sciendo
Control and Cybernetics
vol. **52** (2023) No. 4
pages: 405-439
DOI: 10.2478/candc-2023-0044

A survey on UAVs security issues: attack modeling, security aspects, countermeasures, open issues*

by

Fargana Abdullayeva[1] **and Orkhan Valikhanli** [2]

[1,2]Institute of Information Technology, 9A, B. Vahabzade Street, Baku AZ1141, Azerbaijan
[1] a_farqana@mail.ru
[2] orkhanvalikhanli@gmail.com

Abstract: The Unmanned Aerial Vehicles (UAVs) are being actively used in various fields including agriculture, surveillance, scientific research, and delivery. Despite their widespread use, UAVs face significant cybersecurity challenges due to their vulnerabilities as cyber-physical systems. UAVs are vulnerable to cyberattacks, which target cyber or physical elements, the interface between them, wireless connections, or a combination of several components. Given the complexity of securing these systems, this paper provides a comprehensive survey of the current state of UAV cybersecurity. Moreover, different cybersecurity issues of UAVs are analyzed, various features, and functions of UAVs are considered. UAV attack classification scheme is constructed and attacks on various components are accounted for. Also, countermeasures against cyberattacks that target UAVs are discussed. Finally, UAV cyber security datasets for research purposes are indicated, and the remaining open issues in this field are identified.

Keywords: UAV, cybersecurity, vulnerability, cyberattacks, countermeasures

1. Introduction

According to statistics, the global UAV market size worldwide is anticipated to grow from 26.3 billion U.S. dollars in 2021 to 54.6 billion U.S. dollars by 2030 (Laricchia, 2023). This dramatically fast growth is attributed to several factors that make UAVs increasingly popular. UAVs are robust, fast, and may even be cheaper compared to other systems. With shrinking electronics size

*Submitted: May 2023; Accepted: August 2024.

and increasing computer power, UAVs are becoming the best option for any given mission (Bayraktar and Feron, 2009). UAVs can be used for various kinds of missions. Delivering cargo with the help of UAVs is not only fast but also environmentally friendly. UAVs can also be used in search and rescue missions (Półka, Ptak and Kuziora, 2017). Some areas may be too dangerous to send the rescue teams there. Implementation of UAVs to operate in those areas is very convenient. In recent years, UAVs also became an integral part of warfare. Today's military UAVs are able to target almost any enemy units. Military UAVs are cheaper compared to warplanes and are remotely controlled, which ensures the safety of pilots. Then, the industrial environment is expected to undergo a paradigm change with the advent of Industry 5.0, which will integrate modern technologies with human intelligence and creativity. UAVs are expected to be a major part of this transition. UAVs are predicted to rule Industry 5.0 in a number of areas, including environmental monitoring and sustainability, supply chain and inventory management, customized and flexible manufacturing, disaster response and management, real-time data collection and analysis, and customized and flexible manufacturing (Jain et al., 2022). The number of Remotely Piloted Air Systems (RPASs), also known as drones, will rise quickly in the foreseeable future, as predicted by the Federal Aviation Administration (Salamh et al., 2019).

The widespread use of UAVs has created serious problems related to their cybersecurity. Recently, UAVs are considered to be the most exposable technical systems to the influence of the cyberattacks (Hartmann and Steup, 2013). Cyberattacks against UAVs may have catastrophic results, such as injuries and even deaths. Specially, consumer type UAVs are vulnerable to cyberattacks due to lack of security measures. It is not a very difficult task to carry out some kind of cyberattack against such UAVs. This is because devices, which are used for performing cyberattacks, are available on the market. One type of those devices is called software-defined radio (SDR). Attackers can easily use SDR to perform spoofing and jamming attacks against UAVs. Military UAVs are also vulnerable to cyberattacks. In 2011, US military UAV named Lockheed Martin RQ-170 Sentinel was captured by Iranian forces (Yağdereli, Gemci and Aktaş, 2015). Both GPS spoofing and jamming attacks were used to capture the UAV.

The integration of UAVs with other advanced technologies further complicates ensuring their cybersecurity. IoT (Internet of Things) based UAV system along with the security problems of the UAV contains also the security problems of the IoT (Hossein Motlagh, Talen and Arouk, 2016). For this reason, it is necessary to take a comprehensive approach to ensure the security of UAVs.

The cybersecurity problems of UAVs are being studied in many literature sources. Previous researchers carried out an analysis of attacks on UAVs and countermeasures using anti-UAV techniques (Chamola et al., 2021; Abdullayeva

and Ibrahimov, 2022; Abdullayeva and Valikhanli, 2022). Madan, Banik and Bein (2019) proposed a conceptual model of a UAV and demonstrated cyber threats to its separate components. Haider, Ahmed and Rawat (2022) studied security solutions of UAV assisted cyber physical systems (UAV-a-CPS). They stated that UAV-a-CPS is still vulnerable to cyberattacks and that multi-layer based adaptive security approaches could protect those systems. Multi-layer based adaptive security approaches include no-trust authentication, lightweight cryptographic protocols, AI-assisted jam-resilient aerial waveform design, and AI-driven blockchain. Shafique, Mehmood and Elhadef (2021) analyzed and identified the vulnerabilities in existing security protocols. Cyberattacks such as jamming, GPS spoofing, fuzzing, and false data injection were also discussed.

The main shortcoming of the existing studies is that the security issues of UAVs have not been investigated in detail in these studies, and, in particular, cyberattacks targeting UAVs have not been classified by different components of the UAV system. It is considered necessary to develop new approaches to overcome the limitations of existing security solutions.

The present paper is organized as follows. Section 2 introduces the overall UAV system architecture. Section 3 describes the operation principles of the UAV. Section 4 presents the security aspects of UAVs. Section 5 introduces the classification of UAV attacks. Section 6 describes the security issues of UAVs. Section 7 presents countermeasures against cyberattacks on UAVs. Section 8 introduces UAV related datasets for research purposes. Section 9 identifies open issues related to UAV cyber security, and finally Section 10 presents the conclusion of the work.

2. UAV system architecture

To analyze the security of UAVs, it is necessary to identify the components, which constitute their architecture. There are two main components of UAS (Unmanned Aerial Systems) as shown in Figure 1: the UAV and the Ground Control Station (GCS).

The UAV part itself consist of components such as flight control system, navigation system, communication links, sensors, and avionics. The flight control system is the most important component of UAV. It manages all system inputs/outputs and allows the internal components of the UAV to work together. Moreover, the flight control system stabilizes UAV, manages its speed and other aspects. The flight control system may be considered to be the “brain” of UAV. The navigation system is another important component of UAV. There are many options, which can be implemented in navigation system. The most common satellite navigation systems are GPS, Galileo, BeiDou navigation satellite system, global navigation satellite system. But recently, many cyberattacks tar-

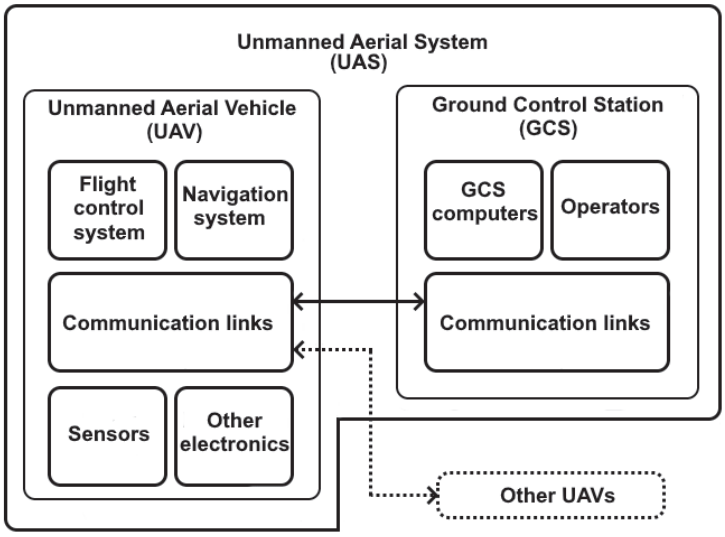

Figure 1. UAS components

geted the UAV navigation systems, which implement only satellite navigation. Therefore, other navigation methods are becoming more popular. UAVs also have various on-board sensors, such as barometer, gyroscope, accelerometer, magnetometer, etc. Flight controller system receives sensor data and processes it for further operations. The "other electronics" part includes components such as Electronic Speed Controller (ESC), and Power Distribution Board (PDB).

The GCS part consist of computers, operators, and communication links. GCSs are designed in different sizes and shapes. Depending on definite application, GCS can be deployed as stationary or portable. Stationary GCSs are typically built into large containers. There are several computers (servers) inside stationary GCSs, which are used to process data and perform other important tasks. GCSs also contains several operator workstations. Each operator has an individual task assigned. Pilot controls UAV, payload operator controls mission payload, and another operator monitors map activity on display. GCSs have several antennas attached to them to communicate with UAVs. The portable GCSs are also widely used. They are designed to be much smaller in size and to be easily moved around. They also include computer, several antennas and display.

