Advanced protection methods of unmanned aircraft vehicle against attack by radio techniques

Robert Sierzputowski*[a], Rafal Polak[a], Damian Wojtyra[a], Dariusz Laskowski[b]
[a]Transbit Sp. z o.o., Lukasza Drewny 80 str., 02-968 Warsaw, Poland; [b]Military University of Technology, Faculty of Electronics, Gen. S. Kaliskiego 2 str., 00-908 Warsaw, Poland

ABSTRACT

There are many solutions in the world used to combat an unmanned aerial vehicles (UAVs) in a non-kinetic way. Considering the costs associated with the kinetic combat of UAV, technological development makes it possible to replace such annihilation of the threat in favor of non-kinetic combat. However, the degree of complexity in developing effective non-kinetic combat does not allow the easy introduction of appropriate solutions to ensure high efficiency. An important element of systems combating UAVs is to detect threats, but the use of appropriate measures to combat the threat depends on the effectiveness. Considering the latest technical solutions, UAVs systems have interference-proof control systems, enabling them to return to the starting place, as well as other elements hindering their eradication. There are few solutions in the world combining kinetic and non-kinetic control. Considering the degree of technical sophistication of such systems, there is not much of such systems in the world. The most common are manual systems that enable electromagnetic pulse interaction or the transmission of appropriate interference signals. In the civil market, UAVs systems most often use frequencies close to Wi-Fi. Connectivity relationships can easily be distorted by commercially available Wi-Fi interfering devices. A more difficult issue is military UAVs systems. The possibility of communication between the operator and the aircraft expands to more available radio frequencies, and therefore to technologies boosting their immunity. Therefore, the article presents an analysis of current methods of non-kinetic combat UAVs systems. Next, the solutions of non-kinetic UAVs combat were reviewed to present the conclusions from the multifaceted tactical and technical analysis of the possibilities of currently used solutions in the subject area. Based on the knowledge from the area of the advantages and disadvantages of these systems it is possible to submit a proposal to increase the resistance against the destructive non-kinetic combat UAVs.

Keywords: UAVs systems, combating UAVs, intentional interferences, UAV immunization

1. INTRODUCTION

Nowadays, virtually all unmanned aircraft systems (UAVs) use wireless communication with the operator. For this purpose, different protocols and frequencies are used depending on the applications. Civil connectivity solutions use frequencies designed for Wi-Fi standards due to the availability of specific bands. UAVs communication systems form their own network to which the operator is connected and sends appropriate aircraft control messages via communication protocols. This way of communication, working at previously mentioned frequencies, can easily be disrupted. There are lots of devices available on the market to disrupt frequency bands for Wi-Fi networks. UAVs systems intended for military use are more difficult to disrupt, due to the larger number of available radio bands, as well as technologies that make radio communication resistant to intentional interference.

Another way to implement UAVs control is to control from a ground station where the operator can program the flight trajectory of an unmanned aircraft. [6] Each UAVs mission consists of three phases, followed immediately after each other – take-off, flight along a given route, landing. [3] [10] The control system is responsible for the correct autonomous performance in all phases of flight trajectory defined by the operator while maintaining constant stabilization of the flight. [4] The design of the system should have a modular structure in which you can distinguish elements responsible for the delivery and processing of flight-specific data, and modules responsible for performing mission algorithms saved in the system's memory or sent from the ground station.

*robert.sierzputowski@transbit.com.pl; phone +48 534 604 739; fax +48 22 550 48 10, tansbit.com.pl

Radioelectronic Systems Conference 2019, edited by Piotr Kaniewski, Jan Matuszewski, Proc. of SPIE
Vol. 11442, 114420Y · © 2020 SPIE · CCC code: 0277-786X/20/$21 · doi: 10.1117/12.2565296

The project implemented in this way is a tool with which the operator is able to determine the height at which UAVs should move, as well as its total speed of the defined flight path. This way of communication of UAVs with the operator is characterized by greater interference resistance due to the lack of continuous signal transmission. Current technological progress enables, in programmed UAV control systems, the use of GPS, compasses and inertial navigation when determining their position relative to the operator or the starting point. [5] [9] The use of inertial navigation is the most advanced and difficult to combat solution, due to its own path stabilization and memory system and the lack of messages sent to the UAV operator.

