Methods for Drone Detection and Jamming

Vladimir Matić, Vladimir Kosjer, Aleksandar Lebl, Branislav Pavić, Jovan Radivojević
Radio communications department, IRITEL a.d.
Belgrade, Serbia
vmatic@iritel.com, vladimir.kosjer@iritel.com, lebl@iritel.com, bane@iritel.com, jovan.radivojevic@iritel.com

Abstract— **This paper presents methods for drones' detection and for jamming. Implementation of drones in malicious activities highly increases in the last years and the methods implemented for drone detection are numerous. The characteristics of the most detector types: radar, radiofrequency, acoustic, optical and thermal are emphasized in the paper. The goal of this analysis is to give the guidelines in choosing which techniques to use and combine for drone detection. The paper emphasizes the guidelines for drone successful jamming while presenting IRITEL solutions implementation for drones malicious function prevention and drones role in jamming efficiency improvement.**

I. INTRODUCTION

Today we are faced with the increasing efforts in designing drones – unpiloted aircrafts. The other, often used designation for drones is unmanned aerial vehicle (UAV). Besides UAVs, we may also find the term unmanned aerial system (UAS). UAS is the more wide definition than UAV. It includes, besides drones, everything that enables drone functioning: drone ground control (its pilot), communication between the pilot and the drone (commands transmission from the pilot towards the drone and collected data from the drone towards the user) and all equipment intended for drone operation.

There are several implemented constructions for drone realization. It is possible to find the drone in a shape of classical aeroplane. But, such construction is not too often applied. The more often implemented constructions are multicopters (quadcopters, hexacopters or octocopters). This second construction is intended for smaller UAVs, whose speed is significantly smaller than the first construction and may be easily implemented even in urban areas [1], [2].

There are plenty of activities, where drone implementation is very useful. Aerial photography, traffic supervision, disaster monitoring [3], precise agriculture, industrial inspection [1] are only some of the fields where drone implementation is today very important and, even, unavoidable. But, besides such drones applications, which are serving to advance human activity, drones are today often used for malicious missions. Such hostile missions we may expect in each place, where we have our personnel and/or our equipment and devices and where explosive devices may cause great injury: airports, stadiums, urban (crowded) areas. They may be applied for spy missions, smuggling illicit materials over borders or into and out of the prisons, and so on [1], [3]. The places of malicious actions by drones are numerous. Besides the mentioned ones, they are residential areas, governmental facilities, important events, commercial and industrial facilities, including nuclear plants as probably the most important, etc. The fight against malicious drone missions is the motivation for this paper.

In last several years drone implementation is highly increasing, causing that it becomes very dangerous weapon in the enemy hands. Reliable drone detection is very difficult and demanded task and the great majority of solutions analyzed in this paper are realized in the last four years.

The fight against hostile drone functioning consists of two phases: drone detection and drone jamming. The selection of optimum detection algorithm combination and adequate jamming strategy present research questions in this paper. The aim is to achieve reliable results in malicious drone prevention in the great variety of environmental conditions and implemented drone types. IRITEL has great experience in both these fields, when the aim is to prevent adverse activities, realized by different facilities. IRITEL realized devices are in the fields of radio surveillance and jamming, remote controlled improvised devices (RCIED) activation jamming and cellular jamming [4] - [12].

II. METHODOLOGY OF DRONE DETECTION

There are several techniques intended for drone detection. Each of them has its pro and contra, i.e. situations when they are suitable for implementation and when their results in detection are not satisfactory. That's why usually several different techniques are implemented together (for example [3], [13] - [15]). The most often applied techniques are radar, radiofrequency (RF), acoustic, optical and thermal (infra-red) sensing. In solution [3] are combined audio, video and RF detection, while solution [13] combines radar, RF audio and video detection. Two most complete solutions presented in [14] include radar, RF, optical and thermal sensors. On the contrary, solution in [15] combines only optical and acoustic sensors with the emphasis on optical detection. There is no dominant method of detection – it is preferable to have some combination of detectors. The place of protection has influence on the choice of detection systems to combine.