GCS and UAV communicate with each other with the help of communication links via a wireless network. During this communication, commands are received

from the GCS and the collected data is sent to the GCS. Also, the GCS not only manages and coordinates the movement of the UAV, but also processes the data received from the UAV. In the literature, UAV communication is being categorized into the following types (Chriki et al., 2019):

1. Direct UAV communication. In this communication type, communication between UAV and GCS is established directly. This is the simplest communication type.
2. UAV to UAV (to GCS) communication. This communication type allows multiple UAVs to communicate with each other and also to communicate with GCS. This situation is also referred to as A Flying Ad hoc Networks (FANETs). There are many wireless technologies that are used in this communication type such as WiFi, Bluetooth, ZigBee, etc.
3. UAV to Cellular (to GCS) communication. In this communication type, UAV communicates with cellular stations and may also communicate with GCS. Since it uses cellular networks, wireless technologies applied include GSM, GPRS, 3G, 4G, 5G, etc.
4. UAV communication via satellite. It is quite frequent that UAVs and GCS happen to be located at very long distances. In situations like this, establishing communication via satellites is very convenient. This allows for data exchange between UAV and GCS to pass through satellites. However, compared to other communication types, this solution is expensive.

Chamola et al. (2021) classified UAVs based on their weight, altitude, and range. Additionally, classification based on their rotors, wings, and applications is also proposed. The classification of UAVs on the basis on their rotors and wings structures can be as follows:

- Single-rotor. UAVs with a single rotor are structurally similar to helicopters.
- Multi-rotor. UAVs with multiple rotors can also be classified as tricopters (3 rotors), quadcopters (4 rotors), hexacopters (6 rotors), and octocopters (8 rotors).
- Fixed-wing. UAVs with fixed wing(s) are structurally similar to airplanes.
- Hybrid-wing. UAVs with hybrid wing(s) combine the features of rotary and fixed wing structures.

Classification based on UAV applications include personal (consumer), commercial, law enforcement, and military kinds of applications. Consumer UAVs can be used for photography, videography, and entertainment. Commercial UAVs include cargo transport, journalism, aerial surveillance, scientific research. Law enforcement UAVs are used to fight against crimes such as, in particular, terrorism and poaching. Military UAVs are largely used for reconnaissance and targeting enemy units.

3. Operation principle of the UAV

There are several types of UAVs, as commented upon before, but the working principle of those is similar. The main component of the UAV is the flight controller (FC). FC has several tasks such as communicating with GCS and recording flight data. But the most important task of FC is to control actuators or the speed of motors. For this purpose, FC continuously reads sensor values to stabilize the UAV and waits for input commands. The movement of a UAV can be changed with the help of pitch, roll, and yaw. Pitch (lateral axis) is used for moving forward and backward. Roll (longitudinal axis) is used for moving left and right. And yaw (vertical axis) is used for rotating clockwise and anti-clockwise. For multi-rotor type UAVs, all those movements are executed by controlling the speed of respective motors. But for fixed-wing type UAVs, all movements are possible with the help of actuators such as elevators, ailerons, and rudders.

To send control commands and receive necessary information from UAVs, GCS is used. GCS can be any system such as a smartphone, tablet, and personal computer. Complex UAV systems such as military ones, use specially built GCS. During GCS-UAV communication, important data including commands, battery level, altitude, velocity, GPS information, as well as, possibly, video stream, are transmitted. As described in Section 2, various wireless technologies are used for communication. There are also messaging protocols such as MAVLink and Multiwii, which are specially designed for UAV communication.

The ways of operation of UAV can be classified as follows (Yaacoub et al., 2020):

1. Manual control – human fully operates UAVs.
2. Semi-autonomous control – UAV self-operates, but human intervention is possible for some tasks.
3. Autonomous control – the operation of a UAV is fully automatic.

Especially for autonomous UAVs, navigation is essential. The most common navigation system for UAVs is GPS. GPS is an accurate and very convenient navigation system. But as with other navigation systems, GPS also has some drawbacks. Thus, it can be the target of cyberattacks, and also GPS cannot be used in indoor environments. Therefore, other systems are also implemented for navigation. These include implementation of IMU, camera, LiDAR, and ultrasonic sensors. Recently, not one but multiple navigation systems are implemented together to overcome impediments. So, if one method fails, other ones keep providing navigation. Implementation of multiple navigation systems is possible with the help of sensor fusion process. In navigation systems, sensor fusion refers to the process of combining input from several sensors to get more accurate and reliable information than could be obtained by using each sensor

alone. There are various fusing algorithms. However, typically Kalman filters (KF) are used for sensor fusion (Balamurugan, Valarmathi and Naidu, 2016; Valikhanli, 2023).

4. Security aspects of UAVs

The goal of UAV security systems is to ensure such features as: availability, confidentiality, completeness, authenticity, and non-repudiation. **Availability** refers to the UAV's ability to provide effective service even when it is under the influence of an attack. **Confidentiality** ensures that communication data between UAVs is not leaked to unauthorized users. **Integrity** ensures that the data transmission process is not tampered with and that the received information is the same as the sent information. The destruction of integrity has serious consequences. In this case, the use of distorted information in the decision-making process can easily result in making wrong decisions. If an attacker performs a Man-in-the-middle (MITM) attack on the command and control (C2) data sent to the UAV, he can easily hijack the UAV's operations. By the same token, if an attacker modifies signals from a satellite to be used in a military decision-making system, the results can be definitely dire. **Authentication** means that each node can recognize the identifier of the node with which it will establish a connection. **Authorization** is used to allow an entity to perform certain operations. **Non-repudiation** ensures that a node cannot deny that it has produced any information. Some literature sources also include in this list the **trust issues** of UAV.

Threats to UAVs include jamming, meaconing, spoofing, eavesdropping, Information Injection, Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), and De-authentication attacks (He, Chan and Guizani, 2017). These kinds of cyberattacks can be described as follows:

Jamming

Jamming attacks can target GPS as well as communication systems, too. The purpose of jamming attacks is to prevent authentic signals from reaching the receiver. This attack is carried out by sending interference signals with a higher power within the same frequency range. When an attack targets a GPS system, then the navigation system may fail to operate. Jamming attacks may also target communication systems so that the connection between GCS and UAV will get interrupted.

GPS spoofing

During a GPS spoofing attack, the attacker generates and transmits counterfeit signals which are similar to the real ones. As a result, the attacker deceives

the victim and takes control over navigation. After taking control, an attacker can easily crash or hijack a UAV.

Meaconing

Meaconing is very similar to a GPS spoofing attack. The difference is that real GPS signals are previously recorded and transmitted later to deceive the victim.

Eavesdropping

The aim of eavesdropping is to seize information. Eavesdropping can be done with the help of a MITM attack. During the MITM attack, the attacker secretly takes a position between parties. It gives attackers an opportunity to alter, delete or eavesdrop regarding the information in question.

Data injection

This is a type of cyberattack in which an attacker injects false data into the system. For example, an attacker may inject false commands and crash the UAV.

DoS and DDoS

DoS/DDoS attacks are used to deplete the resources (CPU, RAM, etc.) of the UAV system. This is made possible by sending a huge amount of packets (requests) to the victim. DoS attack is similar to DDoS. The only difference is that during a DDoS attack multiple sources target victims instead of just one.

De-authentication

De-authentication is a type of DoS attack. During the attack, continuous de-authentication packets are sent to the victim. As a result, the victim loses connection.

5. Classification of UAV Attacks

Threats and attacks on UAVs are performed with respect to their functional modules (He, Chan and Guizani, 2017). In the present paper, the attack points that can destroy the UAV are identified, and specific attacks on these attack points are classified into different groups, as shown in Fig. 2.

UAV attack classification scheme, which is shown in Fig. 2, describes the potential attack surface of the UAVs. According to this classification scheme, attacks are made against the following modules: sensors, navigation, air traffic control, fault handling, telemetry channel, flight controller, GCS networks, wireless data link, GCS computers, RFID, and actuators.

Attacks on the flight controller result in the falsification of existing rules for flight control. Attacks on Navigation Sensors can result in the loss of position

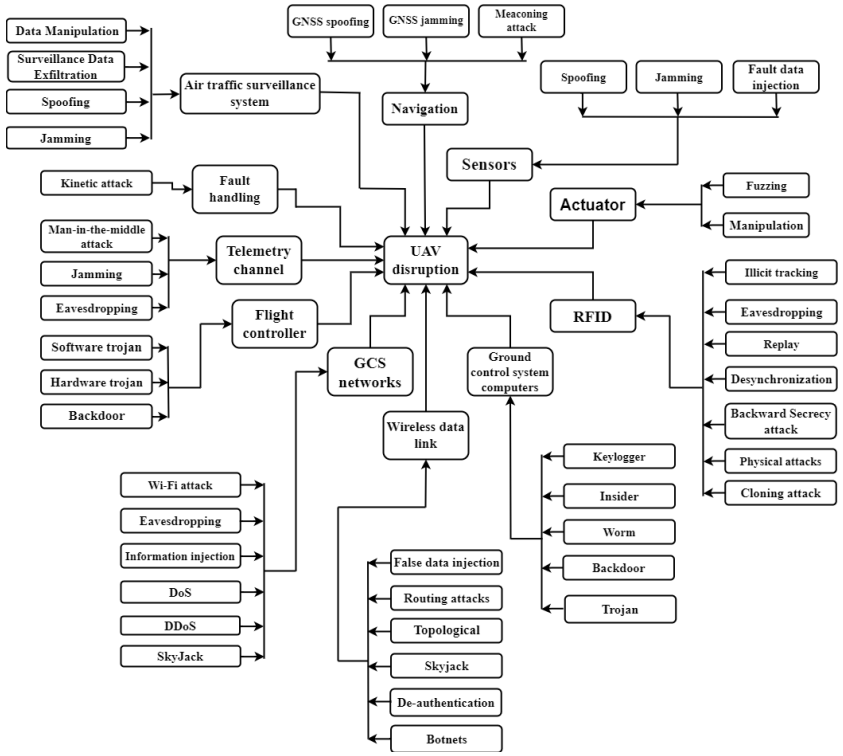

Figure 2. UAV attack classification scheme

information or in the reception of altered or misleading feedback information. Shepard et al. (2012) identified various spoofing techniques that can be performed on onboard GPS sensors. Communications Channel attacks on a UAV can result in loss of communication with the GCS or sending malicious commands to the UAV. Attacks on this component include SkyJack (RT, 2013).

