World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

Securing the skies: A comprehensive survey on internet of drones security challenges and solutions

Oroo Oyondi Felix *

Jaramogi Oginga Odinga University of Science and Technology, Kenya.

World Journal of Advanced Research and Reviews, 2023, 20(03), 780–800

Publication history: Received on 28 October 2023; revised on 14 December 2023; accepted on 17 December 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.20.3.2491

Abstract

The rapid proliferation of Unmanned Aerial Vehicles (UAVs) in the Internet of Things (IoT) era has given rise to the Internet of Drones (IoD), introducing a myriad of security challenges. This survey paper provides a comprehensive examination of the security landscape within the IoD ecosystem. Delving into communication security, authentication mechanisms, data integrity safeguards, firmware and software vulnerabilities, counter-drone measures, and regulatory compliance, the paper explores the multifaceted dimensions of securing UAVs in interconnected environments. By synthesizing current research findings, industry developments, and regulatory frameworks, this survey not only highlights the evolving threat landscape but also presents an overview of state-of-the-art security solutions. The objective is to offer a holistic understanding of IoD security, fostering awareness and providing a foundation for further research and practical implementations. As the integration of drones into various domains becomes increasingly pervasive, this survey aims to contribute to the ongoing discourse on ensuring the safe and responsible utilization of UAV technology within the broader IoT landscape.

Keywords: Internet of drones; Blockchain; Security; Attacks; Vulnerabilities

1. Introduction

Internet of Things (IoT) and fog computing attracted a great deal of interest in contact with the Unmanned Ariel Vehicle (UAV). UAV has remotely interacted with fog computing, web technologies, and service-oriented architecture (SOA) through newly developed IoT. Mainly, the concept of the Internet of Drones (IoD) is framed to access and control the moments of drones in airspace using layered control architecture with navigation services between locations [1]-[6]. The three major layered architectures are mobile network, air traffic control network, and the IoT, which are provided for different UAV applications that are present implementation of the architecture.

The context of fog computing robotics has been coined that are an effort to incorporate robotics across the internet with fog computing [7]-[11]. The drawbacks of low-cost UAVs are processing, storage capacities, and battery-powered UAVs that are efficient in computing specific applications with real-time data and reliability constraints. Basically, IoD refers to the integration of unmanned aerial vehicles (UAVs), commonly known as drones, into the broader framework of the IoT. This concept envisions a network where drones are connected to the internet, enabling them to communicate with each other, ground-based systems, and other devices [12]-[16]. The goal is to create a seamless and interconnected ecosystem that enhances the capabilities and functionalities of drones for various applications. The key components and features of the Internet of Drones are described in Table 1 below:

---

* Corresponding author: Oroo Oyondi Felix

Table 1 Key features of IoD

Feature	Particulars
Data Sharing and analysis	IoD involves the sharing of data among drones and with centralized systems [17], [18]. Drones collect data through sensors and cameras, and this information can be analyzed to make informed decisions, optimize operations, and enhance situational awareness.
Autonomous operation	IoD aims to enable drones to operate autonomously or semi-autonomously. Advanced algorithms and artificial intelligence (AI) are employed to enhance navigation, obstacle avoidance, and decision-making capabilities, reducing the need for human intervention [19]-[22].
Diverse applications	The Internet of Drones has applications across various industries, including agriculture (precision farming), construction (site monitoring), surveillance and security, environmental monitoring, disaster response, and delivery services [23], [24].
Collaborative swarming	Drones in the IoD can operate collaboratively in swarms, coordinating their movements and actions [25]. This enables them to accomplish tasks more efficiently [26], cover larger areas, and respond to dynamic situations in a coordinated manner.
Connectivity	Drones in the Internet of Drones are equipped with communication modules such as Wi-Fi, 4G/5G, or satellite links, allowing them to connect to the internet [27]-[32]. This connectivity enables real-time data exchange and remote control.
Security and safety	IoD incorporates security measures to protect drones and the data they generate. This includes encryption of communication channels, authentication protocols, and safeguards against cyber threats [33]-[35].
Remote monitoring and control	Operators can remotely monitor and control drones through dedicated software applications [36]-[38]. This allows for real-time adjustments to flight paths, mission parameters, and data collection processes.
Regulatory considerations	The integration of drones into the IoT landscape requires careful consideration of regulatory frameworks to ensure safe and responsible operations [39]. Authorities need to establish guidelines for airspace management, privacy, and security.

As technology continues to advance, the Internet of Drones holds the potential to revolutionize industries by providing innovative solutions to challenges and opening up new possibilities for automated and intelligent aerial systems.

1.1. Internet of Drones

IoD is coined from IoT by replacing “Things” with “Drones” but conjoined on properties. IoD is anticipated to become an integral milestone in the development of UAVs. IoD is a “layered network control architecture”, which supports UAVs in coordinating [40]-[44]. In the IoD environment, many drones combine and form a network while transmitting and receiving data from each other. IoD offers to provision for being operated remotely or through the Internet via IP addresses. UAVs pave a way for many applications, but their use-case terms of Mobile security faces challenges.

The expanded development and diverse mission operations of unmanned air vehicles (UAV) have exposed information security (INFOSEC) and communication security (COMSEC) concerns that are not easily addressed in traditional federated or currently deployed integrated modular avionics (IMA) systems. The need to operate military UAVs in civil airspace communicating over unclassified links to foreign air traffic control systems and keep sensitive and/or classified information separated without increasing space, weight and power (Swap) poses challenges to UAV systems architecture [45], [46].

