2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH) | 978-1-6654-0973-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/SMARTTECH54121.2022.00048

Security Challenges for Drone Communications: Possible Threats, Attacks and Countermeasures

Moez Krichen
Al-Baha University
Al-Baha
Saudi Arabia
mkreishan@bu.edu.sa
ReDCAD Laboratory
University of Sfax
Sfax, Tunisia
moez.krichen@redcad.org

Wilfried Yves Hamilton Adoni
Engineering School
International University of Casablanca
Casablanca
Morocco
adoniwilfried@gmail.com

Alaeddine Mihoub
Department of Management Information Systems and Production Management
College of Business and Economics
Qassim University
P.O. Box: 6640, Buraidah: 51452, Saudi Arabia
a.mihoub@qu.edu.sa

Mohammed Y. Alzahrani
Al-Baha University
Al-Baha
Saudi Arabia
msawileh@bu.edu.sa

Tarik Nahhal
University of Hassan II of Casablanca
Casablanca
Morocco
t.nahhal@fsac.ac.ma

***Abstract*—The current development of drones and the prospects in this field have positive repercussions, in particular for employment and industrial development, with the key to growth and job creation possibilities. Drones have the ability to conduct operations in emergency situations, where human intervention is impossible or difficult. They could help save lives in humanitarian emergencies, nuclear accidents or natural disasters, etc. As with any technology, there are also risks that must be seriously considered by stakeholders, regulators, institutions and citizens, in order to prevent, minimize and avoid possible negative consequences of certain applications of this technology. In fact, drones today also present risks of cybersecurity breaches and malicious use. In this paper, we concentrate on security challenges related to the use of drones. More specifically, we give a short overview of the possible threats, attacks and countermeasures related to drone communications. The considered countermeasures are mainly based on the use of: Blockchain Technology, Machine Learning (ML) Techniques, Fog Computing and Software Defined Networks (SDN).**

***Index Terms*—Security, Drones, Communication, Attacks, Threats, Countermeasures, Blockchain, Machine Learning (ML), Fog Computing, Software Defined Network (SDN).**

I. Introduction

A drone [1] or Unmanned Aerial Vehicle (UAV) is an aircraft without passengers or pilots that can fly autonomously or be controlled remotely from the ground. The size of an aerial drone can range from a few centimeters for miniature models to several meters for specialized drones. The flight time ranges from a few minutes to over 40 hours for long endurance drones. The concept of the drone emerged during the First World War. Originally, the drone was a military target aircraft [2], [3]. Its development followed the rhythm of the great conflicts of the twentieth century. Drones are more economical while avoiding jeopardizing the lives of pilots and deploying ground troops, in particular for reconnaissance, surveillance and targeted attacks. Their use within armies and police forces has become predominant. In the civil sector, many fields (health [4], agriculture [5], environment [6], etc.) have seen drones give rise to new applications thanks to their ability to embed cameras, infrared cameras or environmental sensors. Several companies specializing in transport (DHL, UPS, Allship, La Poste) as well as the e-commerce giant Amazon are working on delivery drone concepts [7].

Recreational drones have experienced a significant boom from the 2010s with the arrival of miniaturized devices, affordable and manageable enough to be accessible to novices. Drones also have less well-known but more specialized applications that are neither commercial, nor hobby, nor military. When they have a built-in camera [8], they can be utilized for monitoring infrastructures in hard-to-access areas of livestock, ancient monuments, or forest fires. They may also include specialized sensors for geological surveys.

Not all of these categories of drones are safe. Only the military drone can be considered relatively safe. All others can be hijacked or misused, just like any other connected device. They can pose a threat to our privacy, cybersecurity and physical security [9]. Drones present several cyber threats. Non-military drones are relatively easy to take over. In 2017, a security expert built a device (called Icarus) which allowed him to tune the drone's communication frequencies [10]. The communication channels would jump every eleven milliseconds, but while waiting on a channel, Icarus could take advantage of those 11 milliseconds to hack the drone's encryption and hijack it. Small Raspberry Pi processors may be carried by even recreational drones [11]. They may be programmed to detect Wi-Fi signals. Ethical researchers have used these drones to test the safety of isolated infrastructure (like power plants), which can not be accessed directly from the Internet. If the researchers succeed, you can be sure that the hackers too. The threat drones pose to our physical security [12] ranges from accidental damage and targeted attacks to miscalculations. An uncontrollable drone can cause accidents. It could be a legitimate user or a hacker losing control, software or hardware malfunctions within the devices. Whatever the causes, drone that fall from the sky on a human beings cause critical damages, and even more if it is large [13].

