ANALYSIS OF METHODS AND SYSTEMS FOR DETECTING AND COUNTERING UAVS

Elena Basan¹, Vyacheslav Pshikhopov¹, Maria Lapina², Massimo Mecella²,³

¹ Southern Federal University, Chekov st., 2, 347922, Taganrog, Russia
² North-Caucasus Federal University, Stavropol, Pushkin str., 1, 355017, Russia
³ SAPIENZA Università di Roma, via Ariosto 25, I-00185 Roma, Italy

E-mail ele-barannik@yandex.ru

Abstract. This article discusses methods for detecting UAVs in the radio frequency range. The analysis of the existing UAV detection systems is carried out. An overview of ways to counter UAVs is presented, in particular, by carrying out attacks on navigation and communication systems. A prototype of the UAV detection system, which is based on the UAV, is presented. The UAV detection function has been implemented based on the analysis of the radio frequency spectrum.

Keywords: Unmanned aerial vehicles; detection; opposition; convolutional neural network; training.

1. Introduction

Today, the problem of counteracting small-size unmanned aerial vehicles (SUAV) a copter type, is becoming quite acute. Such devices can damage critical infrastructure. In particular, this is evidenced by the latest incidents with oil bases and airports, when SUAV either blocked the operation of the facility, or their appearance led to significant economic consequences and disruption of the technological process. Counteraction to SUAV may include disruption of accessibility, disruption of functional capabilities of SUAV, disruption of the ability to transmit data through communication channels, interference and manipulation of the communication channel, substitution of transmitted information. Most of the vulnerabilities that can be exploited to compromise the security of SUAV are related to threats to communication channels. If we consider counteraction to the adversary from the point of view of implementing attack scenarios, then we can say that it is necessary to implement an external attack on SUAV. Any external attack scenario begins with reconnaissance. To begin with, it is necessary to find an SUAV to obtain information on the structural and functional characteristics. Information about SUAV can be obtained by several unmasking features:

- noise (acoustic);
- optical (visible);
- infrared (thermal);
- radar (radio);
Interfering with the operation of wireless communication channels, intercepting information over radio channels and radar signals, as well as finding transceivers and repeaters of communication is an important tactical task in countering SUAV. Such methods of impact on individual SUAV, such as: interception, jamming, changing location by using a more powerful signal - are fundamental in the implementation of attacks on SUAV groups. The battle space, which previously had only four dimensions (latitude, longitude, altitude and time), now has a fifth dimension: frequency [1].

The author of [1] pays great attention to the issues of stable data transmission, in particular, the connectivity of the information flow or information operations. The concept of information operations has a key meaning in the organization of military operations. In many respects, the successful implementation by the UAV of such actions as reconnaissance, observation, delivery of payload, weapons depend on the success of information operations.

The purpose of this study is to develop a method and system for counteracting small-sized unmanned aerial vehicles (SUAV) through active attacks on communication channels.

2. Analysis of the problem of detecting enemy UAVs

Let's consider some methods of UAV detection. The main means of detecting SUAV are radio location stations. In some cases, SUAV are a difficult target for existing radars. These devices have a small effective scattering area (ESR), which makes their detection difficult enough. In particular, the maximum detection range decreases [2]. In the literature, various methods for detecting unmanned aerial vehicles have been proposed with various approaches, such as: approaches based on the analysis of audio information [3] [4] [5], approaches based on video image analysis using cameras [6], [7] and approaches based on radio frequency sensing [8], [9]. However, each of these approaches has advantages and limitations. Sound techniques can be confused by other sounds in noisy environments, have a limited range and cannot detect SUAVs using noise reduction techniques. Whereas camera-based approaches require good lighting conditions, high-quality lenses and ultra-high-resolution cameras to detect SUAVs at long distances, this is certainly much more expensive and more difficult to implement. Radio frequency techniques based on the use of active radar are vulnerable to radio frequency interference [10]. However, the use of deep learning methods offers a great advantage in detecting and classifying SUAV using deep neural networks (DNN), which is also known as multilayer perceptron (MLP). Newer deep learning architectures such as Convolutional Neural Networks (CNNs) are used to detect UAVs. CNNs are used to detect UAVs using CCTV cameras [11] from surveillance images in [12] and Doppler signatures in [13]. In addition, deep learning has been used to solve various time series classification problems using a one-dimensional convolutional neural network (1 DCNN) architecture. This architecture has shown high performance and reliability in the classification of electrocardiogram (ECG) and phonocardiogram (PCG) signals [14], [15]. Multichannel 1DCNN is an extended version of basic 1DCNN with the only difference – the number of input channels. Multichannel 1 DCNN has been used to classify multivariate time series, although it can handle more than one input simultaneously [16]. However, these architectures were only time-dependent and highly dependent on the characteristics of the time domain.

