Journal of Global Science ISSN: 2453-756X (online) http://www.jogsc.com

Anti-drone systems

Ing. et Ing. Stanislav Szabo, jr., PhD., MBA.
Technical University of Košice
Faculty of Aeronautics
Rampová 7, 041 21 Košice, Slovakia
stano.szabo@tuke.sk

Ing. Lucia Melníková, PhD.
Technical University of Košice
Faculty of Aeronautics
Rampová 7, 041 21 Košice, Slovakia
lucia.melnikova@tuke.sk

Abstract
The research was devoted to the description of drones, their use, and methods of detection and destruction of drones. The main goal of this research was to examine the systems of protection against drones that are currently available on the market. The research was mainly focused on methods of locating and disposing of drones (C-UAV), which can compromise security. Methods for locating and disposing of drones are constantly evolving and it is necessary to map their development along with the development of drones. The possibilities of drones have increased since their first launch on the market so that they can cause security breaches of important objects if handled improperly.

Key words
UAV, safety, security, drone

Information
This work was supported by the Visegrad Fund under Grant no. 52110652.

1. Introduction

As drones grew in popularity, the terms used to describe them flooded the news. Words and acronyms like UAVs and quadcopters can be seen every day on social media, often without explaining the difference between them. While drones, UAVs, and quadcopters have the same meaning, knowing how to distinguish them is easy [1-3].
A drone is a general term for all drones. They can be powered either by remote control or by computers pre-programmed and placed on board. Drones are a broad category of vehicles that do not only include the popular recreational quadcopters that are constantly seen on television, but also vehicles such as hobby RC cars and unmanned military helicopters. The word "drone" originally came from the US military during the development of the UAV. Drones are used by corporations, universities, militants, and civilians - as a category

they are not defined by their use. In the media, they have become a buzzword for military UAVs and recreational quadcopters, but there are many other drones with countless other purposes.
While "drone" refers to anything from remote-controlled cars to military weapons, UAVs - or unmanned aerial vehicles - refer specifically to flying drone contingents. UAVs come in many designs, including airplanes, helicopters, and quadcopters. UAVs can be used for a variety of applications as well as they can. However, the term UAV is commonly used in a military or governmental context to refer to aircraft used as weapons or for research and search. UAVs are part of the UAS - unmanned aerial system. The UAS includes not only the UAV, but the physical controller, human operator, and even any satellites or computers needed for advanced processes; it is the whole system needed to complete the operation of the UAV. Like the UAV, the UAS is an abbreviation used mainly by the military or governments, and people working in the robotics / UAV industry tend to prefer UAV abbreviations to the word "drone" [4].

2. Military and civilian use of drones

The idea of using unmanned aerial vehicles to attack is much older than it might seem. As early as 1849, the Austro-Hungarian army used hot air balloons loaded with explosives to attack Venice during the Italian War of Independence. Although the result was meager due to bad weather conditions, balloons were occasionally used in subsequent conflicts. During Operation Outward in 1942-1944, the British Army launched hydrogen balloons, which were equipped with tow wires or incendiary devices and were intended to damage high-voltage power lines or to start fires in Germany or occupied Europe. However, due to technological progress, military balloons ceased to be used shortly after World War II. To this day, however, Palestinians from the Gaza Strip, for example, are attacking Israel with the help of similar devices [5-7].
Of course, not only conventional armies showed interest in using drones for their operations. In the last decade, there has been a significant shift in technology and drones are becoming more powerful, more affordable, and cheaper. The development of drones was very rapid - the first license for the common use of drones began to be issued by the US Federal Aviation Administration (FAA) only in 2014. At that time, the cheapest drones cost about a thousand US dollars, better quality drones were significantly more expensive and poorly accessible to ordinary people [8-10].
In 2020, however, the situation on the drone market is diametrically different - drones are quite commonly available in electronics stores, while they are advertised, for example, as a suitable gift for children for Christmas. The price of the cheapest devices is in the tens of dollars, and for about $ 1,000 it is possible to buy a drone that can carry an object weighing over 5 kilograms, can shoot videos in Ultra HD resolution, are able to fly at speeds over 50 km / h and its range is approximately 10 kilometers. It is therefore clear that drones are currently available to a large part of the population [11].
However, the use of drones by ordinary people can also lead to unintentional security threats. Currently, two types of potential threats are most often mentioned - espionage and airport security breaches. Although drones are forbidden to get closer to people in most countries, there are a huge number of recorded cases around the world where drone pilots have not respected these rules, and people have felt threatened by the drone or felt spied on by someone else. These cases are also the focus of a growing segment of drone defense systems designed for ordinary people and businesses to protect their own land. However, it should be noted that the use of these systems by other entities than state security forces is illegal in many countries [12].

