ANALYSIS OF THE VULNERABILITIES OF UNMANNED AERIAL VEHICLES TO CYBER ATTACKS

Grigore Eduard JELER
Military Technical Academy "Ferdinand I", Bucharest, Romania (eduard_jeler@yahoo.com)
ORCID: 0000-0002-8829-0027

Gelu ALEXANDRESCU
"Carol I" National Defense University, Bucharest, Romania

DOI: 10.19062/1842-9238.2020.18.2.2

Abstract: *Recently, the use of unmanned aerial vehicles (UAVs), also known as drones, has increased significantly and the technical advencements in the field have led to new possibilities in several fields, both military and civilian. Air drones help reduce human life risks and costs, and can be used to carry out dangerous and costly missions by replacing human operators. Unmanned aircraft have a wide range of use, from entertainment for enthusiasts to military operations. Large investments, especially in the field of robotics, electronic miniaturization, sensors, network communication, information technology and artificial intelligence help to accelerate and diversify areas of use. The operation of unmanned systems and the applications that use these systems depend, to a large extent, on the cyber systems that are used for data collection, storage, processing and communication. However, these systems also have certain vulnerabilities, which has led various (state or non-state) hybrid actors to develop methods of conducting cyber attacks on drones.*

Keywords: *cybernetic attack, UAV, Spoofing GPS*

1. INTRODUCTION

The modern world is changing rapidly with the development of revolutionary new technologies used in various fields. But along with significant benefits, there are many ways to use technology for malicious purposes. Unmanned Aerial Vehicles (UAVs) are not exempt from this either. They have been used by various military organizations for a decade, but in recent years, UAVs have demonstrated significant potential for use in commercial, industrial, security and entertainment applications. Drone testing is performed in applications such as pizza delivery, medical supplies delivery and emergency medical care.

The modern world is changing rapidly with the development of revolutionary new technologies used in various fields. But along with significant benefits, there are many ways to use technology for malicious purposes. Unmanned Aerial Vehicles (UAVs) are not exempt from this either. They have been used by various military organizations for a decade, but in recent years, UAVs have demonstrated significant potential for use in commercial, industrial, security and entertainment applications. Drone testing is performed in applications such as pizza delivery, medical supplies delivery and emergency medical care.

However, each technology can be used improperly, as in the case of drones. The rapid evolution of relatively cheap and easy to operate unmanned aircrafts is a new type of challenge for the public defence.

Whether the operator is a careless enthusiast or a malefactor, an undetected drone can pose a significant threat to safety and security. The continuous need to develop drones will lead to a new possibility of use, with extensions that can be mounted as shown in Fig. 1.

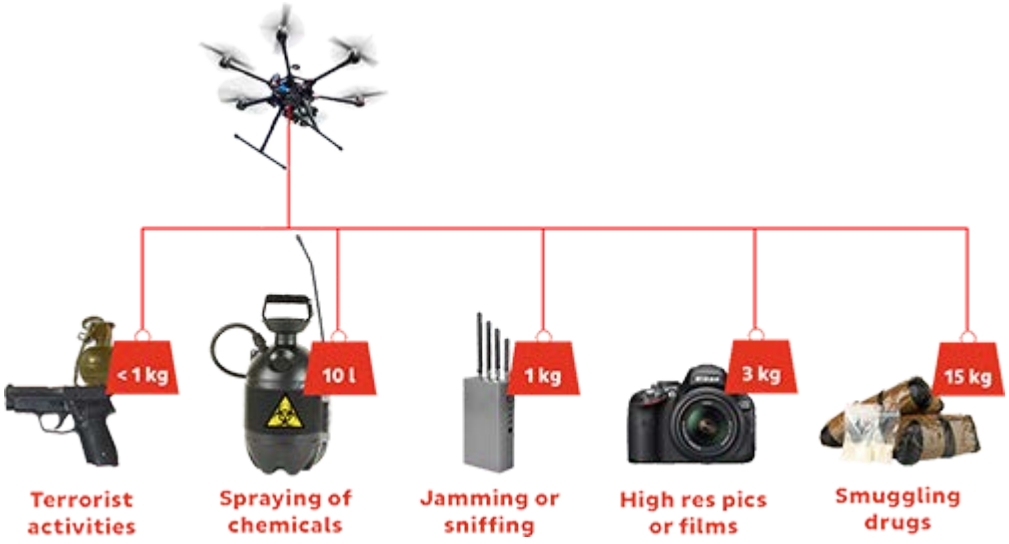

FIG.1 Useful loads that can be used for improper purposes [1]

