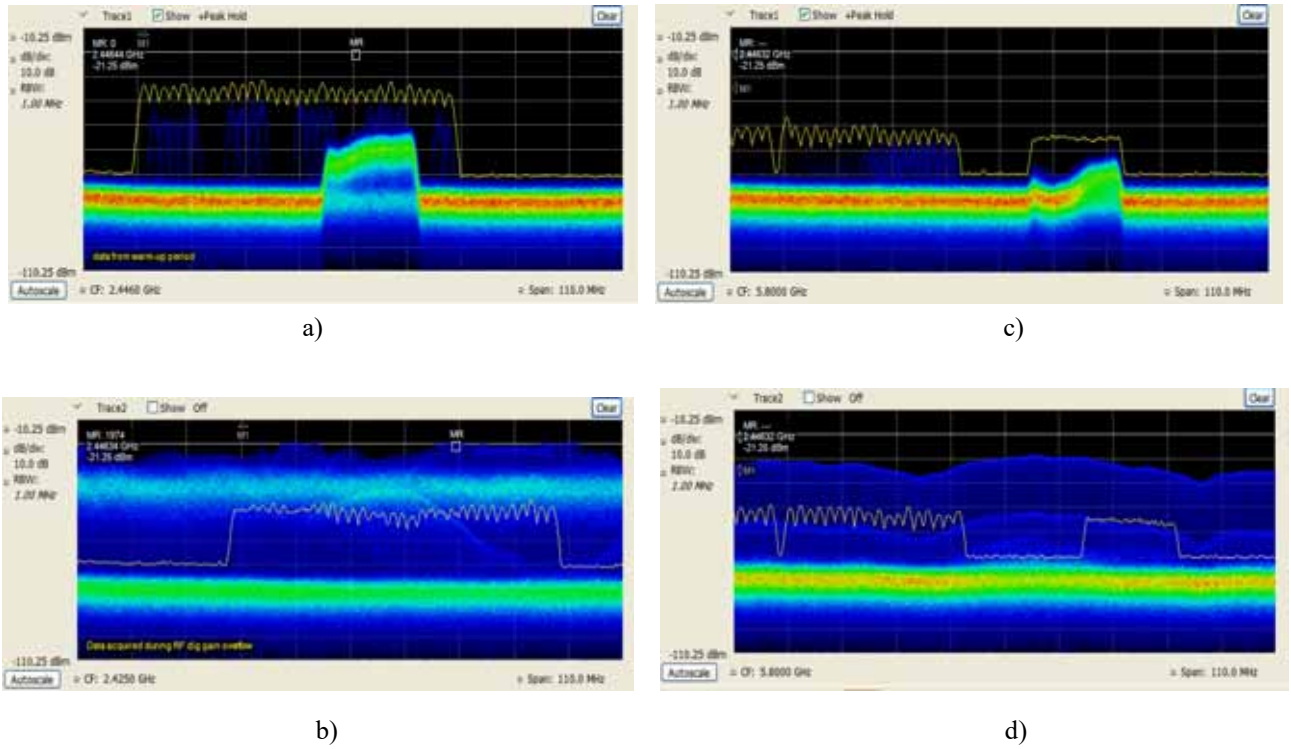


Figure 4 – Drone RC and video signal jamming: a) drone signal in the band at 2.4GHz; b) drone and sweep jamming signal in the band at 2.4GHz; c) drone signal in the band at 5.8GHz; d) drone and sweep jamming signal in the band at 5.8GHz

4. CONCLUSIONS

This paper presents development of the drone jammer system ADRO, which is performed in the Institute IRITEL. The characteristics of the realized solution are better or at least comparable to the other similar solutions in the world. Comparison is performed for the most important properties intended to drone jammer reliability prediction: the bandwidth of jammed frequency spectrum, the characteristics and the number of implemented jamming strategies and the distance of successful jamming. The reliably jammed signals are over RC link for receiving commands from a pilot, telemetry link for sending flight data and status to RC, video link for sending images to RC and GNSS. This statement is illustrated in the paper based on the test which successfully prevented drone communication over RC and video link. The most important jamming strategies may be used in the solution (sweep, barrage and multisweep jamming). The successful jamming could be achieved in the radius larger than 2km according to the maximum jamming signal level. Operator may manage ADRO functions from its operational position or by using specially developed remote control unit.

ACKNOLEDGEMENT

The results of the development are obtained as a part of the joint project with Military Technical Institute.

References

[1] V. Matić, V. Kosjer, A. Lebl, B. Pavić, J. Radivojević: „Methods for Drone Detection and Jamming“, 10th 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.

