The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2022

Volume 21, Pages 258-265

IConTES 2022: International Conference on Technology, Engineering and Science

Cyber Attacks on Unmanned Aerial Vehicles and Cyber Security Measures

Mustafa COSAR
Hitit University

Abstract: Unmanned Aerial Vehicles (UAVs) are air vehicles that can be controlled by themselves or via a ground station, can operate with mission-route definition, and can stay in the air in a limited range and time. Today, UAVs are used for various missions in line with military and civilian purposes such as reconnaissance, observation, research, search, control and transportation. In the models used for military purposes, the gun can be mounted and turned into an armed UAV. Attacks on hardware and software systems of UAVs, which are increasingly used in line with developing life conditions and technologies, are also increasing. Especially attacks on communication systems and coordinate information come to the fore. Cyber attacks on UAV systems in general include Data transmission link attacks, GPS (Global Positioning System) Scam attack, authentication attacks such as Brute Force, attacks against source code vulnerabilities, and hardware port and protocol attacks. It is known that attacks on UAV systems cause loss of life and property. It also results in other damages such as task delay, data breach, task failure, and loss of prestige. In this study, after the components, features and introduction of UAV systems, security threats to UAV systems and cyber attacks are defined. Then, the precautions to be taken against threats and attacks are listed. Some of these, importance are subjecting UAV software, hardware and transmission systems to vulnerability and risk scanning, ensuring the security of transmission with data encryption methods, controlling data traffic with a firewall application and making access control secure.

Keywords: UAV, Cyber threat and attack, Risk analysis, Cyber security

Introduction

One of the most important purposes of technology is to remove barriers and support human life. Unmanned Aerial Vehicle (UAV) is a technology developed in this direction. UAVs, which are widely used today; It is used for various missions in line with military and civilian purposes such as reconnaissance, observation, research, search, control, transportation and logistics. It comes to the fore especially in tasks that threaten human health and life safety. Another usage purpose is to be able to perform operations that exceed manpower, incorrectly and difficult to access, with the help of UAVs. It is possible to see many academic studies for these purposes in the literature. For example; Ariansyah, Dewi, and Susanto (2018) provide control and security of critical infrastructures; Falorca, Miraldes and Lanzinha (2021) in visual inspection of buildings and structures; Mademlis et al. (2019) discussed the use of UAVs in the film and advertising industry.

Every new technology has advantages as well as disadvantages. Among the advantages that can be counted; environmental awareness, high mission performance, removing obstacles and helping to provide monitoring-supervision-control-security. On the other hand, its disadvantages include energy needs, range constraints, command-control difficulties, hardware and software constraints, and low resistance to environmental conditions.

The use of UAVs in recent years, from logistics to research and development activities, from military operations to meteorological purposes, has made it a center of attraction. Therefore, it is seen that it also serves malicious purposes despite its beneficial purposes. It is also known to be used for malicious purposes such as unauthorized

and unallowed information gathering, intelligence studies, attack and destruction. In addition to these, cyber attacks against the components, systems and missions of the UAV also contain malicious purposes.

UAVs are aircraft that can be operated remotely or autonomously. The physical elements on a drone use a network of sensors and actuators that communicate with the ground control system via a wireless link (Altawy and Youssef, 2016). By their nature, UAVs consist of mechanical and electronic equipment, software codes, peripherals and payloads. The structures, working patterns, communication architectures and protocols of these units can be designed in a way that is open to threats and attacks. Attackers can even cause the UAV to crash when they catch the slightest gap.

Perhaps the most important components of UAVs exposed to cyber attacks are software systems and data transmission technologies. Among the software systems used by UAVs; autonomous driving software, image recording and processing software, map software, control center software and security software. Among communication systems, it is classified as UAV-ground control center (Ground Control Station-GCS), UAV-satellite system, UAV-UAV communication. Different signals, protocols and technologies are used between each of these communication centers.

In this study, after the components, features and introduction of UAV systems, security threats to UAV systems and cyber attacks are defined. Then, the precautions to be taken against threats and attacks are listed. Some of these measures are; Subjecting UAV software, hardware and transmission systems to vulnerability and risk scanning, ensuring the security of transmission with data encryption methods, controlling data traffic with a firewall application and providing access control.