Incidents with commercially purchased drones are reported almost daily in the international press. There have been situations in which drones have been observed in the vicinity of airports or even on the airways of aircrafts, at political events, spying over car test tracks, and even being used to smuggle drugs into prisons or transport them across the border, etc. [2]. The most spectacular use of autonomous systems in hybrid threats is the Houthi rebels' drone attack on Saudi oil facilities. Saudi Arabia has the most modern automated AA defense system under the name of Peace Sheild (17 American fixed radars AN / FPS-117, 6 American mobile radars AN / TPS-43, 5 E-3 A aircraft and 2 SAAB-2000 (AWACS), 10 medium-range missile batteries MIM-23 HAWK, 5 long-range missile batteries MIM-114 Patriot and dozens of Crotale short-range missile batteries and AA artillery. The attack had devastating effects on the economy of Saudi Arabia and the oil-rich sultanates in the Gulf area [3].

An attacker can be classified:

1. In terms of his location in the system:

- external location - An external attacker is more common. Because it is external to the system, it does not require authentication or authorization and can easily perform low-cost attacks.

- internal location - The internal attacker is a trusted person of the system (pilot, ATC controller, airport technician, etc.).

2. In terms of the physical position of the attacker:

- on the ground - This type of attacker is the most common. Against this type of attacker there are possibilities to counteract the attacks using different detection and attenuation techniques;

- aerial - This type of attacker, capitalizing on technological advances, may include drones, UAVs, autonomous activation of luggage devices or passengers with miniature devices capable of carrying out attacks.

3. According to the attacker's objectives:

- pranks - These types of attackers are the least dangerous but nevertheless, the impact on security can be considerably greater than expected. For example, attackers may be unprepared pilots, technology testers, and so on.

- abusive utilization - this type of attackers may have different motivations, including money, fame, messaging, paparazzi and, finally, pilots who intentionally abuse their access to ADS-B technology;

- criminal intentions - such attackers can have two main motivations - money and / or terrorism.

- military / intelligence - these attackers may be motivated at the state level, such as espionage, sabotage, etc. and may include military or intelligence-related agencies [4].

2.THE GENERAL STRUCTURE OF THE UAV SYSTEM AND POTENTIAL CYBER ATTACKS TARGETTING THE UAV

An overly simplistic perspective of an UAV is that it is an aircraft from which the human crew has been replaced by a computer system and a radio link. The aircraft is only one part, although an important part, of a total system. The entire system functions as a complete and includes, as shown in figure no. 2, the following components:

- a) a ground control station (CGS) that shelters the system operators, the interfaces between the operators and the rest of the system;

- b) the aircraft carrying the payload (video camera, various sensors, radar, etc.);

- c) the communication system between the CGS that transmits control inputs to the aircraft and returns the payload data and other data from the aircraft to the CGS (this is usually obtained by radio transmission);

- d) support equipment which may include maintenance and transport items [5].

Due to the fact that the UAV system contains systems that work together, cyber attacks on the UAS target in parallel both the aircraft in flight (flight controller, payload operation), GCS, and communications. Figure 2 shows examples of cyber attacks against various components of UAV systems, having as an effect the defective conduct of the drone mission, taking control or crashing them.

