Proceedings of the Third International Conference on Intelligent Sustainable Systems [ICISS 2020]
IEEE Xplore Part Number: CFP20M19-ART; ISBN: 978-1-7281-7089-3

De-Authentication Attacks on Rogue UAVs

Kadripathi KN
Dept. of Aerospace Engineering
International institute for Aerospace Engineering and Management, Jain Deemed-to-be-university, Bengaluru, India.
kadripathi.knk@gmail.com

L Yethinder Ragav
Dept. of Aerospace Engineering
International institute for Aerospace Engineering and Management, Jain Deemed-to-be-university, Bengaluru, India.
yethinder@gmail.com

Shubha KN
Dept. of Aerospace Engineering
ACS College of Engineering, Bengaluru, India.

P Hareena Chowdary
Dept. of Computer Science Engineering
Sri Venkateswara University College of Engineering, Tirupati, India.

2020 3rd International Conference on Intelligent Sustainable Systems (ICISS) | 978-1-7281-7089-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICISS49785.2020.9316032

***Abstract* - In this new commercial era, Unmanned Aerial Vehicles (UAVs) popularly known as drones have become easily accessible, and their possible unlawful use poses new security threats. Therefore, limiting the illegal use of UAVs in some regions, such as airports, military camps, nuclear power plants, and international borders has become highly recommended. In remote control systems, most commercially available UAVs rely on spread spectrum techniques such as direct sequencing and frequency hopping. This minimizes the impact of interference from adjacent communications systems and increases resistance to jamming.**

In this research, an efficient mechanism is designed to attack and disconnect Wi-Fi controlled UAVs using Raspberry Pi 3 motherboard (System On Chip-SOC). The proposed technique in this prototype uses the de-authentication process to attack UAVs Wi-Fi module that connects the flight controller in the UAV to the ground control station. The experimental results show this method can effectively be used to cease and disconnect the UAVs operating within a 50 m radius around the proposed prototype without disturbing any other non-target electronic signals around.

Keywords— Unmanned aerial vehicles (UAV), Security threats, Wi-Fi controlled UAVs, Raspberry Pi 3, De-authentication, Ground control station.

I. INTRODUCTION

The world has recently witnessed a substantial increase in the number of UAVs used and exponential growth in its demand for multi-purpose applications. The prominent demand for these UAVs is due to their ability to respond to people's needs and user-friendly operation. The malicious use of UAV, however, has recently started to appear among criminals and cybercriminals. The probability and frequency of these attacks are both high and disastrous. The need for detective, defensive, and preventive counter-measures is therefore highly needed. Potential anti-social groups have enough resources to outfit themselves and make small modifications to enable the delivery of dangerous chemicals or explosives. The possible misuse against civilians or security forces of these means is eminent. Non-military UAVs have often been reported to cause hazards to aircraft, people, and property on the ground. Safety issues have been advanced due to airborne UAVs' potential to destroy an aircraft's engine easily. Many near-miss incidents and confirmed crashes have involved hobbyist UAV operators flying in violation of aviation safety regulations [1].

Various malicious and considerate uses of UAV have been in Figure 1.

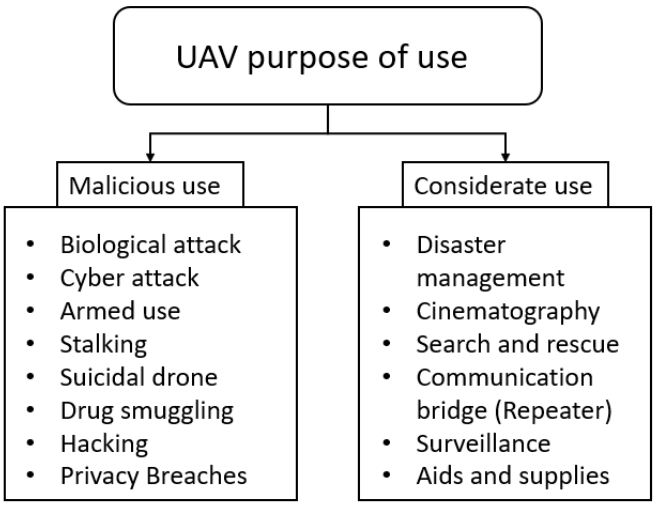

Fig. 1. Various malicious and considerate uses of UAV [1]