When implementing the UAV detection task, it is also necessary to analyze the spectrum, determine the type of signal modulation, determine at which radio frequencies the highest activity is recorded, and distinguish between noise and a useful signal. Having studied the research on the topic, it can be summarized that the trends in the development of cognitive radio have reached the possibility of solving more complex problems [17]. These tasks include: Classification of new types of modulation as certain types of signals; Classification of unknown signals; Identification of fake signals or signal replay attacks, as well as noise-reduction; Identification of cases of overlapping signals, highlighting each individual signal from the user.

To date, there is a large amount of work devoted to the application of deep learning methods for the classification of radio frequency signals. Examples include spectrum detection [18], MIMO detection [19], channel estimation and signal detection [20], physical layer communication [21], interference
detection, [22], stealth suppression [23], [24], power control [25], signal alteration detection [26], and transmitter-receiver scheduling [27]. The classification of radio frequency signals can be used for various applications, for example, radio capture [28], which ultimately can be used in cognitive radio systems [29] subject to dynamic and nondeterministic interference [30]. The classification of modulation using deep neural networks is considered in [31], [32], [33], [34], where the goal is to classify this signal according to the known type of modulation. Various types of datasets have been used to train a deep neural network for modulation classification.

A review of the literature on the concept of UAV detection through object detection and classification using machine learning technologies showed that the use of machine learning facilitates the detection of UAVs in a binary classification model as "UAV" or "not UAV". However, some research in the literature goes beyond the traditional classification for a multiclass classification that identifies UAV types. The first part of the article discusses various tasks such as UAV detection, verification, UAV classification, characterization, and an approach to multiple UAV detection based on radar signals using machine learning methods. The use of high-quality 3D holographic radar along with machine learning in the time domain has been identified as an important research in UAV detection.

The authors of [35] proposed an improved method for UAV detection based on radio frequencies. The proposed methods allowed data to be obtained through a series of experiments in real-world environments using the Phantom 4 drone. Background filtering removes noise to obtain a better dataset. In addition, a frequency estimation method is used using the statistical characteristics of radio frequency signals from the UAV, which helps to identify the presence of the UAV in the controlled area. During the processing phase, UAV detection is programmed through two frequency estimates obtained from statistical fingerprint analysis and spectrum accumulation. The next step is to determine the presence of the drone using a comparison with the bandwidth, which is 9.8 MHz. To analyze and determine the performance of the current algorithm, the obtained data were compared with three well-known methods, such as ANN, CFAR and HOC. The application of the proposed method, along with the elimination of interference, led to the suppression of interference and an increase in the detection efficiency. In addition, the proposed methods provide an estimate of radio frequency at distances from 500 to 2800 m.