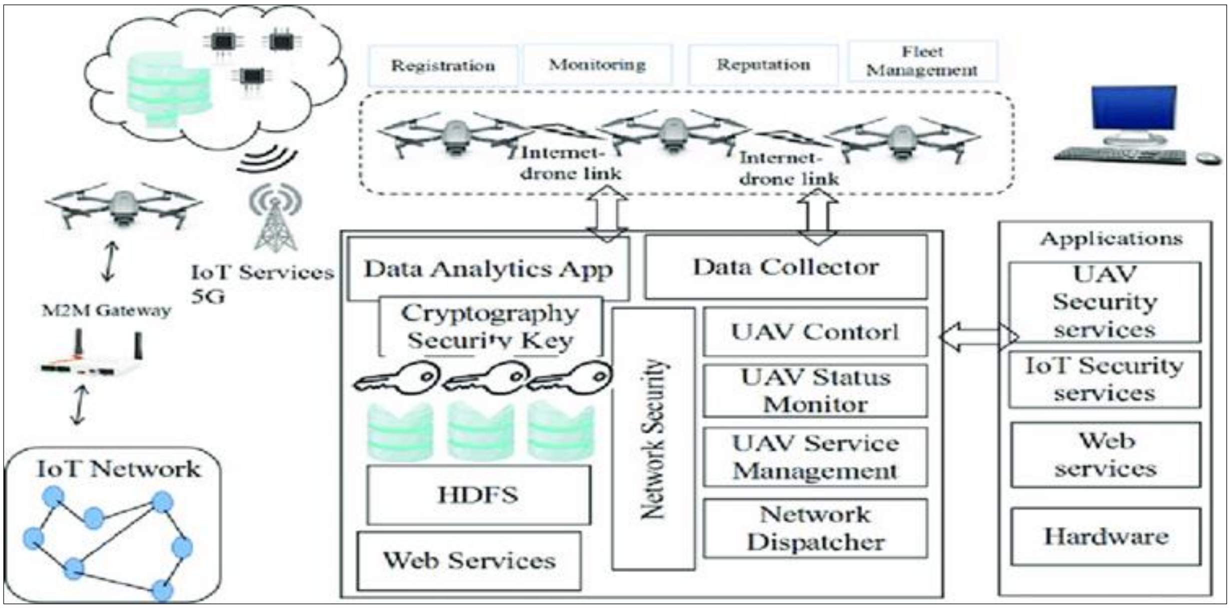

Figure 1 Internet of Drones (IoD) security architecture

In addition to the security vulnerabilities, the UAV communication network must also be more reliable and has low delay, and fault tolerance. These can be achieved with the usage of fifth generation (5G) communication network, which has already given revolution to the industries, especially to Io-based industries, where delay, energy efficiency, network coverage, and quality of service (QoS) is of prime concern [47]-[50]. Although, 5G network has lots of advantages to UAV networks, but still has its own set of security vulnerabilities like paging occasion and stingrays. Therefore, the 5G-enabled UAV communication network need to be secure against network attacks. To address the aforementioned issues, block chain (BC) technology is a viable solution with a huge potential. It is a chain of blocks (contains transactions), which is connected through the hash value of the previous block in the chain and so on. BC is a distributed ledger in which the stored transactions are immutable, faster access, and transparent to all participating members of the BC. It is secure and reliable because of the decentralized consensus, which makes it suitable for various applications like banking, e-games, music, healthcare, and transportation [51]-[56]. Moreover, it has the concept of smart contracts (SC) also called digital agreement written in specific programming language known as Solidity or Go. SCs are self-enforceable programming code (set of rules) between multiple parties involved in a block chain. It is self-executable, self-verifiable, and tamper proof, which will change the method of interaction in BC and automate various processes like payments, shares, and properties.

BC technology enables UAVs to be equipped with cryptographic techniques to ensure secure communication and being used in various applications such as defense and financial applications. It is being adopted by many industries as it reduces the security risks associated with UAV communication. This leads to increased UAV participation in BC network, but current communication channels resist due to latency and scalability issues [57], [58]. Therefore, the 5G as a communication channel in UAV can achieve ultra-low latency (<*1* ms), ultra-high reliability (*99.999%*), and massive connectivity.

The integration of 5G and BC technology has a great potential in commercial and defense sectors, especially in military services and must be completely secured. Military information can be confidential information or mission critical and thus should be secured against all possible network attacks [59]-[62]. The integration of BC (for security) and 5G (for communication) make the UAV communication more secure against network vulnerabilities. IoD offers drones coupling vehicle as well as cloud mobility functions to allow remote drone access and control, as well as seamlessly scalable offloading and capabilities of remote cloud storage [63]-[67]. Figure 2 illustrates the IoD environment that includes base stations, signal link, and cloud environments.

UAVs may make use of non-power supply techniques to make gliding more efficient. It is also worth noting that fixed-wing airplanes can carry a greater payload for longer distances when flying with less power giving them the capability to carry a combination of bigger more advanced sensors with a pair of complementary sensors. Until recently, UAVs were operated individually, but today a higher number of coordinated drones may work together to accomplish complex missions. In these circumstances, drone communication is absolutely essential. In other words, it is vital for users to fully comprehend UAV communication systems. One additional kind of wireless channel and network protocol is utilized in drone communications, but on the other hand, several distinct types of wireless routes and network protocols are applied in drone communications [68]-[73]. For this reason, the network design for UAVs is determined by their application. As a basic example, researchers have discovered that a point-to-point line-of-sight link between a drone and a gadget may maintain continuous data transmission even when transmission is extended. Drones that use satellite communications to talk to each other for surveillance, when employed for safety defense, or more broad outreach activities, satellite communication is a better option for drones. Alternatively, cellular communications systems are more commonly used in civic and personal applications. For example, indoor communication, in particular for the mesh network and WSN, P2P protocols such as Bluetooth have shown to be more efficient. When applied to drones, working with a multi-layered network can be a difficult and challenging procedure.

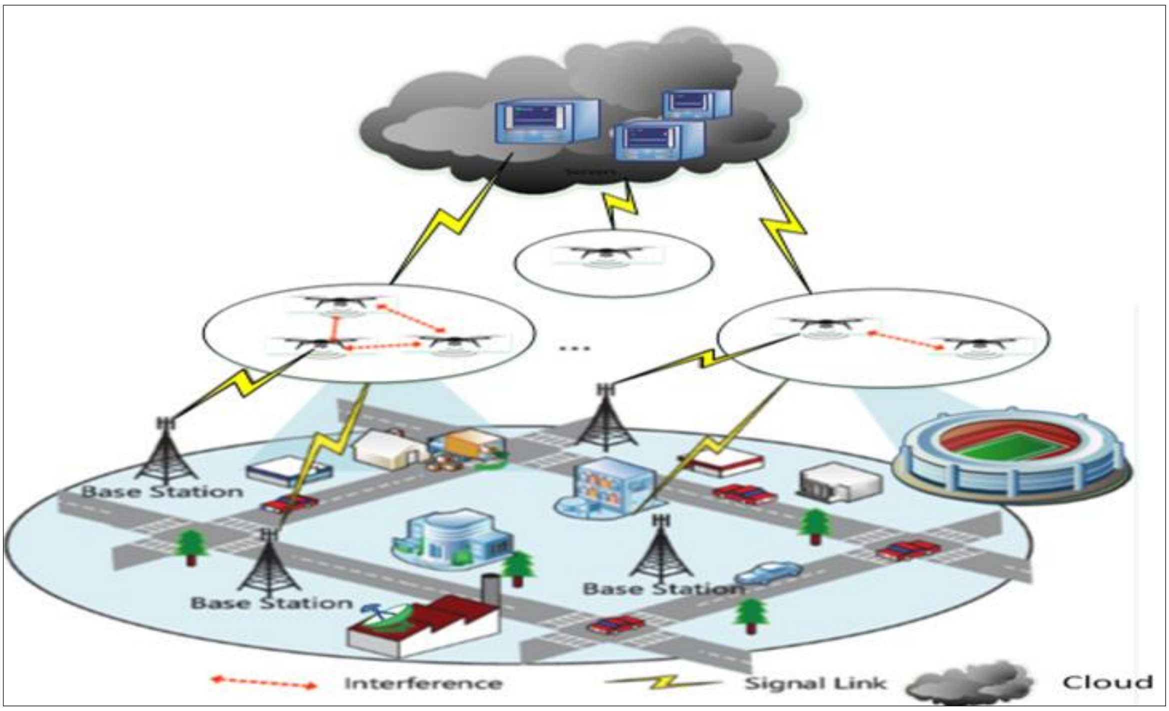

Figure 2 IoD environment

A remote hijacking of the drones could be achieved by leveraging the vulnerability in the software of the UAVs that act as a sophisticated tool for military purposes. Global positioning system (GPS) signals are under the influence of malware programs on drones that can be controlled by malicious users for malicious objectives (attackers). By doing this, unreasonable attacks, such as dropping bombs, could be committed by the attacker, endangering lives. The control signal is a significant feature of IoD environments due to the different communications among entities and should not be disclosed or exposed in any circumstance [74]-[78]. There is a need for robust security measures to avert harm from security attacks. Moreover, to facilitate personal and business drones for independent flight, a certain type of authentication and key exchange protocols are required between the two entities in the sky. Both the entities then create a symmetric security key for future data transmission.