A. Radar detection

Radar systems are widely used in everyday life and in military applications. These, conventional radar systems are adjusted to detect relatively great objects. They are not suitable for small drone detection, especially when the drone's speed is small, when they are flying on the low altitude or

when they hover. The high manoeuvrability is also the limiting factor in drone detection [16]. Besides, drone dimensions and the way how they are moving makes them similar to birds for the radar reflection. The effect of all these challenging drone flight features is that the number of reliable solutions for drone detection by radar is not great. A few of such realized systems are presented in [1], [17].

The benefits of radar detection may be summarized in several points, according to [1]: 1. when implemented in environment without obstacles, it is suitable for long range detection; 2. it is possible do detect drones, which are autonomous when they are moving, i.e. when there is no their communication with a pilot or supervisory centre; 3. the satisfactory drone detection is possible in bad weather conditions and in low or no light conditions; 4. it is possible (although not easily) to separate drones from birds. The drawbacks of such detection are: 1. all materials do not reflect radar signals in a same intensity (some of them even nearly not reflect); 2. radar detection is not possible behind obstacles, which especially contributes to degraded detection possibilities in urban areas; 3. the necessary high radar emission power radiation is unhealthy, meaning that radar implementation in crowded areas is inappropriate [3].

Several radar realization concepts are possible in drone detection. These are: 1. monostatic pulse radar; 2. frequency modulated continuous wave radar (FMCW); 3. high frequency FMCW; 4. passive radar on the base of commercial signals. The specific benefits and drawbacks of each of emphasized concepts in the case of drone detection are standard for these radar solutions. The protection of a huge object, as an airport, may be realized by one surface movement radar (SMR) or by multiple, smaller radars with lower capabilities. The benefit of the second solution is that it is easier to avoid unprotected areas existence behind some objects, which have no line of sight (LOS) with radar [18].

The contribution [19] is realized as monostatic pulse radar. It is completely faced to multicopters detection by radar and the way how they are differentiated from birds. This differentiation is based on specific micro-Doppler signature of drone's propeller rotation. The obtained micro-Doppler spectra figures in [19] have clearly specific and repetitive shape as multicopter reflects radar signal, while these characteristics may not be noticed in any angle of bird's flight in relation to radar beam. Figures in [19] are obtained when drone propellers are rotating. The radar characteristics, which have to be considered to achieve good-quality micro-Doppler signature are polarization, carrier frequency, pulse repetition frequency, implemented pulse width and integration time.

Radar cross section (RCS) of the drone as the key parameter responsive for drone successful detection is analyzed in [20]. Here it is determined for several stationary drone types, whose propellers are not rotating or are rotating very slowly. On the base of RCS value, the maximum distance R_{max} between the drone and the detector to guarantee successful detection may be determined starting from well known radar equation [18].

The special technology in the area of radars, which may be used for drone detection, is Light Detection and Ranging (LIDAR). This technology could be also analyzed in the group of optical detectors, because it is the combination of light and radar implementation. The possibilities of LIDARs in drone detection are limited by the fact that they usually have sparse resolution and that drones' laser RCS, which is important for reliable detection by LIDAR, is small. The benefits of LIDAR implementation are: 1. it is relatively easy to separate the object from foreground and background; 2. the detection is not dependent on weather conditions; 3. the exact object position is easily determined after its detection [21]. It is possible to implement LIDARs with higher resolution possibilities. According to [18], the pulsed laser light is used to obtain high resolution images, applicable for drone detection. Generally, LIDARs are still pretty expensive for drone detection, but it is expected their price is going to drop in near future.

IRITEL has long-year experience in the development of radar solutions [22], [23] and in modernization of old-generation radars [24] - [26], as, particularly, in development of all components constituting radar solution. This knowledge presents the starting point in our development of radar based detector of drone presence.

B. RF detection

There is usually a continuous two-way data transmission between a drone and a pilot on the ground. These data are sent in several different frequency bands, which are also used for wireless Internet and WLAN functioning. This fact complicates drone communications detection.