[2] J. Mead, C. Bobda, T. and JL. Whitaker: „Defeating Drone Jamming with Hardware Sandboxing”, 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST) Conference, 19-20. December 2016., Yilan, Taiwan, pp. 1-6.

[3] S. Friedberg: „A Primer on Jamming, Spoofing and Electronic Interruption of a Drone“, 19. April 2018.,

https://www.dedrone.com/ blog/primer-jamming-spoofing-and-electronic-interruption-of-a-drone.

[4] Optix: „Anti-Drone System Compact“.

[5] https://www.perfectjammer.com/drone-signal-jammers.html.

[6] http://jammers4u.com/drones-jammer.

[7] https://www.thesignaljammer.com/blog/everything-you-need-to-know-about-drone-jammers/.

[8] A. L. Drozd: „Spectrum-secure Communications for Autonomous UAS/UAV Platforms”, MILCOM 2015 - IEEE Military Communications Conference, Tampa, Florida, 26-28. October 2015.

[9] Drone Killer 6 – powerful UAV (GPS WIFI5GHz) Jammer – 120W, https://www.jammer-store.com/drone-killer-6.html.

[10] 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.

[11] K. Pärlin: „Jamming of Spread Spectrum Communications Used in UAV Remote Control Systems“, Master’s Thesis, Tallinn University of Technology, Tallinn, 2017.

[12] „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.

[13] „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.

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

[15] 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“, 25th Telecommunications Forum (TELFOR), November 21-22, 2017., Proceedings of Papers, pp. 151-154, ISBN 978-1-5386-3072-3, https://ieeexplore.ieee.org/ document/8249309.

[16] M. Mileusnić, B. Pavić, V. Marinković-Nedelicki, P. Petrović, D. Mitić, and A. Lebl, „Analysis of jamming successfulness against RCIED activation”, 5th 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.

[17] M. Mileusnić, B. Pavić, V. Marinković-Nedelicki, P. Petrović, D. Mitić, and A. Lebl, „Analysis of jamming successfulness against RCIED activation with the emphasis on sweep jamming“, the extended and revised version of the paper from the IcETRAN 2018, Facta Universitatis, Series Electronics and Energetics, Vol. 32, No 2, April 2019., pp.211-229, https://doi.org/10.2298/FUEE1902211M.

[18] M. Mileusnić, P. Petrović, B. Pavić, V. Marinković-Nedelicki, V. Matić, and A. Lebl, „Jamming of MPSK modulated messages for RCIED activation”, 8th International Scientific Conference on Defensive Technologies OTEH 2018, Belgrade, 11-12. October 2018.

[19] N. Remenski, B. Pavić, P. Petrović, M. Mileusnić, and V. Marinković-Nedelicki, „Integrisana radio-oprema za zaštitu prostora od mobilnih veza (Treća generacija radio-opreme), tehničko rešenje – novi proizvod s oznakom CJ-1P na projektu tehnološkog razvoja TR-11030 “Razvoj i realizacija nove generacije softvera, hardvera i usluga na bazi softverskog radija za namenske aplikacije”, 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.

[20] M. Mileusnić, P. Petrović, B. Pavić, V. Marinković-Nedelicki, V. Matić, and A. Lebl, „A New method of GSM Systems Jamming Based on Connection Quality Impairment”, 26th Telecommunications Forum (TELFOR), November 20-21, 2018., Proceedings, pp. 160-163, ISBN 978-1-5386-7170-2, https://ieeexplore.ieee.org/document/8612015.

[21] M. Mileusnić, P. Petrović, A. Lebl, B. Pavić: „Comparison of RCIED Activation Responsive and Active Jamming Reliability“, 6th International Conference IcETRAN 2019, Srebrno Jezero, June 3-5. 2019., Proceedings of Papers, pp. 988-993, ISBN 978-86-7466-785-9, awarded as the best paper in the Section of Telecommunications.

[22] A. Lebl, M. Mileusnić, B. Pavić, V. Marinković-Nedelicki, P. Petrović: „Programmable Generator of Pseudo-White Noise for Jamming Applications“, 27th 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.

[23] V. Marinković-Nedelicki, A. Lebl, M. Mileusnić, P. Petrović: „Combined Jamming in RCIED Activation Prevention“, 19th International Symposium „INFOTEH Jahorina 2020“, Jahorina, 18-20. March 2020., ISBN: 978-1-7281-4775-8, pp. 1-6 DOI: 10.1109/INFOTEH48170.2020.9066329.

[24] 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.