In this paper, we are interested in security challenges related to the use of drones. In particular, we aim to identify the main

978-1-6654-0973-5/22/$31.00 ©2022 IEEE
DOI 10.1109/SMARTTECH54121.2022.00048

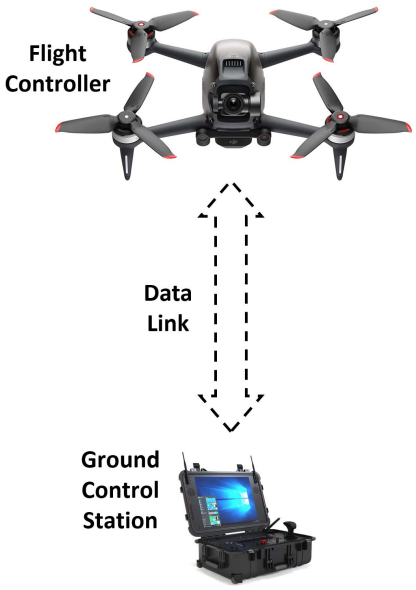

Fig. 1. Drone Architecture.

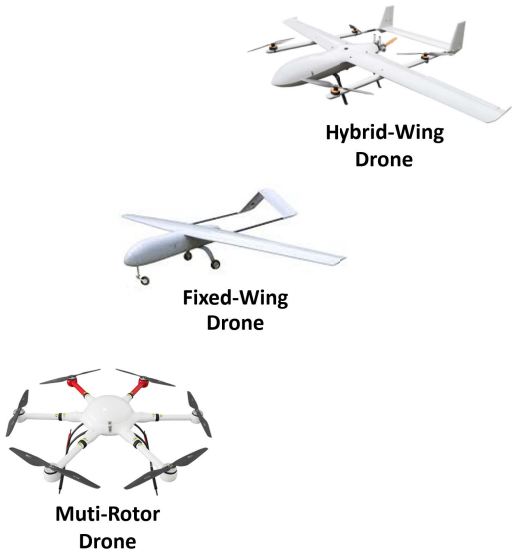

Fig. 2. Different Types of Drones.

types of security attacks which may be carried out against drones and respectively the different countermeasures that may be adopted for dealing with these threats and attacks. The considered countermeasures are based on: Blockchain [14], [15], Machine Learning (ML) [16], Fog Computing [17] and Software Defined Networks (SDN) [18].

Our article is organized as follows. In Section II, we recall some preliminaries about the Drone Technology. In Section III, we identify the main security vulnerabilities of drones. Section IV enumerates the main possible attacks against drones. Section V presents corresponding countermeasures. Finally, Section VI concludes the paper and proposes some future possible extensions.

II. Prelminaries about Drones

In this section, we propose a brief overview about the Drone Technology [19]: architecture, different types of communications, different types of drones and possible control methods.

A. Architecture

As shown in Figure 1, any drone architecture is generally made up of three basic components, namely: Flight Controller, Ground Control Station and Data Link.

- Flight Controller: it is considered as the main processing unit of the drone.
- Ground Control Station: It supplies human operators with the tools they need to remotely control and monitor drones during missions.
- Data Link: It is utilised to communicate and control data flow between the ground control station and the drone.

Drone communications are divided into four categories, namely: Drone-To-Ground Station, Drone-To-Network, Drone-To-Satellite and Drone-To-Drone.

- Drone-To-Ground Station: This sort of connection uses well-known and standardized communication protocols like Bluetooth and Wi-Fi. However, the majority of these sorts of communications are public and insecure, rendering them exposed to many types of attacks.
- Drone-To-Network: This method of communication allows users to select a network based on the level of security they require. Cellular communication may also be included. When such wireless communication networks are deployed, it is critical to keep them safe.
- Drone-To-Satellite: The GPS network uses this sort of communication to send real-time coordinates. This allows any drone to be summoned back to its original station if it wandered beyond the line of control. Satellite communications are thought to be secure and reliable. They do, however, come at a hefty price and demand a lot of maintenance [20].
- Drone-To-Drone: This form of communication has yet to be standardized. It can be thought of as a P2P (peer-to-peer) communication, making it subject to various P2P assaults [21].