Vattapparamban et al. (2016) identified SkyJack and De-authentication attacks on the wireless network of drones. Rodday, Schmidt and Pras (2016) identified a MITM attack on communication between a UAV and remote control. Madan, Banik and Bein (2019) demonstrated the possibility of attacking the GCS of the UAV through the insider, worm, key logger, and Trojan-type malicious programs. The purpose of the malicious action in this case is to steal passwords and other personal information.

Madan, Banik and Bein (2019), Khaitan and McCalley (2015) referred to the UAVs as Cyber-physical systems from the cyber security point of view. UAVs display vulnerabilities against attacks targeting cyber or physical elements, the interface between them, wireless connections, or a combination of several components (Constantinides and Parkinson, 2008). Protecting cyber-physical systems from cyber threats is much more difficult than in the case of the traditional systems. This is because a cyber-physical system, such as a UAV, requires real-time control, and its essential system requirement is physical security. CSRA and NIST (2013) define security requirements for cyber-physical systems. Madan, Banik and Bein (2019) identified malware injection attacks (viruses, worms, and trojans) on GCS computers. In their work, the possibility of DDoS attacks on GCS networks was also noted.

Since UAVs have an open communication architecture, attacks on them can possibly occur in three situations: in communication between UAVs and GCS, in satellite signal reception and in communication between UAVs. Attacks on the communication between UAVs and the GCS can be made to violate the availability of information, for example, DoS, black hole attack, and can also be made to violate the integrity of information, for example, False Data Injection Attack (FDIA), replay attack, MITM attack. Gu et al. (2021) investigated the vulnerabilities existing between UAVs and GCSs, and mainly considered the FDIA on the wireless network. In the work quoted, the characteristics of FDIA attacks are analyzed and the FDIA model is constructed to launch the FDIA attack on the wireless communication channel of the UAV. A mechanism based on combining multiple features is proposed for FDIA attack detection. Gope, Millwood and Saxena (2021) identified the attack types such as illicit tracking attacks, eavesdropping attacks, replay attacks, desynchronization or DoS attacks, backward secrecy attacks, physical attacks, and cloning attacks, targeting radio-frequency identification (RFID) based UAVs. Bera, Das and Sutrala (2021) identified DoS, replay, MITM, unauthorized root access, packet

spoofing, Ephemeral Secret Leakage (ESL), drone impersonation, and drone physical capture attacks on drones' wireless communication channels. Fotohi (2020) identified Wormhole, Black hole, Gray hole, and Fake Information Dissemination (FID) attack types targeting the communication channel to interfere within the UAV system.

6. Security issues of UAV

As a result of the analysis performed, several security issues regarding UAVs were identified. These are attack detection, threat modeling, unauthorized UAV detection, data protection, trust and privacy, network security, authentication, and UAV system resiliency.

Attack detection

Huang and Wang (2018) investigated the physical security of UAV-based wireless systems from the point of view of authentication and detected the eavesdropping attack on UAVs using log-likelihood radio. Xiao et al. (2018) used reinforcement learning to detect eavesdropping in UAV-based wireless systems. Hoang, Nguyen and Duong (2020) proposed a prediction model to detect eavesdropping attacks on UAV-based wireless systems using a one-class support vector machine and the k-means clustering method. Pyzynski and Balcerzak (2021) investigated the potential cyber threats targeting UASs and proposed possible solutions for applying an aviation cybersecurity approach to UAS operations. Those solutions include establishing a shared understanding of cybersecurity between stakeholders, conducting awareness campaigns, engaging with research communities and academia, creating dialogues among stakeholders to protect systems and data, ensuring appropriate regulations and standards, facilitating information sharing, and developing education and training programs. Nunez, Tran and Katangur (2019) analyzed attacks on the security vulnerabilities of the AR parrot 2.0, 3DR Solo, and the DJI Phantom 4 Pro drones. In this work, gaps in autopilot systems and safety protocols were evaluated.

To detect hijacked drone that uses an Inertial Navigation System (INS) data (e.g., angle velocity and acceleration) and GPS data (e.g., longitude and latitude). Feng et al. (2020) proposed a two-stage approach based on the idea of GA-XGBoost algorithms. The proposed method first adjusts the values of the training parameters through the Genetic Algorithm and then trains the model. Experiments were conducted on a quadrotor drone to evaluate the effectiveness of the method. Abdullayeva and Valikhanli (2022) developed a new approach, based on the Convolutional Neural Network (CNN) method for the detection of GPS spoofing attacks. As a result of conducted experiments, high-accuracy

detection of GPS spoofing attacks has been provided. Bada et al. (2021) proposed GPS spoofing detection mechanism for FANETs inspired by a 'burglary scenario,' where distinguishing between active and passive witnesses plays a crucial role. In this context, distinguishing active signals from passive ones allows the target to detect GPS spoofing attacks using two parameters: absolute power and carrier-to-noise density. According to the simulation results, 98.4% accuracy was achieved.

Sharifi-Tehrani, Sabahi and Danaee (2021) proposed GNSS jamming detection methods based on random matrix theory for UAV ground control station. By using limiting distribution of mean vector and asymptotic behavior of the defined test statistic, a hypothesis test is introduced and evaluated to detect the presence of a jamming signal. According to the simulation results, the performance of the proposed method was better compared to other ones tried out. Dang et al. (2022) proposed GPS spoofing detection method using CNN and transfer learning. The proposed CNN model allows to compare differences between the base station theoretical and real-time path losses. Moreover, transfer learning was implemented to decrease model training time and also increase detection accuracy. Overall, 88% accuracy was achieved. Greco et al. (2021) proposed a novel framework for detection of jamming attacks in UAV networks. The proposed framework is based on machine learning methods including Multilayer Perceptron (MLP) and Decision Tree (DT). Throughput, Packet Delivery Rate (PDR) and Received Signal Strength Indicators (RSSI) are used as main parameters. In the training process, both publicly available dataset and dataset created using simulations were used. According to the results, both MLP and DT showed good performance. But MLP was better than DT when applied to the communication scenarios, for which it has not been trained. Overall, 96% accuracy was achieved.

Threat modelling

The process of ranking threats is called threat modeling. This method allows for making of proactive decisions to prevent threats at the initial stage (Gharibi, Boutaba and Waslander, 2016). Threat modeling is the process of systematically ranking all possible threats that could affect a system.

There are many methodological approaches for modeling threats targeting devices such as Spoofing identity, Tampering with data, Repudiation, Information disclosure, DoS, Elevation of privilege (STRIDE) (Hussain et al., 2014), Attack Trees (Kordy, Pièvre-Cambacédès and Schweitzer, 2014), The Process for Attack Simulation and Threat Analysis (PASTA) (Shevchenko et al., 2018), Abuser Stories (Singhal and Banati, 2011), CORAS (Lund, Solhaug and Stolen,

2011), and Common Vulnerability Scoring System (CVSS) (Johnson et al., 2018).

STRIDE is a threat model developed by Microsoft. The threats accounted for are Spoofing, Tampering, Repudiation, Information disclosure (privacy breach or data leak), DoS, and Elevation of privilege. Some of these threats intrude on the required properties with most of the applications: availability, authenticity, authorization, confidentiality, integrity, and non-repudiation (Khan et al., 2017).

Javaid et al. (2012) analyzed various security threats to the UAV system and developed a cybersecurity threat model depicting possible attack paths. Madan, Banik and Bein (2019) performed UAV threat modeling and risk analysis using the STRIDE approach. Almulhem (2020) addressed the threat modeling issue. The threat tree built in that study allows for analyzing the threats affecting the Internet of Drones (IoD) architecture. The constructed threat tree represents a complete view of the threats that can affect the IoD system. This work identified the threats to the communication, mobility, non-mobility, drone, and routing components of the IoD system. Yaacoub et al. (2020) conducted an analysis of attacks on drones and attacks from drones and countermeasures for their elimination. Ly and Ly (2021) classified cyberattacks on UAVs based on the STRIDE model.

Unauthorized UAV detection

Unauthorized UAV detection refers to the usage of different technologies and techniques intended to detect UAVs that are not authorized to operate in certain environments. These detection systems require robust methods to ensure the accuracy and integrity of the data collected.

A blockchain is a distributed ledger that protects data through encryption protocols such as a hashing function and cryptographic public keys. This technology is also used to ensure the authenticity of the processed data and increase the security and transparency of the UAV. Bera, Das and Sutrala (2021) proposed a blockchain based access control model called ACSUD-IoD for unauthorized UAV detection and neutralization in the IoD environment. Through the authenticated transactions collected at the Ground Station Server (GSS), the blocks are formed, verified, and added to the blockchain, which is then used for mining in the blockchain through the Practical Byzantine Fault Tolerance (PBFT).