3. Methodology

The information given in the previous sections shows that there will be more and more drones in the sky, which logically also leads to the emergence of measures and systems to identify and possibly neutralize drones. These systems are currently being introduced into the armaments of some armies, special armed forces, or police forces, and this trend will certainly continue. In addition, these systems are often installed at the airport. C-UAV systems need to be developed specifically for drones, because earlier air defense systems, long used to protect airspace, were mostly designed regarding piloted aircraft. This means that they are optimized for detection, tracking, and shooting down large and fast-moving objects. The result is usually that they are unable to capture small, slow, and low-flying drones. Even large-scale air defense systems sometimes fail to destroy primitive drones. In July 2016, an ordinary Russian drone that flew into Israeli airspace from Syria was able to escape without damage after the attack of two Patriot missiles and the shooting of an Israeli fighter jet. The incident took place in a specially guarded area of the Golan Heights, where the Israeli armed forces have a large military force.

Threat Actor - Capability Level	Likely UAS type	Possible scenario use	Flight Method	Range
Low	Multi-copter	Disruption, surveillance	Line of Sight (LoS) with First Person View (FPV) assistance	400m
	Multi-copter + additional payload	Delivery of restricted item/ explosives	LoS with FPV assistance	400m
Medium	Multi-copter	Disruption, surveillance	FPV	1km
	Multi-copter + additional payload	Delivery or restricted item/ explosives	FPV	500m
	Fixed-wing	Disruption, surveillance	GPS with FPV assistance	5km – 30km
	Fixed-wing + additional payload	Delivery or restricted item/ explosives	GPS with FPV assistance	5km – 30km

Figure 1. Example of UAS as a threat [13]

Systems that try to prevent drone attacks face three basic challenges - detecting the flying object, identifying it (i.e., determining that it is an unmanned aircraft) and destroying it, or preventing its further flight.

4. Results and discussion

The first step, which is important to prevent the threat of a terrorist drone attack, is the ability to detect and identify the drone sufficiently soon to be able to respond effectively to its presence. The identification of conventional aircraft currently depends on an onboard transponder that transmits a coded signal that is received and decoded by air traffic control. A similar measure could theoretically be introduced for drones, but it would be costly and difficult to enforce, so it is not an acceptable option. Therefore, other methods are used to identify drones. Their basic overview is provided in the work of Counter-Drone Systems are shown below:

1. Radar detection - The system detects the presence of small, unmanned aircraft according to their radar signature, which is generated when the aircraft encounters high-frequency pulses transmitted by the detection element.
2. Radio Frequency Detection - The system searches for and identifies drones by scanning the frequencies at which most drones operate.
3. Detection using optics - Identifies and monitors drones based on their visual trace, i.e., using cameras.
4. Infrared Detection - Identifies and monitors drones based on their heat traces.
5. Sound Detection - Detects drones by recognizing unique sounds produced by their engines. Acoustic systems rely on a library of sounds produced by known drones then adapted to the sounds detected in the operating environment. Special microphones are used to capture sounds.