Military unmanned systems differ from civil systems not only in their size, but also in their equipment in various types of security systems, ranging from interference suppression systems to systems preventing kinetic effects. UAV design for military applications is most often similar to regular aircraft, allowing them to reach higher flight speeds while emitting a lower sound level. Unmanned military-related aircraft are mainly used for reconnaissance missions and cargo handling. A large number of these systems do not require a remote-control system, rather systems using different types of navigation devices to minimize the risk of detecting the object itself as well as the exact location of the information collection point. [11] Additional properties of military UAVs systems are the use of encryption devices, using highly complex algorithms, in order to hamper control takeover and reduce the risk of combating UAVs.

2. ANALYSIS OF COMBATING UAV WITH THE USE OF COOPERATING KINETIC AND NON-KINETIC SYSTEMS

Due to the degree of advancement of non-kinetic systems to combat unmanned aircraft, there are few systems of this type. Most often these are manual systems enabling the creation of an electromagnetic beam directed at the object being controlled or sending appropriate interfering signals. Quite rarely, they are combined with kinetic variants.

One such system is The Battelle – a relatively simple system mounted on RIS (Rail Interface System), used to mount additional equipment in U.S.-type M4-type rifles. The Battelle system does not perform the function of guiding, tracking or eliminating the target with a laser. The range of the system is similar to the range of the rifle. The degree of effectiveness of UAVs combat using the Battelle system is comparable to rifle ammunition, while doing less damage.

The use of The Battelle disrupts control between the receiver mounted on the aircraft and the operator controller. As a result of this action, the aircraft goes into FailSafe mode. The functions of this mode, depending on the manufacturer and technical assumptions of the facilities, are implemented in various ways, e.g. landing at the place of loss of communication, returning to the starting point, or departing without control while maintaining the speed, direction and altitude of the flight, until the batteries are discharged.[21]

Another system that uses kinetic and non-kinetic methods to combat UAVs is The Red Sky System – 2. It is a short-range antiaircraft system through which the borders and strategic facilities of urban areas are effectively protected. The system is used to capture aerial targets by automated means, using autonomous scanning, tracking and combat capabilities. Red integrates advanced radar, an innovative electrooptical thermal imaging camera, as well as a threat identification system and tracking system. Since the threat is detected, the system tracks the target and allows the operator to interrupt and neutralize the threat at safe distances from the protected zone. As a result of the interference, communication between the operator and UAV on several transmission channels is blocked and navigation capabilities (GPS interference) are eliminated. Red Sky – 2 is a constantly developed system, and long-term development plans are focused on the installation of an additional miniature laser to destroy the smallest UAVs close to the launcher to increase the efficiency and capabilities of the system.[22]

The most advanced UAV eradication system is the T-Rex system. Tactical – Robotic Exterminator), which was commissioned by the U.S. Department of Defense. It is a project that integrates the AUDS system (Anti-UAV Defense System) with M230LF 30mm cannon. The AUDS system detects unmanned aerial vehicles using an electronic micro-Doppler radar, tracking UAV using a precisely controlled infrared camera system and daylight with embedded, advanced video tracking software. To destroy UAVs, AUDS system, uses a non-kinetic radio frequency inhibitor (RF). The AUDS system was established in accordance with the highest military standards and underwent field verification tests under harsh operational conditions. It is able to work in difficult weather conditions regardless of the time of day or night. Design assumptions include the concept of kinetic connection and non-kinetic combat of air objects, which translates

into an increase in the strategic capabilities of the system. The AUDS system can be used at stationary or wheeled vehicles. It provides a flying object at a range of 10km in a time of up to 15s. [20]

3. ANALYSIS OF THE POSSIBILITIES OF A NON-KINETIC SYSTEM

Currently, there are many solutions that enable non-kinetic combat of UAVs. In particular, these are solutions designed to combat unmanned civilian aircraft. Technologies used in this field, after proper modification, can effectively combat UAVs for military purpose. Non-kinetic solutions most often use the following techniques:

- Technique for disrupting control signals;
- Technique for disturbing the GPS transmitter;
- Technique of taking control over UAV.