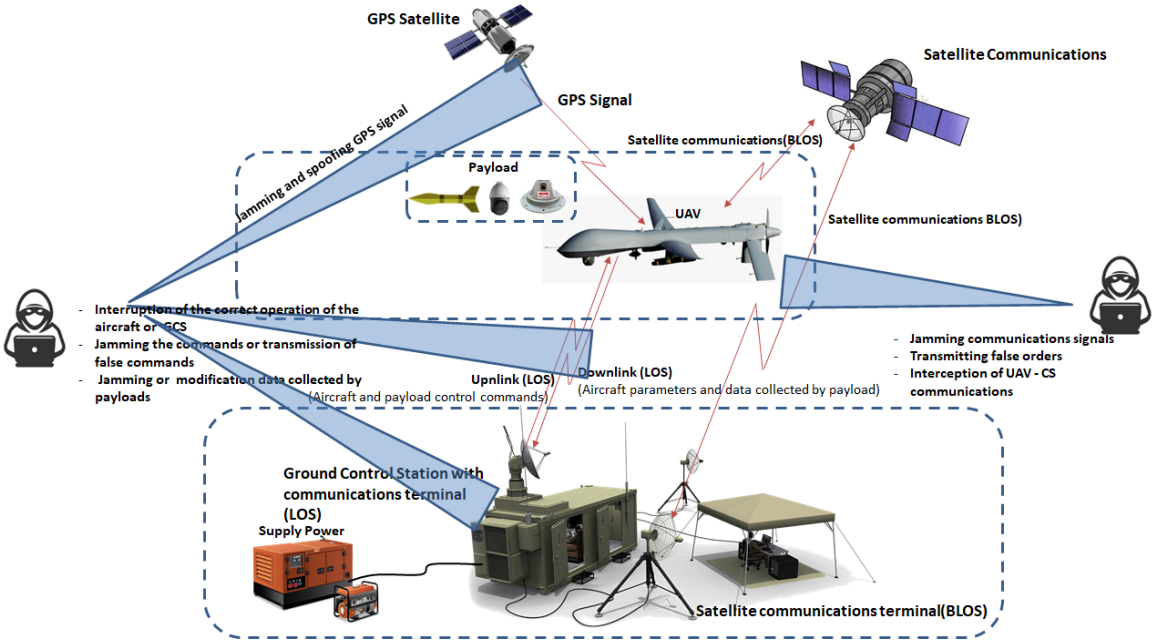

FIG. 1 Possible cybernetic attacks on UAV systems [6]

3. ATTACKS ON DATA LINKS

Communications within a UAV system are made through the following types of connections:

- GCS data link: data link between UAV and GCS (LOS)
- SatCoom data link: the connection between the GCS and the UAV via a communications satellite (BLOS)
- GPS data link: data link between UAS and GPS satellites

For a UAV to fulfill its mission successfully, it must communicate reliably with various entities in its network. These include CS, GPS navigation systems and satellite communications systems. However, these systems are vulnerable to various cyber-attacks such as packet data capture, message injection, message deleting, blocking and GPS spoofing. Attacks on communication systems can be classified as it follows:

1. Passive attacks (Packet data capture) are those in which the attacker tracks the data transmitted within the UAV system without interfering with them. This type of attack does not cause damage, has an increased risk (notice changes in the network - newly introduced equipment, changing configurations, etc.) and is difficult or even impossible to detect. These attacks can be performed by a variety of methods, such as surveillance of telephone or radio connections, exploitation of emitted electromagnetic radiation, routing of data through additional less protected nodes. Although they do not present direct risks, this type of cyber-attack is preparing to carry out active attacks on drones. The higher risks of passive attack, interception of network information (actual or identifying data) occur in wireless networks. Examples of passive attacks on UAV systems are presented below:

- packet sniffing (Passive attack by simple observation or "listening" to traffic). Thanks to the omnidirectional antennas used in Wi-Fi standards, Wi-Fi is susceptible to the packet sniffing attack.

In the UAV network, attackers can target communications between aircraft and other network nodes if the network is not or is poorly encrypted. Intercepting data via packet sniffing can be used as a first step to launch complicated attacks, such as GPS spoofing and attacks by injecting ADS-B messages [7]. The press reported that the Iraqi insurgents, using commercial software (Sky Grabber) that captures music and TV images, went live in video streams from American UAVs. Hacking was possible because the planes used unprotected communications to increase performance [8].