Focusing on the problem of unwanted drones flying over critical airspace to perform malicious actions, the authors of [36] propose a solution based on the analysis of RF signals. The authors investigated the ability to distinguish radio frequency signals received from UAVs from signals transmitted by other wireless devices. In addition, the detection process used a detector developed using a fusion algorithm that combines analysis of vibration from the UAV structure, detected by monitoring peak frequencies in a specific range from 20 to 50 Hz, as well as to register the shifts of the UAV structure using a detector based on wavelets into a unified classifier for UAV detection. Matthan's proposed solution has been tested in 3 different locations using 7 different UAVs from different manufacturers to ensure the reliability of the solution. The paper shows the effectiveness of using Matthan to distinguish UAV signals from signals generated by other moving devices, and the accuracy of detection, recall and accuracy exceeded 90% in scenarios where the UAV was at a distance of up to 50 meters. Even though the results dropped to 80–85% at a detection distance of 600 meters, the system performance is considered acceptable. However, Matthan's weak point is that he cannot distinguish between different UAVs.

Another study by the authors [37] was aimed at developing an autonomous unmanned aerial vehicle detection system for the classification of unmanned aerial vehicles based on radio frequency signals generated through direct communication between the unmanned aerial vehicle and the PND. The proposed system was developed using two methods. The first method was to implement an active detection and tracking system, in which the system sends a signal and continuously listens to the reflected signals from the UAV propellers. The second method used a passive detection system that listens for signals sequentially. Once the signal is received, it is extracted and analyzed further. According to the authors, the active system was able to distinguish changes between different UAV modes; for example, between stationary and flying, by significantly increasing the reflection strength of UAV rotor signals at a distance of 3 meters from a frequency of less than 100 Hz. In addition, the
authors concluded that the passive eavesdropping detection system was able to distinguish the UAV signals from other signals transmitted or reflected by other objects, such as the UAV camera, engines, propellers, which could affect the communication between the UAV and the PND. In addition, the authors claim that the communication channel between the UAV and the controller was detected at a frequency of 30 Hz in the frequency domain. However, the disadvantage of the system was the fact that changing the distance between the UAV and the detection system from 5 to 50 meters negatively affected the performance of the proposed detection system.

Likewise, a recent study aimed at creating an open-source UAV radio signal dataset and a system that is not only capable of detecting, but also identifying a UAV based on RF communications between the UAV and its PND was published in [38]. The main distinguishing feature between what was discussed above, and this work is that the authors chose to use deep learning algorithms as the main methodology for detecting and classifying UAVs. Three deep neural networks (DNNs) were designed in such a way that the system could achieve three main goals: detection that there is a UAV with an accuracy of 99.7% and f1_score 99.5%, detection and identification of its type with 84.5% and f1_score 78.8%, as well as detection, identification, and determination of flight modes with an accuracy of 46.8% and f1_score 43%. The authors also reported that the algorithm was unable to identify the two UAVs that were manufactured by the same company and their modes. Hence, a solution with different deep learning architectures like CNN can contribute to solving this problem.

3. Development of a system for detecting and countering unwanted SUAV

The analysis of the UAV detection methods showed that this problem can be solved using deep learning methods. At the same time, in most works it is noted that the most suitable tool for solving these problems is the use of ultra-precise neural networks. At the same time, there are even ready-made ground-based systems for detecting UAVs in the radio frequency range, which declare high detection accuracy and range. One of the tasks of the study is not only the detection of the UAV, but also the collection of detailed information about it for the purpose of further countermeasures. At the same time, the methods of countering UAVs, as a rule, are reduced to attacks on the navigation system, noise of the radio channel, suppression using electronic warfare or physical impact, which is confirmed by patent research. The existing set of data for detecting different types of UAVs, as well as the type of UAV activity, is rather limited. It is targeted only at civilian, consumer UAVs. The creation of such a base for military UAVs could be a promising task. In addition, when transmitting data via wireless communication channels, different frequencies, different types of modulation and coding of the transmitted information can be used. Therefore, it is necessary to provide not only activity detection, but also determination of other characteristics of the wireless channel. Thus, for further research, it is proposed to develop a test bench for collecting data on the UAV. The test bench layout is shown in Figure 1. In this diagram, it is proposed to use HackRF as a means of generating and receiving a radio signal. The HackRF One from Great Scott Gadgets is a software-defined radio device capable of transmitting or receiving radio signals from 1 MHz to 6 GHz. HackRF One is an open source hardware platform that can be used as a USB peripheral or programmed to run autonomously. It is designed to test and develop modern radio communication technologies. Device characteristics: Frequency range: 1 MHz - 6 GHz; Bandwidth: 20 MHz. Thus, we can say that this device is not inferior in characteristics to what was used in the previously reviewed works of other researchers. The most important characteristics are frequency range and bandwidth. ONNX (Open Neural Network Exchange) is an open software library for building deep learning neural networks. With ONNX, AI developers can exchange models between different tools and choose the best combination of these tools [39].