The benefits of using RF detection are [1]: 1. there is no need for signal sending, only passive sensor of RF signal is necessary; 2. there is possibility to locate the pilot; 3. detector may be with no restrictions implemented also in urban areas, because there is no radiation. As a consequence of no need to have a transmitter, the construction of equipment is simpler than in the case of radar implementation. The drawbacks in the RF detection are: 1. it is not possible to detect drones, which do not communicate with the pilot; 2. the extensive wireless Internet and WLAN traffic on the frequencies intended for drone communications presents significant noise source for drone communications detection; 3. drones often use directional antennas, so it is difficult or even sometimes impossible to detect their communications if the detector is not positioned near the direction of antenna waves beam.

The characteristic of RF signal transmission, especially in urban areas, is its attenuation, which is greater than in free space. This attenuation is modelled by environmental propagation coefficient (γ). In free space it is γ=2 and in other situations the value of γ varies from 1.6 (for some corridors in buildings or in situations with the effect as in valleys in mountainous region) to 6 (in buildings with a lot of obstacles) [27] - [29]. In urban areas the values of γ are always between 3 and 5 and this model is for path loss when signal is transmitted from the drone to the pilot. As a consequence of higher values of γ, the range of RF detector is reduced and it is necessary to implement denser network of RF sensors, if the goal is to protect the greater urban area [30].

The reliability of RF detection may be improved by positioning more separated sensors and, then, implementing

time analysis besides frequency analysis. Time difference of arrival (TDOA) is determined between the moments of drone RF signal detection in the geographically separated sensors [31]. The more sensors connected in the network overcome the problem of increased signal attenuation in urban areas and the problem of greater detection miss, because there are a plenty of other signal sources in the same frequency bands.

One specific analysis in [32] presents the possibility to detect drone presence on the basis of specific physical signature in drone's RF communication. Drone body vibrations and shifting as propellers rotation produce characteristic changes in wireless signal, which is transmitted from a drone towards the pilot. The principles of software defined radio (SDR) may be applied in the analysis of the received signal to distinguish the signal, whose origin is drone transmitter emission from the emissions on the same frequencies, which are generated by the other sources. SDR principles are also applied for RF detection of drones in [33], but with emphasis on machine learning models. Once well trained by recording RF spectrum during drone flight, this method may achieve satisfactory detection reliability, thus making it a candidate for practical implementation.

IRITEL has a number of solutions realized on the base of SDR [22], [24]. The whole project whose realization has just finished and whose leader is IRITEL has the accent on the implementation of SDR algorithms [34].

The special group of solutions in the area of RF detection is the possibility to identify drone media access control (MAC) address. The advantages of this method are: 1. it does not depend on the drone size and material; 2. line of sight is not necessary to exist between the drone and the sensor; 3. there is nearly no need for specialized hardware and software tools intended for the analysis [35] (the solution in [35] is realized in open source software and using commercial hardware modules). On the other hand, the drawbacks of this method are: 1. it is only possible to detect open MAC address; 2. it is difficult to make and update the database of all MAC addresses of new drones; 3. drone MAC address may be spoofed in order to avoid drone detection [3].

C. Acoustic detection

There are special microphones, which may be used in acoustic drone detection. As at radar and RF detection, each drone type has its specific acoustic signature generated by multicopter propellers and motors. As the sound speed in air is low, it is possible to locate a drone on the base of difference in the sound time-of-arrival to several distant sound sensors [1].

Many algorithms implemented for speech analysis may be also used for drone detection, because these two have similarities. The analysis method in [36] is autocorrelation to calculate linear predictive coding (LPC) coefficients. The applied algorithm includes also the slope of the frequency spectrum and the zero crossing rate.

The analysis in [37] is based on the base of different algorithm. The computed local features are short time energy, temporal centroid (balancing point of audio signal amplitudes distribution), spectrum centroid (balancing point of audio spectrum), spectral roll-off (frequency below which some in advance defined percent of signal energy is located), zero crossing rate and so on. Whether analysis is performed according to [36] or [37], it is necessary to compare the obtained results to the drone acoustic signature.