The work has the following architecture. In the first part, the structure and technologies of UAVs are introduced. In the second part, the types of threats and attacks against the security of UAVs are explained. In the third chapter, precautions and solutions that can be taken against threats and attacks are presented. In the last part, there are the Conclusion and Evaluation stages. It is thought that the study will enable engineers, researchers and enthusiasts, who are involved in the design and use of UAV systems, to look at the cyber security window and have knowledge in this field.

2. Structure and Technologies of UAVs

2.1. General Structure of the UAV

Although nearly a century has passed since its development and first use, the UAV has become especially popular in recent years. These devices, which are popularly known as drones and their armed models are called armed UAVs (Unmanned combat aerial vehicle-UCAV), contain structures such as mechanical, electronics, and computer software and data transmission technologies. It should be assumed that these systems, whose general view is given in Figure 1, are similar, but may show changes based on the task.

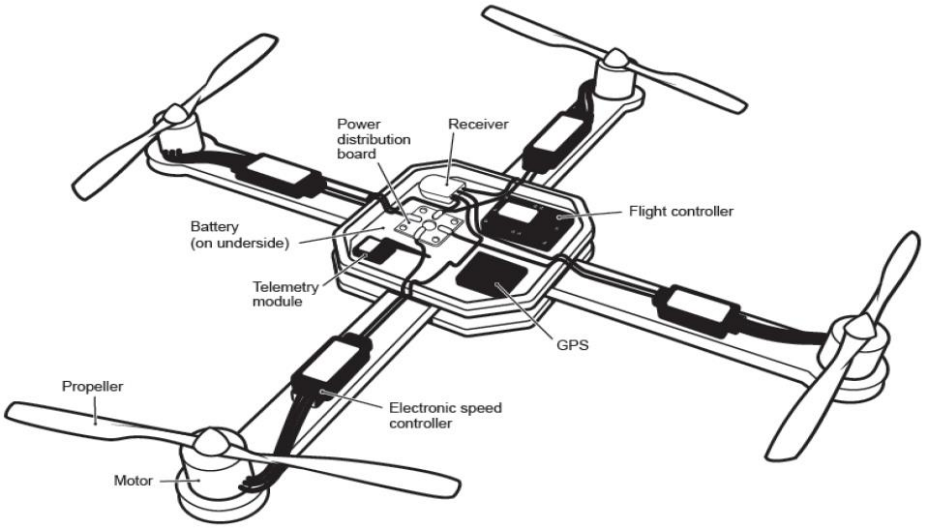

Figure 1. A standard uav structure (Karunakar et al. (2017))

As seen in Figure 1, the structure of an UAV consists of the body, electronic circuits, two or more propellers, speed and flight control devices, remote access module, GPS (Global Positioning System), energy source (battery). In addition, various sensors, transceiver antennas, data storage units, camera and weapon systems can also be found. Other mobile devices such as computers, tablets and smartphones can also be added to these components. A general view of the components of a UAV is given in Figure 2.