Intel Neural Compute Stick 2 is a computing module designed to perform tasks related to artificial intelligence, machine learning, etc. The device is based on Intel Movidius Myriad X Vision Processing Unit (VPU) - a specialized SoC containing 16 general-purpose computing cores, as well as hardware components for acceleration [40].
Figure 1. Generalized structural and functional diagram of the stand for preparing UAV detectors

With the help of HackRF, which is connected to a computer with SDR (Software-defined radio, SDR) installed, an RF signal is generated. The signals will be generated according to the developed algorithms, which will include emulation of retail modulation types, and network activity of the UAV. HackRF, on the other hand, will intercept this signal and convert it using the module being developed for the program of the LabView system. The resulting datasets will be fed to the input of the convolutional neural network for training, and then the generated ONNX file will be sent to the Intel Neural Compute Stick 2. Thus, the final device for detecting the UAV is Intel Neural Compute Stick 2, which has quite powerful computing resources, with compactness and small dimensions. After training the neural network and testing the result, it is necessary to integrate the detected UAV module into the UAV adaptive defense system, as well as into the enemy UAV countermeasure system. The architecture was chosen 1D CNN (one-dimensional convolutional neural network), which is shown in Figure 2.

Figure 2 shows that the architecture consists of several blocks:
1) conv-layer of one-dimensional convolution. Convolution is a linear transformation of a special kind of input. If x_{l} is a feature map in layer l, then the result of a two-dimensional convolution with a kernel of size 2d + 1 and a weight matrix W of size (2d + 1) × (2d + 1) on the next layer will be as follows:

\[ y_{i,j}^{l} = \text{func} \left( \sum_{-d \leq a,b \leq d} W_{a,b} x_{i+a,j+b}^{l} \right), \]

where func is the activation function; y_{i,j}^{l} is the result of convolution at level l; x_{i,j}^{l} is input, that is, the output of the entire previous layer.

2) batchnormalization – batch normalization layer. Batch normalization is a technique that solves the problem of changing the distribution of each layer during training relative to the changes in the previous layers. This problem significantly slowed down the learning process and set serious requirements for the initialization of model parameters.
The idea of the method is to normalize all the values of the features of a given batch independently, by putting a checkmate expectation at 0, and standard deviation at 1. All calculations are performed according to the formulas:

$$\mu_B = \frac{1}{m} \sum_{i=q}^{m} x_i,$$

$$\sigma_B^2 = \frac{1}{m} \sum_{i=q}^{m} (x_i - \mu_B)^2,$$

$$\hat{x}_i = \frac{x_i - \mu_B}{\sqrt{\sigma_B^2 + \varepsilon}},$$

$$y_i = \gamma \hat{x}_i + \beta,$$

where $\mu_B$ – batch waiting; $\sigma_B^2$ – batch variance; $\hat{x}_i$ - intermediate normalization value; $y_i$ – total normalization value; $\gamma$, $\beta$ – trained parameters.

3) pad – an auxiliary layer that adds zero values to the left and right of the input matrix,
4) averagepool – average subsampling layer. Downsampling is a transformation that reduces the dimension of the input data with minimal loss of information. For example, in face recognition with a convolutional network, it is much more important to understand whether there is a face in a photo than to find out which specific pixel it begins and where it ends. Therefore, it is possible to "generalize" the distinguished features, having lost some of the information about their location, but at the same time reducing the dimension.