B. Types of Drones and Control Methods

As illustrated in Figure 2, the exist three types of drones, namely: Multi-Rotor Drones, Fixed-Wing Drone and Hybrid-Wing Drone.

- Multi-Rotor Drone [22]: It is based on the notion of vertical take-off and landing. It is maneuvered with great precision and accuracy. Its mobility, on the other hand, is limited, and it consumes a lot of energy.
- Fixed-Wing Drone [23]: It has the ability to glide and travel at great speeds while transporting large cargoes. Its key benefit is that it is energy efficient. Because of its Horizontal Take-Off and Landing capability, it requires a

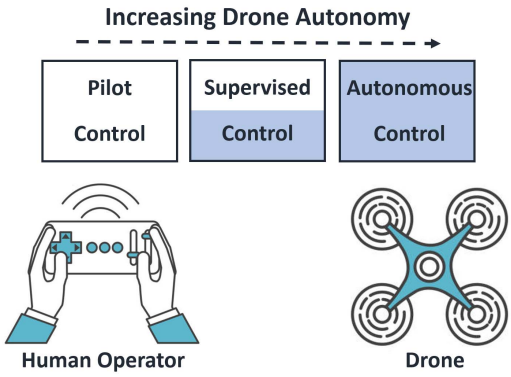

Fig. 3. Drone Autonomy Spectrum.

runway to take off and land. Another disadvantage is that it is unable to hover over fixed sites.

- Hybrid-Wing Drone [24]: It is a drone with both fixed and rotating wings that has lately entered the market. This sort of drone can quickly reach its objective by gliding through the air and hovering using four rotors.

As shown in Figure 3, Controlling drones can be divided into three types, namely: autonomous Control, supervised control and pilot control.

- Autonomous Control: In this case, the drone can make all of the necessary decisions to complete the task successfully without the need for human assistance [25].
- Supervised Control: This sort of control allows the drone to launch and complete a mission process on its own while still permitting for operator interaction if necessary.
- Pilot Control: All decisions are taken by a human remote manager in this situation.

III. Main Drones Security Vulnerabilities

Among the weaknesses of drones that can cause security problems, we cite the following points [26]:

- A drone's Flight Controller and Ground Control Station both have security vulnerabilities that could lead to cyber or physical attacks. Hardware failures, physical drone collisions, and hardware trojans [27] are all examples of hardware-level vulnerabilities and dangers.
- Drones are highly sensor-dependent gadgets [28]. As a result, they rely on sensor readings to function effectively. However, because these sensors handle sensitive data, a malevolent operator could use them to jeopardize the flight operation. Civil GPS transmissions, for example, are unauthenticated and unencrypted [29]. As a result, an adversary can take advantage of this flaw by imitating a GPS signal to fool the operator.
- Drone malware [30] can result in the loss of sensitive data as well as control of the operated drone system. An attacker with access to the drone's flight stack might theoretically shut down the drone system, resulting in a denial-of-service assault and disrupting the flight mission.

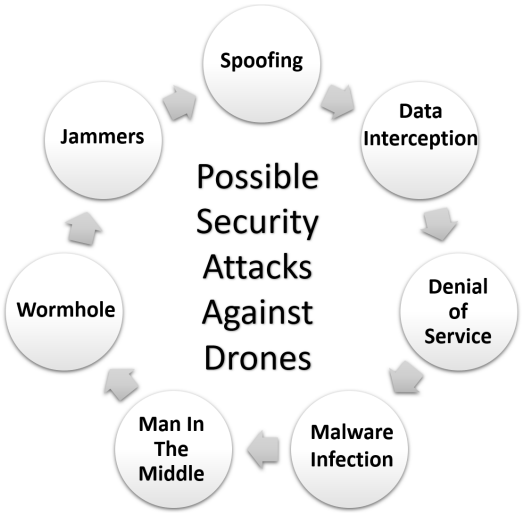

Fig. 4. Possible Security Attacks against Drones.

Incorporating such spyware into drones can jeopardize their privacy and security.

- Communication is an essential component of the drone system for flight control and data transfer. The majority of drones communicate with the ground control station via wifi [31]. The wireless communication network's complexity and dynamic nature may be a source of possible vulnerabilities and serious dangers.