To regulate the usage of UAVs in a restricted area, national and local aviation authorities have passed specific rules and regulations for UAV pilots. The pilot has to adhere to those instructions, failing which the operator has to face the judiciary's severe punishment. In certain accidents, which under Major catastrophic past incidents of rogue UAVs, the UAV pilot stays anonymous and instructs it to cause destruction. In such cases, disabling the rogue UAV operation and grounding it is significant. Certain electronic warfare techniques and signal jammers have been extensively used in

recent times to counter malicious UAV attacks. These devices generate high electromagnetic noise and direct them towards the target and they effectively combat malignant UAV attacks to damage all other electronic devices on their path. Electronic warfare equipment and jammers need a skilled operator who is readily available all around the clock to combat and attack. It is highly challenging to provide uninterrupted service in remote areas and inaccessible geographic regions [2][3].

II. MAJOR CATASTROPHIC PAST INCIDENTS OF ROGUE UAVS

a) In December 2018, London's Gatwick Airport was paralyzed by drones. Because of drones' sightings over the airfield, which mysteriously appeared as the airport attempted to reopen, around one thousand planes were grounded for over a day. A total of one hundred forty thousand passengers were affected by the incident. Moreover, the suspects were never discovered, leading to rumors that they did not even exist [4]. This event is proof that such dangerous acts can be executed remotely without leaving any clue. In the hands of technically sound terrorists, drones can be an anonymous weapon of mass destruction.

b) In the year 2017, a light-engine aircraft originated from the Canadian province of Quebec had crashed into a UAV at an altitude of 450 meters (about 1,500 feet above sea level), about five times as high as UAVs are permitted. Fortunately, that plane with eight passengers landed safely, suffering minor damage to the engine. The effects could have been even more severe. A few years later, researchers from the University of Dayton showed that even a light drone could cause serious damage to an aircraft [4].

c) A drone carrying methamphetamine (a narcotic drug) crashed in Mexico near the US border in January 2015. The drone was carrying more than six pounds of crystal meth when it crashed into a supermarket parking lot in the Mexican town of Tijuana. According to the United States Drug Enforcement Administration (DEA), drones are becoming a common means of transporting drugs across the border [4].

d) In July 2014, a drone collided narrowly with an Airbus A320 as it departed from London's Heathrow Airport. The aircraft was approximately 700 feet away when the incident occurred, and BBC confirmed that the Civil Aviation Authority (CAA) classified the incident as a "significant risk of collision," the highest rating [4].

e) A drone crash-landed on the White House lawn in January 2015. The White House does have its own unique flight restrictions, but the drone was not easy to detect immediately after the attack, the White House was locked up, and security questions were raised [4].

III. RELATED WORK

A. *Drone radio signal jammers*

Radio signal jamming is a procedure often used to counter-attack malicious or suspicious signals in the radio frequency spectrum. Jammers operate by sending radio signals, usually a noise that interrupts communication between the signal receiver and transmitter by decreasing the signal-to-noise ratio. This idea can be used in wireless data networks to interrupt information flow and mislead the suspect. It is a standard method of censorship in totalitarian countries to prohibit unwanted or spying radio signals from crossing the border [5].

Jammer signal transmitter module is tuned to the same frequency as the opponents receiving equipment with the same modulation phase so that the target receiver cannot differentiate between the genuine signal and the jammer signal; however, this method is inefficient to differentiate between the friendly receiver and a malicious receiver because all commercially available receivers operate in the same frequency with a similar type of modulation phase. Hence, it affects and misleads all the receivers in the vicinity [6].

B. *Electronic Warfare on UAVs*

Electronic warfare technique involves producing focused high energy electromagnetic spectrum and directing towards the suspect UAV; this uses radio, infrared, or radar to sense, protect, and communicate with an opponent.

This procedure involves the following techniques:

1. Sensing the environment: It involves sensing and scanning all the signals in its surrounding. This is capable of identifying a friendly receiver and malicious receiver and their associated electromagnetic spectrum.
2. Analyzing the environment: After sensing, it is capable of analyzing the frequency, waveform, phase, and energy associated with the suspect signal.
3. Response to the environment: Once it detects a malicious signal or a receiver, it directs a high energy density electromagnetic spectrum towards the target and causes lethal damage to the receiver by electromagnetic interference.