There are three strategies for microphone positioning for sound direction detection [38]: 1. only one unidirectional microphone, which is slowly moving over the surface of hemisphere, driven by two servomotors, one rotating the microphone in horizontal plane and the other changing the elevation angle in the vertical plane; 2. eight stationary unidirectional microphones positioned in one plane in the vertices of octagon, the distance between these microphones is low (less than 10cm) – the sound direction is determined on the base of time when the same sound signal is detected; 3. eight microphones are positioned in one plane as in previous case, while the ninth microphone is in the second plane – this, last microphone detects drone's elevation angle, while the previous ones detect drone's direction in horizontal plane.

The benefits of acoustic drone detection are [1]: 1. sound may bypass some obstacles, thus allowing detection when LOS does not exist; 2. it is possible to detect drones, which have no communication links to the pilot. When considering drawbacks, there are several ones: 1. the range of detection is limited; 2. as the sound speed is low, it is possible that drone travels a pretty great distance while the sound reaches a distant sound sensor; 3. sound sensors are sensitive to rain and, especially, wind; 4. extensive background sound (noise) in urban environment makes detection more difficult; 5. drones, besides sound frequencies, generate ultrasound, which is highly exposed to atmospheric loss; 6. drone development is going in the direction of more and more quiet models; 7. the solutions based on acoustic detection are expensive, especially when the cluster of microphones is implemented; 8. the problem in detection arises when more susceptible drones are present in the same time [1], [35].

D. Optical detection

Optical detection of drone presence is based on technology, which is already developed for other applications: digital cameras, surveillance cameras and face recognition software [1]. The benefits of optical detection implementation are: 1. it is possible to use already developed cameras; 2. long range detection is achievable thanks to good quality optical zoom in these cameras; 3. objects are detected and classified using software tools; 4. it is possible to spread detection to the night period by the application of infrared (IR) cameras. The drawbacks of this detection are: 1. detection performances are poor in bad weather conditions; 2. it is necessary to analyze many pixels in a short time to cover a whole space in horizontal and vertical plane; 3. additional maintenance activities are necessary to keep lens clean; 4. if IR camera is not applied, the detection is not reliable in low light conditions; 5. it is difficult to estimate drone speed and distance if it is moving towards the camera [1].

Solution [15] is mainly based on optical detection. Each node consists of 30 cameras, which are connected in the LAN. Cameras form several concentric discs placed in multiple layers, thus covering the whole hemisphere about them

without idle spaces for detection. On the contrary, solution [39] uses only one high-resolution camera as one of implemented sensors in combination with thermal camera.

E. Thermal (infrared) detection

Thermal (infrared) cameras differ from conventional cameras in the characteristic that they may give pictures during night. This is their main advantage in the detection of drones over optical detection. Besides this, the benefits are: 1. thermal cameras are small, easy and cheap; 2. there is no or just minimum need for maintenance; 3. cameras may withstand all weather conditions, considering temperature and precipitations [40]. The drawbacks of thermal detection are: 1. the possibilities to detect drone highly depends on drone's heat production (many models of drones are made of plastic with electric motors, so in such cases it is more probable to detect a bird instead of a drone [1]); 2. the resolution of thermal camera is usually limited, so small drones on relatively greater distances may not be detected [15]. This, second, point may be illustrated by an example from [41]. The small number of pixels in this case causes that already at the distance of about 100m or less, drone is registered in camera by only one pixel, which does not allow the reliable detection. The maximum distance of detection is further reduced when drone is not moving at angle of 90^o in relation to camera axis and because usually not a whole drone is the source of thermal radiation.

To improve possibilities in the distance of detection, it is necessary to use more expensive cameras with greater resolution, which allow simultaneous following of more drones at distances of several kilometres when there is LOS [42]. High-resolution thermal camera, implemented in solution [39] with optical camera, still has about six times smaller number of pixels than this optical camera.

F. Selection of detection algorithm

The main conclusion of this section is that there is no preferred detection method. Detection reliability depends on many factors as, for example, characteristics of drone which has to be detected, weather conditions, drone distance from detector, and so on. This is the reason why the best solution has to be defined as a combination of two or more detector types. In our system we are going to implement four of five presented detector types: radar, RF, optical and thermal detector. We are not going to implement acoustic detector because of its limited distance of detection and problems of detection in noisy areas.