The technique of interfering with control signals works by sending a high-power signal at a certain frequency and with a certain modulation. By adjusting publicly available radio systems (usually working on the Wi-Fi band), this technique allows to easily prevent civilian UAVs communication with the operator. In the case of disturbing UAVs for military purposes, the situation is more difficult, because military UAVs are most often equipped with anti-interference solutions from external systems. These systems work based on frequency jumps with short switching time. Disrupting such a system is very difficult to implement, because the only one 100% effective solution is to disrupt the entire frequency band. Another way to disrupt control signals could be searching for a signal in a wide range. This method is also difficult to implement due to the complex algorithms for determining the frequency, as well as a very small-time interval between switching. In addition, some military solutions have the ability to detect bandwidth usage and automatically switch transmission to the least busy band. In this case, the disruption of the specified band will also not be effective.

Technical solutions for newer and professional UAVs systems use satellite navigation systems for movement. Therefore, the non-kinetic system can be equipped with systems that allow GPS navigation to be disturbed or sent distorted geographic coordinates. The public GPS navigation technical documentation allowed many navigation interference systems to be produced. They cut off UAVs from coordinate information so that the programmed route cannot be completed. Disruption of GPS transmitter can also be realized by impersonating their transmitter as a GPS transmitter. This method involves sending distorted geographical positions into the system. As a result, the UAV performs a flight along an incorrect path or loses geographical orientation. Military satellite navigation systems are most often equipped with an additional cryptographic module SAASM. The use of the SAASM module makes it difficult to break the coordinates of geographic coordinates. GPS navigations for military purposes are devices with increased resistance to interference that obtain a more accurate position of the device. [19]

The most difficult technique for non-kinetic UAV combat is the technique of taking control of UAVs. In the case of civil solutions, well-known communication protocols are facilitated, enabling the operator to contact an unmanned aircraft. The multi-faceted aspect of security for military applications does not allow the introduction of standard communication protocols to UAV and other systems. Even if the military solution uses such techniques, the physical transmission of any information is preceded by the processing of information by various types of cryptographic devices. Encrypting data in military solutions makes it very difficult to capture control of UAV. Algorithms used in military solutions have additional encryption keys that practically prevent decryption of information, and even if there was such a possibility, it takes too much time for the control system to perform this operation. The only way is to have a database of encryption algorithms obtained through military intelligence services.

4. ANALYSIS OF METHODS FOR PROTECTING UAV COMMUNICATION AGAINST ATTACKS WITH THE USE OF RADIO MEANS

As part of the above-mentioned area of Electronic Warfare, modern radio stations are actively implementing two mechanisms defined in the field of Electronic Protection, i.e. Electronic Warfare Hardening and Emission Control. These mechanisms are designed to protect radio stations from the effects of such use of the frequency spectrum, which degrades, neutralizes or completely blocks their ability to work. Electronic protection measures minimize the enemy's ability to detect, track and intercept (Electronic Warfare Support) and the ability to effectively perform an Electronic

Attack. [7] Spectrum management mechanism is implemented outside of radio stations and is aimed at coordinating and eliminating conflicts of the use of frequency spectrum by both own and opponent forces. [16] [17] [18]