Data link is used for sending and receiving data, namely, the downlink transmission from UAV to ground station or satellite, and uplink transmission from the ground station or satellite to UAV [79], [80]. In general, the capacity requirement of this data link depends on the applications.

There are two types of CNCP available, namely, the primary CNPC link, which is the preferred control link, and the secondary CNPC link. The former link can be used via satellite as a backup link to enhance reliability and robustness. The primary CNPC link is established directly during takeoff and landing. On the other hand the secondary CNPC link can be established via satellite when the UAV is in operation.

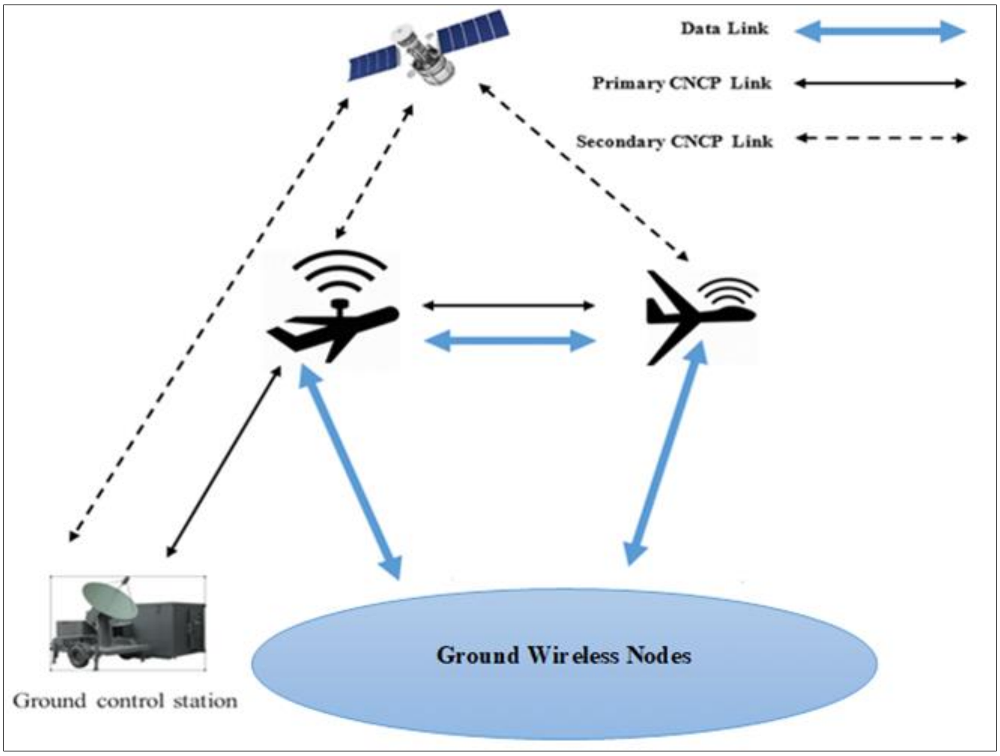

Figure 3 Types of UAV communication

1.2. UAV system design requirements

Designing an Unmanned Aerial Vehicle (UAV) system involves considering a range of requirements to ensure the successful development, deployment, and operation of the drone. The specific requirements can vary based on the intended use and application of the UAV, but Table 2 presents common considerations.

Table 2 UAV system design requirements

Requirement	**Details**
Performance	Endurance/Range: Define the desired flight time or range the UAV should be able to achieve on a single charge or tank of fuel [81]. Speed: Specify the required maximum and cruising speeds based on mission requirements [82].
Environmental Considerations	Weather Resistance: Define the UAV's ability to operate in specific weather conditions (e.g., wind resistance, rain, temperature extremes) [83], [84]. Operational Altitude: Specify the maximum and minimum operating altitudes [85].
Navigation and Guidance	GPS Accuracy: Ensure the UAV has precise GPS capabilities for accurate navigation [86], [87]. Obstacle Avoidance: Include features for obstacle detection and avoidance to enhance safety during flight [88], [89].
Mission Requirements:	Purpose: Clearly define the mission objectives, whether it's aerial photography, surveillance, data collection, search and rescue, or any other specific task [90]. Payload Capacity: Determine the payload capacity required for the mission, considering the weight and dimensions of the equipment or sensors to be carried [91], [92].
Safety	Redundancy: Incorporate redundancy in critical systems (e.g., propulsion, navigation) to enhance reliability [93]. Emergency Procedures: Include protocols and features for emergency situations, such as loss of communication or critical system failures [94].

Autonomy and Control	Autonomous Capabilities: Determine the level of autonomy required, such as autonomous takeoff, landing, navigation, and decision-making capabilities [95], [96]. Remote Control: Specify the range and reliability of the communication link between the UAV and the ground control station [97].
Power System	Power Source: Choose the appropriate power source (e.g., batteries, hybrid systems, or internal combustion engines) based on mission requirements and duration [98].
Communication Systems	Data Link: Define the type of data link required for communication between the UAV and the ground station (e.g., radio, satellite, or cellular) [99]-[101]. Command and Control Link: Specify the requirements for the link used to transmit commands from the ground control station to the UAV [102].
Cost and Budget Constraints	Budget: Consider financial constraints and design the UAV system within the allocated budget [103]. Cost-Benefit Analysis: Evaluate the cost-effectiveness of different design choices [104].
Regulatory Compliance	Airspace Regulations: Ensure that the UAV design [105] complies with relevant aviation regulations and restrictions in the intended operating area. Certification: Plan for the necessary certifications and approvals required for legal operation [105].
Maintenance and Support	Ease of Maintenance: Design the UAV with accessibility and ease of maintenance in mind [107]. Support Infrastructure: Develop a plan for technical support, spare parts, and maintenance procedures [108].

It is evident that designing a UAV system involves a multidisciplinary approach, considering aerodynamics, avionics, communication systems, and more. Collaboration between engineers, software developers, and domain experts is crucial to meeting all the requirements and achieving a successful outcome.

2. UAV system architecture

The architecture of a UAV system encompasses the structure, components, and interactions that enable the drone to perform its intended tasks [109], [110]. UAV system architecture is typically organized into several layers, each responsible for specific functions as shown in Figure 4.

Basically, the architecture of a UAV system is a comprehensive framework that integrates various components to enable the drone's effective operation. The system typically comprises an airframe, encompassing the physical structure and propulsion system, avionics with flight control and navigation units, communication infrastructure connecting the Ground Control Station (GCS) and the UAV, autonomous control features for navigation and collision avoidance, a payload section housing sensors and data processing units, a power system with distribution mechanisms, security measures including encryption, health monitoring and diagnostic tools, and adherence to regulatory standards [111], [112]. The architecture is designed to facilitate seamless communication, control, and coordination, ensuring the UAV's successful performance in a range of missions while emphasizing modularity and compliance with safety and regulatory requirements.