Abdullayeva and Ibrahimov (2022) proposed an approach for detecting UAVs flying over unauthorized areas based on audio signals. Features were extracted from the sound signals and their ensemble was created. The new data thus created were fed to the input of neural network models in the form of vectors

and drones were detected. The effectiveness of the proposed approach has been tested on several databases.

Data protection

Encryption, secure communication protocols, and various access control measures are all part of data protection, which keeps sensitive information about UAV operations safe from unauthorized access or manipulation. Naeem et al. (2021) proposed an approach to protect the privacy of the 3D spatial data transmitted by the GPS to the GCS, indicating the location of the drone when it is in service. The model developed in that study is based on the obfuscation of spatial data obtained from sensor devices. The goal of the approach is to increase the security and resilience of a drone flying in the air against malicious targeting from the attackers by hiding the UAV's true flight trajectories.

Ch et al. (2020) proposed a method based on blockchain technology to protect the data privacy of the UAVs. Pentatope based Elliptic curve and Secure Hash Algorithm (SHA) encryption algorithms were used to ensure security when data is stored on the cloud platform. This data was then applied to perform blockchain transactions. Since the main issue of UAVs is to collect information and conduct their in depth analysis, one of their most critical subsystems is the communication system (data link). For this reason, it is considered important to develop methods that ensure secure data transmission for UAVs.

In order to ensure the safety of the UAV systems, risk analysis should be performed to analyze and predict the risks and threats that may occur. Dursun and Çuhadar (2018) conducted a study regarding risk analysis in the data link layer of UAV. In this study, a methodology for data link systems of UAVs was developed by combining risk analysis and multi-criteria decision-making. Also, the risk analysis methodology was used to determine criteria and weights in decision-making. Risks are expressed as the product of threat magnitude and value of probability and used as input data in a multi-criteria decision-making method. Threats are taken as alternatives and risks as weights of the alternatives.

Trust and privacy

In the context of UAV security, "trust" refers to the level of confidence that the various entities, including the UAV itself, GCSs, and other related systems will behave in safe, and reliable manner during operations. In this context, "privacy" refers to protecting private data associated with such operations against unauthorized access or disclosure. Recently, trust has been considered as an alternative criterion for ensuring the safety of UAVs. Barka et al. (2019) pro-

posed an approach based on blockchain and Bayesian inference algorithm to ensure the security of UAVs and trust management between UAVs and their corresponding GCSs. Singh and Verma (2018a) proposed a genetic algorithm-based trust model to ensure the security of UAVs. Firstly, in FANET, nodes were classified into different clusters and trust values of uncertain nodes went through risk assessment. Then based on risk assessment nodes were selected as benign or malicious. Singh and Verma (2018b) proposed a fuzzy logic-based trust model to classify nodes into three classes (good, neutral, bad). During experimental testing, the model was able to detect malicious UAVs with high accuracy in the presence of a large number of nodes. The model could not detect malicious UAVs (selfish or malicious nodes) when the number of real nodes in the network was low. Data transmitted over a wireless network, for example, UAV identification data, belongs to the class of personal data. The interception of this data has a direct effect on the violation of privacy of the UAV. As a solution, Brik, Ksentini and Bouaziz (2016) proposed a Federated Deep Learning (FDL) or distributed Deep Learning (DL) approach, where the basic idea is to keep raw data where it is generated while sending only users' local trained DL models to the centralized entity for aggregation. Su (2021) proposed a novel trust-based security scheme for 5G UAV communication networks. Trust scheme helps to manage the behavior of UAVs in the networks. Moreover, a trust evaluation scheme was developed for UAV communication systems. In this way, the malicious UAVs can be filtered out. Finally, detection scheme based on Q-learning technology was developed to protect the system from malicious attacks. Lv et al. (2021) implemented blockchain to protect the privacy of UAV big data. In addition, privacy protection scheme was proposed based on Number Theory Research Unit (NTRU) cryptographic algorithm. According to the performance evaluation results, the proposed privacy protection scheme is effective and has low computational cost.

Network security

Drones controlled by means of Wi-Fi use IEEE 802.11 standards. All the communication between the drone and GCS typically uses the Wi-Fi network, which is vulnerable to security breaches. The network formed by UAVs is called FANETs. The mobile nodes of this network are UAVs. In this network, UAVs communicate with each other for data delivery, positioning, accuracy, and collision avoidance. Javaid et al. (2012) defined a simple architecture of a UAV consisting of a combination of seven separate, but interdependent systems: Data Acquisition Module, Altitude and Heading Reference System, Navigation System, Control Module, Data Logging Module, Telemetry Module and the Communication System Module. Altawy and Youssef (2016) identified security threats against UAVs. Ouiazzane, Addou and Barramou (2022) proposed a

model based on the MuliAgent System and machine learning techniques to detect DoS cyberattacks targeting the networks of drones. The proposed approach has made it possible to detect DoS attacks using multi-agent systems and the machine learning DT algorithm, which was chosen after testing several machine learning algorithms. The model enables the detection of known and unknown DoS attacks in UAV networks with high accuracy and low false-positives and false-negatives rates. Lei et al. (2021) proposed Optimized Identity Authentication Protocol (ODIAP), a lightweight security authentication protocol for the UAV network. The proposed protocol has forward and backward security, which means that other information in the network will not be affected in the case of session key leakage. Also, the Chinese residual theorem was used in the protocol. By this method, the computational load was transferred from nodes to servers. According to security analysis, the proposed protocol can resist multiple attacks including replay attacks, DoS attacks, MITM attacks, brute force attacks, traceability attacks, and impersonation attacks.

The drone community forms a FANET using a collection of special purpose drones. Ensuring the security of FANETs is considered an important issue. Condomines, Zhang and Larrieu (2019) considered security issue of FANETs formed by UAVs. For this purpose, their study proposed an approach to detect security anomalies (DDoS) in UAV ad hoc network traffic. The proposed hybrid approach for intrusion detection performs spectral analysis of traffic and anomaly evaluation within UAV networks. Zhao et al. (2021) proposed a novel cluster-based secure routing scheme for FANETs. To make this possible, an Improved Artificial Bee Colony algorithm (IABC) was proposed. According to the results from this study, IABC performed better compared to other selected algorithms, such as Artificial Bee Colony Optimization (ABC), Particle Swarm Optimization (PSO) and Grey Wolf Optimization (GWO). Furthermore, optimal cluster head selection algorithm and a novel lightweight consensus algorithm was also proposed to make algorithm more resilient against cyberattacks.

Mairaj, Majumder and Javaid (2019) developed a game theory model, which simulates the interaction between the attacker and the countermeasures of its victim (UAV). The paper identifies a game-like situation, when a single UAV is under a DDoS attack, while a genuine UAVNet is trying to communicate with it. Two different cases of this common attack are simulated, namely, User Datagram Protocol (UDP) flooding, and Internet Control Message Protocol (ICMP) flooding (Ping flooding). In both cases, the intensity of these attacks is gauged by different choices made by the attacker and the target alike. Finally, the decisions related to the attacker and the victim are identified.

Authentication

The UAV must be authenticated before flying in safe airspace. However, traditional authentication methods based on dynamic keys or username/password combinations offer low security. Another certification method requires a large session key, which cannot meet the lightweight authentication requirements of the FANET. Gope, Millwood and Saxena (2021) proposed a novel anonymous authentication scheme for RFID enabled UAV applications using Physically Unclonable Functions.

One of the mechanisms to prevent GPS spoofing attacks is to implement the authentication of GPS signals. Here the main direction of thrust is to strengthen the authentication by traditional cryptographic methods. However, this is considered to be a very complex issue and requires introduction of changes in the infrastructure of the satellite system.

Jain et al. (2022) present an artificial intelligence based UAV-borne secure communication with classification (AIUAV-SCC) framework for an Industry 5.0 environment. The proposed AIUAV-SCC model involves two major phases, namely image steganography based secure communication and DL based classification. At first, with discrete wavelet transformation, the image steganography method is developed, then for the optimal pixel selection quantum bacterial colony optimization is applied, and finally encryption is provided. Secondly, for the classification of UAV images the Bayesian optimization is applied. This model is referred to by the authors as SqueezeNet. By the use of Bayesian optimization the parameters of the SqueezeNet are optimally tuned.

Safavat and Rawat (2021) proposed a modified Elliptic Curve Cryptography (ECC) based lightweight identity authentication method, which consists of two main steps, i.e., i) the Certificate Authority (CA) which maps UAV's unique identifier information with cryptographic keys using the ECC algorithm; ii) detection of malicious UAV using received periodic status information of UAVs. These steps are supposed to make sure no malicious UAVs are present in the FANET.

UAV system resilience

UAV system resilience is achieved when it can continue its dedicated mission despite encountering trouble. Trouble may arise from various factors such as sensor failures, cyberattacks, environmental conditions, communication interruptions, etc. Ensuring resilience in the UAV system is crucial for preventing the undesirable situations.