IV. Different Types of Threats and Attacks

As illustrated in Figure 4, we consider the following possible types of attacks [32]:

- GPS Spoofing Attack [33]: is a type of assault in which a nearby radio transmitter is used to interfere with authentic GPS signals. The hacker could send no data at all or coordinates that are incorrect.
- Data Interception Attack [34]: is done using a packet sniffing software, which examines data packets as they travel over the network. The data acquired is forwarded to the hacker.
- Denial of Service Attack [35]: consists in sending an excessive number of requests that the drone cannot manage. The drone enters busy mode, preventing authorized users from accessing it. If a drone is assaulted, it will lose contact with its owner and may be unable to complete the task at hand.
- Malware Infection Attack [36]: is a type of security attack in which malware takes control of the victim's drone and does unlawful operations. Malicious software covers a wide range of assaults, including spyware, ransomware, control and command, and other.
- Man In The Middle Attack [37]: occurs when an attacker places himself in the middle of a discussion between a user and a system, either to spy or to mimic one of the participants, making it look as if a normal information flow is taking place.

- Wormhole Attack [38]: is one of the most common attacks in which an attacker node entraps packets from a single location in the network and tunnels them to another malicious node at a remote location.
- Jamming Attack [39]: is a type of Denial of Service attack in which one node obstructs other nodes from interacting by occupying the channel on which they are communicating.

V. Main Countermeasures for Enhancing Drones Communications Security

In this section, we will go through the four key new technologies that are being significantly used and investigated for making drone communications more reliable and secure.

A. Blockchain Technology for Enhancing Drones Communications Security

Blockchain [40] is a technique which allows to store data in a manner that it is hard or even impossible to alter, corrupt, or cheat it. Blockchain are digital logs of transactions which are replicated and shared across the blockchain's complete network of computers and devices. Every block on the chain contains a set of transactions, and each time new transactions occur on the blockchain, new corresponding records of them are added to all participants local ledgers. Distributed Ledger Technology (DLT) is a decentralized database which is managed by a large number of people.

Blockchain technology has the potential to set new standards in the drone business by reducing security issues. Even if a drone slips into the wrong hands, the data it contains will be safe because it is encoded. More specifically, blockchain technology may help to improve the security of drone communications on the following levels:

- Drones' real-time location can be updated using blockchain. Because the data on the blockchain that will be used is public, other drones will be able to see where other drones are, allowing them to avoid and prevent collisions entirely. Information on prohibited areas can also be updated in real time. Drones will be unable to enter restricted regions as a result of this.
- A blockchain-based identifying system will track the flight of registered drones and generate complaints that authorities can investigate further. All of this may be done without jeopardizing the privacy of the drone's owner. All information that is classified as confidential will be kept private.
- Blockchain distributed ledger technology can be used to furnish drones with cryptographic data. The data transmitted by drones will be secure since it will be encrypted. Drones can therefore be employed to complete sensitive missions and activities.

However as with many other application sectors, blockchain technology still faces several significant challenges, for instance:

- Only very restricted number of possible transactions per unit of time.
- Blockchains not being as scalable as their counterpart centralized systems.
- Blockchain technology using a lot of energy, which is inconvenient for drones.

B. Machine Learning Techniques for Enhancing Drones Communications Security

Machine Learning [41]–[44] is a branch of artificial intelligence (AI) that allows computers to learn and improve on their own without having to be explicitly coded. Machine learning is concerned with the creation of computer software that can read data and learn on their own without the need for human involvement, and to change their behavior accordingly. The study reported in [45] outlines the primary drone security challenges that have been researched in the literature, as well as the machine learning solutions that have been used to address them:

- Machine learning techniques are employed to reduce latency and increase the reliability of data that must be transferred to the cloud [46].
- Support Vector Machines (SVM) and Neural Networks are used to detect Denial of Service Attacks using Machine Learning-based models [47].
- A machine learning model based on Recurrent Neural Networks (RNN) and Convolution Neural Networks (CNN) was used for adversary detection andfor avoiding adversarial attacks [48].
- Machine learning techniques may be utilized in radar detection to solve a variety of identification and tracking issues that plague classic radar detection approaches [49].
- The use of machine learning methods to prevent privacy leaks in drone communications has recently been investigated as well [50].