4.1 Detection systems advantages and disadvantages

1. Radar - The main disadvantage of conventional radar systems is the fact that they are not suitable for detecting small drones, especially when the drone is moving slowly or when flying at low altitudes or hovering on the spot. In addition, the dimensions of the drone and the way the drones move are very difficult for radars to differ from the movement of birds. Radars must also emit high-energy radiation for successful detection, which can be dangerous to health, which means that the use of radar in densely populated areas is inappropriate. Among the advantages could be the fact that if the radar is used in an environment where there are very few obstacles, it can detect drones over long distances. Unlike radio frequency detection, the radar is also able to identify the drone even if the drones do not communicate with the pilot and are completely autonomous in their motion. The advantage is the fact that the detection of drones by radar is possible in bad weather or light conditions.
2. Radiofrequency - The main disadvantage is the fact that with the help of radiofrequency it is not possible to intercept drones that do not communicate with the pilot, on the other hand, there are currently very few such drones. Extensive use of the 2.4, 5, and 5.8 GHz bands is also a problem in densely populated areas, which can make it more difficult to identify drones. Some drones use directional antennas, which makes them virtually undetectable from the wrong direction. The advantage of this method is the fact that the systems do not have to transmit any signal, the device must be equipped only with a passive high-frequency signal sensor. This makes the construction of these devices simpler. Another significant advantage is that the systems can also locate the pilot who controls the drones.
3. Optics - The main disadvantage of these systems is poor detection in case of bad weather. Other disadvantages include the difficulty of determining the speed and distance of the drone when moving towards the camera. Good lens maintenance on the camera is also essential to keep it clean and functional. The whole system is also performance-intensive, as it must be very fast to be able to have a larger range. The advantage is that it is possible to use already developed and deployed cameras, which can also have a long-range thanks to high-quality optical zoom.
4. Infrared radiation - The main advantage of these systems are low acquisition costs, small size, and very low maintenance. Another advantage is that the cameras provide the same quality performance regardless of the weather, such as temperature or precipitation. On the other hand, drone detection depends very much on how much heat the drone produces, as many drone models are made of plastic and equipped with electric motors, in which case the device is more likely to detect a bird than

a drone. Likewise, the resolution of a thermal camera is usually relatively limited, so small drones at greater distances may not always be detected.

5. Sound - Sound detection systems probably have the most disadvantages of all the systems described. Their disadvantages are, for example, the high cost of many expensive microphones, short-range or the fact that they are very affected by weather and especially wind. The slowness of the whole system is also a big drawback, as the speed of sound is low, and the drone can fly a relatively long distance before the sound reaches the remote sensor. Another negative is the fact that most drones are already very quiet, and their development is moving towards less and less noisy models, and conversely, some (mostly urban) environments are very noisy, which continues to make detection difficult. On the contrary, the advantage is rather small. Sound detection can also detect drones that do not communicate with the pilot, as well as drones that are not at the exemplary angle of the device because sound can bypass some obstacles.

4.2 Methods of destruction

If drones can still be detected and identified, the next step is to prevent their next flight. First, I will present methods that prevent the drone from moving without destroying it. Their main advantage is the fact that an undamaged drone can provide important information about the person who controlled it and the intention that the person had with it.

1. High-frequency interference - The system interrupts the high-frequency connection between the drone and its operator by generating a large amount of high-frequency interference. Once the high-frequency connection is lost, the drone usually either descends to the ground or initiates a return maneuver to the place from which it was sent.
2. Global Positioning Satellite System (GNSS) Interruption - Disconnects a drone satellite connection used for navigation (most commonly GPS). Drones that lose their satellite connection usually float on the spot, land, or return to where they were sent.
3. Spoofing – This allows to take control of the target drone or redirect it by creating a false communication or navigation connection. This category may also include cyberattacks, protocol manipulation, high-frequency connection, or global positioning systems.
4. Drone Glare - Uses a high-intensity light beam or laser to dazzle and "blind" the camera on the drone.

Figure 2. Anti-drone jammer [14]

Another category is methods that intentionally destroy the drones, or because of their use, the drone falls to the ground, which can damage it.