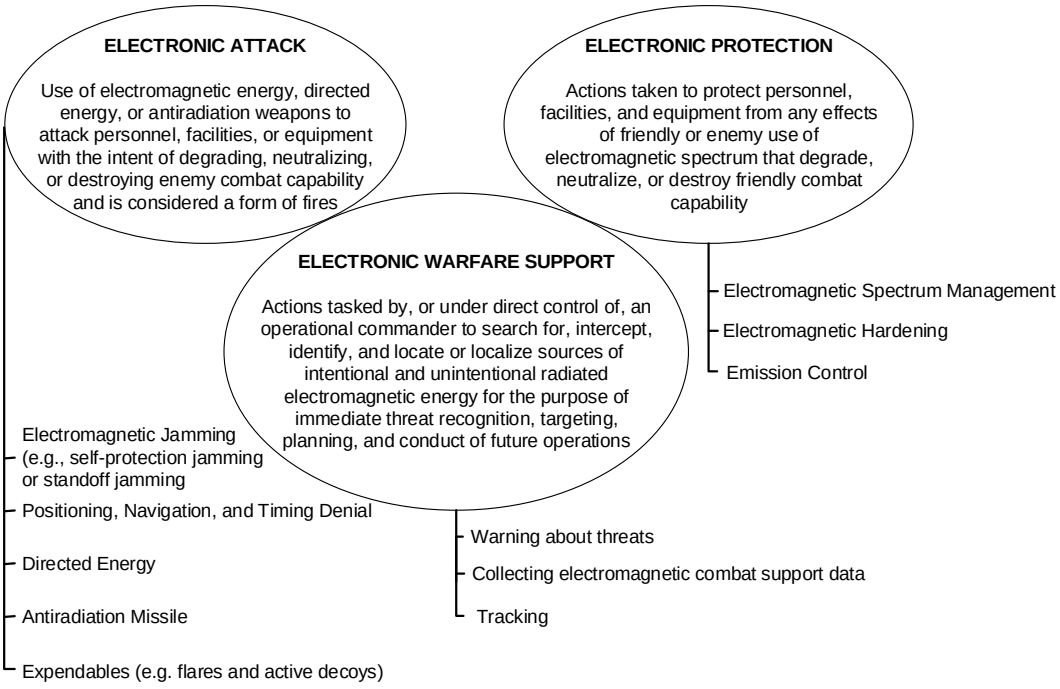

Figure 1. Area of Electronic Warfare (EW) activities [1].

Classification of mechanisms that immunize radio stations for intentional interference (EW Hardening, Anti-Jamming Techniques, Electronic Counter Countermeasures, Electronic Precaution Measures) presented on Figure 2.

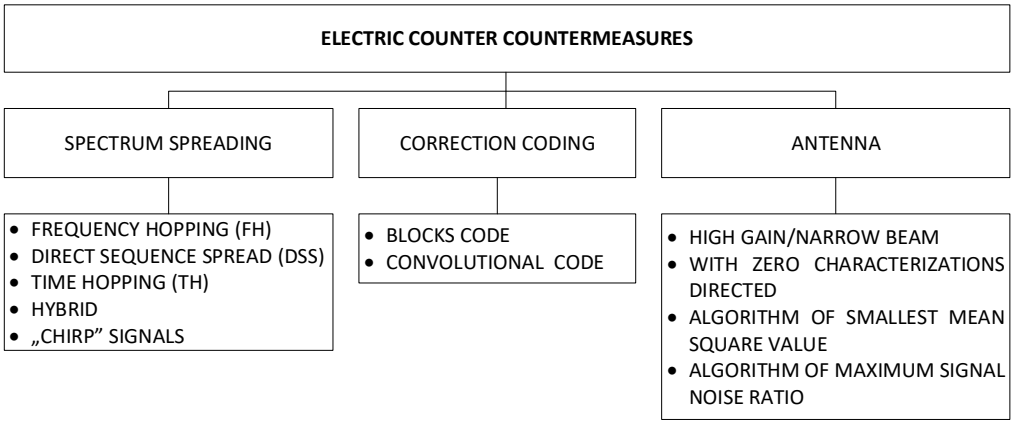

Figure 2. Classification of mechanisms that immunize radio stations for intentional interference [12].

In the VHF / UHF frequency range, SST (Spread Spectrum Techniques, Direct Sequence Spread) and ECC, FEC (Error Control Coding, Forward Error Coding) coding mechanisms are practically applicable. Anti-interference mechanisms associated with antennas do not have practical application in this place. The purpose of the mechanisms indicated above

is to force the system to disrupt the dispersion of its resources in the field of frequency, time and space, thereby reducing its effectiveness.