C. Fog Computing Technology for Enhancing Drones Communications Security

Fog computing [51] is a distributed computing framework in which resources, such as data and programs, are placed in logical positions between the data source and the cloud. The goal is to deliver fundamental analytic services to the network edge, which will improve performance by bringing computing resources closer to where they are necessary and so boosting overall network performance and efficiency. Fog computing can also be used for security purposes, since it can split bandwidth flow and add multiple firewalls to a network for added protection. Next, we enumerate some examples about how fog computing may be used for enhancing drones communication security:

- For ensuring the confidentiality of data, heavy security and cryptographic processes (e.g., key generation and hashing) are delegated to more powerful nodes in the fog as proposed in [52].
- A system for intrusion detection and intrusion prevention and which allows to handle man-in-the-middle attacks at the fog layer was presented in [53].

- A fog-to-cloud computing system based on established military anti-drone technology for detecting jamming attacks GPS spoofing was presented in [54].
- A Fog Computing solution which allows to optimize the latency in drone communications was proposed in [68].

D. Software Defined Languages for Enhancing Drones Communications Security

A Software Defined Network (SDN) [55] is a network management strategy that allows for dynamic efficient network design to increase network performance. SDN was created to solve the fact that old networks' static architecture is decentralized and complex, whereas today's networks require more flexibility and ease of troubleshooting. By decoupling the forwarding of network packets from the routing process, SDN seeks to consolidate network intelligence in a single network component (controller machine).

Next, we list some applications of the SDN-Technology for strengthening drones communications security:

- A lightweight model based on the use of SDN controller for avoiding malfunctioning devices was presented in [56]. The SDN controller plays the role of authenticating the network devices requesting to join the network.
- In order to develop scalable DoS-attack resistant networks, an SDN-based protocol called NetFence was proposed in [57].
- A security model called Middlebox-Guard [58], which is based on software defined networks, regulates dataflows to ensure network efficiency and reduce network latency.
- A technique for detecting and mitigating Distributed DoS assaults in drones was presented in [59]. This technique is also capable of detecting the device that launched the assault in a short time.

VI. Conclusion

Drones are still in their infancy. Their capacities will develop over the coming decades [60]. Society and governmental institutions must be aware of the threats they present. Devices developed for noble purposes can be misused. For example, China has developed solar-powered drones which will be able to fly continuously [61]. If you integrate an ultra-powerful and modern camera and facial recognition technology into it, you get drones which may fly perpetually until it detects preprogrammed targets. A target can be found and automatically killed with a tiny warhead that does not require military-grade drones. Although it may appear to be science fiction, it is already possible. The only significant issue is that drones are not adequately regulated. No one has yet claimed the authority to govern them so that they do not pose a severe threat to society [62]. An interesting approach for future works related to the security of drones will be to adopt formal methods based on the use of sophisticated mathematical models in order to obtain rigorous results [63]–[65].

References

[1] N. S. Labib, M. R. Brust, G. Danoy, and P. Bouvry, "The rise of drones in internet of things: A survey on the evolution, prospects and challenges of unmanned aerial vehicles," *IEEE Access*, vol. 9, 2021.

[2] C. Candelmo, "Drones at war: The military use of unmanned aerial vehicles and international law," in *Use and Misuse of New Technologies*. Springer, 2019, pp. 93–112.

[3] G. Choudhary, V. Sharma, and I. You, "Sustainable and secure trajectories for the military internet of drones (iod) through an efficient medium access control (mac) protocol," *Computers & Electrical Engineering*, vol. 74, pp. 59–73, 2019.

[4] B. Hiebert, E. Nouvet, V. Jeyabalan, and L. Donelle, "The application of drones in healthcare and health-related services in north america: A scoping review," *Drones*, vol. 4, no. 3, p. 30, 2020.

[5] Y. Al-Mulla and A. Al-Ruehelli, "Use of drones and satellite images to assess the health of date palm trees," in *IGARSS 2020-2020 IEEE International Geoscience and Remote Sensing Symposium*. IEEE, 2020.

[6] Ö. Yildirim, K. Diepold, and R. A. Vural, "Decision process of autonomous drones for environmental monitoring," in *2019 IEEE International Symposium on INnovations in Intelligent SysTems and Applications (INISTA)*. IEEE, 2019, pp. 1–6.