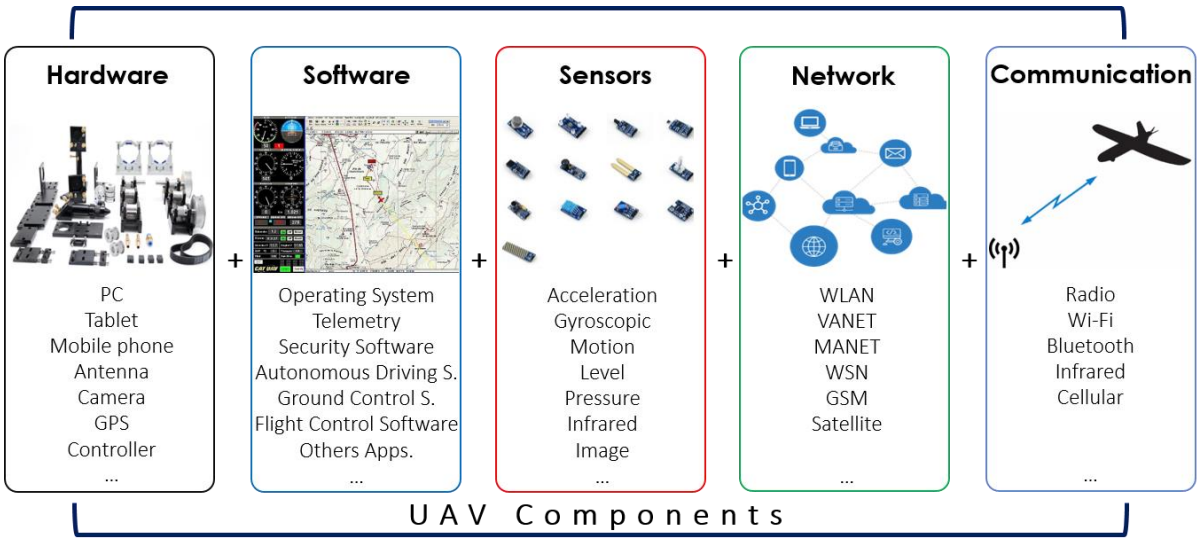

Figure 2. Basic components that make up the UAV

In addition to these components, the fuselage, wings and payload components that will not be subject to a cyber attack can be added. In addition, electronic and mechanical parts, cables and motors should be included in this system. UAV systems established with wireless network architecture adopt the rules developed by the International Institute of Electrical and Electronics Engineers (IEEE) IEEE 802.11 standards group. Private Dynamic Networks (Ad-Hoc) are networks based on collaboration of mobile nodes communicating without a general and fixed architecture. In this network architecture, as the nodes move independently, randomly and alternately, uncertain route and uncertain topology changes are experienced (Yalçın & Boyacı, 2020). Different network architectures can be established under the Ad-Hoc architecture for UAV systems. The first of these is the Mobile Ad-hoc Network (MANET) architecture. In this architecture, there are mobile devices using wireless infrastructure that can follow a random or predetermined route. In these networks, each device is considered a node, while each node has the freedom to roam freely by using its own routing protocol and its own mobility model. For this reason, losses in routing data packets, security vulnerabilities in network communications and access control vulnerabilities are seen.

The other is the Vehicle Ad hoc Network (VANET) architecture. In this network architecture, which is a subcategory of MANET networks, independent mobile devices and connection devices are connected wirelessly with sensors. Another Ad-Hoc network architecture is Wireless Sensor Networks (WSN). It is an Ad-Hoc network type created by more than one sensor. In this network architecture, the sensor nodes communicate with each other and with a base station. The most negative situation in this architecture is the intensity of energy use. Therefore, cyber attacks on the communication of the sensors in the network may cause extra energy consumption.

2.2. UAV Operation Procedures

UAVs are aerial vehicles that can be operated with remote control or autonomously. A UAV records various stages during takeoff and return from a ground point. These are respectively;

Start: Before takeoff, a system is created containing the ID of all UAVs and GCS and key pairs that allow cooperation with other UAVs. One UAV is selected as the backbone; the others are registered as group members. A control signal is sent from the GCS to the backbone UAV, which then acts as a gateway to communicate with other UAVs.

Operation: UAVs cooperate with each other to expand their mission scope, exchange information and avoid collisions. Mission information is published by the GCS and by the backbone UAV. It is then transferred from one UAV to the others.

Join: When a new UAV arrives in UAV swarms and the network, an authorization request is sent to the backbone UAV. After the backbone UAV authorizes the new UAV with ID and key pairs, it initiates communication using encrypted channels.

Flight: UAVs can move at a speed of approximately 45-285 km/h. At these speeds, itinerary planning, mission execution, flying and communicating can be difficult. For this, Static, Random, Time and Route based, Mission based, Swarm based and Topology based flight plans are prepared.

Critical Decisions: UAVs may be out of mission, leave the swarm, or even crash due to low battery levels, changes in environmental factors, time of attack, or disconnections. In such a case, the GCS and the backbone UAV may have to make new decisions. They may need to report this decision to other UAVs in the swarm. The information of a UAV in a difficult situation should also be reported to the backbone UAV or GCS. In this way, the backbone UAV can de-authenticate the UAV that has left the swarm correctly on the network. Some of these management decisions are; flight management, swarm management, service recovery management, communications management, energy management and network management decisions. Brief information about them can be given as follows.