III. DISCUSSION OF SOLUTIONS FOR DRONES JAMMING

After drones successful detection follows the phase of their jamming. Jamming is not the unique, but it is probably the most efficient way of fight against drones (the other applied techniques being some kind of drone destruction and birds (eagles) catching drones [1]). It is possible to implement directional or all round RF jamming of drone links. When directional jamming is implemented, jamming range is greater than if all round jamming is implemented. On the other hand, all round jamming is more reliable, because it does not depend on the successfulness of drone detection [43]. The drawback of all round jamming is, besides lower range, causing malfunction of other devices in the vicinity, which are operating on the jammed frequency. The aim in jamming is to distort the signal to the level when receiver is completely unable to detect it or at least to achieve that some parts of the system lose their integrity, resulting in total or partial denial of service [44]. In most situations drone uses remote control (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 Global Positioning Systems (GPS and GLONASS). Drone's GPS successful jamming is the most effective way of disabling it. As a consequence of GPS frequencies jamming, the drone will crash. On the contrary, if other frequencies important for drone function are jammed and GPS not, the drone will land itself, or will fly a safe "Return Home" towards its starting point [45]. Besides jamming drone operation, spoofing is a more intelligent way of drone disabling, which is a process of taking over the control of drone flight and function [45].

There is a variety of solutions intended for drone jamming and [46] - [49] is a part of literature representing these solutions. The form of jammer may be different: as a gun, portable as a suitcase, as a desktop, installed on specialized vehicles, and so on. As the most often implemented frequencies for drone function realization are well-known, jammer realization is significantly simplified comparing, for example, to RCIED activation jamming. The frequencies applied for drone communications and for video and telemetry links are 433MHz, 868MHz, 915MHz, 1,2GHz, 2.4GHz, 5.8GHz, as well as 1176MHz, 1227MHz and 1.57-1.62GHz for locating by GPS or GLONASS systems [3], [48] - [52]. In the solution [51] the majority of these frequencies are jammed. The older drone systems use frequencies 27MHz, 35MHz, 49MHz, 72MHz or 75MHz [33]. It is interesting to emphasize that jamming may be realized on frequencies different than nominal ones, but the signal level has to be higher than on nominal frequencies. The reason is that GPS signals have very low level at the place of GPS receiver (typically lower than -120dBm). That's why the satisfactory signal level may be achieved also by out-of-band signal, signal spectral side-lobs or as the result of intermodulation producing signal harmonics [53]. According to the test results for various GPS receiver types presented in [54], the jamming to signal power ratio J/S=25dB causes maximum position error between 129m (the worst receiver) and 16m (the best receiver), while during time of observation the position was unchanged between 16% of time and 100% of time, respectively. The results in [55] emphasize that jamming signal power of 13dBm (20mW) disrupt all GPS receivers till a distance of 2km. Further, the graph from [56], i.e. from figure 2.5 in [55] allows us to determine more precisely the necessary jamming signal level depending on the desired protection distance and the degree of localization loss. This is very important when GPS signal jammer is designed not only to decrease necessary power consumption, but also to cause as little as possible influence on other GPS receivers in the protected area.

The implemented techniques for drone jamming are the same as for other system types jamming: barrage, tone, sweep

jamming, as well as protocol-aware jamming [57]. Two behaving modes may appear when drone jamming is realized. The first one means that jamming signal level is relatively high, so that GPS localization is not possible. The absence of localization is present in wider area, degrading also the function of a number of other devices in the protected area besides eventually present drones. The second mode is present when jamming signal is lower. In that case GPS localization is possible, but the resultant determined position is wrong [58]. The protected area is smaller and the effects of jamming are less visible, because localization is not completely lost. IRITEL jamming solutions [6] - [12] are a guarantee for successful development of drone jammer. Preliminary testing results of these IRITEL jammer solutions, which are not intended directly for drone disabling, prove that they may be successfully used for drones' jamming even in the present variant. One of these IRITEL solutions is presented at the Defense & Security International Exhibition Eurosatory 2018 in Paris as well as at the 9th International Defence Exhibition Partner 2019 in Belgrade. The solution is verified for its full military application. For drones jamming, it is not necessary to jam the whole available frequency spectrum, but only the regions around the above emphasized frequencies, using already developed and tested jamming methods.