[7] C. D. Burzichelli, "Delivery drones: Will amazon air see the national airspace," *Rutgers Computer & Tech. LJ*, vol. 42, p. 162, 2016.

[8] C. W. Chen, "Drones as internet of video things front-end sensors: challenges and opportunities," *Discover Internet of Things*, vol. 1, no. 1, pp. 1–12, 2021.

[9] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala, "Internet of drones security and privacy issues: Taxonomy and open challenges," *IEEE Access*, vol. 9, 2021.

[10] J. O'Malley, "Pirates of the skies," *Engineering & Technology*, vol. 12, no. 3, pp. 32–35, 2017.

[11] S. Benhadhria, M. Mansouri, A. Benkhlifa, I. Gharbi, and N. Jlili, "Vagadrone: Intelligent and fully automatic drone based on raspberry pi and android," *Applied Sciences*, vol. 11, no. 7, p. 3153, 2021.

[12] J. A. Johnson, M. R. Svach, and L. H. Brown, "Drone and other hobbyist aircraft injuries seen in us emergency departments, 2010–2017," *American journal of preventive medicine*, vol. 57, no. 6, pp. 826–829, 2019.

[13] C. H. Koh, K. Low, L. Li, Y. Zhao, C. Deng, S. K. Tan, Y. Chen, B. C. Yeap, and X. Li, "Weight threshold estimation of falling uavs (unmanned aerial vehicles) based on impact energy," *Transportation Research Part C: Emerging Technologies*, vol. 93, pp. 228–255, 2018.

[14] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in iot-enabled internet of drones deployment," *Computer Communications*, vol. 153, pp. 229–249, 2020.

[15] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, 2020.

[16] R. Gupta, A. Kumari, and S. Tanwar, "Fusion of blockchain and artificial intelligence for secure drone networking underlying 5g communications," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, p. e4176, 2021.

[17] M. Al-Khafajiy, T. Baker, A. Hussien, and A. Cotgrave, "Uav and fog computing for ioe-based systems: a case study on environment disasters prediction and recovery plans," in *Unmanned Aerial Vehicles in Smart Cities*. Springer, 2020, pp. 133–152.

[18] C. Pan, J. Yi, C. Yin, J. Yu, and X. Li, "Joint 3d uav placement and resource allocation in software-defined cellular networks with wireless backhaul," *IEEE Access*, vol. 7, pp. 104 279–104 293, 2019.

[19] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, 2020.

[20] S. Bhatnagar, L. Gill, S. Regan, S. Waldren, and B. Ghosh, "A nested drone-satellite approach to monitoring the ecological conditions of wetlands," *ISPRS Journal of Photogrammetry and Remote Sensing*, vol. 174, pp. 151–165, 2021.

[21] L. Wang, "Attacks against peer-to-peer networks and countermeasures," in *T-110.5290 Seminar on Network Security*. Citeseer, 2006, pp. 1–9.

[22] A. Bahabry, X. Wan, H. Ghazzai, G. Vesonder, and Y. Massoud, "Collision-free navigation and efficient scheduling for fleet of multi-rotor drones in smart city," in *2019 IEEE 62nd Int. Midwest Symposium on Circuits and Systems (MWSCAS)*. IEEE, 2019, pp. 552–555.

[23] T. Elijah, R. S. Jamisola, Z. Tjiparuro, and M. Namoshe, "A review on control and maneuvering of cooperative fixed-wing drones," *Int. Jour. of Dynamics and Control*, vol. 9, no. 3, pp. 1332–1349, 2021.

[24] D. Todeschini, L. Fagiano, C. Micheli, and A. Cattano, "Control of vertical take off, dynamic flight and landing of hybrid drones for airborne wind energy systems," in *2019 American control conference (ACC)*. IEEE, 2019, pp. 2177–2182.

[25] A. Suleiman, Z. Zhang, L. Carlone, S. Karaman, and V. Sze, "Navion: a fully integrated energy-efficient visual-inertial odometry accelerator for autonomous navigation of nano drones," in *2018 IEEE Symposium on VLSI Circuits*. IEEE, 2018, pp. 133–134.