- Service recovery management: Occurs because of network outage mainly caused by radio signal interference and communication failures. In this case, the UAV has to continue with its autonomous driving feature.
- Energy management process: With the help of this process, the UAV controls battery consumption by balancing data transmission and flight parameters and focuses on completing the mission.
- Network management process: It is the management of WLAN and WSN networks formed by the participation of two or more nodes between GCS, UAV, swarm and satellite. For example, in this process, it is possible to regulate conflicts that occur when data exchange at the same time and to ensure network security.

3. Cyber Threats and Attacks against UAVs

Cyber attacks against UAV systems; each of the hardware, software, network, sensor and communication components of the UAV given in Figure 2 are discussed separately. Since the development, production and assembly phases of each component require a separate architecture, security vulnerabilities may occur in each. It should not be forgotten that vulnerabilities related to the components of the UAV that help make critical decisions might include threats and attacks.

Cyber attacks are threats and attacks against the confidentiality, integrity and accessibility of information (Coşar, 2022). The diagram given below gives a general classification of attacks that can occur on UAV wireless networks. The types of attacks given in Figure 3 can be made separately for each of the components or against all components. For this reason, it is necessary to take the measures that can be taken against the attack by considering the whole system.

When Figure 3 is carefully examined, it is seen that the most common type of attack is network attacks. These attacks, which are sub grouped as active and passive attacks, are aimed at the network topology, network communication system, network protocols and data created by the GCS, UAV and UAV swarm. Therefore, Communication attacks, the last component given in the figure, can be included in this group. Transmission layers and routing protocols, which are an important structure of the network architecture, constitute the system that functions from the beginning to the end of the transmission. For this reason, cyber attacks against this structure include both active and passive attacks.

Routing protocols are a set of rules that ensure the appropriate and secure transmission of data packets created during transmission. Attacks against a network or a node are classified as active and passive attacks as summarized in Figure 3 (Ünal and Akçayol, 2008). Active attacks are attacks that violate the principles of confidentiality, integrity and availability to prevent the normal operation of a UAV. Passive attacks, on the other hand, are attacks on the confidentiality of information without harming the operation of the UAV. These two types of network attacks are listed in the Table 1 below.

Table 1. Types of cyber attacks against the network component of the UAV

Attack Type	Name	Definition
Active Attacks	MITM (Man in The Middle)	It is an attack in which the attacker sneaks in between two-way communication and causes the transmission to be made over himself. The attacker, who begins to listen to the transmission, begins to seize personal data, passwords, bank information, change the data or impersonate one of the parties.
	Worm Hole	Collaborating malicious nodes establish a channel with high communication quality between each other. They then announce this channel for routing and collect data packets from the surrounding nodes. Packets passing over this channel are not forwarded to their real destination or they are forwarded by changing.
	Black Hole	When the attacking node positions itself between two nodes that are communicating without encryption, it can make all kinds of changes to the packets. In a black hole attack, the malicious node responds incorrectly to routing requests on the network, presents itself to its neighbors as the shortest route, and takes all incoming packets. The malicious node can perform a denial of service attack by deleting all the packets it receives, or it can listen and redirect the packets to its true path so that the attack is not detected.
	Fabrication	The attacker attacks other nodes with false routing messages that will cause confusion in the network in order to consume resources or disrupt the functioning of the network. Example attacks: Route salvaging, sleep deprivation, and replay.
	Interrupt	It is done to prevent the transmission of packets between the source node and the destination node. When an attacker wants to break the reach of the target node, they can modify the content of the routing messages to destroy all paths to the target node.
	DoS	A denial of service attack is to prevent the network and node from working by exceeding the communication limit that the network and nodes can handle. It is generally done to consume resources such as consuming bandwidth by creating unnecessary traffic, forcing memory, CPU and disk space to process.
	SYN Flood	It is a denial of service attack. It is done by sending SYS requests to the node and the network to communicate over the limit of the data traffic that the system can handle.
	Brute Force	It is an attack of multiple login attempts to guess a user name and password on an access-controlled system. The username and password guessing process varies according to the difficulty and complexity of the information.
	Birthday Attack	It is an attack against hashing algorithms used to verify the integrity of a message, software, or digital signature. A fixed-length representative summary message of the message used for communication is created. With this attack, the probability of randomly generating the same digest message on the network is calculated. If the attacker calculates the same digest, he can replace the user's message with his own, and the recipient will not be able to detect the replacement even if they compare the digests.
Passive Attacks	Eavesdropping	The attacker listens by passing through the network traffic and analyzes by obtaining unauthorized information.
	Modification	The attacking node will redirect the packets to the wrong destination, causing the packets to circulate unnecessarily on the network and drop the packets from the network at the end of their lifetime. While packets circulating in the network cause congestion across the network, the source node that cannot deliver the packets to their original destination will unnecessarily consume its limited energy and bandwidth as it will constantly generate packets again. Example attack Misrouting.