1. Laser - Destroys vital segments of the drone with directed energy, causing it to fall to the ground.
2. High Power Microwave Radiation - Directing pulses of high-intensity microwave energy directed at the drone deactivates its electronic systems.
3. Nets - The system fires a net that is designed to entangle the targeted drone and/or its rotors.
4. Projectiles - Ordinary or custom-designed ammunition is used to destroy drones.
5. Another drone - A drone designed and sent to destroy an enemy drone.

5. Conclusion

The research was devoted to the description of drones, also called UAV / UAS. Drones are unmanned vehicles that have found their use in both the military and civilian industries. Not only for air transport, but they are also a growing threat. With the capabilities of drones, devices for their disposal are also emerging on the market. Systems that try to prevent drone attacks face three basic challenges - detecting the flying object, identifying it (i.e., determining that it is an unmanned aircraft) and destroying it, or preventing its further flight. Research has been devoted to various methods of detecting and disposing of drones. Research has shown that there are several ways to detect and destroy drones on the market. The company must choose the method of ensuring protection according to its material and financial capabilities.

References

1. J. Drozdowicz et al., 35 GHz FMCW drone detection system, 2016 17th International Radar Symposium (IRS), Krakow, 2016, pp. 1-4, DOI: 10.1109/IRS.2016.7497351.
2. S. Szabo et al., Airframes and systems, Technical University of Kosice, 1. edition, 155 p., ISBN 978-80-553-3838-5.
3. X. Chang, et al., A Surveillance System for Drone Localization and Tracking Using Acoustic Arrays, DOI: 10.1109/SAM.2018.8448409.
4. J. Sabo et al., Economic comparison of UAVs and helicopters used for terrain mapping, In: 5th International Conference on Smart and Sustainable Technologies. - New York (USA): Institute of Electrical and Electronics Engineers p. 1-4, ISBN 978-953-290-100-9
5. K. Lee et al., Identification of a flying multi-rotor platform by high-resolution ISAR through an experimental analysis, International Conference on Radar Systems (Radar 2017), Belfast, 2017, pp. 1-5, DOI: 10.1049/cp.2017.0435.
6. P. Koščák et al., UAV Negative Impact on the Safety of Air Traffic in the Area of International Airports, In: International Conference - Social and humanistic sciences and technical sciences – the scope of cooperation for social and technological advance, Gliwice, Silesian University of Technology Press p. 1-8.
7. T. Multerer et al., Low-cost jamming system against small drones using a 3D MIMO radar-based tracking, 2017 European Radar Conference (EURAD), Nuremberg, 2017, pp. 299-302, DOI: 10.23919/EURAD.2017.8249206.
8. P. Petríček et al., Pre-Research of Updated Criteria for Recovery State Processes within Integrated Flight Preparation and Training, In: MOSATT 2019: Modern Safety Technologies in Transportation, Košice, Institute of Electrical and Electronics Engineers p. 130-133, ISBN 978-1-7281-5082-6
9. Z. Zhang et al., An intruder detection algorithm for vision-based sense and avoid system, 2016 International Conference on Unmanned Aircraft Systems (ICUAS), Arlington, VA, 2016, pp. 550-556, DOI: 10.1109/ICUAS.2016.7502521.
10. P. Koščák, Use of UAVs for mapping and characterization of landslide, In: Research Journal of Mining, Vol. 2, I. 1 (2018), p. 14-18, ISSN 2453-9996
11. N. Dalal et al., Histograms of oriented gradients for human detection, 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), San Diego, CA, USA, 2005, pp. 886-893 vol. 1, DOI: 10.1109/CVPR.2005.177.
12. M. Pilát et al., Ramp Safety – Aircraft Marshalling, In: Bezpečnosť a doprava 2018: Teória a prax v bezpečnosti a krízovom riadení v doprave, Brno, Akademické nakladatelství CERM p. 435-449, ISBN 978-80-7623-002-6
13. Example of UAS as a threat, available online: https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf
14. Anti-drone jammer, available online: https://www.blighter.com/products/auds-anti-uav-defence-system/