[26] Y. Mekdad, A. Aris, L. Babun, A. E. Fergougui, M. Conti, R. Lazzeretti, and A. S. Uluagac, "A survey on security and privacy issues of uavs," *arXiv preprint arXiv:2109.14442*, 2021.

[27] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware trojans: Lessons learned after one decade of research," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 22, no. 1, pp. 1–23, 2016.

[28] P. Sniatala *et al.*, "Drone as a sensors' platform," *Modern Technologies Enabling Safe and Secure UAV Operation in Urban Airspace*, vol. 59, p. 115, 2021.

[29] X.-C. Zheng and H.-M. Sun, "Hijacking unmanned aerial vehicle by exploiting civil gps vulnerabilities using software-defined radio," *Sensors and Materials*, vol. 32, no. 8, pp. 2729–2743, 2020.

[30] W. Niu, X. Zhang, X. Zhang, X. Du, X. Huang, M. Guizani *et al.*, "Malware on internet of uavs detection combining string matching and fourier transformation," *IEEE Internet of Things Journal*, 2020.

[31] J. Gordon, V. Kraj, J. H. Hwang, and A. Raja, "A security assessment for consumer wifi drones," in *2019 IEEE International Conference on Industrial Internet (ICII)*. IEEE, 2019, pp. 1–5.

[32] O. B. Fredj, O. Cheikhrouhou, M. Krichen, H. Hamam, and A. Derhab, "An owasp top ten driven survey on web application protection methods," in *International Conference on Risks and Security of Internet and Systems*. Springer, Cham, 2020, pp. 235–252.

[33] M. Majidi, A. Erfanian, and H. Khaloozadeh, "Prediction-discrepancy based on innovative particle filter for estimating uav true position in the presence of the gps spoofing attacks," *IET Radar, Sonar & Navigation*, vol. 14, no. 6, pp. 887–897, 2020.

[34] S. Gogineni, S. Umar, and A. Hemanth, "A study of data interception in wireless sensor networks," *International Journal of Science, Engineering and Computer Technology*, vol. 3, no. 7, p. 239, 2013.

[35] J. Chen, Z. Feng, J.-Y. Wen, B. Liu, and L. Sha, "A container-based dos attack-resilient control framework for real-time uav systems," in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2019, pp. 1222–1227.

[36] R. P. Ojha, P. K. Srivastava, G. Sanyal, and N. Gupta, "Improved model for the stability analysis of wireless sensor network against malware attacks," *Wireless Personal Communications*, vol. 116, no. 3, pp. 2525–2548, 2021.

[37] B. Bhushan, G. Sahoo, and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking—a review," in *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*. IEEE, 2017, pp. 1–6.

[38] A. Bhawsar, Y. Pandey, and U. Singh, "Detection and prevention of wormhole attack using the trust-based routing system," in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE, 2020.

[39] Z. Li, W. Qiao, Y. Lu, and H. Lei, "Optimal controller placement in mec-aided software-defined uav networks against jamming attack," in *Proceedings of the 2020 2nd International Conference on Robotics, Intelligent Control and Artificial Intelligence*, 2020, pp. 74–79.

[40] R. Jabbar, E. Dhib, A. b. Said, M. Krichen, N. Fetais, E. Zaidan, and K. Barkaoui, "Blockchain technology for intelligent transportation systems: A systematic literature review," *IEEE Access*, 2022.

[41] A. Mihoub, O. B. Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques," *Computers & Electrical Engineering*, vol. 98, p. 107716, 2022.

[42] O. Ben Fredj, A. Mihoub, M. Krichen, O. Cheikhrouhou, and A. Derhab, "Cybersecurity attack prediction: a deep learning approach," in *13th International Conference on Security of Information and Networks*, 2020, pp. 1–6.

[43] A. Mihoub, H. Snoun, M. Krichen, R. B. H. Salah, and M. Kahia, "Predicting covid-19 spread level using socio-economic indicators and machine learning techniques," in *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*. IEEE, 2020, pp. 128–133.

[44] S. Mian Qaisar, N. Alyamani, A. Waqar, and M. Krichen, "Machine learning with adaptive rate processing for power quality disturbances identification," *SN Computer Science*, vol. 3, no. 1, pp. 1–6, 2022.

[45] P. S. Bithas, E. T. Michailidis, N. Nomikos, D. Vouyioukas, and A. G. Kanatas, "A survey on machine-learning techniques for uav-based communications," *Sensors*, vol. 19, no. 23, p. 5170, 2019.