Besides jamming malicious drones, it is worth mentioning opposite solution types when drones are implemented in friendly missions to prevent various malicious activities. There is a plenty of possible missions, as for example commercial airplanes protection from heat-seeking missiles [36], or IRITEL original solution of drone carrying a jammer against Remote Controlled Improvised Explosive Devices (RCIED) activation. The protection range is increased when drone carries a jammer comparing to jammer positioning on the ground. IRITEL solution is tested against frequency hopped activation messages and presented at the 9th International Defence Exhibition Partner in Belgrade 2019.

IV. CONCLUSIONS

This paper first, as a main contribution, presents techniques, which may be used for drones' detection. After that, it emphasizes main points important to realize successful drones' jamming. The techniques for drones' detection are radar, RF, acoustic, optical and thermal (infra-red) sensing. These techniques are mutually compared, while citing benefits and drawbacks of each technique. There is no clear advantageous technique, comparing one to the other. To overcome the problem of drones' detection under different conditions, several techniques are combined in one solution.

In the area of drones jamming, the implemented techniques correspond to conventional jamming techniques, where sweep and barrage jamming are the most popular ones. The primary goal is to disable drone GPS localization and this is the most effective way for jamming realization. It is presented how IRITEL jammers may be used for drones jamming and how drones may be used to improve IRITEL jammers efficiency.

REFERENCES

[1] 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.

[2] M. Marina, and P. D. Mirosavljević: „Technic of flight drones in air traffic and transport", Tehnika, Vol 65, No.5, October 2018., pp. 683-688., DOI: 10.5937/tehnika1805683M., in Serbian.

[3] X. Shi, C. Yang, C. Liang, Z. Shi, and J. Chen: „Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges", IEEE Communications Magazine, Vol. 56, Issue 4, April 2018., pp. 68-74., DOI: 10.1109/MCOM.2018.1700430.

[4] „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.

[5] „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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] Advanced protection systems: "Ctrl+sky drone detection and neutralization system", 2017., http://apsystems.tech/wp-content/uploads/2018/01/aps_broszura_web.pdf.

[14] Droneshield: „Product Information", October 2018.

[15] H. Liu, F. Qu, Y. Liu, W. Zhao, and Y. Chen: „A drone detection with aircraft classification based on a camera array", 2018 IOP Conference Series: Materials Science and Engineering 322 052005, 2018., pp. 1-7, DOI: 10.1088/1757-899X/322/5/05200.

[16] F. Hoffmann, M. Ritchie, F. Fioranelli, A. Charlish, and H. Griffiths: „Micro-Doppler Based Detection and Tracking of UAVs with Multistatic Radar", 2016 IEEE Radar Conference (RadarConf), 2-6.