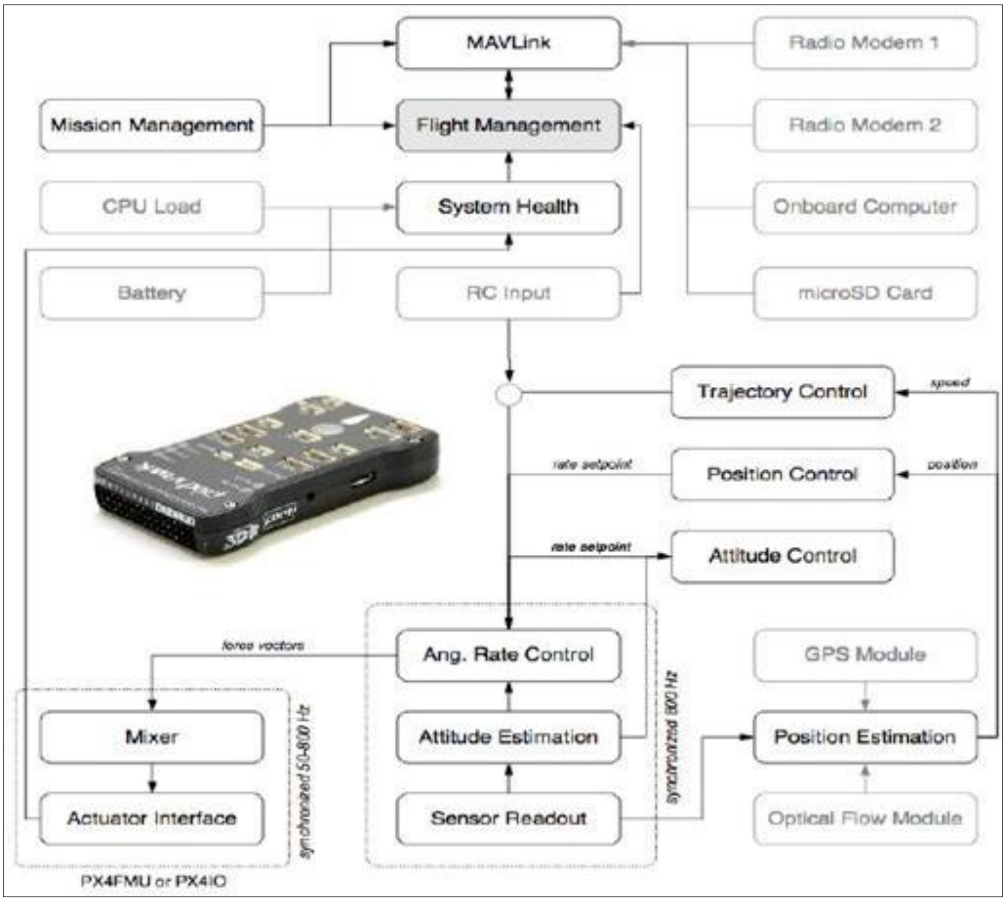

Figure 4 The Pixhawk architecture

2.1. Layers of UAV Drone

The architecture of a UAV can be conceptualized in several layers, each serving a specific function in ensuring the drone's effective operation. These layers include the Physical Layer, Communication Layer, Control and Autonomy Layer, Payload Layer, and Software Layer.

The physical layer encompasses the tangible components that make up the drone's structure and mechanics. This includes the airframe, propulsion system, and physical elements essential for flight. The airframe design is influenced by the drone's purpose, whether it's a fixed-wing or rotary-wing configuration [113]-[116]. The propulsion system, whether electric or combustion-based, provides the necessary thrust for flight. Factors like materials, aerodynamics, and weight distribution are critical considerations at this layer to ensure optimal performance and durability.

The communication layer focuses on the exchange of information between different elements of the UAV system. It involves the communication systems on the drone, such as data links, telemetry systems, and control links connecting the UAV to the Ground Control Station (GCS). Reliable and secure communication is crucial for real-time data transfer, command transmission, and receiving telemetry data [117], [118]. Encryption protocols are often employed to secure communication channels, safeguarding the integrity and confidentiality of the transmitted information [119].

At the heart of UAV functionality is the control and autonomy layer, comprising avionics and software responsible for guiding and controlling the drone. This layer includes the flight control system, navigation algorithms, and autonomy features allowing the UAV to operate autonomously or semi-autonomously [120]-[124]. Advanced sensors such as accelerometers, gyroscopes, and GPS receivers contribute to precise navigation, while collision avoidance systems enhance the drone's ability to navigate safely. The control and autonomy layer orchestrates the drone's movements and responses to external stimuli.

The payload layer encompasses the sensors, cameras, and other instruments carried by the UAV to fulfill specific mission objectives. Payloads vary widely based on the application, including tasks such as aerial photography, surveillance, mapping, or environmental monitoring [125]-[128]. The design and integration of the payload layer are critical to ensuring the drone collects accurate and relevant data. Data processing units within this layer handle computation and storage, facilitating real-time analysis or later retrieval depending on mission requirements.

The software layer acts as the overarching framework that ties together various components of the UAV system. This includes flight control software interpreting data from sensors, mission planning software used by operators, and autonomy features like waypoint navigation and obstacle avoidance algorithms [129]-[132]. Software updates, diagnostic tools, and security protocols are managed in this layer to ensure the drone operates efficiently, securely, and in compliance with relevant regulations. The software layer plays a critical role in the adaptability, functionality, and overall performance of the UAV system. Figure 5 shows a typical layered architecture for UAV drones IoT communication to a ground station.

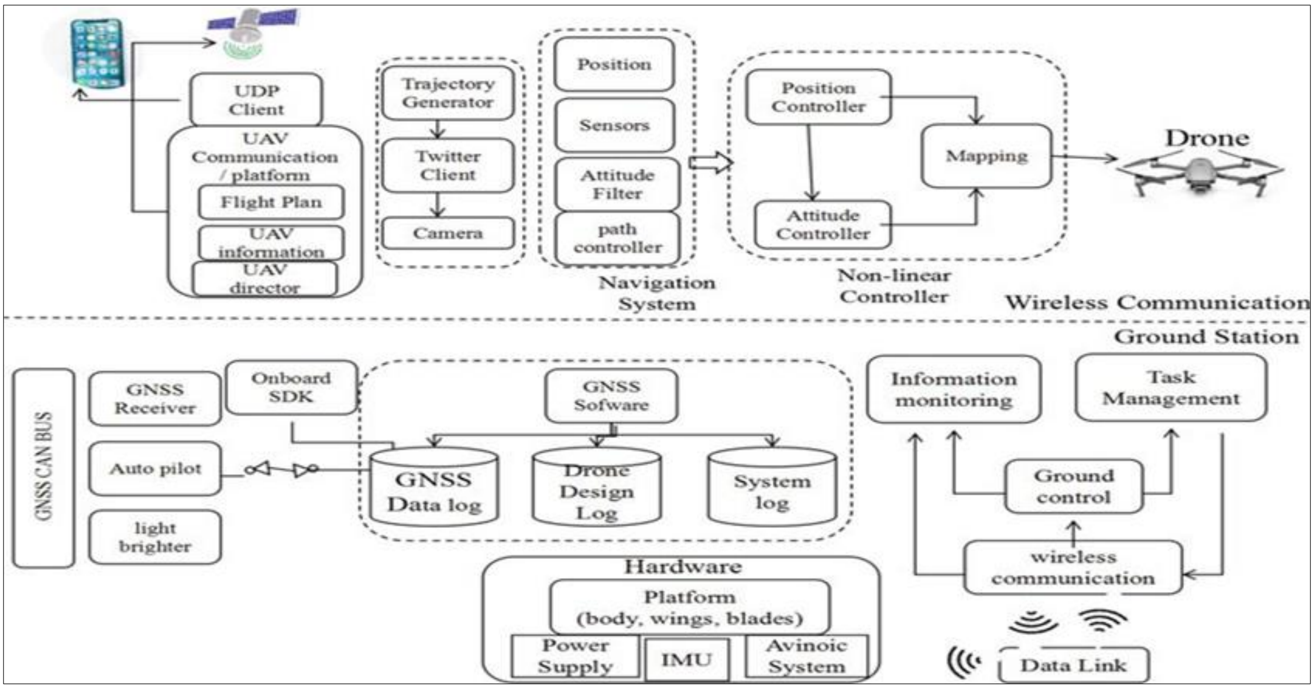

Figure 5 Layered architecture for UAV drones

2.2. UAV Sensor Technologies in 5G Networks

Integrating UAVs with 5G networks presents a range of opportunities to enhance sensor technologies, allowing for more sophisticated and efficient operations as shown in Figure 6. Table 3 presents some ways in which UAV sensor technologies can benefit from 5G networks.