- Keylogger is a form of spyware developed to monitor user keyboard actions without user consent, so that hackers can access personal information, such as login details, passwords, etc. Keylogging software is usually installed on your computer through your own unintentional downloads, with someone physically installing it on your computer without your consent. In the case of UAVs, the virus records the keystrokes of pilots while controlling drones in military operations, being able to take over passwords, commands, etc.

Undetected passive attacks aimed at taking over the encryption keys represent a major risk for the network, because not knowing the compromised keys creates gaps in the information security system by encrypting the traffic [9].

2. Active attacks (because it changes the state of computer systems, data, or communication systems) are those attacks in which the intruder engages either in stealing messages, or in modifying or inserting fake messages, or by overloading the network with packets (flooding). This means that the attacker can delete, delay or modify messages, can insert fake messages, can change the order of the messages, either in a certain direction or in both directions of a logical channel. These attacks can be classified into:

- **DoS (Denial of Service):** In this attack, the attacker aims to prevent the communication systems in a network from transmitting and / or receiving data, sending numerous false signals to the targets, as shown in the figure no. 3. In any form, the DoS attack deprives beneficiaries of the right to the service or resource they are waiting for. In the case of UAS communications, a DoS attacker can send high-power wireless signals to block any of the data links. The attacker can also flood the communication channels by continuously sending known remote and control signals to consume bandwidth and interrupt the services provided by the network [7].

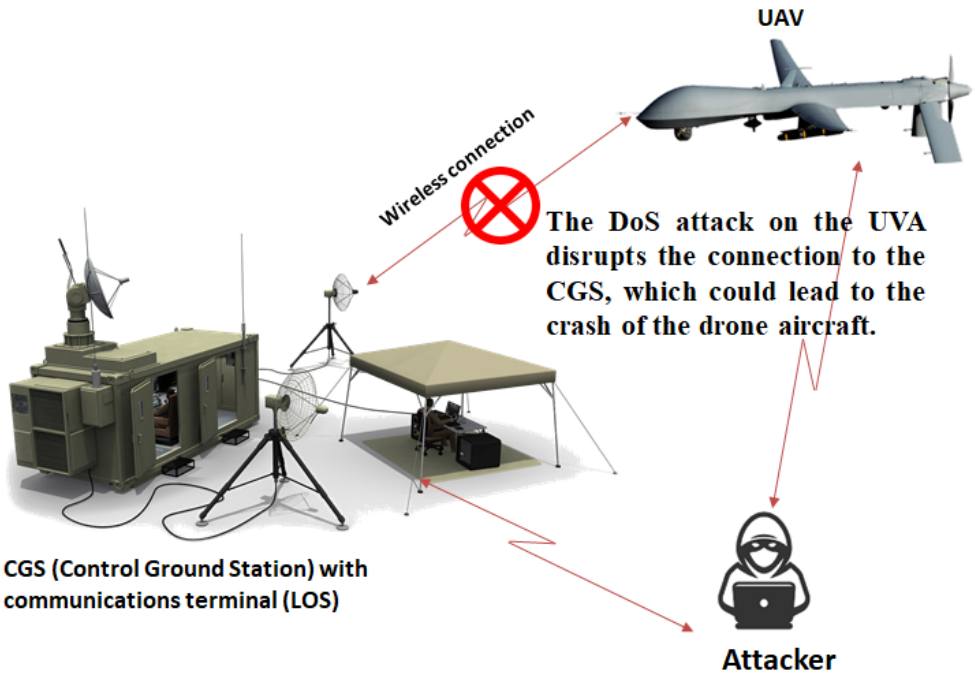

FIG. 3 DoS attack on a UAV [10]

The algorithm for performing a DoS attack is:

1. Compilation of vulnerable agents

- The network is scanned for potential vulnerabilities for the attacker to compile the list of agents to attack.
- There is the possibility of attacking systems by configuring automatic software to scan the network and take control of vulnerable agents.