The DSSS (Direct Sequence Spread Spectrum) system has a relative simplicity due to the lack of a requirement for a fast frequency synthesizer. The transmitted signal is multiplied by a pseudo-random sequence with a high bit rate, which results in broadening the spectrum of the signal and reducing its spectral density. The transmitted signal acquires a noise-like form, which makes it harder to detect LPD (Low Probability of Detection) and more difficult to intercept LPI (Low Probability of Intercept) in relation to the signal without scattering. [13]

In a system with a frequency hopping FH (Frequency Hopping), the signal carrier frequency changes in a pseudo-random manner in a wide band. Although a potential opponent can detect a signal, it cannot be captured (Low Probability of Intercept). Systems in which more than one symbol falls on a given carrier frequency are called systems with a slowly jumping frequency LFH (Low Frequency Hopping). Otherwise, we are dealing with a system with a fast frequency hopping FFH (Fast Frequency Hopping). [15]

CSS (Chirp Spread Spectrum) systems are systems that use pulses with a monotonically changing frequency from the minimum frequency f_1 to the maximum frequency f_2 or vice versa. [2] The difference in these frequencies is a good estimate of the signal band. High signal resistance is obtained when the product of the chirp signal band and the duration of its pulse is much greater than one (this is accompanied by constant spectral density of the signal power). CSS systems are especially useful when the signal bandwidth is much higher than the binary data rate (Ultra-Wideband Systems). Chirp Spread Spectrum systems belong to the LPI class.

ECC coding techniques (FEC) allow the formatted information to be transmitted to resist noise and interference. This process is associated with the introduction of controlled redundancy into the transmitted data stream for the purpose of detecting and correcting errors in the receiver. Coding is characterized by so-called coding efficiency R being the ratio of the number of data symbols transmitted to the total number of code symbols transmitted. [14]

5. THE CONCEPT OF ARCHITECTURE OF A COMMUNICATION SYSTEM FOR UAV IMMUNISED TO ATTACKS BY RADIO MEANS

The concept of radio communication system architecture for UAV immune to radio attacks is based on devices manufactured by Transbit Company. The proposed radio solution works in the military band 4.4-5GHz and 235-380MHz and is dedicated to reconnaissance unmanned aerial vehicles. An Airplane Radio Line (SLR) was used to establish communication between the Ground Base Station (NSB) and UAV. The SLR consists of the following devices:

- Aircraft radio module– SMR;
- Base radio module– BMR;
- Antenna set.

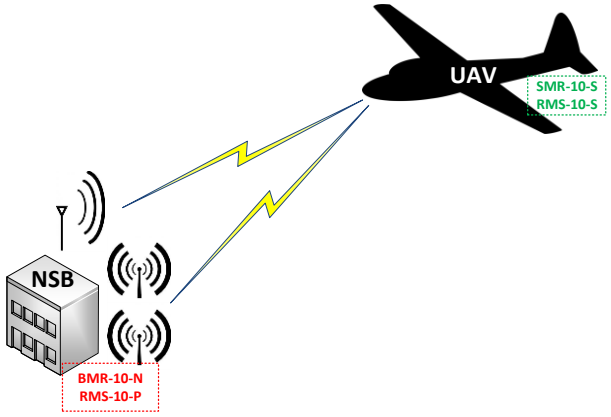

Figure 3. The concept of UAV radio communication with NSB using Airplane Radio Line.

The set of above-mentioned radio devices (SMR and BMR) enables bidirectional transmission of UAV telemetry and control data as well as various other types of data (e.g. video stream) from UAV to the ground base station.