5G networks provide significantly higher data transfer rates and lower latency compared to previous generations of mobile networks [133]-[134]. This high bandwidth and low latency enable UAVs to transmit large amounts of sensor data in real-time. This is particularly crucial for applications such as high-definition video streaming, live aerial surveillance, and other data-intensive tasks that require instant feedback.

UAVs equipped with various sensors, including cameras, LiDAR, multispectral and hyperspectral imaging, benefit from the improved connectivity provided by 5G. These sensors can capture detailed and high-resolution data for applications like agricultural monitoring, environmental surveys, and infrastructure inspections [135]-[139]. With 5G, the data collected can be transmitted to ground stations or cloud-based processing centers rapidly, facilitating timely analysis and decision-making.

5G networks support edge computing, allowing UAVs to process data locally rather than relying solely on remote servers. This is particularly advantageous for UAVs with onboard sensors, as it reduces the need for extensive data transmission to ground stations or the cloud [140]-[145]. By processing data at the edge, UAVs can make quicker decisions, improving autonomy and responsiveness in dynamic environments.

5G networks enable efficient communication and coordination among multiple UAVs forming collaborative swarms. These swarms can share sensor data and coordinate actions in real-time, enhancing their collective capabilities [146]-[148]. This is valuable for applications such as search and rescue missions, surveillance of large areas, or coordinated delivery services. The low latency of 5G facilitates synchronized actions among UAVs within a swarm.

5G networks offer improved security features, including encryption and authentication protocols, which are crucial for protecting the data transmitted between UAVs and ground stations. Additionally, the reliability and stability of 5G connectivity enhance the overall performance of UAVs, ensuring consistent and robust communication even in challenging environments[149], [150], [151]. This is vital for applications where uninterrupted connectivity is essential, such as critical infrastructure inspections or emergency response scenarios.

The integration of UAVs with 5G networks enhances sensor technologies by providing high bandwidth, low latency, and reliable connectivity [152]-[156]. This synergy opens up new possibilities for applications ranging from surveillance and monitoring to collaborative UAV swarms, offering increased efficiency, responsiveness, and real-time data analysis capabilities.

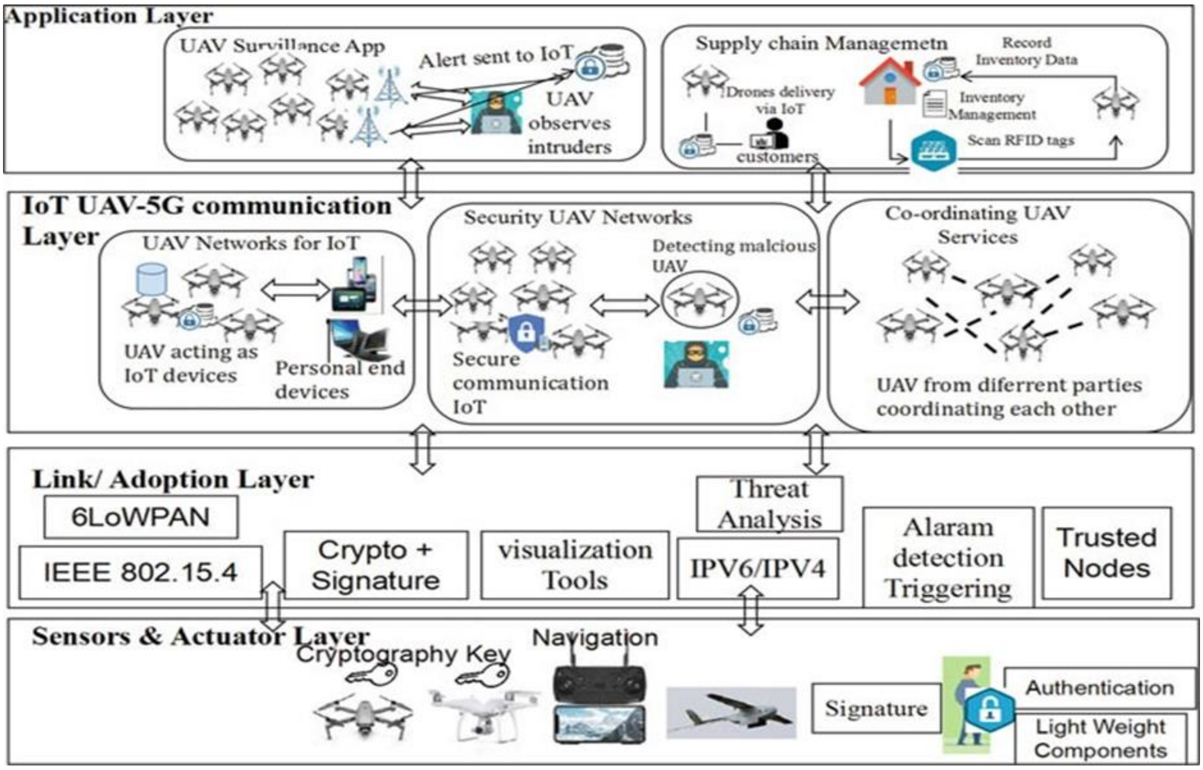

Figure 6 Secured 5G mobile communication layers in UAV drones IoT

3. Security Threats and Attacks of IoDT (internet of drones things)

Security in the Internet of Drones (IoD) is a critical consideration given the potential risks associated with unmanned aerial vehicles operating in interconnected environments. Protecting data integrity, communication channels, and preventing unauthorized access are paramount. Encryption protocols safeguard sensitive information transmitted between drones, ground control stations, and other devices within the IoD ecosystem [157]-[162]. Robust authentication mechanisms ensure that only authorized personnel can access and control drones, mitigating the risk of malicious interference. Additionally, securing the software and firmware of drones against cyber threats is essential to prevent unauthorized modifications or control. As the IoD landscape continues to evolve, a comprehensive approach to security that includes regular updates, adherence to industry standards, and proactive threat detection is crucial to fostering trust and ensuring the safe and reliable operation of drone systems. Figure 7 shows the vulnerability of IoT drones to detect contact pathways and attacks a variety of vulnerabilities. These are the techniques used to hacking the UAV drones from channel jamming and to Spoof malware, such as the Middle-Man attack Figure 7 IoT security attacks for communication with IoT and the GNSS spoofing [163]. The adoption of link layers non-lethal solutions to counter these threats to be various malware such as highly inefficient and the data presents some of the issues related to drone communication pathways that threats are in highly-ineffective and unreliable [164].