2. Defusing

- Weak points in terms of security and vulnerability of systems are misused by the attacker.
- Software codes are used to automatically attack and disable the control system for the person responsible for the availability, security, maintenance, and support of the system.
- Actions taken by the attacker to protect the code deployed for DDoS startup.

3. Connection

- Protocols such as TCP or UDP used to connect to multiple agents and plan attacks according to a specific program.
- Attacks can be directed to either a single agent or to multiple agents [11]
- **MITM (Man-In-The-Middle)** – the attacker intercepts communications between the UAV and the control station and gains control of sensitive data, as shown in the figure no. 4. Users at the end are usually unaware of the attacker's manipulation.

A simple example of a MITM attack is the spoofing message disguised as a genuine email that misleads the user into a fake site. The user is then tricked into authenticating while the attacker listens to and collects credentials, such as passwords, usernames, and so on. The attacker falsifies the data and gains control over the communications network between the drone user and the remote-control device. The system details collected from the initial data capture help him to send the authentication commands to the drone as if it were the original user [12].

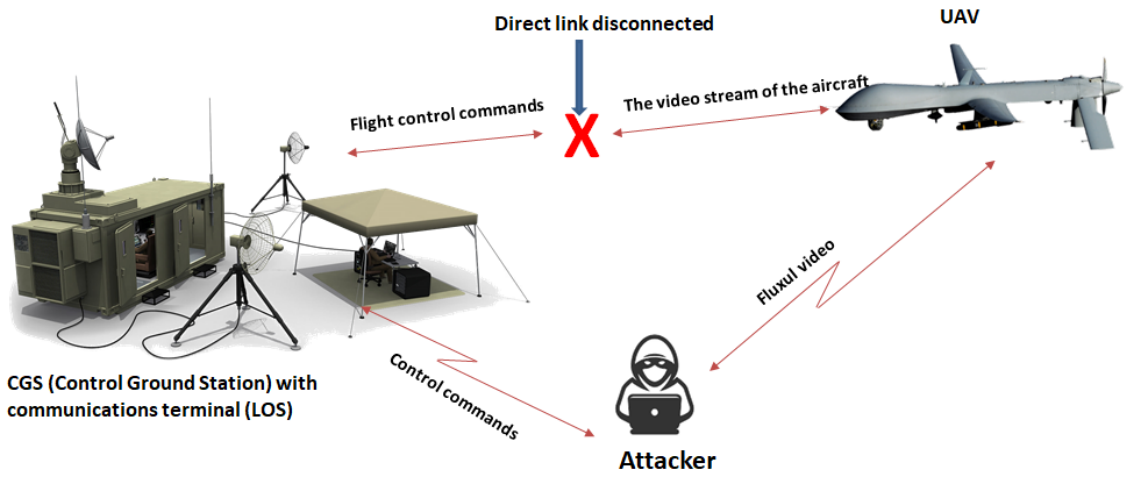

FIG. 4 MITM attack on a UAV [10]

If the wireless network is password protected, the authentication keys can be obtained by the methods that will be presented below. A password, sometimes called an access code, is usually an arbitrary string of characters, including letters, numbers, or other symbols, used to confirm a user's identity.

- a brute force attack: is a crypto-analytic attack, which can be used for any type of encrypted data. Brute force attacks are effective for breaking passwords with a shorter length. This method involves systematically checking all possible keys until the correct key is found. In the worst case, this method involves traversing the entire search space.

- dictionary - attacks: looks for open ports, which are similar to the "brute-force" type, but to break the password are used words from the dictionary, combinations between them and alphanumeric characters. The system will check if there are all possible permutations and combinations until the password is broken [13].

- aircracking: This exploit is used to decrypt wireless passwords, it is a free security application that can recover passwords from packets captured with other applications (CommView, Wireshark, etc.) [14].

8. ATTACKS ON THE AIRCRAFT AND GROUND CONTROL STATION

The operation of the flight controller depends exclusively on the information received from the ground control station via the data link and purchased by its environmental sensors. Due to the almost complete dependence of UAV operations on several inputs from the external environment, most attacks start with malicious external modifications of these inputs. In the following, we identify the attacks targeting the flight controller and GCS.