He et al. (2021) proposed a method to maintain UAVs' trajectory during an attack. The proposed path planning method is based on Pontryagin's max-

imum principle. Chen et al. (2019) proposed a DoS attack tolerant framework named ContainerDrone. The ContainerDrone framework is designed to protect UAV resources, such as the central processing unit (CPU), memory, and communication channel, from DoS attacks. The developed framework is based on Linux containers. Pengtao et al. (2022) proposed a model to ensure the resilience of UAVs in the form of a swarm. In most cases, it becomes necessary to use a swarm of UAVs to perform any mission. UAVs in the form of a swarm continuously exchange information with each other. Any problem that occurs in information exchange (attack, malfunction) can lead to mission failure. To overcome this problem, the task of the failed UAV is transferred to other units. In some cases, this creates an additional load, which gives rise to the need to provide balance. In the article cited, the authors developed a model for ensuring this balance. Petrlík et al. (2020) proposed a method for autonomous control of UAVs in areas that are difficult to explore. The involvement of human resources in certain areas can be dangerous, especially during search and rescue operations. For situations like this, it is safer to use systems such as robots or UAVs in respective areas. This, in turn, requires the aforementioned systems to be extremely flexible and resilient. Considering all this, in the article cited, a two-dimensional (2D) localization technique was proposed. This was made possible by the use of LiDAR, IMU, and cameras in the UAV.

Detailed information regarding the characteristics, aims, and main scientific contributions of the selected methods analyzed in this paper's survey is provided in Table 1.

7. Countermeasures against cyberattacks on UAV

Abbaspour and Yen (2016) proposed an algorithm based on adaptive neural networks for detecting fault data injection attacks on UAV sensors. In this study, for the online tuning of the weights of the neural network, the embedded Kalman filter (EKF) was used. Moosbrugger, Rozier and Schumann (2017) identified security threats related to the communication channels, sensors, and software. For performing dynamic monitoring, threat detection, and security diagnostics on UAVs onboard, an approach named R2U2 was developed. In order to provide fast detection of attacks, a signal processing block consisting of moving average and Fast Fourier Transform algorithms was included in the R2U2 model. Hoang, Nguyen and Duong (2020) constructed a prediction model based on one-class support vector machines (OC-SVM) and k-means clustering algorithm to detect an eavesdropping attack on a UAV in the authentication stage.

A traditional GPS spoofing method uses a GPS generator to create a fake copy of the original signal. GPS spoofing can be produced also in another way.

Table 1. A literature review of UAV system cybersecurity

Reference	Proposed approach	Main contribution	Future directions	Used method
Madan, Banik and Bein (2019)	Modeling and risk analysis of threats to UAV	• An attack tree aimed at stealing the confidentiality of the data collected by the UAV is constructed.	• Improving the method to make the proposed approach applicable to UAVs to be deployed in cyber systems	STRIDE threat modeling and CVSS Risk analysis tools
Altawy and Youssef (2016)	Development of the three layered security architecture for UAV systems. In the architecture, to ensure security of various UAV components, several layers are involved: software-based services, hardware-based services, and physical security services.	• Study of security, privacy, and physical security aspects related to application of civilian drones in national airspace. • Attacks aimed at the capture of drones are studied, and security issues of UAVs analyzed. • Cyber-physical threats to the target components of the UAV are determined with their classification.	Identifying the risks posed by the integration of drones into the national airspace	

Moosbrugger, Rozier and Schumann (2017)	Identification of communication channel, sensor, and software related security threats of the UAV system.	• R2U2 approach proposed, which performs dynamic monitoring, threat detection, and security diagnostics in the UAVs onboard. • To ensure fast detection of attacks, R2U2 includes a signal processing block consisting of moving average and Fast Fourier Transform algorithms.	Reconsideration of the flight software related issues. Applying the proposed method to different types of aircraft.	Linear and metric temporal logic and Bayesian networks
Javaid et al. (2012)	Analysis and modeling of cyber security threats to UAS	• Various security threats to UAV system analyzed • Cyber threat modeling provided	Deeper analysis of some of these threats and use of mission information to model the threats more accurately.	ETSI threat assessment methodology
Bera, Das and Sutrala (2021)	Unauthorized UAV detection in the Internet of Drones (IoD) environment	• Blockchain-based access control model ACSUD-IoD proposed. • Through authenticated transactions collected at the Ground Station Server (GSS), the blocks are formed, verified, and added to the blockchain, which is then used for mining in the blockchain.		Practical Byzantine Fault Tolerance (PBFT)

Naeem et al. (2021)	Increasing the drone security and resilience against malicious actions of attackers by hiding the true 3D flight trajectories of the drone using the obfuscation method.	• The obfuscation concept for the 3D trajectory of the drone is developed. • A taxonomy of 3d obfuscation algorithms is given. • New obfuscation operators and their formal notations are proposed.	• Calculation of optimal obfuscation parameters, while addressing the safety, reliability and stage/service-specific privacy constraints in dense traffic scenarios, while modeling the system as a constraint satisfaction problem. • Robustness evaluation of the proposed obfuscation algorithms against different de-obfuscation attacks. • Performance analysis of hybrid operators under diverse use-case scenarios. • Design of novel operators offering reversible 3D obfuscation for trusted operators/nodes.	3D obfuscation method
Feng et al. (2020)	Hijacking detection of the drone, which uses INS and GPS data for trajectory.	• A two-stage GA-XGBoost model is developed to detect GPS spoofing attacks. • Parameters tuned with a genetic algorithm.	• Applying the model to different types of UAVs. • Development of attack prevention algorithm in addition to detection of UAV hijacking.	Genetic algorithm and XGBoost algorithm

Singh and Verma (2018b)	Classification of the UAV-related FANET network nodes, construction of fuzzy trust management technique for UAVs related FANETs.	• Fuzzy logic-based trust model to classify nodes into three classes (good, neutral, bad). • Using the Quality of Service (QoS) and social parameters (recommendation) of the network calculates the trust value of each node.	Extension of the fuzzy classification trust model for different weights of QoS parameters.	Fuzzy logic
Birnbaum et al. (2014)	Monitoring UAV behavior and detection of the attacks.	• Automatic detection of changes in UAV airframe dynamics indicative of mechanical degradation. • Automatic detection of changes in UAV flight control law indicative of cyber-attacks.		Recursive Least Squares

In this case, by installing malicious software on the GPS receiver, based on the received satellite signals, a different trajectory, different from the calculated trajectory, is produced. Psiaki and Humphreys (2016) analyzed the methods for detecting and mitigating GPS spoofing attacks. These methods include signal processing, encryption, drift analysis, and monitoring the Direction-of-Arrival (DoA) of the signals. Meurer et al. (2016) proposed GNSS spoofing detection based on DoA measurements. It is well known that real GNSS signals are transmitted from different locations by using satellites. But during GNSS spoofing, the attacker typically transmits signals from one source. Thus, determining the direction of the signal plays an important role for detecting the attacks. Manfredini, Motella and Dovis (2015) used Signal Quality Monitoring Technique (SQMT) to detect GNSS spoofing attacks. The implementation of SQMT makes it possible to detect signal distortions during an attack. In addition, a new metric is introduced, which can distinguish GNSS spoofing attacks and environmental factors. Abdullayeva and Valikhanli (2022) presented a GPS spoofing detection method based on CNN. Flight log files were used in the training process. As a result of the experimental verification, 99% detection accuracy was achieved.

The proposed methods for preventing GPS spoofing attacks on UAVs may sometimes be insufficient. Another solution for this problem is to use alternative navigation methods. Wu et al. (2013) proposed a vision-based and inertia-based navigation system to provide autonomous navigation of a drone. Shen et al. (2022) proposed a method based on LIDAR technology in an environment where GPS signals are not available. To make the method more convenient, joint use of LIDAR and inertial measuring devices is envisaged.

Other examples of UAV signals include telemetry data and video streams transmitted to a GCS. Spoofing of these types of signals can directly affect operator commands and cause the drone to crash. GCS verifies the authenticity of drone signals using the Message Authentication Code (MAC). In addition, distance bounding protocols are used to determine the proximity of the source of the received signals and compare them with the last known position of the UAV.

All external sensors affecting the drone, such as radar, infrared and electro-optical sensors, can be manipulated. This kind of attack aims to destabilize the UAV and break the secure control by injecting fake entries into the flight controller by compromising a set of sensors (Mo and Sinopoli, 2010). Son et al. (2015) demonstrated the loss of control and crash of the drone due to altering of the gyroscope output data by interfering with the UAV's resonant frequency.

Fotohi (2020) proposed an approach called cyber security threat immune scheme to detect Wormhole, Black hole, Gray hole, and Fake Information Dissemination attacks on UAS by applying a human immune system based algo-

rithm. Data injection rate, message modified rate features were used to detect the abovementioned attacks.

Alladi et al. (2020), Aggarwal et al. (2019), Kuzmin and Znak (2018) investigated the possibilities of application of blockchain technology in the protection of UAV communication channels, and in the protection of UAV-type data, such as UAV identifier, flight route control, sensor data, and flying schedule.