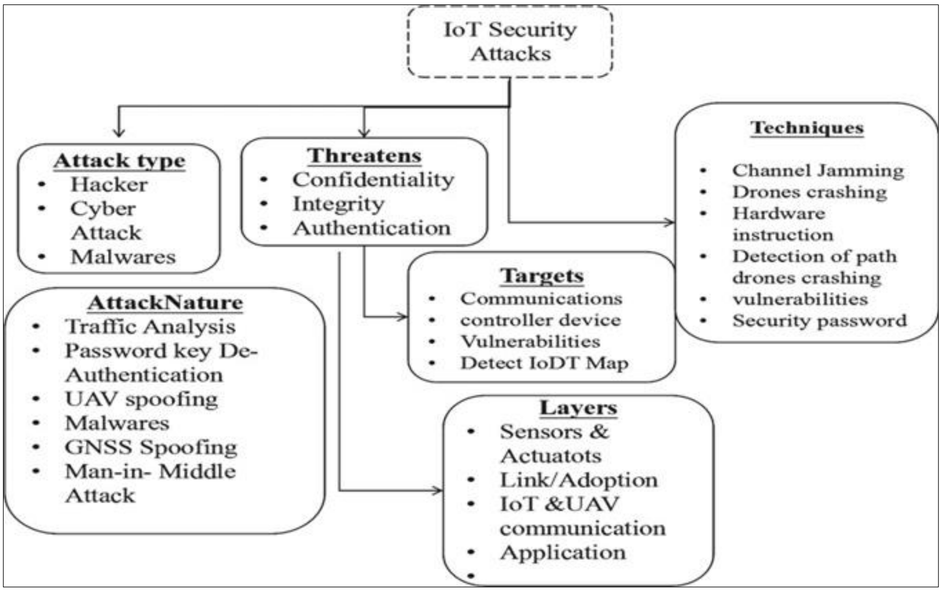

Figure 7 IoT security attacks for communication with IoT

UAV fault-tolerant control present in the device architecture, using a neural network adaptive framework for the identification and isolation of the network design. In this scheme, real-time detection in drones ensures real-time identification and isolation of faults in actuators to configure network issues that are tolerant in order to reconfigure the controller or have an impact on efficiency [165]. In this Wi-Fi jamming, the approach is observed to be implemented as these drones use a 2.4 GHz frequency.All these jams are wireless contact within a specific area of coverage. However, very small jamming capacity cannot be easily identified in the environment, and other nearby frequencies are jammed. This approach is based on a three-way handshake router and newly installed rogue computers [166], [167]. It allows the attacker to de-authenticate, or jam, the connection between the drones and the control unit. The Wi-Fi attack that was present enables the attacker to search for drones to communicate the DDoS attack, which interprets the transfer of the particular data, either delaying it, which allows the attacker to leads the de-authenticated attack. A DOS assault that intercepts network traffic and floods with a request to interrupt a drone/device link Denial of service will be performed either by de-authenticated of the UAV drones that access can be sent periodically to the drone network security event commands. This leads to the estimation of the location of the drone unit for the GNSS signal simulator used by drones to launch a GPS spoofing attack, which transmits false signals to the control system of each drone, normally more powerful than the fake signals instead of the original ones [168]. GNSS allows drone navigation non-encryption of easily spoofed signals that are directly managed by anti-spoof algorithms operator that can help mitigate GPS spoof attacks. A drone that uses GPS could be targeted by jamming the GNSS signal that makes the drones unable to determine their location. Jamming the objective of disrupting all satellite communication during antenna selection and orientation can help to minimize jamming attacks. Eavesdropping successfully dealt with in Man-in-Middle attacks allows the attacker to track violation of drone confidentiality. Some of the confidential information that collects through IoT when it classifies them in terms of privacy and trust, with their respective tasks. If the data is interferes with the data access to adjust the cluster controller and the malicious actions of the controller to gain control of the drones. The main task is to safely store IoT data integrity, data protection, and encrypted data that is not available to anyone without any key for decryption.

Therefore, security in the IoD is a multifaceted challenge that involves protecting various layers of the ecosystem, encompassing both hardware and software components. Ensuring the security of drone systems is essential to prevent unauthorized access, protect sensitive data, and maintain the integrity of operations. Table 3 describes some of the security considerations in the Internet of Drones.

Table 3 Security considerations in the Internet of Drones

Security issue	Particulars
Authentication and Authorization	Robust authentication mechanisms are critical to ensuring that only authorized entities can access and control drones. Biometric authentication, multi-factor authentication, and secure credential management systems can help prevent unauthorized personnel from manipulating or taking control of a drone [169]-[172]. Additionally, proper authorization mechanisms ensure that users have the appropriate permissions for their roles within the IoD system.
Communication Security	Secure communication is fundamental in the IoD, as drones rely on data exchange with ground control stations, other drones, and potentially cloud-based systems [173]-[175]. Implementing strong encryption protocols, such as TLS (Transport Layer Security) or VPNs (Virtual Private Networks), helps safeguard data transmitted over communication channels, preventing eavesdropping or unauthorized access.
Firmware and Software Security	Ensuring the security of the drone's firmware and software is crucial to prevent exploitation by malicious actors. Regular software updates that include security patches, code reviews, and adherence to secure coding practices are essential [176]. Employing code signing and integrity verification mechanisms helps ensure that only authorized and unmodified software runs on the drone, reducing the risk of unauthorized access or control.
Data Integrity and Privacy	Protecting the integrity of data collected by drones is paramount, especially in applications like surveillance or data mapping. Employing encryption and secure storage mechanisms on the drone and during data transmission helps prevent tampering [177]-[180]. Privacy concerns related to the collection of sensitive information by drones should be addressed through compliance with relevant regulations and the implementation of anonymization or aggregation techniques when handling personal or confidential data.
Physical Security	Physical security measures are necessary to protect drones from theft or tampering. This includes secure storage facilities, anti-tamper mechanisms, and tracking systems to locate and recover stolen drones [181]. Implementing geofencing and geo-restriction features can also prevent drones from operating in restricted or unauthorized areas.
Counter-Drone Measures	In addition to securing drones from external threats, it's essential to consider counter-drone measures to protect against unauthorized UAVs [182]. This involves implementing detection systems that can identify rogue drones and deploying mitigation techniques such as signal jamming or geofencing to prevent their intrusion.
Regulatory Compliance	Adherence to existing and emerging regulations is crucial for ensuring the security and safety of drone operations. Compliance with aviation authorities' guidelines, privacy laws, and industry standards helps establish a framework for secure and responsible drone use within the legal and ethical boundaries [183].
Incident Response and Forensics	Establishing robust incident response plans and forensic capabilities is essential for mitigating the impact of security incidents [184], [185]. This involves monitoring for anomalies, conducting regular security audits, and having procedures in place to investigate and respond to security breaches promptly.

Therefore, security in the Internet of Drones is a comprehensive effort that involves securing communication channels, authenticating users, protecting data integrity, ensuring software and firmware security, implementing counter-drone measures, addressing physical security concerns, complying with regulations, and establishing incident response capabilities. A holistic and proactive approach to security is essential to foster trust, protect against evolving threats, and ensure the safe and responsible integration of drones into the broader IoT landscape.