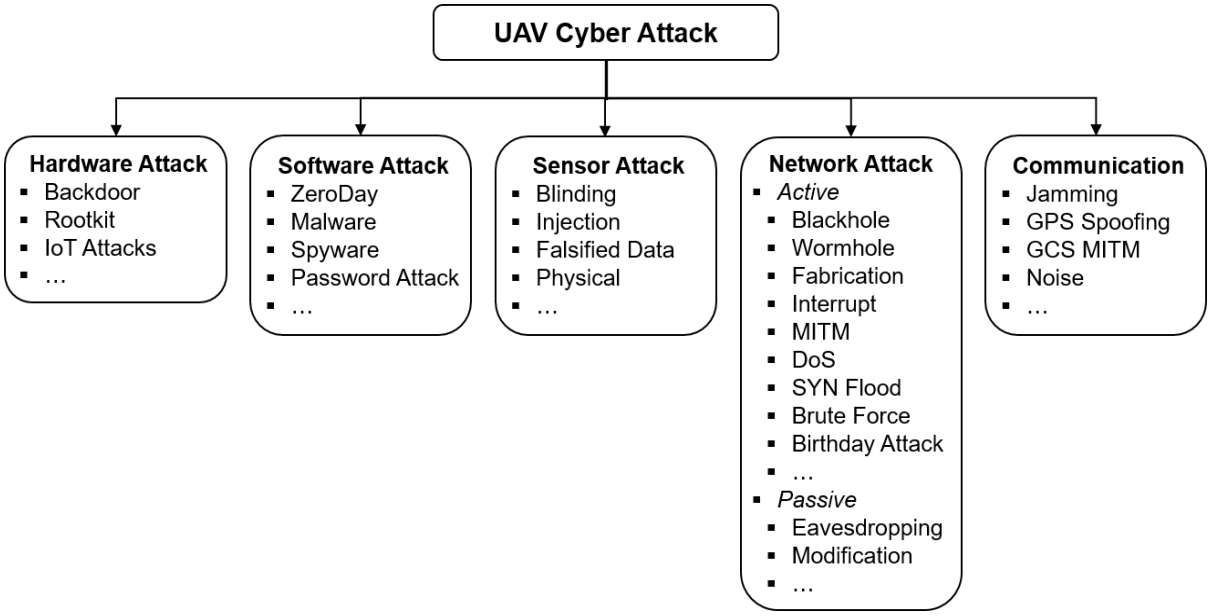

Figure 3. Cyber attack scheme for UAV components

The rapid development of information technologies and the development of new techniques help the development of both attack and defence methods in the cyber field. It should not be forgotten that it will be difficult to ensure the security of a system with such uncertainty and different communication structure.

4. Cyber Security Measures

It is known that controlling, managing and defending a remotely controlled, autonomous driving and decision-making system involves some difficulties. Some control units control and regulate the system operation on an autonomous vehicle. Information from these control units is transferred to a central ECU (Electronic Control Unit) with the help of the Controller Area Network (CAN). Xu et al. (2018), a gateway bridge can route selected data between these two layers. Therefore, there is a possibility that malicious data packets may enter the low-speed CAN layer of the AV without any detection or suspicion before being transmitted to the high-speed CAN layer via the gateway bridge, leading to consequences that are more serious. It is recommended to have message authentication code (MAC) algorithms to protect and verify the integrity of the data. To ensure that AV controllers are trustworthy, it is recommended to use certificates, firewall and cryptographic analysis to support the authentication process.