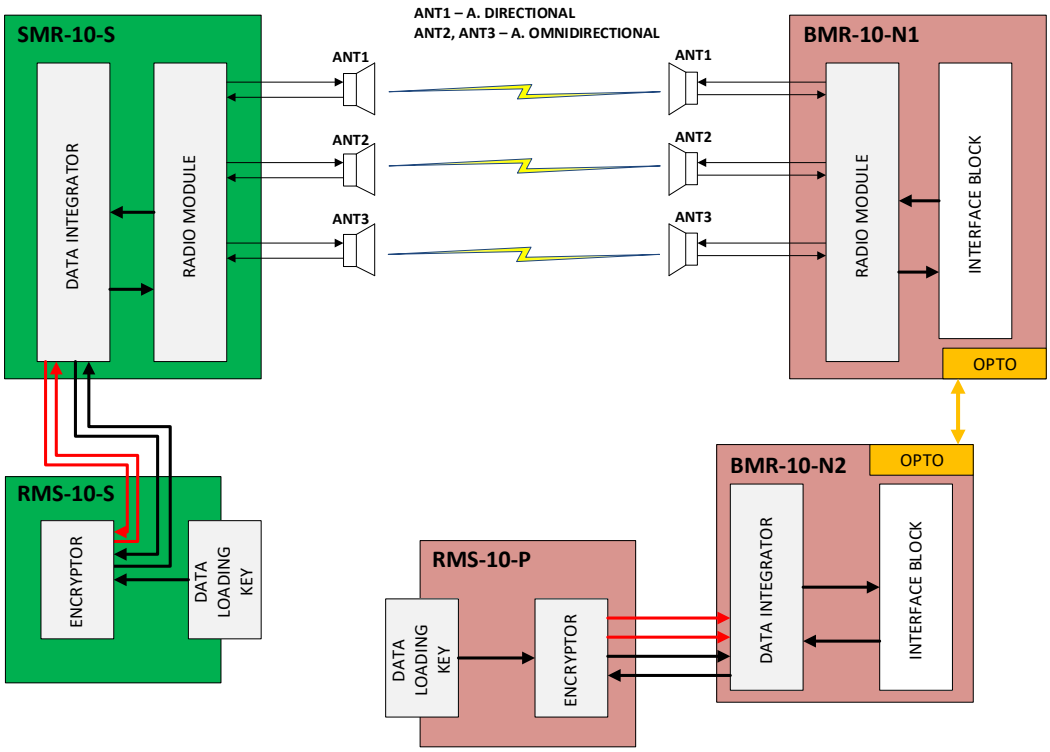

Figure 4. Block scheme of a radio communication system.

The aircraft radio module (SMR-10-S) is used to realization radio links between UAV and NSB. It is an advanced radio module designed in SDR technology, enabling the programmatic implementation of various work patterns, adapted to the requirements of cooperation with a given unmanned aircraft vehicle. The software selection of the SMR-10-S operating scheme allows you to maintain compatibility with many types of UAV systems, without having to replace the equipment. SMR-10-S can be used to transfer various types of data in a transmission channel with program-defined bit rate. It enables two-way communication with system objects. The aircraft radio module works with a set of two omni-directional antennas and one directional antenna. The use of two omnidirectional antennas is designed to eliminate the phenomenon of fading (signal loss due to multi-path) by the implementation of collective reception. Method of selection of antennas - combined ratio - effectively prevents atrophy of the deep while allowing to achieve communications without increasing the radiated power of the transmitter NSB. Using this module, it is possible to achieve effective radio communication over a distance of 0km to over 100km while maintaining LoS (Line of Sight).

The base radio module BMR-10-N is the equivalent of an aircraft radio module with extensive architecture, due to the installation of the device. It consists of two modules BMR-10-N1 and BMR-10-N2. The first (BMR-10-N1) is responsible for the performance of radio functions identical to the SMR-10-S module. The BMR-10-N1 module is made of transceiver sets – power amplifier, band filter, LNA amplifier sets.

The BMR-10-N1 block performs radio channel selection operations, modulation and demodulation processes, coding of radio signals and functions ensuring low probability of detection - LPD, low probability of interception - LPI and resistance to interference (Anti-Jamming) - AJ. All these functionalities are realized programmatically. BMR-10-N1 is designed for installation with a directional antenna.