However, this involves bulky and costly equipment operated by a skilled workforce on a ground station. It is highly challenging to provide uninterrupted service in remote areas and inaccessible geographic regions. Moreover, killing UAVs using this method will destroy evidence that might help trackback the malicious pilot [7][8][9][10].

C. *Physical attack against UAVs*

Long-range rifles and missiles are being effectively used to combat large UAVs. Aerial creatures like eagles and vultures are being trained by the Dutch police to attack small UAVs abiding by local Aviation law. However, if the bird is harmed in this process, it violates animal protection law, which is a risky procedure.

IV. PROPOSED METHOD

This prototyping method aims to address an efficient method to detect, attack, and disconnect Wi-Fi controlled rogue UAVs. Unlike the other conventional combat methods discussed under the section related work, this process proceeds

uniquely and does not disturb any other device except the malicious target. The designed prototype is a ground-based handy, user-friendly, and cost-effective model. This design can also be integrated with airborne systems to increase its operating range. Raspberry pi 3 computer board with a 5-volt power supply is required to build a prototype that scans and sends an infinite de-authentication request to the target UAV to disconnect it from the pilot control.

A. Understanding the De-authentication process

A Wi-Fi de-authentication attack is a kind of attack that targets router-device communication and deactivates the Wi-Fi connection on the system. A schematic diagram of the Wi-Fi de-authentication attack is shown in figure 2.

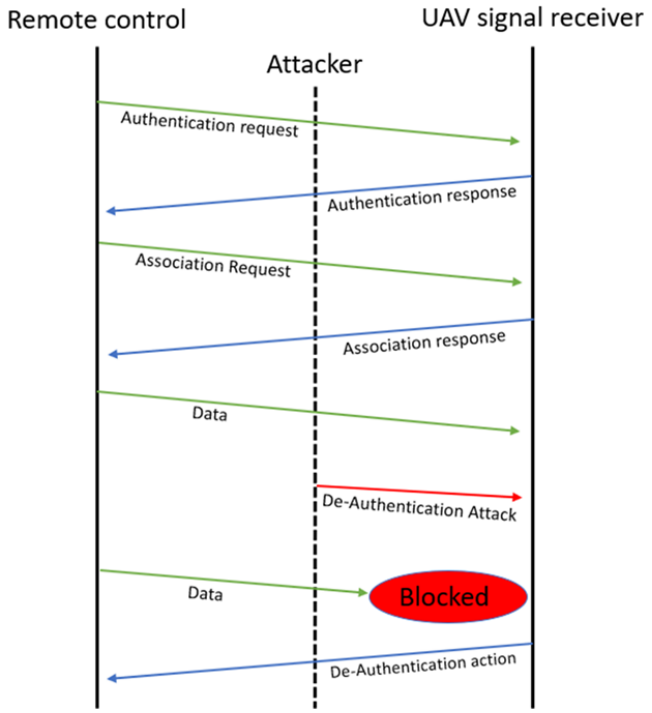

Fig. 2. Schematic diagram of Wi-Fi de-authentication attack

Figure 2 depicts the operation overflow between the client and the access point. The remote controller as a client requests accesses to the UAV signal receiver to pair through authentication requests providing all the necessary credentials. In response to the request, the access point provides a channel to read and rewrite the data authentication is valid is not. If the attacker finds any suspicious network while scanning, the attacker steals the remote controller's identity through the handshake technique which affects the client. The mimicking attacker sends a connection request to the UAV signal receiver, and the receiver senses two clients with the same identity requesting to connect. Meanwhile, the attacker sends reauthentication requests to the access point and plea to examine the requested clients' authenticity. However, once a reauthentication frame enters the communication process, it causes havoc in the communication workflow on both sides, and communication terminates data exchange. The data acquisition is blocked by the access point until the client proves its authenticity.

De-authentication is a standard IEEE 802.11 protocol used in real-world implementations to notify and disconnect the router communication with the device. In technical terms, it is called the "licensed technique to notify a rogue station that they have been isolated from the network." This means that a network computer is not meant to be on the network. When this command reaches the router, it immediately disconnects a specific BSSID (or ESSID) address device and allows it to reconnect. Meanwhile, the attacker sends an infinite de-authentication request pack to the router; hence it is almost impossible for a user or pilot to reconnect to the network.