Trojan horse cyber-attack: It is a type of malicious code or software that looks legitimate but can take control of the computer from CGS or UAV and that actually allow unauthorized access to a computer, respectively copying files, and even controlling the commands of the penetrated computer. A Trojan is designed to damage, disrupt, steal or, in general, cause other harmful actions on data or network. A Trojan acts as a bona fide application or file that can trick you into loading and running malware on your device. Once installed, a Trojan can perform the action for which it was designed. Thus, cyber attackers are able to infect computers in the UAV system with a Trojan virus and force it to land or crash, its pilot unable to intervene, to engage the systems. electronic weapons of the enemy, to deactivate or deceive the electronic equipment of the aircraft [15].

Spoofing GPS:

GPS (Global Positioning System) refers to a group of satellites that provide signals from space that transmit positioning and synchronization data to ground receivers. Receivers then use this data to provide information to devices and vehicles, such as their position, timing, and speed. GPS satellites transmit both military (P-Code) and civilian signals [16]. The most common navigation method for a UAV is to use a system consisting of an inertial measurement unit (IMU) and a GPS receiver. A fundamental part of GPS is PRC (Pseudo Random Code), which is just a very complicated digital code or, in other words, a complicated sequence of “on” and “off” pulses. The signal is so complicated that it looks almost like a random electrical noise, hence the name “Pseudo-random.” GPS satellites transmit signals on two carrier frequencies: the L1 carrier has 1575.42 MHz and carries both the status message and a pseudo-random code for synchronization, the L2 carrier has 1227.60 MHz and is used for the much more accurate pseudo-random military code. There are two types of pseudo-random codes:

- C / A (Course Acquisition) code that modulates the L1 carrier. It repeats every 1023 bits and modulates at a rate of 1 MHz. Each satellite has a unique pseudo-random code. The C / A code is the basis for the civilian use of GPS.

- P code (Precise). It is repeated in a seven-day cycle and modulates both the L1 and L2 carriers at a rate of 10 MHz. This code is intended for military users and can be encrypted. When encrypted, it is called a "Y" code. Because the P code is more complicated than the C / A, it is more difficult for ground receptors to detect it. Therefore, many military receivers start by first purchasing the C / A code and then switching to the P code [17].

GPS signals can be falsified (spoofing - performed by using directed interference with digital coordinate transmission systems between GPS transmitters and receivers [18]. As previously presented if military GPS signals are encrypted, thus resistant to spoofing, civil GPS waveforms are unencrypted, unauthenticated and openly specified in documents available to the public [19]. The combination of the known signal structure and the predictability of the data bit makes the GPS receiver on the UAV an easy target for spoofing attacks, with devastating effects on the aircraft (capture, misleading and directing to collide with other targets). The signal coming from the satellite is weak. Therefore, if an attacker uses a local transmitter on the same frequency, this signal would be stronger than the original satellite signal. The driver receives authentic signals from the visible GPS satellite, decodes them, falsifies the code phase, carrier phase and Doppler frequency and transmits them to the UAV as legitimate signals. false positions for the target UAV. In this particular case, the UAV would then be hijacked and put on hold for the attacker's next command [20]. Figure no. 5 shows a GPS spoofing attack targeting a GPS-guided UAV aircraft.