There are several downsampling operations:
1) operation of taking the maximum:

\[ y_{i,j}^{l} = \max(-d \leq a \leq d, -d \leq b \leq d) x_{i+a,j+b}^{l}. \]  

(6)

2) average operation:

\[ y_{i,j}^{l} = \frac{1}{d^2} \sum_{a=0,b=0}^{d} x_{i+a,j+b}^{l}. \]  

(7)

where \( y_{i,j} \) is the result of downsampling at the \( l \) level; \( x_{i,j} \) is its input; \( d \) is the size of the downsampling window.

5) relu - a layer using the ReLU activation function. ReLU is one of the most popular non-linear activation functions today:

\[ f(x) = \max(0,x), \]  

(8)

where \( x \) is the input value of the function.

Basically, this function is used in the input and hidden layers of the neural network.

6) gather, Unsqueeze, Shape, Reshape – auxiliary layers that change the shape of a multidimensional array into a one-dimensional array,

7) gemm – multilayer perceptron layer,

8) input and output blocks are input and output layers, respectively.

DroneRF was chosen as the dataset. It consists of records of segments of radio frequency activity of several types of drones under the following conditions: 1) in the absence of drones, 2) in the presence of a drone operating in various modes: a) turned on and connected to the controller, b) automatic hovering in the air without physical intervention and control commands from the controller, c) flight without video recording, d) flight with video recording.

The records contain 10.25 seconds. RF activity without drones and about 5.25 sec. drone radio frequency activity in each mode. There are 227 segments in total, each segment is di-vided into 2 equal parts, each of which contains 107 samples. Each sample represents the amplitude of the signal. Note that, based on the analysis of the sources, the most effective and often implemented are attacks on the navigation system and the physical properties of the UAV.

The drones are assumed to be using a 2.4GHz WiFi network. Specification: number of channels: 2, frequency range: 1.2 GHz – 6 GHz, frequency step: <1, gain range: 0 dB - 37.5 dB, maximum instantaneous bandwidth: 40 MHz, maximum I / Q sampling rate: 200 MS / s, ADC resolution: 14 bit. Since the maximum instantaneous bandwidth is 40 MHz, at least 2 receivers (HackRF) must operate to capture the Wi-Fi spectrum (80 MHz), where the first receiver captures the lower half of the frequency band and the second receiver captures the upper half. For training, each segment was divided into 20 virtual channels (106 samples / channel). Each channel was divided into 2048 parts, from each of which an average value was taken. As a result, the minibunch for training was a two-dimensional array of size (20.2048).

UAV protection uses silencers to block control signals and GPS (optional) so that the UAV no longer receives the signals necessary for orientation. If so, the UAV is forced to land and therefore no longer poses a threat. One of the advantages of this method is that it does not damage the UAV. HackRF allows not only receiving but also sending signals. In addition, HackRF can be used to attack navigation systems and noise.
4. Conclusion
The proposed UAV countermeasure detection architecture is a compact and lightweight hardware solution with a sufficiently high computing power, which is very important for a UAV. In addition, unlike the existing UAV detection systems, this solution will be located on the UAV, which performs reconnaissance functions and, due to the possibility of changing the position, can calculate the unwanted UAV in any place, not the required distance.

5. Acknowledgment
This work was supported by the RFBR grant 18-07-00212 "Development of a method and protocol for decision-making for detecting anomalous node behavior in group control systems for autonomous mobile robots".