V. IMPLEMENTATION

To implement this technique, which is capable of targeting the interacting remote-control systems, and a de-authentication request approach is used via the IEEE 802.11 protocol. The prototype consists of a monitored Raspberry Pi motherboard loaded with Raspbian OS and Aircrack-ng software tool, capable of transmitting and receiving signals of bandwidth 2.4GHz to 5.0GHz and it is powered by a 5-volt 1-ampere power source.

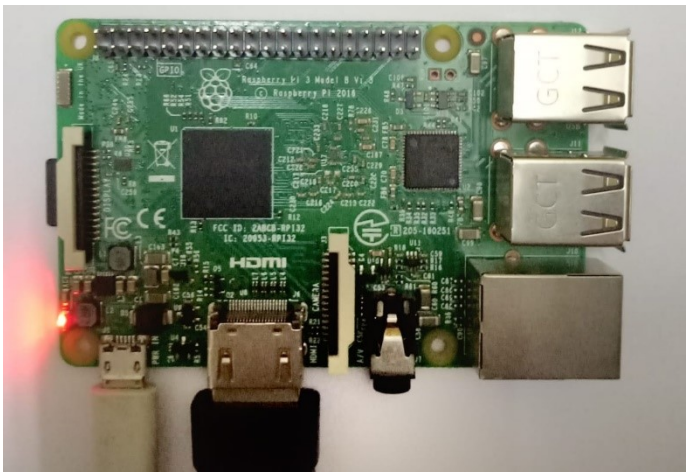

Fig. 3. Raspberry Pi loaded with Raspbian OS and Aircrack-ng software tool.

Figure 3 shows the hardware of the proposed prototype. It consists of a Raspberry Pi 3 Model B+ loaded with Raspbian OS and Aircrack-ng software tool. This computer board is integrated with Cortex-A53 (ARMv8) 64-bit processer with 1 GB RAM, 2.4GHz and 5GHz IEEE 802.11.b/g/n/ac wireless LAN.

Initially, the prototype is turned on and the process is initiated and the next process is to scan the prototype for all available networks. After a suspected signal is found, the prototype starts the handshake technique and collects the necessary information to mimic the rogue UAV's original controller/transmitter signal. Subsequently, if the mimicking is completed then the prototype sends a de-authentication request to the UAV's receiver, which disconnects the UAV from its original transmitter/controller.

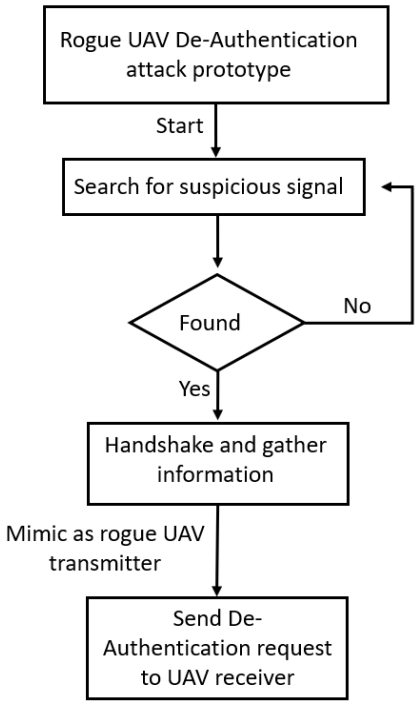

Fig. 4. Flowchart of rogue UAV De-Authentication attack prototype working.

Steps required to realize the de-authentication request and disconnect the rogue UAV has been discussed in the following section.

A. Launching the tool and searching for the malicious network:

Once the shell opens for a secured command prompt in Raspbian OS is processed to launch the Aircrack-ng tool and inject the following command in a secure shell to start a de-authentication attack.

Command "sudo airmon-ng start wlan1"

This instructs Aircrack-ng to access the Wi-Fi through wlan1 protocol and turns on raspberry pi Wi-Fi adopter. The interface starts scanning all available networks around the adapter. The monitor screenshot of the same has been shown in figure 5.