The BMR-10-N2 module is responsible for the construction of radio channels suitable for the properties of data received on the Ethernet interface. It is also responsible for handling the data received on the receiving channels, mediates management schemes work communications system, and by installing the RMS-10-P encrypts and decrypts data to be

transmitted / received by the module WMD-10-N1.Communication between the BMR-10-N1 and BMR-10-N2 modules takes place via an optical interface.

The RMS-10-S and RMS-10-P radio encryption modules are separate hardware modules. They are equipped with connectors that allow data transmission in two separate two-way channels (encryption / decryption is independent in each direction) and a connector that allows connecting the carrier with key information consistent with the USB standard at the logical level. Their main task is to ensure the confidentiality of transmitted information and the authenticity of data origin. It has an AES algorithm implemented in accordance with FIPS 197 (with parameters: block - 128 bits, number of rounds - 14, key length - 256 bits), working in counter mode (CTR compatible with NIST: SP800-38A) and in Galois Counter Mode (GCM - NIST: SP800-38D). The module for operation requires key material provided on the Cryptographic Information Carrier – NIK. This material should have shared keys (PPK / PSK) in accordance with the DS-100-1 structure described in EKMS308f.

In order to achieve a high level of resistance to intentional interference and to prevent the acquisition of sensitive data by the enemy in the proposed solution, the following measures are taken:

- Channel coding - to enable error correction during data transmission in the interfered environment;
- Frequency Hopping Spread Spectrum;
- Realization of NSB to UAV and UAV to NSB connections on other subbands to mask transmission channels;
- Use of radio communication band 4,4-5GHz only because of the greater attenuation of propagation of radio waves in comparison to streaks operating at lower frequencies and the lack of ground wave;
- Application of DSSS technique for narrowband channels;
- Encryption of transmitted data;
- Realization of the radio link using a directional antenna;
- Adaptive power control;
- The ability to use the backup channel.

CONCLUSION

The article presents an analysis of non-kinetic methods of combating UAV for civil and military use. In addition, physical solutions have been described that are based on kinetic and non-kinetic methods of combating unmanned aerial vehicles. All of the described methods are used at the present time, often bringing positive effects in action.

An analysis was made of the solutions immunizing the UAV radio transmission with the operator or ground base station. Taking into account the results of the analyzes carried out and using radio devices manufactured by Transbit, proposals were made of the concept of radio communications for UAV for military purpose to conducting reconnaissance missions. The most important functionalities of individual elements of the proposed architecture were discussed. In the authors' opinion, the use of the described techniques in hardware implementation effectively reduce the risk of interference or interruption of radio communication between UAV and NSB.

REFERENCES

[1] „*Electronic Warfare In Operations, Field Manual FM 3-36*," Headquarters Department of the Army Washington, DC, February (2009).

[2] Ianelli Z, „*Introduction to Chirp Spread Spectrum (CSS) Technology*," Nanotron Technologies GmbH, Berlin, Germany (2003).

[3] Konatowski, S., Pawłowski P., „*Application of the ACO algorithm for UAV path planning*," Przeglad Elektrotechniczny, Vol. 95, Issue 7, pp. 115-118, doi:10.15199/48.2019.07.24 (2019).

[4] Konatowski, S., Pawłowski P., „*PSO algorithm for UAV autonomous path planning with threat and energy cost optimization*," Proceedings of SPIE, Vol. 11055, Bellingham, USA, pp. 1-9 (2019).

[5] Łabowski, M., Kaniewski, P., Konatowski, S., „*Estimation of Flight Path Deviations for SAR Radar Installed on UAV*," Metrology and Measurement Systems, Vol. 23, No 3, pp. 383-391, doi.org/10.1515/mms-2016-0034 (2016).

[6] Lubkowski, P., Laskowski, D., "*The Effective Identification of Objects in Selected Areas of Transport Transhipment*," Journal of Konbin, Vol. 49, Issue 1, pp. 7-30, March (2019).