4. Conclusion

Ensuring robust security in the Internet of Drones (IoD) is paramount for the safe and effective integration of unmanned aerial vehicles into interconnected ecosystems. The multifaceted nature of IoD security demands comprehensive measures spanning communication encryption, authentication protocols, data integrity safeguards, firmware/software security, counter-drone strategies, physical protection, regulatory compliance, and incident response capabilities. As drones become integral to various industries, addressing privacy concerns, adhering to evolving regulations, and employing proactive security practices are imperative. A resilient IoD security framework not only protects against potential threats such as unauthorized access and data breaches but also fosters trust in the technology, facilitating its responsible and widespread adoption. Continuous vigilance, collaboration between industry stakeholders, and adherence to best practices will be essential to navigate the evolving landscape of IoD security challenges effectively.

Compliance with ethical standard

Acknowledgement

I wish to thank all my colleagues for the help they offered during the drafting and writing of this work.

Disclosure of conflict of interest

The author declares that he has no any conflict of interest.

References

[1] Derhab A, Cheikhrouhou O, Allouch A, Koubaa A, Qureshi B, Ferrag MA, Maglaras L, Khan FA. Internet of drones security: Taxonomies, open issues, and future directions. Vehicular Communications. 2023 Feb 1, 39:100552.

[2] Bine LM, Boukerche A, Ruiz LB, Loureiro AA. IoDMix: A novel routing protocol for Delay-Tolerant Internet of Drones integration in Intelligent Transportation System. Ad Hoc Networks. 2023 Sep 1, 148:103204.

[3] Svaigen AR, Boukerche A, Ruiz LB, Loureiro AA. Security in the Industrial Internet of Drones. IEEE Internet of Things Magazine. 2023 Sep 20, 6(3):110-6.

[4] Haider SK, Nauman A, Jamshed MA, Jiang A, Batool S, Kim SW. Internet of drones: Routing algorithms, techniques and challenges. Mathematics. 2022 Apr 29, 10(9):1488.

[5] Heidari A, Jafari Navimipour N, Unal M, Zhang G. Machine learning applications in internet-of-drones: systematic review, recent deployments, and open issues. ACM Computing Surveys. 2023 Mar 3, 55(12):1-45.

[6] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[7] Mohsan SA, Othman NQ, Li Y, Alsharif MH, Khan MA. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. Intelligent Service Robotics. 2023 Mar, 16(1):109-37.

[8] Mohsan SA, Khan MA, Noor F, Ullah I, Alsharif MH. Towards the unmanned aerial vehicles (UAVs): A comprehensive review. Drones. 2022 Jun 15, 6(6):147.

[9] Messaoudi K, Oubbati OS, Rachedi A, Lakas A, Bendouma T, Chaib N. A survey of UAV-based data collection: Challenges, solutions and future perspectives. Journal of Network and Computer Applications. 2023 May 16:103670.

[10] Mohsan SA, Othman NQ, Khan MA, Amjad H, Żywiołek J. A comprehensive review of micro UAV charging techniques. Micromachines. 2022 Jun 20, 13(6):977.

[11] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[12] Heidari A, Jafari Navimipour N, Unal M, Zhang G. Machine learning applications in internet-of-drones: systematic review, recent deployments, and open issues. ACM Computing Surveys. 2023 Mar 3, 55(12):1-45.

[13] Tanveer M, Alasmary H, Kumar N, Nayak A. SAAF-IoD: Secure and Anonymous Authentication Framework for the Internet of Drones. IEEE Transactions on Vehicular Technology. 2023 Aug 24.

[14] Heidari A, Navimipour NJ, Unal M. A Secure Intrusion Detection Platform Using Blockchain and Radial Basis Function Neural Networks for Internet of Drones. IEEE Internet of Things Journal. 2023 Jan 20.

[15] Aboueleneen N, Alwarafy A, Abdallah M. Deep Reinforcement Learning for Internet of Drones Networks: Issues and Research Directions. IEEE Open Journal of the Communications Society. 2023 Mar 2.

[16] Fan G, Liu Z, Qin Y, Long B, Li H, Li J. Airflow characteristics of rotorcraft plant protection UAV operating in rice fields. Biosystems Engineering. 2023 Feb 1, 226:209-22.

[17] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Dec 1; 23(4):145-62.

[18] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[19] Zhuo M, Zhang J. Efficient, Traceable and Privacy-Aware Data Access Control in Distributed Cloud-based IoD Systems. IEEE Access. 2023 May 2.

[20] Michailidis ET, Vouyioukas D. A review on software-based and hardware-based authentication mechanisms for the Internet of Drones. Drones. 2022 Feb 8, 6(2):41.

[21] Abualigah L, Diabat A, Sumari P, Gandomi AH. Applications, deployments, and integration of internet of drones (iod): a review. IEEE Sensors Journal. 2021 Sep 23, 21(22):25532-46.

[22] Vaddempudi KR, Rao GN, Saravanan D, Sindhura S, Kumar SG, David DD. Marine Area Remote Sensing Monitoring Withadvanced Flight Regulator and Self-Directed Regulator. Turkish Journal of Physiotherapy and Rehabilitation. 2021, 32(3):1584-90.

[23] Dinelli C, Racette J, Escarcega M, Lotero S, Gordon J, Montoya J, Dunaway C, Androulakis V, Khaniani H, Shao S, Roghanchi P. Configurations and Applications of Multi-Agent Hybrid Drone/Unmanned Ground Vehicle for Underground Environments: A Review. Drones. 2023 Feb 14, 7(2):136.

[24] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1, 142:103117.

[25] Alsamhi SH, Ma O, Ansari MS, Almalki FA. Survey on collaborative smart drones and internet of things for improving smartness of smart cities. Ieee Access. 2019 Aug 13, 7:128125-52.

[26] Alsamhi SH, Afghah F, Sahal R, Hawbani A, Al-qaness MA, Lee B, Guizani M. Green internet of things using UAVs in B5G networks: A review of applications and strategies. Ad Hoc Networks. 2021 Jun 1, 117:102505.

[27] Hildmann H, Eledlebi K, Saffre F, Isakovic AF. The Swarm Is More Than the Sum of Its Drones. Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead. 2021 Feb 15, 332:1.

[28] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[29] Mishra D, Natalizio E. A survey on cellular-connected UAVs: Design challenges, enabling 5G/B5G innovations, and experimental advancements. Computer Networks. 2020 Dec 9, 182:107451.

[30] Rana B, Singh Y. Internet of things and UAV: An interoperability perspective. Unmanned Aerial Vehicles for Internet of Things (IoT) Concepts, Techniques, and Applications. 2021 Aug 24:105-27.

[31] Koulouris C, Dimitrios P, Al-Darraji I, Tsaramirsis G, Musa MA, Papageorgas P. A Preliminary Study and Implementing Algorithm Using Finite State Automaton for Remote Identification of Drones. Applied Sciences. 2023 Feb 11, 13(4):2345.

[32] Paladin Z, Lukšić Ž, Kapidani N, Montagud M, Fernández-Dasí M, Srinidhi S, Wöllert T, Boustras G. The 5G-supported Unmanned Aerial Vehicles for Emergency Cases Response. In2023 46th MIPRO ICT and Electronics Convention (MIPRO) 2023 May 22 (pp. 1376-1381). IEEE.

[33] Muzaffar R, Hummel KA. Experimental Validation of Networked Aerial IoUT Solutions: Testbeds and Measurements. InInternet of Unmanned Things (IoUT) and Mission-based Networking 2023 Apr 29 (pp. 173-199). Cham: Springer International Publishing.

[34] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1, 133:102763.