8. UAV related datasets for research purposes

To detect and mitigate cyberattacks that target UAV systems, it is necessary to have diverse information pertaining to this field, for purposes of analysis, as well as testing and verification of the approaches proposed. That is why several datasets were created and made available for this purpose. We would like to mention here the following ones:

- UAV attack dataset (Whelan et al., 2020). This dataset consists of logs from a benign flight as well as one where the UAV experiences GPS spoofing and jamming attacks. The dataset contains both simulated and real GPS spoofing/jamming attacks.
- Malicious UAVs Detection dataset (Jamil, 2020). The dataset contains image and sound files for various flying vehicles including UAVs.
- Drone identification and tracking (Street, 2021). This dataset consists of data gathered from radar and radio direction finding sensors. The dataset also consists of log files, giving the exact tracks over which each UAV flew. Radar data timestamps can be correlated with log file timestamps to test the accuracy of radar data.
- DroneDetect Dataset: A Radio Frequency dataset of Unmanned Aerial System (UAS) Signals for Machine Learning Detection & Classification (Swinney and Woods, 2021). This dataset contains 7 different models of Unmanned Aerial Systems (UAS). The applied models are DJI Mavic 2 Air S, DJI Mavic Pro, DJI Mavic Pro 2, DJI Inspire 2, DJI Mavic Mini, DJI Phantom 4 and the Parrot Disco. Recordings were collected using a Nuand BladeRF SDR and open-source software GNURadio.
- Unmanned Aerial Vehicle (UAV) Intrusion Detection Datasets (Zhao et al., 2018). The datasets contain encrypted WiFi traffic data records of the UAVs. Those UAVs are Parrot Bebop 1, DBPower UDI, and DJI Spark. By monitoring traffic data, it is possible to detect whether the current traffic is from a UAV or not. Moreover, datasets contain data for both traffic modes: bidirectional-flow mode and unidirectional-flow mode;
- AirLab Failure and Anomaly (ALFA) Dataset (Keipour, Mousaei and Schere, 2020). ALFA dataset includes the data collected from multiple autonomous flights for failure detection and anomaly detection. There are

four collections of data available in datasets: processed data, raw bag files, telemetry logs, and dataflash logs. For dataset collection, the Carbon-Z T-28 fixed-wing UAV was used.

- Cyber-Physical Dataset for UAVs Under Normal Operations and Cyber-Attacks (Hassler, Mughal and Ismail, 2023). The dataset contains 4 types of attacks including DoS, replay, false data injection, and evil twin attacks. It also includes benign data.

9. Open issues

As a result of the survey study conducted in the field of cybersecurity of UAV systems, the following open issues that need to be resolved in the future have been identified.

1. Development of methods for the reconstruction of behavior of a drone before its crash. These methods can help in understanding the sequence of events leading up to a drone crash, enabling better design, operation, and safety measures for future flights.
2. Development of drone authentication methods. Device fingerprinting can be used for this purpose.
3. Development of methods of forensic analysis of drones. For investigation of the operation of the drone after the flight it is necessary to provide a forensic analysis. Forensic analysis of drones involves systematically examining a drone, its components, and related data to determine the causes of an incident, identify the operator, and gather evidence for legal or regulatory purposes. The structured approach to forensic analysis can involve malware detection, reverse engineering, log file analysis, trajectory analysis, failure mode analysis, etc. in order to thoroughly investigate drone incidents.
4. Deployment of UAV systems over an Infrastructure as a Service (IaaS) cloud. To enhance scalability, flexibility, and efficiency, it is important to integrate drone operations with cloud computing resources.
5. Development of a specific cybersecurity approach for UAVs. UAVs are treated as aircraft according to international, regional, and national aviation legislation. As there is currently no special cyber security approach for UAVs, national aviation cyber security approaches should be applied in the operation of UAVs (Pyzynski and Balcerzak, 2021).
6. Providing security and privacy at the level of FANETs. Ensuring security and privacy for UAVs within the context of FANETs involves implementing a comprehensive strategy that addresses the unique challenges and requirements of these networks. Security and privacy for UAVs in FANETs can involve issues related to encryption, message integrity, access control, anomaly detection, data anonymization, and authentication.

7. Secure trajectory planning. Involves the development of the safe trajectory generation methods that allow drones to reach their destination despite unknown attacks (Liu, Bianchin and Pasqualetti, 2020). Dai et al. (2020) proposed a two-stage architecture for quadrotor UAV to avoid obstacles automatically in unknown and unstructured environments. In the first phase of the architecture CNN provides a prediction. The model predicts the steering angle and the collision probability. In the second phase the model implements changes to the yaw angle of the UAV.
8. Implementing new methods for ensuring the autonomous secure navigation of UAVs. These involve a range of methods and technologies designed to protect the UAV's operational integrity and privacy while navigating. Dynamic path planning, obstacle avoidance, and anti-spoofing serve to achieve this goal.

10. Conclusion

In this paper, unmanned aerial systems are extensively analyzed, and general information about their components, various characteristics, used sensors, and architecture of UAS is provided. The issues related to the cybersecurity of UAVs are analyzed, main contributions, future directions, and used methods in the pertinent studies are investigated. The cybersecurity issues of UAVs are divided into attack detection, threat modeling, unauthorized UAV detection, data protection, trust and privacy, network security, authentication, and UAV system resilience categories. Definitely, UAVs are susceptible to cyberattacks, which are common to most cyber-physical systems. Success in cyberattacks can have serious consequences. In the paper, in addition to the detection methods of the cyberattacks, countermeasures against them are also surveyed. It should also be noted that although there are many methods for the cybersecurity of UAVs, some issues still remain a problem. Considering this point of view, the persisting cybersecurity problems of UAVs are identified also in this paper.

Funding

This work was supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (Contact No. 3 LR-AMEA).

References

Abbaspour, A. and Yen, K. K. (2016) Detection of Fault Data Injection Attack on UAV Using Adaptive Neural Network. *Procedia Computer Science*. **95**, 193−200. //doi.org/10.1016/j.procs.2016.09.312

Abdullayeva, F. and Ibrahimov, R. (2022) Neural network models for detection of unmanned aerial vehicles based on spectrogram analysis. *Problems of Information Technology*. **13**(2), 16–23. //doi.org/10.25045/jpit.v13.i2.02

Abdullayeva, F. and Valikhanli, O. (2022) Development of a method for detecting GPS spoofing attacks on unmanned aerial vehicles. *Problems of Information Technology*, **13**(1), 3–8. //doi.org/10.25045/jpit.v13.i1.01

Aggarwal, S., Shojafar, M., Kumar, N. and Conti, M. (2019) A new secure data dissemination model in Internet of drones. *Proc. of the IEEE International Conference on Communications*. IEEE, 1−6. //doi.org/10.1109/ICC.2019.8761372

Alladi, T., Chamola, V., Sahu, N. and Guizani, M. (2020) Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications*. **23**, 100249. //doi.org/10.1016/j.vehcom.2020.100249

Almulhem, A. (2020) Threat modeling of a multi-UAV system. *Transportation Research Part A: Policy and Practice*. **142**, 290−295. //doi.org/10.1016/j.tra.2020.11.004

Altawy, R. and Youssef, A. M. (2016) Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. *ACM Transactions on Cyber-Physical Systems*. **1**(2), 1−25. //doi.org/10.1145/3001836

Bada, M., Boubiche, D., Lagraa, N., Kerrache, C., Imran, M. and Shoaib, M. (2021) A policy-based solution for the detection of colluding GPS-Spoofing attacks in FANETs. *Transportation Research Part A: Policy And Practice*. **149**, 300-318. //doi.org/10.1016/j.tra.2021.04.022

Balamurugan, G., Valarmathi, J. and Naidu, V. P. S. (2016) Survey on UAV navigation in GPS denied environments. *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*. IEEE, 198−204. //doi.org/10.1109/SCOPES.2016.7955787

Barka, E., Kerrache, C. A., Benkraouda, H., Shuaib, K., Ahmad, F. and Kurugollu, F. (2019) Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure. *Transactions on Emerging Telecommunications Technologies*. **33**(8), pp. 1−10. //doi.org/10.1002/ett.3706

Bayraktar, S. and Feron, E. (2009) Experiments with small unmanned helicopter nose-up landings. *Journal of Guidance, Control, and Dynamics: a publication of the American Institute of Aeronautics and Astronautics devoted to the technology of dynamics and control*. **32**(1), 332–337. //doi.org/10.2514/1.36470

Bera, B., Das, A. K. and Sutrala, A. K. (2021) Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment. *Computer Communications*. **166**, 91−109. //doi.org/10.1016/j.comcom.2020.12.005

Birnbaum, Z., Dolgikh, A., Skormin, V., O'Brien, E. and Muller, D. (2014) Unmanned Aerial Vehicle Security Using Recursive Parameter Estimation. *Proc. of the IEEE International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 692−702. //doi.org/10.1109/ICUAS.2014.6842314

Brik, B., Ksentini, A. and Bouaziz, M. (2016) Federated Learning for UAVs-Enabled Wireless Networks: Use Cases, Challenges, and Open Problems. *IEEE Access*. **8**, 1−10. //doi.org/10.1109/ACCESS.2020.2981430

Ch, R., Srivastava, G., Reddy Gadekallu, T., Maddikunta, P. K. R. and Bhattacharya, S. (2020) Security and privacy of UAV data using blockchain technology. *Journal of Information Security and Applications*. **55**, 102670. //doi.org/10.1016/j.jisa.2020.102670

Chamola, V., Kotesh, P., Agarwal, A., Naren, N., Gupta, N. and Guizani, M. (2021) A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques. *Ad Hoc Networks*. **111**, 102324. //doi.org/10.1016/j.adhoc.2020.102324

Chen, J., Feng, Z., Wen, J., Liu, B. and Sha, L. (2019) A Container-based DoS Attack-Resilient Control Framework for Real-Time UAV Systems. *Proc. of the IEEE Europe Conference & Exhibition (DATE) on Design, Automation & Test*. IEEE, 1216−1221. //doi.org/10.23919/DATE.2019.8714888

Chriki, A., Touati, H., Snoussi, H. and Kamoun, F. (2019) FANET: Communication, mobility models and security issues. *Computer Networks*. **163**, 106877. //doi.org/10.1016/j.comnet.2019.106877

Condomines, J., Zhang, R. and Larrieu, N. (2019) Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation. *Ad Hoc Networks*. **90**, 101759. //doi.org/10.1016/j.adhoc.2018.09.004

Constantinides, C. and Parkinson, P. (2008) Security challenges in UAV development. *Proc. of the IEEE/AIAA Digital Avionics Systems Conference*. IEEE, 1−8. //doi.org/10.1109/DASC.2008.4702757

Cyber Security Research Alliance and NIST (2013) Designed-in Cyber Security for Cyber-Physical Systems. *Workshop Report*. NIST.