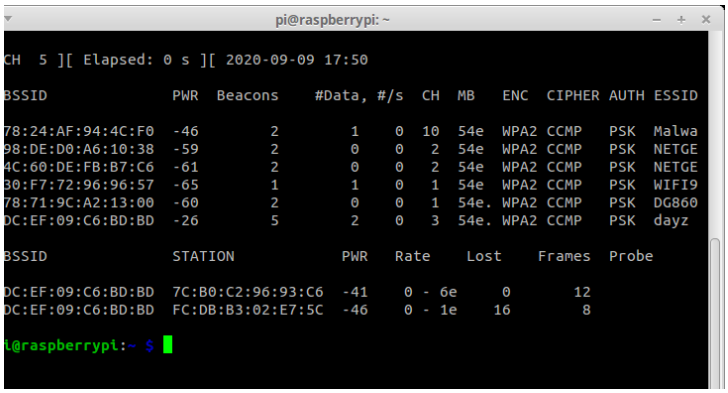

Fig. 5. Scanning for available networks.

A list of all available networks with unique identification id (BSSID AND ESSID) will be listed on the screen. For demonstration purposes, ESSID with "dayz", BSSID "DC:EF:09:C6:BD:BD" is considered as the target malicious UAV operator network.

B. Capturing target data and mimicking:

After identifying the target, the network's raw data has to be gathered using the 4-way handshake technique. This procedure reveals all the necessary data needed to mimic that target network. The monitor screenshot of the same has been shown in figure 6.

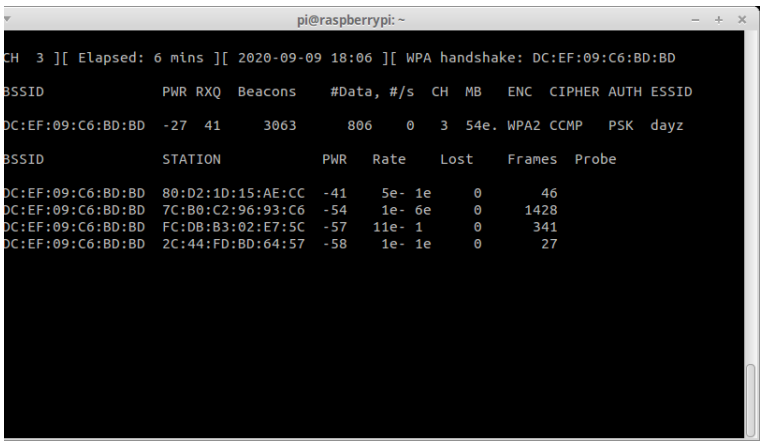

Fig. 6. 4-way WPA handshake to gather station data.

After capturing the suspicious target identity data like BSSID and ESSID, rename the prototype ID using the following commands

"sudo airodump-ng --bssid XX:XX:XX:XX:XX -c X --write dayz wlan1mon"

Where XX:XX:XX:XX:XX is the BSSID of suspicious target. This command replaces attackers BSSID with suspicious targets.

C. Sending De-authentication request.

The UAV pilot's transmitter aids to identify the data using the Raspberry pi Wi-Fi module and any changes its address values will mimic the original malicious pilot transmitter and starts sending a de-authentication request to the UAV's Wi-Fi

receiver module. Technically this request says to the receiver that "some unauthorized third party has connected with you using my credentials." and this request from the mimicked module confuses the receiver and disconnects the communication. The notification of unauthenticity is sent to the rogue UAV pilot transmitter and instructs to send a genuine reconnection request. Meanwhile, the mimicked transmitter operated by the proposed prototype keeps sending de-authentication requests infinite times. Hence it is not possible for the rogue UAV pilot to re-establish the connection. The monitor screenshot of the same has been shown in figure 7.

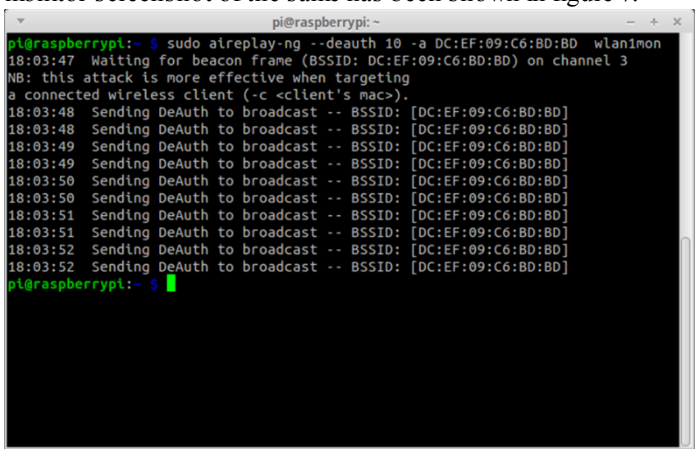

Fig. 7. Mimicked transmitter sending De-authentication request to target UAV receiver.