May 2016., Philadelphia, USA, ISBN: 978-1-5090-0863-6, ISSN: 2375-5318, DOI: 10.1109/RADAR.2016.7485236.
[17] Robin Radar Systems, „Drone Detection Radar", https://www.robinradar.com/files/robinradar-brchr-dronedetectie-jan-2018.pdf.
[18] R. L. Sturdivant, and E. K. P. Chong: „Systems Engineering Baseline Concept of a Multispectral Drone Detection Solution for Airports", IEEE Access, Vol. 5, June 2017., pp. 7123-7138, DOI: 10.1109/ACCESS.2017.2697979.
[19] B. Karlsson: „Modeling multicopter radar return, A study in discrimination of multicopter UAVs from birds using the micro-Doppler effect", Master thesis in Applied Physics, Chalmers University of Technology, Goethenburg, Sweden, 2017.
[20] C. J. Li, H. Ling: „An Investigation on the Radar Signatures of Small Consumer Drones", IEEE Antennas and Wireless Propagation Letters, Vol. 16, 2017., pp. 649-652., DOI: 10.1109/LAWP.2016.2594766.
[21] M. Hammer, M. Hebel, B. Borgmann, M. Laurenzis, and M. Arens: „Potential of LIDAR sensors for detection of UAVs", Proceedings of SPIE Vol. 10636, SPIE Defense&Security 2018, Orlando, USA, pp. 1-8.
[22] P. Petrović: „Research in Software Defined Radio and AESA Radar Technology", Serbia-Italia/Status and Perspectives of the Scientific and Technological Bilateral Cooperation, 2012., pp. 19-20.
[23] P. Jovanović, M. Mileusnić, and P. Petrović: An Approach to Analysis of AESA Based Radio systems, XII International Scientific-Professional Symposium INFOTEH 2013, March 2013, Vol. 12., pp. 372-376, ISBN: 978-99955-763-1-8.
[24] P. Petrović, V. Marinković-Nedelicki, B. Pavić, and B. Mišković: Modernizacija OAR P-12 na bazi softverski definisanog radija i perspektive (Modernization of OAR P-12 based on software-defined radio and its perspective), Okrugli sto „Softverski definisan radio" (Round-table „Software Defined Radio"), Military Technical Institute, 2012., in Serbian.
[25] B. Pavić, V. Marinković-Nedelicki, M. Mileusnić, N. Remenski, and P. Petrović: „Verifikovani modernizovani radar P-12", tehničko rešenje kategorije M81 u okviru projekata koje finansira Ministarstvo prosvete, nauke i tehnološkog razvoja Republike Srbije, 2013.
[26] V. Marinković – Nedelicki, B. Pavić, B. Mišković, M. Mileusnić, P. Petrović, A. Lebl, D. Borjan, D. Ivković, and D. Nikolić: „Modernization of the Radar P12", 7th International Scientific Conference on Defensive Technologies OTEH 2016, 6-7. October 2016., ISBN 978-86-81123-82-9, pp.417-421.
[27] M. Mileusnić, M. Popović, A. Lebl, D. Mitić, and Ž. Markov: „Influence of Users' Density on the Mean Base Station Output Power", Elektronika ir Elektrotechnika, Vol. 20, No. 9, November 2014., pp. 74-79., DOI: http://dx.doi.org/10.5755/j01.eee.20.9.5418.
[28] O. Anthony, and O. Raphael: „Characterization of Signal Attenutation using Pathloss Exponent in South-South Nigeria", International Journal of Emerging Trends in Technology in Computer Science (IJETTCS), Vol. 3, Issue 3, May – June 2014., pp. 100-104., ISSN 2278-6856.
[29] R. Amorim, P. Mogensen, T. Sørensen, I. Z. Kovács, and J. Wigard: „Pathloss Measurements and Modeling for UAVs connected to Cellular Networks", 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), 4-7. June 2017., Sydney, Australia, DOI: 10.1109/VTCSpring.2017.8108204.
[30] L. Willy: „Effects of RadioWave Propagation in Urbanized Areas on UAV-GCS Command and control", master of science thesis in electrical engineering, Naval Postgraduate School, Montery, California, 2003.
[31] B.-P. Teh: „RF techniques for detection, classification and location of commercial drone controllers", Keysight technologies, 2017 AD Symposium.
[32] P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han, and T. Vu: „Matthan: Drone Presence Detection by Identifying Physical Signatures in the Drone's RF Communication", MobiSys'17, Niagara Falls, NY, USA, 19-23. June 2017., pp. 1-14., 2017 ACM. ISBN 978-1-4503-4928-4/17/06, DOI: http://dx.doi.org/10.1145/3081333.3081354.