Dai, X., Mao Y., Huang T., Qin N., Huang D. and Li Y. (2020) Automatic obstacle avoidance of quadrotor UAV via CNN-based learning. *Neurocomputing*. **402**, 346–358. //doi.org/10.1016/j.neucom.2020.04.020

Dang, Y., Benzaid, C., Taleb, T., Yang, B. and Shen, Y. (2022) Transfer Learning based GPS Spoofing Detection for Cellular-Connected UAVs. *International Wireless Communications And Mobile Computing (IWCMC)*. IEEE. //doi.org/10.1109/iwcmc55113.2022.9824124

Dursun, M. and Çuhadar, İ. (2018) Risk based multi criteria decision making for secure image transfer between unmanned air vehicle and ground

control station. *Reliability Engineering & System Safety*. **178**, 31−39. //doi.org/10.1016/j.ress.2018.05.011

Feng, Z., Guan, N., Lv, M., Liu, W., Deng, Q., Liu, X. and Yi, W. (2020) Efficient drone hijacking detection using Two-Step GA-XGBoost. *Journal of Systems Architecture*. **103**, 1−30. //doi.org/10.1016/j.sysarc.2019.101694

Fotohi, R. (2020) Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system. *Reliability Engineering & System Safety*. **193**, 106675. //doi.org/10.1016/j.ress.2019.106675

Gharibi, M., Boutaba, R. and Waslander, S. L. (2016) Internet of Drones. *IEEE Access*. **4**, 1148− 1162. //doi.org/10.1109/ACCESS.2016.2537208

Gope, P., Millwood, O. and Saxena, N. (2021) A provably secure authentication scheme for RFID-enabled UAV applications. *Computer Communications*. 2021, **166**, 19−25. //doi.org/10.1016/j.comcom.2020.11.009

Greco, C., Pace, P., Basagni, S. and Fortino, G. (2021) Jamming detection at the edge of drone networks using Multi-layer Perceptrons and Decision Trees. *Applied Soft Computing*. **111**, 107806. //doi.org/10.1016/j.asoc.2021.107806

Gu, Y., Yu, X., Guo, K., Qiaoa, J. and Guo, L. (2021) Detection, estimation, and compensation of false data injection attack for UAVs. *Information Sciences*. **546**, 723−741. //doi.org/10.1016/j.ins.2020.08.055

Haider, M., Ahmed, I. and Rawat, D. B. (2022) Cyber Threats and Cybersecurity Reassessed in UAV-assisted Cyber Physical Systems. *Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE. 222-227. //doi.org/10.1109/icufn55119.2022.9829584

Hartmann, K. and Steup, C. (2013) The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment. *Proc. of the 5th IEEE International Conference on Cyber Conflict*. IEEE, 1−23.

Hassler, S. H., Mughal, U. M. and Ismail, M. I. (2023) Cyber-Physical Dataset for UAVs Under Normal Operations and Cyber-Attacks [Dataset]. *IEEE DataPort*. Available at: https://ieee-dataport.org/documents/cyber-physical-dataset-uavs-under-normal-operations-and-cyber-attacks (Accessed: August 28, 2024)

He, D., Chan, S. and Guizani, M. (2017) Communication security of unmanned aerial vehicles. *IEEE wireless communications*. **24**(4), 134–139. //doi.org/10.1109/mwc.2016.1600073wc

He, J., Gong, X., Cui, Y. and Huang, T. (2021) Resilient Path Planning of UAVs against Covert Attacks on UWB Sensors. *Robotics*. 1−9. //doi.org/10.48550/arXiv.2102.11696

Hoang, T. M., Nguyen, N. M. and Duong, T. Q. (2020) Detection of Eavesdropping Attack in UAV-aided Wireless Systems: Unsupervised

Learning with One-Class SVM and K-means Clustering. *IEEE Wireless Communications Letters*. **9**(2), 139−142. //doi.org/10.1109/LWC.2019.2945022

Hossein Motlagh, N., Taleb, T. and Arouk, O. (2016) Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives. *IEEE internet of things journal*. **3**(6), 899–922. //doi.org/10.1109/jiot.2016.2612119

Huang, K. and Wang, H. (2018) Combating the control signal spoofing attack in UAV systems. *IEEE Transactions on Vehicular Technology*. **67**(8), 7769−7773. //doi.org/10.1109/TVT.2018.2830345

Hussain, S., Kamal, A., Ahmad, S., Rasool, G. and Iqbal, S. (2014) Threat modeling methodologies: A survey. *Sci. Int.* **26**(4), 1607−1609.

Jain, D. K., Li, Y., Er, M. J., Xin, Q., Gupta, D. and Shankar, K. (2022) Enabling Unmanned Aerial Vehicle Borne Secure Communication with Classification Framework for Industry 5.0. *IEEE Transactions on Industrial Informatics*. **18**(8), 5477−5484. //doi.org/10.1109/tii.2021.3125732.

Jamil, S. (2020) Malicious UAVs Detection [Dataset]. *Kaggle*. Available at: https://www.kaggle.com/datasets/sonain/malicious-uavs-detection (Accessed: August 28, 2024)

Javaid, A. Y., Sun, W., Devabhaktuni, V. K. and Alam, M. (2012) Cyber security threat analysis and modeling of an unmanned aerial vehicle system. *Proc. of the IEEE Conference on Technologies for Homeland Security*. IEEE. 585−590. //doi.org/10.1109/THS.2012.6459914

Johnson, P., Lagerström, R., Ekstedt, M. and Franke, U. (2018) Can the common vulnerability scoring system be trusted? A Bayesian analysis. *IEEE Transactions on Dependable Secure Computing*. **15**, 1002−1015. //doi.org/10.1109/TDSC.2016.2644614

Keipour, A., Mousaei, M. and Schere, S. (2020) AirLab Failure and Anomaly (ALFA) Dataset [Dataset]. *TheAirLab*. Available at: https://theairlab.org/alfa-dataset/ (Accessed: August 28, 2024)

Khaitan, S. K. and McCalley, J. D. (2015) Design Techniques and Applications of Cyberphysical Systems: A Survey. *IEEE Systems Journal*. **9**(2), 350-365. //doi.org/10.1109/JSYST.2014.2322503

Khan, R., McLaughlin, K., Laverty, D. and Sezer, S. (2017) STRIDE-based threat modeling for cyber-physical systems. *Proc. of the IEEE PES Innovative Smart Grid Technologies Conference Europe*. IEEE. //doi.org/10.1109/ISGTEurope.2017.8260283

Kordy, B., Piètre-Cambacédès, L. and Schweitzer, P. (2014) DAG-based attack and defense modeling: Don't miss the forest for the attack trees. *Computer Science Review*. **13-14**, 1−38. //doi.org/10.1016/j.cosrev.2014.07.001

Kuzmin, A. and Znak, E. (2018) Blockchain-base structures for a secure and operate net-work of semi-autonomous unmanned aerial vehicles. *Proc. of the IEEE International Conference on Service Operations and Logistics, and Informatics*. IEEE, 32−37. //doi.org/10.1109/SOLI.2018.8476785

Laricchia, F. (2023) Drone market size worldwide in selected years from 2021 to 2030. *Statista*. Available at: https://www.statista.com/statistics/1234521/worldwide-drone-market/ (Accessed: November 17, 2023)

Lei, Y., Zeng, L., Li, Y., Wang, M. and Qin, H. (2021) A Lightweight Authentication Protocol for UAV Networks Based on Security and Computational Resource Optimization. *IEEE Access*. **9**, 53769-53785. //doi.org/10.1109/access.2021.3070683

Liu, Y. C., Bianchin, G. and Pasqualetti, F. (2020) Secure trajectory planning against undetectable spoofing attacks. *Automatica*. **112**, 108655. //doi.org/10.1016/j.automatica.2019.108655

Lund, M. S., Solhaug, B. and Stølen, K. (2011) *Model-Driven Risk Analysis: the CORAS Approach*. Springer, Berlin-Heidelberg.

Lv, Z., Qiao, L., Hossain, M. and Choi, B. (2021) Analysis of Using Blockchain to Protect the Privacy of Drone Big Data. *IEEE Network*. **35**(1), 44-49. //doi.org/10.1109/mnet.011.2000154

Ly, B. and Ly, R. (2021) Cybersecurity in unmanned aerial vehicles UAVs. *Journal of Cyber Security Technology*. **5**(2), 120−137. //doi.org/10.1080/23742917.2020.1846307

Madan, B. B., Banik, M. and Bein, D. (2019) Securing unmanned autonomous systems from cyber threats. *The Journal of Defense Modeling and Simulation Applications Methodology Technology*. **16**(2), 119–136. //doi.org/10.1177/1548512916628335

Mairaj, A., Majumder, S. and Javaid, A.Y. (2019) Game Theoretic Strategies for an Unmanned Aerial Vehicle Network Host Under DDoS Attack. *Proc. of the IEEE International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 1-9. //doi.org/10.1109/ICUAS.2019.8797939

Manfredini, E. G., Motella, B. and Dovis, F. (2015) Signal Quality Monitoring for Discrimination between Spoofing and Environmental Effects, Based on Multidimensional Ratio Metric Tests. *Proc. of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation*. IOS, 3100−3106.