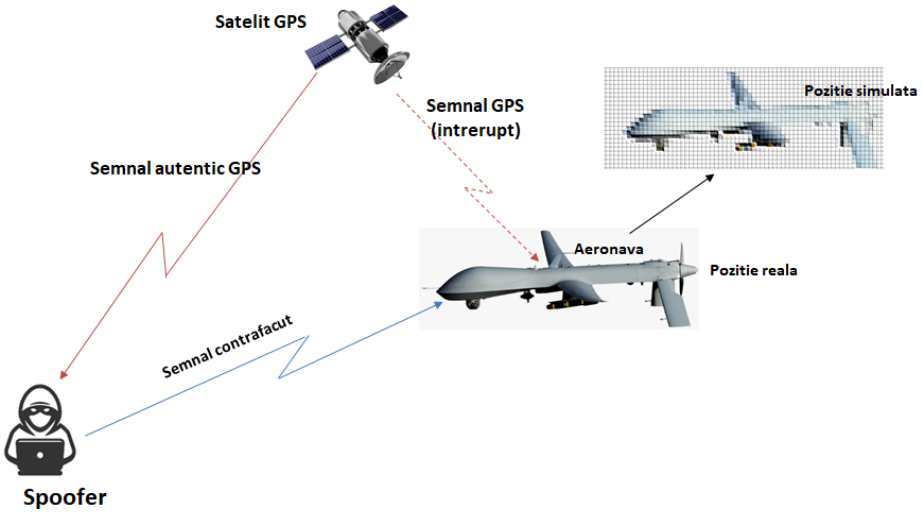

FIG. 5 Spoofing GPS attack on a UAV [21]

Attack on the ADS-B system (Automatic Dependent Surveillance Broadcast): It's a surveillance technology in which an aircraft determines its navigation position through satellite navigation and broadcasts it periodically, allowing for its tracking. The information can be received by the Air Traffic Control Stations, as a replacement to the secondary surveillance RADAR, since interrogation from the ground is not required. It can also be received by other aircraft in order to provide a situation report which is used to prevent collisions. ADS-B is automated, hence it doesn't require an external stimulus; it is dependent, because it relies on the on-board systems to provide surveillance information to other aircraft and control posts. Data is broadcasted, the original source doesn't know who receives the data and there is no interrogation or bidirectional contact [22]. The ADS-B can receive data manipulation attacks, capturing and modification of the ADS-B messages, the real ones can be deleted, false ones can be injected and certain entities' communication channels can be blocked [7].

Jamming of the GCS command and control signals: A foe which tries to take control over a drone will first try to deactivate the reception of GCS control-command signals to the UAV. Loss of said signals forces the aircraft to perform an uncontrolled flight. But UAVs are usually designed to be fitted with a lost connection protocol, which, once the communication from the ground is lost for a certain period of time, the drone could follow a procedure by itself, which can, for example, command the UAV to return to its base, relying on GPS navigation. But in general, if the drone is attacked, it is susceptible that the attacker will also block GPS signals as well, which forces the UAV to fly in an uncontrolled manner [6].

9. CONCLUSIONS

- Unmanned Aerial Vehicles (UAV) are not only military and scientific solutions. The extraordinary growth of drone usage has led to a new era of aviation in the civilian domain, but also in the military, offering several benefits, such as economic, commercial, industrial, mainly because of their autonomy, flexibility and ease of use, with low costs and low energy consumption. However, their usage has led to the rise of multiple security, safety and confidentiality issues, which manifested through different cybernetic attack, threats and challenges.

- Thanks to the omnidirectional antennas used in Wi-Fi protocols, they are susceptible to passive attacks such as sniffing packet or Keylogger. Passive attacks have the following common traits: they don't cause damage (don't delete /modify data), break the confidentiality rules by stealing network information, they're aided by the routing of packages in less protected, high risk network nodes, they observe network changes(new equipment, configuration changes, etc.), they're hard or even impossible to detect. Undetected passive attacks are a major threat to the network, ending in the reveal of the encryption keys and leaving the network vulnerable to active attacks. Precautions can be taken, such as redirecting and encryption, but the risk of interception is still high, since knowing the direction the signals come from is not required to intercept the signal.

- Most drones rely on GPS navigation systems. Predictability and knowledge of the GPS signal properties create the opportunity for attacker to take control over the UAV and use it for personal gain. For this reason, GPS spoofing is one of the major threats to the UAV's.

-The ADS-B system is destined to large scale implementation in air traffic surveillance systems including on UAV's. One of the objectives of ADS-B is to increase the safety of air traffic. But this system is very easy to penetrate for an attacker, even with a less advanced technology. Attacks may vary from passive(listening) to active attacks (message blocking, detouring) endangering air traffic.