VI. LIMITATIONS OF THE PROPOSED PROTOTYPE

1. The proposed technique can only be used if the rogue UAVs BSSID and ESSID are properly differentiated from the friendly UAVs ID. Hence, it is required to enlist all the available friendly UAVs ID and frequent updating.
2. The range of operation in the demonstrated design is up to a 50-meter radius, which is considerably low. However, the range can be significantly increased by using signal boosters or repeaters.
3. The proposed technique needs skilled labour for effective UAV combat; however, it can be automated using machine learning techniques.
4. The proposed technique can only be used if the rogue UAVs and telemetries operating in a Wi-Fi protocol.

VII. RESULTS

The experimental results show that this method can effectively cease and disconnect the UAVs operating within a 50m radius around the proposed prototype, without disturbing any other non-target electronic signals. In the first step, a de-authentication attack is injected in a secure shell command prompt and starts scanning all the available networks in the vicinity, depicted in figure 5. After identifying a suspicious network, a handshake gathers its identity information and uses this data to spoof and request reauthentication. The proposed de-authentication Wi-Fi attack method successfully disconnected the communication between malicious UAV and its pilot control. The attacker stops sending except a de-authentication request to the UAV, it is not possible for the pilot to re-establish a connection with the UAV. Consequently, UAVs lacking return-to-home feature will experience a free fall while the others start moving towards launch destination. This might help to gather primary evidence, and further investigation could reveal the rogue UAV attacker.

VIII. CONCLUSION

The proposed system is an efficient and cost-effective procedure to detect and disconnect the malicious rogue UAV that could harm life and property. Unlike signal jammers and electronic warfare techniques, this process will not damage or attack any other intervening friendly devices that operate in the same frequency. This aims to attack only targeted suspicious communication with Wi-Fi bandwidth, which is the prototype's unique feature. This method can be effectively used to destroy UAV video footage transferring or streaming through Wi-Fi telemetry. In this demonstration, the prototype's range is a 50 meter radius, but this can be extended by using signal boosters or repeaters.

ACKNOWLEDGMENT

The authors like to express their special gratitude to the instructors Dr. Moses Osmond Gemson R and Vinuth Raj T N, who inspired to do this wonderful project. Secondly, we would also like to thank our parents and friends who helped us in finalizing this project within the limited time frame.

REFERENCES

[1] Security analysis of drones systems: Attacks, limitations, and recommendations; https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/

[2] T. Karhima, A. Silvennoinen, M. Hall, and S.-G. Haggman, "IEEE 802.11 b/g WLAN tolerance to jamming," in Military Communications Conference, 2004. MILCOM 2004. 2004 IEEE, vol. 3. IEEE, 2004, pp. 1364–1370.

[3] I. Harjula, J. Pinola, and J. Prokkola, "Performance of IEEE 802.11 based WLAN devices under various jamming signals," in Military Communications Conference, 2011-MILCOM 2011. IEEE, 2011, pp. 2129–2135.

[4] Air alert: 8 dangerous drone incidents; https://www.kaspersky.com/blog/drone-incidents/29000/

[5] H. Wang, J. Guo, and Z. Wang, "Evaluation of security for DSSS under repeater jamming," in Communications, 2007. ICC'07. IEEE International Conference on. IEEE, 2007, pp. 5525–5530.

[6] J. Farlik, M. Kratky, and J. Casar, "Detectability and jamming of small UAVs by commercially available low-cost means," in Communications (COMM), 2016 International Conference on. IEEE, 2016, pp. 327–330.

[7] A. Merwaday and I. Guvenc, "UAV assisted heterogeneous networks for public safety communications," in Wireless Communications and Networking Conference Workshops (WCNCW), 2015 IEEE. IEEE, 2015, pp. 329–334.

[8] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A communications jamming taxonomy," IEEE Security & Privacy, vol. 14, no. 1, pp. 47–54, 2016.

[9] M. Kratky; L. Gacho, "Kinetic Methods Of Defence Against Unmanned Aerial Vehicles" in Zeszyty Naukowe, 2016. ISSN 1641-9723.

[10] M. Kratky; L. Fuxa, "Mini UAVs Detection by Radar" In Proceedings of International Conference on Military Technologies (ICMT). Brno, 2015, p. 617-621. ISBN 978-80-7231-976-3.