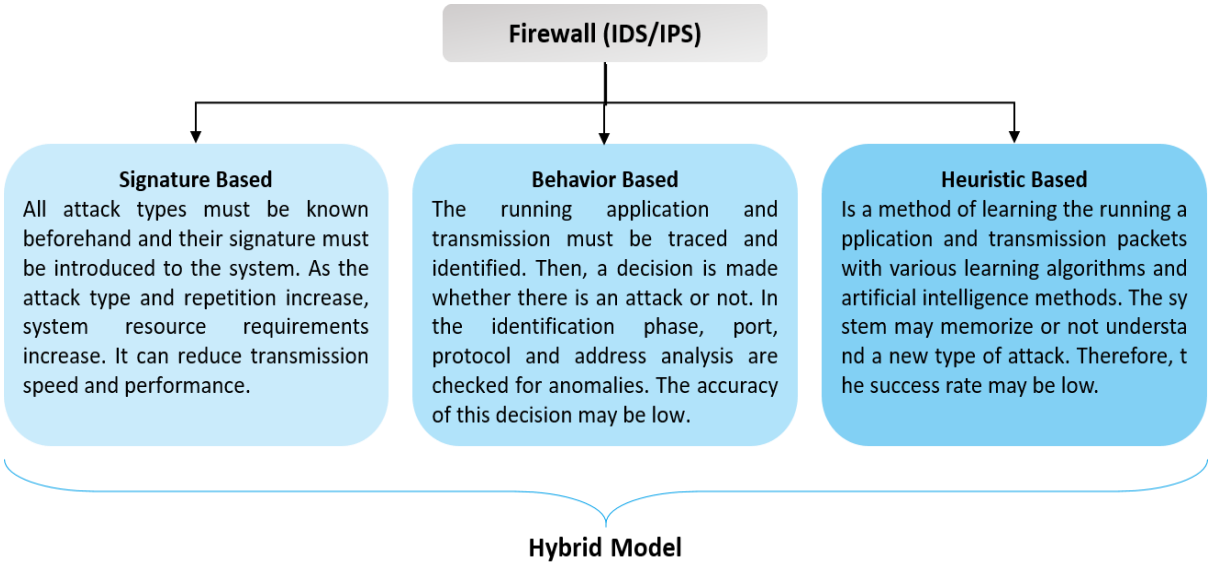

Figure 4. Firewall model for UAV communication

Routing protocols that prioritize security and use node resources efficiently should be used in Ad-Hoc network architecture. Examples of these protocols are; Destination Sequence Distance Vector (DSDV), Wireless Routing Protocol (WRP), ZHLS (Zone-based Hierarchical Link State Routing Protocol), Optimized Link State Routing (OLSR), Secure Efficient Ad Hoc Distance Vector (SEAD), A Secure On-Demand Routing Protocol for Ad-Hoc Networks (ARIADNE), Secure Routing Protocol (SRP) (Tekerek, Vural & Aydos, 2016).

As another solution suggestion, it is suggested to use a firewall with advanced features. This firewall should incorporate Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) features together. In addition, port, protocol, address and application are expected to overcome abnormal situations by doing some checking. In this context, it is proposed to create a hybrid system for IDS and IPS, which is given in Figure 4. As can be seen in Figure 4, the features that a new generation firewall should have are given. These three types of IDS/IPS models have advantages and disadvantages. Especially when measuring performance, resource utilization rates and success rates in detection and prevention stages are decisive. For this reason, it is thought that a combined model will be more advantageous and the success rate will be higher. This hybrid model must be applied in accordance with the structure, intended use and other characteristics of the UAV.

Conclusion

In this study, a cyber attack and security analysis was made by separating the UAVs into their components. It has been demonstrated that a UAV system has hardware, software, sensors, network and communication components. It has been emphasized that each of these components can be exposed to cyber attacks separately. Since these components contain information technology elements, it is seen that the cyber threats and attacks encountered today may also threaten them. For this reason, it has emerged that a security model should be operated by looking at the whole of the UAV from a holistic perspective and its components from a discrete perspective due to the nature of information technologies. In the study of Mejri et al. (2014), it is recommended to create a PKI (Public Key Infrastructure) associated with VANETs and to use digital certificates as a fast authentication method in a vehicle network. To increase the security of autonomous vehicles with ultrasonic sensors, two defense strategies have been proposed, namely single sensor-based authentication (PSA) and multi-sensor consistency check (MSCC), which authenticate signals. Coşar and Kıran (2021), in their study, proposed blockchain technology to protect against cyber attacks against drone swarms. In their study, they determined that blockchain technology provides network communication security and location accuracy of GCS and drone-drone communication packages. In addition, firewalls against cyber threats and attacks, data encryption algorithms and multi-layered access control mechanisms should be applied during secure data transmission and access to hardware and software systems. In addition, multiple modulation techniques, noise canceling and reducing mechanisms should be used for the signals used in the transmission and management system. Finally, vulnerabilities and risks need to be determined beforehand by penetration testing of all components. It is then recommended to use it after the vulnerabilities are closed.