[33] W. D. Scheller: „Detecting drones using machine learning", thesis for master of science, Iowa State University, Ames, Iowa, USA, 2017.
[34] Institut IRITEL, Elektrotehnički fakultet u Beogradu, Elektronski fakultet u Nišu, Institut Mihajlo Pupin: TR32051, projekat pod nazivom „Razvoj i realizacija naredne generacije sistema, uređaja i softvera na bazi softverskog radija za radio i radarske mreže", razvoj kofinansiran učešćem MPNTR Republike Srbije, 2011-2019.
[35] M. Peacock, and M. N. Johnstone: „Towards Detection and Control of Civilian Unmanned Aerial Vehicles", 14th Australian Info. Warfare and Security Conference, Edith Cowan Univ., Perth, Western Australia, 2-4. December 2013, pp. 9-15., DOI: 10.4225/75/57a847dfbefb5.
[36] L. Hauzenberg, and E. Holmberg Ohlsson: „Drone Detection using Audio Analysis", Master's Thesis, Department of Electrical and Information technology, Faculty of Engineering, LTH, Lund University, Sweden, June 2015.
[37] A. Bernardini, F. Mangistordi, E. Pallotti, and L. Capodiferro: „Drone detection by acoustic signature identification", IS&T International Symposium on Electronic Imaging 2017, Imaging and Multimedia Analytics in a Web and mobile World 2017, 29. January – 2. February 2017., San Francisco, United States, pp. 60-64., DOI: https://doi.org/10.2352/ISSN.2470-1173.2017.10.IMAWM-168.
[38] Z. Chua, G. Haroush, C. Leung, A. Malhotra, P. Olexa, A. Wilson, and Y. Zhao: „Detection of Civil Unmanned Aerial Vehicles by Sound Processing", EE2-PRJ E2 Project Interim Report, Imperial College London, January 2016.
[39] AARONIA AG: „Drone Detection System: AARTOS DDS Advanced Automatic RF Tracking and Observation Solution", 2018., pp. 1-16.
[40] „Main Benefits Of The SPYNEL Infrared Sensors", https://www.hgh-infrared.com/Applications/Security/Main-Benefits-Of-The-SPYNEL-Infrared-Sensors.
[41] P. Andraši, T. Radišić, M. Muštra, and J. Ivošević: „Night-time Detection of UAVs using Thermal Infrared Camera", International Conference on Air Transport – INAIR 2017, Transportation Research Procedia 28 (2017), 14-16. November 2017., pp. 183-190.
[42] „HGH Infrared Systems: Drone Tracking and Recognition", https://www.hgh-infrared.com/Documents/Optronics-for-Security/Videos/Drone-tracking-and-recognition.
[43] Optix: „Optix anti-drone system: Product information, specification & scope of supply".
[44] 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.
[45] 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.
[46] Optix: „Anti-Drone System Compact".
[47] https://www.perfectjammer.com/drone-signal-jammers.html
[48] http://jammers4u.com/drones-jammer
[49] https://www.thesignaljammer.com/blog/everything-you-need-to-know-about-drone-jammers/
[50] A. L. Drozd: „Spectrum-secure Communications for Autonomous UAS/UAV Platforms", MILCOM 2015 - IEEE Military Communications Conference, Tampa, Florida, 26-28. October 2015.
[51] Drone Killer 6 – powerful UAV (GPS WIFI5GHz) Jammer – 120W, https://www.jammer-store.com/drone-killer-6.html.
[52] 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.
[53] D. Borio: „A Statistical Theory for GNSS Signal Acquisition", Tesi di Dottorato in Elettronica e delle Communicazioni – XX ciclo, Politecnico di Torino, Marzo 2008.
[54] H. Kuusniemi, E. Airos, M. Bhuiyan, and T. Kröger: „Effects of GNSS Jammers on Consumer Grade Satellite Navigation Receivers", NNF Workshop on GNSS Interference and Jamming, Oslo, Norway, 2012.
[55] 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.
[56] M. Jones: „The Civilian Battlefield: Protecting GNSS Receivers from Interference and Jamming", InsideGNSS, March/April 2011.
[57] K. Pärlin: „Jamming of Spread Spectrum Communications Used in UAV Remote Control Systems", Master's Thesis, Tallinn University of Technology, Tallinn, 2017.
[58] M. A. Farid, M. Ahmad, S. Ahmed, and S. S. Rahim: „Impact and Detection of GPS Jammers and Countermeasures against Jamming", International Journal of Scientific & Engineering Research, Vol. 9, Issue 12, ISSN 2229-5518, December 2018, pp. 47-54.