To conclude, despite their various benefits, UAV's are vulnerable to attacks because they are equipped with various on-board data collection sensors that can expose them. To be more precise, in the absence of human control, attacker have access to sensitive information and can provide false information to the UAV. The drone can also be captured and reprogrammed to carry on clandestine missions which can cause severe damage.

REFERENCES

[1] https://teamsales.eu/en/drone-threat/ - accessed on 22.09.2020;
[2]. A.H. Michel, *Counter-drone systems*,Center for the Study of the Drone at Bard College, 2018, pp. 1-3;
[3] https://www.ziaruldegarda.ro/dronele-houthi-au-deschis-cutia-pandorei-partea-1/ - accessed on 23.09.2020;
[4] A. Costin, A. Francillon, *Ghost in the Air (Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices*, Black Hat USA, pp. 1 -2, 2012*;*
[5] Reg Austin, *Unmanned Aircraft Systems - UAVs Design, Development and Deployment*, 2010 John Wiley & Sons Ltd, pp.1;
[6] Riham Altawyet. all, *Security, Privacy, and Safety Aspects of Civilian Drones: A Survey*, ACM Transactions on Cyber Physical Systems, Vol. 1, No. 2, Article 7, Publication date: December 2016, pp.7:8;
[7] Mohsen RiahiManesh, Naima Kaabouch, *Cyber Attacks on Unmanned Aerial System Networks: Detection, Countermeasure, and Future Research Directions*, Computers &Security (2019);
[8] http://news.bbc.co.uk/2/hi/middle_east/8419147.stm accessed on 30.09.2020;
[9] M. Apetrii, *Introducere în securitatea rețelelor*, Centru de formare și analiză în ingineria riscurilor (CeFAIR), pp.12-13;
[10] CharanGudla et all., Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles, Int'l Conf. Embedded Systems, Cyber-physical Systems, & Applications | ESCS'18 |, pp.111;
[11] Randall K. Nicholset all, *Unmanned Aircraft Systems in the Cyber Domain*, NPP eBooks. 27, 2019, pp.82-83;
[12] HamidrezaModares, et all.,*Security of unmanned aerial vehicle systems against cyber-physical attacks*, The Journal of Defense Modeling & Simulation, November 2015, pp.3;
[13] https://hackout.ro/ghidul-de-securitate-cibernetica/bruteforce/ - accessed on 02.10.2020;
[14] https://www.aircrack-ng.org/ - accesat la data de03.10.2020;
[15] https://www.theaustralian.com.au/national-affairs/opinion/war-by-remote-control/news-story/ - accessed on 04.10.2020;
[16] https://techterms.com/definition/gps - accessed on 05.10.2020;

[17] https://www.trimble.com/gps_tutorial/sub_pseudo.aspx - accessed on 07.10.2020;
[18] https://monitorulapararii.ro/pacalirea-sistemelor-gps-gps-spoofing-1-262 - accessed on 10.10.2020;
[19] National Research Council. 1997. The Global Positioning System for the Geosciences: Summary and Proceedings of a Workshop on Improving the GPS Reference Station Infrastructure for Earth, Oceanic, and Atmospheric Science Applications. Washington, DC: The National Academies Press. https://doi.org/10.17226/9254.;
[20] Omar M. Alhawi, Mustafa A. Mustafa, Lucas C. Cordeiro, *Finding Security Vulnerabilities in Unmanned Aerial Vehicles Using Software Verification*, Computer Science ArXiv, 2019, pp.9;
[21] A. J. Kerns, D. P. Shepard, J. A. Bhatti and T. E. Humphreys, *Unmanned aircraft capture and control via GPS spoofing*, *J. Field Robot.*, vol. 31, no. 4, , 2014, pp. 617-619;
[22] https://www.skybrary.aero/index.php/Automatic_Dependent_Surveillance_Broadcast_(ADS-B). - accessed on 10.10.2020.