Meurer, M., Konovaltsev, A., Appel, M. and Cuntz, M. (2016) Direction-of-Arrival Assisted Sequential Spoofing Detection and Mitigation. *Proc. of the International Technical Meeting of The Institute of Navigation*. IOS, 181−192. //doi.org/10.33012/2016.13395

Mo, Y. and Sinopoli, B. (2010) False data injection attacks in control systems. Proc. of the *First Workshop on Secure Control Systems*, ACM, 1−7.

Moosbrugger, P., Rozier, K. Y. and Schumann, J. (2017) R2U2: monitoring and diagnosis of security threats for unmanned aerial systems. *Formal Methods in System Design*. **51**, 31−61. //doi.org/10.1007/s10703-017-0275-x

Naeem, F., Mohsin, M., Rauf, U. and Khan, L. A. (2021) Formal approach to thwart against drone discovery attacks: A taxonomy of novel 3D obfuscation mechanisms. *Future Generation Computer Systems*. **115**, 374−386. //doi.org/10.1016/j.future.2020.09.001

Nunez, J., Tran, V. and Katangur, A. (2019) Protecting the Unmanned Aerial Vehicle from Cyberattacks. *Proc. of the International Conference on Security and Management*. CSREA, 154−157.

Ouiazzane, S., Addou, M. and Barramou, F. (2022) A Multiagent and Machine Learning Based Denial of Service Intrusion Detection System for Drone Networks. *Geospatial Intelligence, Advances in Science, Technology & Innovation*. Cham: Springer International Publishing, 51−65. //doi.org/10.1007/978-3-030-80458-9_5

Pengtao, Z., Tao, W., Runhua, C., Zi, L. and Jiwei, X. (2022) UAV Swarm Resilience Assessment Considering Load Balancing. *Frontiers in Physics*. **10**, 1−10. //doi.org/10.3389/fphy.2022.821321

Petrlík, M., Báča, T., Heřt, D., Vrba, M., Krajník, T. and Saska, M. (2020) A Robust UAV System for Operations in a Constrained Environment, *IEEE Robotics and Automation Letters*. **5**(2), 2169−2176. //doi.org/10.1109/LRA.2020.2970980

Półka, M., Ptak, S. and Kuziora, Ł. (2017) The use of UAV's for search and rescue operations. *Procedia engineering*. **192**, 748–752. //doi.org/10.1016/j.proeng.2017.06.129.

Psiaki, M. L. and Humphreys, T. E. (2016) GNSS Spoofing and Detection. *Proceedings of the IEEE*. **104**(6), 1258-1270. //doi.org/10.1109/JPROC.2016.2526658

Pyzynski, M. and Balcerzak, T. (2021) Cybersecurity of the Unmanned Aircraft System (UAS). *Journal of Intelligent & Robotic Systems*. **102**, 1−13. //doi.org/10.1007/s10846-021-01399-x

Rodday, N. M., Schmidt, R. O. and Pras, A. (2016) Exploring Security Vulnerabilities of Unmanned Aerial Vehicles. *IEEE/IFIP Network Operations and Management Symposium*. IEEE, 993−994. //doi.org/10.1109/NOMS.2016.7502939

RT (2013) SkyJack: Hacker-drone that can wirelessly hijack & control other drones. *RT International*. Available at: http://rt.com/news/hacker-drone-aircraft-parrot-704/ (Accessed: November 21, 2022)

Safavat, S. and Rawat, D.B. (2021) Securing Unmanned Aerial Vehicular Networks Using Modified Elliptic Curve Cryptography. *Proc. of*

the IEEE Military Communications Conference (MILCOM). IEEE, 1-7. //doi.org/10.1109/MILCOM52596.2021.9652982

Salamh, F. E., Karabiyik, U., Rogers, M. and Al-Hazemi, F. (2019) Drone Disrupted Denial of Service Attack (3DOS): Towards an Incident Response and Forensic Analysis of Remotely Piloted Aerial Systems (RPASs). *Proc. IEEE 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 704−710. //doi.org/10.1109/IWCMC.2019.8766538

Shafique, A., Mehmood, A. and Elhadef, M. (2021) Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles. *IEEE Access*. **9**, 46927-46948. //doi.org/10.1109/access.2021.3066778

Sharifi-Tehrani, O., Sabahi, M. and Danaee, M. (2021) GNSS jamming detection of UAV ground control station using random matrix theory. *ICT Express*. **7**(2), 239-243. //doi.org/10.1016/j.icte.2020.10.001

Shen, H., Zong, Q., Lu, H., Zhang, X., Tian, B. and He, L. (2022) A distributed approach for lidar-based relative state estimation of multi-UAV in GPS-denied environments. *Chinese Journal of Aeronautics*. **35**(1), 59−69. //doi.org/10.1016/j.cja.2021.04.021

Shepard, D. P., Bhatti, J. A., Humphreys, T. E. and Fansler, A. A. (2012) Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, 3591-3605.

Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P. and Woody, C. (2018) Threat modeling: a summary of available methods. *Software Engineering Institute, Carnegie Mellon University*. 1-26.

Singh, K. and Verma, A. K. (2018a) A trust model for effective cooperation in flying ad hoc networks using genetic algorithm. *Proc. of the International Conference on Communication and Signal Processing*. IEEE. 491−495. //doi.org/10.1109/ICCSP.2018.8524558

Singh, K. and Verma, A. K. (2018b) FCTM: A novel fuzzy classification trust model for enhancing reliability in flying ad hoc networks (FANETs). *Ad Hoc and Sensor Wireless Networks*. **40**, 23-47.

Singhal, A. and Banati, H. (2011) Fuzzy logic approach for threat prioritization in agile security framework using the DREAD model. *International Journal of Computer Science Issues*. **8**(4), 182−190. //doi.org/10.48550/arXiv.1312.6836

Son, Y., Shin, H., Kim, D., Park, Y., Noh, J., Choi, K., Choi, J. and Kim, Y. (2015) Rocking drones with intentional sound noise on gyroscopic sensors. *Proc. of the 24th USENIX Conference on Security Symposium*. 881−896.

Street, M. (2021) Drone identification and tracking [Dataset]. *Kaggle*. Available at: https://www.kaggle.com/c/icmcis-drone-tracking/ (Accessed: August 28, 2024)

Su, Y. (2021) A Trust Based Scheme to Protect 5G UAV Communication Networks. *IEEE Open Journal Of The Computer Society*. **2**, 300-307. //doi.org/10.1109/ojcs.2021.3058001

Swinney, C. J. and Woods, J. C. (2021) DroneDetect dataset: A radio frequency dataset of unmanned aerial system (UAS) signals for machine learning detection classification [Dataset]. *IEEE DataPort*. Available at: https://ieee-dataport.org/open-access/dronedetect-dataset-radio-frequency-dataset-unmanned-aerial-system-uas-signals-machine (Accessed: August 28, 2024)

Valikhanli, O. (2023) Analysis of various techniques for ensuring autonomous navigation of unmanned Aerial Vehicles. *Problems of Information Technology*. **14**(1), 8–14. //doi.org/10.25045/jpit.v14.i1.02

Vattapparamban, E., Güvenç, I., Yurekli, A. I., Akkaya, K. and Uluağaç, S. (2016) Drones for smart cities: Issues in cybersecurity, privacy, and public safety. *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 216-221. //doi.org/10.1109/IWCMC.2016.7577060

Whelan, J., Sangarapillai, T., Minawi, O., Almehmadi, A. and El-Khatib, K. (2020) UAV attack dataset [Dataset]. *IEEE DataPort*. Available at: https://ieee-dataport.org/open-access/uav-attack-dataset (Accessed: August 28, 2024)

Wu, A. D., Johnson, E. N., Kaess, M., Dellaert, F. and Chowdhary, G. (2013) Autonomous flight in GPS-denied environments using monocular vision and inertial sensors. *Journal of Aerospace Information Systems*. **10**(4), 172−186. //doi.org/10.2514/1.I010023

Xiao, L., Lu, X., Xu, D., Tang, Y., Wang, L. and Zhuang, W. (2018) UAV relay in VANETs against smart jamming with reinforcement learning. *IEEE Transactions on Vehicular Technology*. **67**(5), 4087−4097. //doi.org/10.1109/TVT.2018.2789466

Yaacoub, J. P., Noura, H., Salman, O. and Chehab, A. (2020) Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*. **11**, 100218. //doi.org/10.1016/j.iot.2020.100218

Yağdereli, E., Gemci, C. and Aktaş, A. Z. (2015) A study on cybersecurity of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation Applications Methodology Technology*. **12**(4), 369–381. //doi.org/10.1177/1548512915575803

Zhao, L., Alipour-Fanid, A., Slawski, M. and Zeng, K. (2018) Unmanned Aerial Vehicle (UAV) Intrusion Detection Datasets [Dataset].

George Mason University. Available at: http://mason.gmu.edu/˜lzhao9/materials/data/UAV/ (Accessed: August 28, 2024)

Zhao, L., Saif, M., Hawbani, A., Min, G., Peng, S. and Lin, N. (2021) A novel improved artificial bee colony and blockchain-based secure clustering routing scheme for FANET. *China Communications*. **18**(7), 103-116. //doi.org/10.23919/jcc.2021.07.009