Scientific Ethics Declaration

The author declares that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the author.

Acknowledgements or Notes

* This article was presented as an oral presentation at the International Conference on Technology, Engineering and Science (www.icontes.net) held in Antalya/Turkey on November 16-19, 2022.

References

Altawy R. & Youssef. A.M. (2016). Security, privacy, and safety aspects of civilian drones: A survey. *ACM Transactions on Cyber-Physical Systems,1*(2), 1-25, Article 7 (November 2016), http://dx.doi.org/10.1145/3001836.

Ariansyah M.R., Dewi A.A. Susanto C.D., & Rahayu Y. (2018). Resheniye drone, the answer of digital oil spill recovery, *Conference: Oil & Gas Seminar and Competition 2*018.

Coşar, M. (2022). Privacy and security on blockchain, In book: *Blockchain innovative business processes and long-term sustainability*, Publisher: Nobel, Editors: Mert Gözde, Zeren Karagöz Seda, Yılmaz Osman, (pp.245 -270), ISBN: 978-625-433-841-0.

Cosar, M., & Kiran, H. E. (2021). Verification of localization via blockchain technology on unmanned aerial vehicle swarm. *Computing and Informatics, 40*(2), 428–445. https://doi.org/10.31577/cai_2021_2_428

Falorca, J. F., Miraldes, J. P., & Lanzinha, J. C. G. (2021). New trends in visual inspection of buildings and structures: Study for the use of drones. *Open Engineering, 11*(1), 734-743. https://doi.org/10.1515/eng-2021-0071

Karunakar, P., Jariso, M. & Kale, P. (2017). A review on geo mapping with unmanned aerial vehicles. *International Journal of Innovative Research in Computer and Communication Engineering*, 5(1), 1170-1177.

Mademlis, I., Torres-González, A., Capitán, J., Cunha, R., Guerreiro, B.J., Messina, A., Negro, F., Barz, C.L., Gonçalves, T.R., Tefas, A., Nikolaidis, N., & Pitas, I. (2019). A multiple-UAV software architecture for autonomous media production. *EURASIP European Signal Processing Conference (EUSI*PCO) 2019.

Mejri, M.N., Jalel, B. & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions, *Vehicular Communications 1*(2), https://doi.org/10.1016/j.vehcom.2014.05.001.

Tekerek, M., Vural, Y. & Aydos, M. (2016). Tasarsız ağlarda yönlendirme güvenliği üzerine kapsamlı bir araştırma. *Bilişim Teknolojileri Dergisi*, *9*(2), 171-180, https://doi.org/10.17671/btd.64124.

Ünal, M. & Akcayol, M. A. (2008). Kablosuz ağlarda güvenli yönlendirme protokolleri. *Bilişim Teknolojileri Dergisi*, *1*(3), 7-13.

Xu, W., Yan, Chen, J., Jia, W., Ji, X., Liu, J. (2018). Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. *IEEE Internet of Things Journal*, *5*(6), 1-14. https://doi.org/10.1109/JIOT.2019.2867917

Yalçın, N. O. & Boyacı, A. (2020). İnsansız hava araçlarının hareket ve yönlendirme protokollerine göre performans ölçümü. *İstanbul Ticaret Üniversitesi Teknoloji ve Uygulamalı Bilimler Dergisi*, *3* (1), 27-40.

Author Information

Mustafa Coşar
Computer Engineering, Hitit University
Turkey
Email: *mustafacosar@gmail.com*

To cite this article:

Cosar, M. (2022). Cyber attacks on unmanned aerial vehicles and cyber security measures. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 21,* 258-265.