References
[1] Adamy, D O 2015 EW 104 EW against a New Generation of Threats. Boston: Artech House
[2] Yabov K How to counteract a drone // Military Review. – URL: https://mensby.com/technology/guns/5386-how-counteract-drone
[3] Bernardini A, Mangiatordi F, Pallotti E, Capodiferro L 2017 Drone detection by acoustic signature identification // IS Tnt. Symp. Electron. Imaging Sci. Technol pp 60-64
[4] Kim J, Park C, Ahn J, Ko Y, Park J, Gallagher J C 2017 Real-time UAV sound detection and analysis system // SAS 2017 IEEE Sensors Appl. Symp. Proc pp 1-5.
[5] Nijim M, Mantrawadi N 2016 Drone classification and identification system by phenome analysis using data mining techniques// IEEE Symp. Technol. Hamel. Secur. HST, 2016. – pp. 1-5.
[6] Aker C, Kalkan S 2017 Using deep networks for drone detection // 14th IEEE Int. Conf. Adv. Video Signal Based Surveillance AVSS-2017
[7] Saqib M, Daud Khan S, Sharma N, Blumenstein M 2017 A study on detecting drones using deep convolutional neural networks // 14th IEEE Int. Conf. Adv. Video Signal Based Surveillance AVSS-2017
[8] Nguyen P, Ravindranathan M, Nguyen A, Han R, Vu T 2016 Investigating cost-effective RF-based detection of drones // DroNet 2016 - Proc. 2nd Work. Micro Aer. Veh. Networks Syst. Appl. Civ. Use co-located with MobiSys pp 17-22.
[9] Ezuma M, Erden F, Anjinappa C K, Ozdemir O, Guvenc I 2019 Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques // IEEE Aerosp. Conf. Proc
[10] Abeywickrama S, Jayasinghe L, Fu H, Nissanka S, Yuen C 2019 RF-based Direction Finding of UAVs Using DNN // 2018 IEEE Int. Conf. Commun. Syst. ICCS 2018 pp 157-161.
[11] Aker C, Kalkan S 2017 Using deep networks for drone detection // 2017 14th IEEE Int. Conf. Adv. Video Signal Based Surveillance AVSS 2017
[12] Shijith N, Poornachandran P, Sujadevi V G, Dharmana M M 2018 Breach detection and mitigation of UAVs using deep neural network // 2017 Recent Dev. Control. Autom. Power Eng. RDCAPE 2017 vol 3 pp 360-365
[13] Kim B K, Kang H S, Park S O 2017 Drone classification using convolutional neural networks with merged doppler images // IEEE Geosci. Remote Sens Lett vol 14 no1 pp 38-42
[14] Kiranyaz S, Ince T, Gabhous M 2016 Real-Time Patient-Specific ECG Classification by 1-D Convolutional Neural Networks // IEEE Trans. Biomed. Eng vol 63 no3 pp. 664-675
[15] Kiranyaz S, Zabihi M, Rad A, Tahir B, Ince A, T, Hamila R 2016 Real-time PCG Anomaly Detection by Adaptive 1D Convolutional Neural Networks
[16] Hamila Y, Liu Q, Chen E, Ge Y, Zhao J L 2016 Exploiting multi-channels deep convolutional neural networks for multivariate time series classification // Front Comput Sci vol 10 no1 pp 96-112
[17] Miroshnikova N E 2013 A review of cognitive radio systems. Information Society Technologies 108-111
[18] Davaslioglu K, Sagduyu Y E 2018 Generative adversarial learning for spectrum sensing // IEEE International Conference on Communications (ICC)

[19] He H, Wen C-K, Jin S, Li G Y 2018 A model-driven deep learning network for MIMO detection,

[20] Ye H, Li G Y, Juang B-H 2018 Power of deep learning for channel estimation and signal detection in OFDM systems // IEEE Wireless Communications Letters

[21] O'Shea T. J., Hoydis J. 2017 An introduction to deep learning for the physical layer // IEEE Transactions on Cognitive Communications and Networking (TCCN)

[22] Shi Y, Sagduyu Y E, Erpek T, Davaslioglu K, Lu Z, Li J 2018 Adversarial deep learning for cognitive radio security: jamming attack and defense strategies // IEEE ICC 2018 Workshop - Promises and Challenges of Machine Learning in Comm Networks

[23] Zheng, Q. Liu, E. Chen, Y. Ge, J. L. Zhao Exploiting multi-channels deep convolutional neural networks for multivariate time series classification // Front. Comput. Sci. / 2016. – vol. 10. – no. 1. – pp. 96-112.