[46] B. Wang, D. Liu, Y. Peng, and X. Peng, "Multivariate regression-based fault detection and recovery of uav flight data," *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 6, pp. 3527–3537, 2019.

[47] S. Umarani and D. Sharmila, "Predicting application layer ddos attacks using machine learning algorithms," *International Journal of Computer and Systems Engineering*, vol. 8, no. 10, pp. 1912–1917, 2015.

[48] P. Fraga-Lamas, L. Ramos, V. Mondéjar-Guerra, and T. M. Fernández-Caramés, "A review on iot deep learning uav systems for autonomous obstacle detection and collision avoidance," *Remote Sensing*, vol. 11, no. 18, p. 2144, 2019.

[49] B. Taha and A. Shoufan, "Machine learning-based drone detection and classification: State-of-the-art in research," *IEEE Access*, vol. 7, pp. 138 669–138 682, 2019.

[50] A. Kurniawan and M. Kyas, "A privacy-preserving sensor aggregation model based deep learning in large scale internet of things applications," in *2019 IEEE 17th World Symposium on Applied Machine Intelligence and Informatics (SAMI)*. IEEE, 2019, pp. 391–396.

[51] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for healthcare 4.0 environment: Opportunities and challenges," *Computers & Electrical Engineering*, vol. 72, pp. 1–13, 2018.

[52] N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, "A mechanism for securing iot-enabled applications at the fog layer," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, p. 16, 2019.

[53] F. Aliyu, T. Sheltami, and E. M. Shakshuki, "A detection and prevention technique for man in the middle attack in fog computing," *Procedia Computer Science*, vol. 141, pp. 24–31, 2018.

[54] G. Ding, Q. Wu, L. Zhang, Y. Lin, T. A. Tsiftsis, and Y.-D. Yao, "An amateur drone surveillance system based on the cognitive internet of things," *IEEE Communications Magazine*, vol. 56, no. 1, 2018.

[55] A. Shaghaghi, M. A. Kaafar, R. Buyya, and S. Jha, "Software-defined network (sdn) data plane security: issues, solutions, and future directions," *Handbook of Computer Networks and Cyber Security*, 2020.

[56] F. Olivier, G. Carlos, and N. Florent, "New security architecture for iot network," *Procedia Computer Science*, vol. 52, pp. 1028–1033, 2015.

[57] X. Liu, X. Yang, and Y. Xia, "Netfence: preventing internet denial of service from inside out," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 4, pp. 255–266, 2010.

[58] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, "Sdn-based data transfer security for internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 257–268, 2017.

[59] D. Yin, L. Zhang, and K. Yang, "A ddos attack detection and mitigation with software-defined internet of things framework," *IEEE Access*, vol. 6, pp. 24 694–24 705, 2018.

[60] J.-A. Tarr, M. Thompson, A. A. Tarr, and J. Ellis, "Drones in the future," in *Drone Law and Policy*. Routledge, 2021, pp. 437–453.

[61] Z. ZHANG, R. ZHANG, Z. Jihong, G. Tong, C. Fei, and W. ZHANG, "Integrated batteries layout and structural topology optimization for a solar-powered drone," *Chinese Journal of Aeronautics*, vol. 34, no. 7, pp. 114–123, 2021.

[62] A. Mustofa *et al.*, "The use of drones: From the perspective of regulation and national defense and security," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 10, pp. 670–677, 2021.

[63] M. Krichen, M. Lahami, O. Cheikhrouhou, R. Alroobaea, and A. J. Maâlej, "Security testing of internet of things for smart city applications: A formal approach," in *Smart Infrastructure and Applications*. Springer, Cham, 2020, pp. 629–653.

[64] M. Krichen and R. Alroobaea, "A new model-based framework for testing security of iot systems in smart cities using attack trees and price timed automata," in *14th International Conference on Evaluation of Novel Approaches to Software Engineering - ENASE 2019*, 2019.

[65] M. Krichen, O. Cheikhrouhou, M. Lahami, R. Alroobaea, and A. J. Maâlej, "Towards a model-based testing framework for the security of internet of things for smart city applications," in *International Conference on Smart Cities, Infrastructure, Technologies and Applications*. Springer, Cham, 2017, pp. 360–365.