[7] Matuszewski J., "*Evaluation of jamming efficiency for the protection of a single ground object,"* Radioelectronic Systems Conference, Jachranka, Poland, Nov 14-16, 2017, Proc. of SPIE, Vol. 10715, Article No. UNSP 107150B, 2018, doi:10.1117/12.2316629 (2017).

[8] Matuszewski J., "*Method of radiolocation object shield zone calculation for ground jammer stations*," XII Conference on Reconnaissance and Electronic Warfare Systems, Oltarzew, Poland, 19-21.11.2018, Proc. SPIE 11055, 110550C (27 March 2019); doi: 10.1117/12.2524527 (2018).

[9] Paszek, J., Kaniewski, P., "*Simulation of Random Errors of Inertial Sensors*," XIII International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science TCSET'2016, Lviv-Slavske, Ukraine, 23-26.02.2016, pp. 153-155 (2016).

[10] Pawłowski P., Konatowski, S., „*Ant Colony Optimization algorithm for UAV path planning*," Proceedings of 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET 2018), Lviv-Slavske, Ukraine, February 20-24, 2018, ISBN (IEEE): 978-1-5386-2555-2, paper 146. pp. 1- 6 (2018).

[11] Pietrow D., Matuszewski J., "*Object Detection and Recognition System Using Artificial Neural Networks and Drones*", Signal Processing Symposium (SPSSympo), Jachranka, 12-14.09.2017, Poland, IEEE Conference, Publisher: IEEE Xplore Digital Library: 02 October 2017, doi: 10.1109/SPS.2017.8053689.

[12] Sen C., „*Thesis Digital Communications Jamming*," Naval Postgraduate School Monterey California, September (2000).

[13] Sliwa J., Matyszkiel R., Jach J., *„Efficient Methods of Radio Channel Access Using Dynamic Spectrum Access That Influences SOA Services Realization - Experimental Results*", 2015 IEEE 81st Vehicular Technology Conference (VTC Spring) (2015).

[14] Matyszkiel R., Kaniewski P., Kustra M., Jach J., *„The evolution of transmission security functions in modern military wideband radios"*, Proc. SPIE 10418, XI Conference on Reconnaissance and Electronic Warfare Systems, 104180E (20 April 2017).

[15] Wisniewski M,, Dobkowski A., Pater G., Matyszkiel R., Kaniewski P., Grochowina B., *„Test results of polish SDR narrowband radio"*, IEEE 2017 Communication and Information Technologies (KIT) Slovakia (2017).

[16] Kosmowski K., Matyszkiel R., *"Verification of the criterion and measures of interferences used in radio planning systems"*, Proc. SPIE 11055, XII Conference on Reconnaissance and Electronic Warfare Systems, 110550J (27 March 2019).

[17] Kosmowski K., *"Frequency re-usage in radio planning systems"*, IEEE 2019 Communication and Information Technologies (KIT) Slovakia (2019).

[18] Wiszniewska-Matyszkiel A., Kaniewski P., Matyszkiel R., Kustra M., *"Application of dynamic games with incomplete information to optimisation of performance of military radio networks (jamming avoidance) "*, Proc. SPIE 11055, XII Conference on Reconnaissance and Electronic Warfare Systems. 1105507 (27 March 2019).

[19] Bugaj J., Górny K., *„Analysis of estimation algorithms for electromagnetic source localization"*, Proceedings of SPIE - The International Society for Optical Engineering, Volume 11055, Article number 110550W (2019).

[20] White A., *"DSEI 2017: T-REX makes an entrance into C-UAS"* Liteye, 27 February 2017, https://liteye.com/t-rex-makes-an-entrance-into-c-uas (13 November 2019).

[21] Zawadzak M., *"The Battelle DroneDefender – ręczny system antydronowy"* SwiatDronow, 13 October 2015, http://www.swiatdronow.pl/the-battelle-dronedefender-reczny-system-antydronowy (13 November 2019)

[22] Eshel N., *"Red-Sky 2 Short Range Air Defense System"* Defense-Update, 1 February 2005, https://defense-update.com/20050201_red-sky-2-2.html (13 November 2019).