[24] Kwang C. C., Prasad R. Cognitive radio networks / 2009. – p.359

[25] E. G. Villegas, E. López-Aguilera, R. Vidal, J. Paradells Effect of adjacent-channel interference in IEEE 802.11 WLANs // Proc. 2nd Int. Conf. Cogn. Radio Oriented Wirel. Networks Commun. Crown Com / 2007. – pp. 118-125.

[26] Y. LeCun, K. Kavukcuoglu, C. Farabet, Convolutional networks and applications in vision // ISCAS 2010 – 2010 IEEE Int. Symp. Circuits Syst. Nano-Bio Circuit Fabr. Syst. / 2010. – pp. 253-256.

[27] S. Al-Emadi, F. Al-Senaid Drone Detection Approach Based on Radio-Frequency Using Convolutional Neural Network // IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT’20), 2020

[28] . Shi Y, Erpek T, Sagduyu Y E, Li J 2018 Spectrum data poisoning with adversarial deep learning // IEEE Military Communications Conference

[29] . Sagduyu Y E, Shi Y, Erpek T 2019 IoT network security from the perspective of adversarial deep learning // IEEE International Conference on Sensing, Communication and Networking (SECON) Workshop on Machine Learning for Communication and Networking in IoT

[30] . Erpek T, Sagduyu Y E, Shi Y 2019 Deep learning for launching and mitigating wireless jamming attacks // IEEE Transactions on Cognitive Communications and Networking

[31] Shi Y., Davaslioglu K., Sagduyu Y. E. Generative adversarial network for wireless signal spoofing // ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML), 2019.

[32] Abu Zainab N et al. 2019 QoS and jamming-aware wireless networking using deep reinforcement learning // T. Erpek, K. Davaslioglu, Y. E. Sagduyu, Y. Shi, S. Mackey, M. Patel, F. Panettieri, M. Qureshi, V. Isler, A. Yener / IEEE Military Communications Conference (MILCOM)

[33] Restuccia F et al 2019 DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms // S. D’Oro, A. Al-Shawabka, M. Belgiovine, L. Angioloni, S. Ioanidis, K. R. Chowdhury, T. Melodia / ACM Intl. Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)

[34] O’Shea T, Corgan J, Clancy T C 2016 Convolutional radio modulation recognition networks // International Conference on Engineering Appli-cations of Neural Networks,

[35] O’Shea T J, Roy T, Clancy T C 2018 Over-the-air deep learning based radio signal classification // IEEE Journal of Selected Topics in Signal Processing

[36] Nguyen P et al Matthan 2017 Drone presence detection by identifying physical signatures in the drone's rf communication // H. Truong, M. Ravindranathan, A. Nguyen, R. Han, T. Vu, / Proceedings of the 15th Annual International Conference on Mobile Systems Applications and Services ser. MobiSys ‘17 ACM

[37] Nguyen P et al 2016 Investigating cost-effective rf-based detection of drones // M. Ravindranatha, A. Nguyen, R. Han, T. Vu / Proceedings of the 2Nd Workshop on Micro Aerial Vehicle Networks Systems and Applications for Civilian Use ser. DroNet’16 ACM
[38] Zhao M et al 2018 Through-wall human pose estimation using radio signals // T. Li, M. Abu Alsheikh, Y. Tian, H. Zhao, A. Torralba / The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)

[39] Open Neural Network Exchange [Electronic resource]. URL: https://onnx.ai/ (date of accessed 07.11.2020)

[40] Intel Neural Compute Stick. Artificial intelligence on a flash drive - 2. [Electronic resource]. URL: https://habr.com/ru/company/intel/blog/430492/ (date of accessed 07.11.2020).