[35] Alturki N, Aljrees T, Umer M, Ishaq A, Alsubai S, Saidani O, Djuraev S, Ashraf I. An Intelligent Framework for Cyber–Physical Satellite System and IoT-Aided Aerial Vehicle Security Threat Detection. Sensors. 2023 Aug 14, 23(16):7154.

[36] Bhasin N, Tarar S, Cengiz K. Security Issues in the Internet of Drones (IoDs). The Internet of Drones: AI Applications for Smart Solutions. 2022 Nov 3:67.

[37] Dhatterwal JS, Kaswan KS, Jaglan V, Vij A. Machine learning and deep learning algorithms for IoD. The Internet of Drones: AI Applications for Smart Solutions. 2022 Nov 3:237.

[38] Hussein M, Nouacer R, Corradi F, Ouhammou Y, Villar E, Tieri C, Castiñeira R. Key technologies for safe and autonomous drones. Microprocessors and Microsystems. 2021 Nov 1, 87:104348.

[39] Besada JA, Bernardos AM, Bergesio L, Vaquero D, Campaña I, Casar JR. Drones-as-a-service: A management architecture to provide mission planning, resource brokerage and operation support for fleets of drones. In2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) 2019 Mar 11 (pp. 931-936). IEEE.

[40] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28, 15(13):10264.

[41] Labib NS, Brust MR, Danoy G, Bouvry P. The rise of drones in internet of things: A survey on the evolution, prospects and challenges of unmanned aerial vehicles. IEEE Access. 2021 Aug 16, 9:115466-87.

[42] Jan SU, Qayum F, Khan HU. Design and analysis of lightweight authentication protocol for securing IoD. Ieee access. 2021 Apr 29, 9:69287-306.

[43] Liao S, Wu J, Li J, Bashir AK, Yang W. Securing collaborative environment monitoring in smart cities using blockchain enabled software-defined internet of drones. IEEE Internet of Things Magazine. 2021 Mar 30, 4(1):12-8.

[44] Ahmed GA, Sheltami TR, Mahmoud AS, Imran M, Shoaib M. A novel collaborative IoD-assisted VANET approach for coverage area maximization. IEEE Access. 2021 Apr 12, 9:61211-23.

[45] Wazid M, Das AK, Lee JH. Authentication protocols for the internet of drones: taxonomy, analysis and future directions. Journal of Ambient Intelligence and Humanized Computing. 2018 Aug:1-0.

[46] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9, 3(5):364.

[47] Grote M, Pilko A, Scanlan J, Cherrett T, Dickinson J, Smith A, Oakey A, Marsden G. Sharing airspace with Uncrewed Aerial Vehicles (UAVs): Views of the General Aviation (GA) community. Journal of Air Transport Management. 2022 Jul 1, 102:102218.

[48] Bassi E. From here to 2023: Civil drones operations and the setting of new legal rules for the European single sky. Journal of Intelligent & Robotic Systems. 2020 Nov, 100:493-503.

[49] Mishra AK, Wazid M, Singh DP, Das AK, Singh J, Vasilakos AV. Secure Blockchain-Enabled Authentication Key Management Framework with Big Data Analytics for Drones in Networks Beyond 5G Applications. Drones. 2023 Aug 2, 7(8):508.

[50] Harbi Y, Medani K, Gherbi C, Senouci O, Aliouat Z, Harous S. A Systematic Literature Review of Blockchain Technology for Internet of Drones Security. Arabian Journal for Science and Engineering. 2023 Feb, 48(2):1053-74.

[51] Ren X, Cao J, Ma R, Luo Y, Guan J, Zhang Y, Li H. A Novel Access and Handover Authentication Scheme in UAV-Aided Satellite-Terrestrial Integration Networks Enabling 5G. IEEE Transactions on Network and Service Management. 2023 Feb 20.

[52] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[53] Mehta P, Gupta R, Tanwar S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. Computer Communications. 2020 Feb 1, 151:518-38.

[54] Kumar M, Raj H, Chaurasia N, Gill SS. Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems. 2023 May 29.

[55] Alam S, Bhatia S, Shuaib M, Khubrani MM, Alfayez F, Malibari AA, Ahmad S. An overview of blockchain and IoT integration for secure and reliable health records monitoring. Sustainability. 2023 Mar 23, 15(7):5660.

[56] Zhang Q, He Y, Lai R, Hou Z, Zhao G. A survey on the efficiency, reliability, and security of data query in blockchain systems. Future Generation Computer Systems. 2023 Aug 1, 145:303-20.

[57] Rahman A, Islam MJ, Band SS, Muhammad G, Hasan K, Tiwari P. Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. Digital Communications and Networks. 2023 Apr 1, 9(2):411-21.

[58] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 Sep, 33(9):e4528.

[59] Hadi HJ, Cao Y, Nisa KU, Jamil AM, Ni Q. A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. Journal of Network and Computer Applications. 2023 Apr 1, 213:103607.

[60] Ch R, Srivastava G, Gadekallu TR, Maddikunta PK, Bhattacharya S. Security and privacy of UAV data using blockchain technology. Journal of Information security and Applications. 2020 Dec 1, 55:102670.

[61] Wu X, Du Y, Fan T, Guo J, Ren J, Wu R, Zheng T. Threat analysis for space information network based on network security attributes: a review. Complex & Intelligent Systems. 2023 Jun, 9(3):3429-68.

[62] Ahmad H, Dharmadasa I, Ullah F, Babar MA. A review on c3i systems' security: Vulnerabilities, attacks, and countermeasures. ACM Computing Surveys. 2023 Jan 13, 55(9):1-38.

[63] Rugo A, Ardagna CA, Ioini NE. A security review in the UAVNet era: threats, countermeasures, and gap analysis. ACM Computing Surveys (CSUR). 2022 Jan 17, 55(1):1-35.

[64] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19, 11(3):55.

[65] Koubâa A, Qureshi B, Sriti MF, Allouch A, Javed Y, Alajlan M, Cheikhrouhou O, Khalgui M, Tovar E. Dronemap Planner: A service-oriented cloud-based management system for the Internet-of-Drones. Ad Hoc Networks. 2019 Apr 1, 86:46-62.

[66] Al-Turjman F, Abujubbeh M, Malekloo A, Mostarda L. UAVs assessment in software-defined IoT networks: An overview. Computer Communications. 2020 Jan 15, 150:519-36.

[67] Kuru K. Planning the future of smart cities with swarms of fully autonomous unmanned aerial vehicles using a novel framework. IEEE Access. 2021 Jan 5, 9:6571-95.

[68] Abir MA, Chowdhury MZ, Jang YM. Software-Defined UAV Networks for 6G Systems: Requirements, Opportunities, Emerging Techniques, Challenges, and Research Directions. IEEE Open Journal of the Communications Society. 2023 Oct 10.

[69] Nyangaresi VO, Abood EW, Abduljabbar ZA, Al Sibahe MA. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. In2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 Oct 22 (pp. 1-6).

[70] Tsao KY, Girdler T, Vassilakis VG. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. Ad Hoc Networks. 2022 Aug 1, 133:102894.

[71] Mansoor N, Hossain MI, Rozario A, Zareei M, Arreola AR. A Fresh Look at Routing Protocols in Unmanned Aerial Vehicular Networks: A Survey. IEEE Access. 2023 Jun 28.

[72] Rovira-Sugranes A, Razi A, Afghah F, Chakareski J. A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook. Ad Hoc Networks. 2022 May 1, 130:102790.

[73] Kim T, Lee S, Kim KH, Jo YI. FANET Routing Protocol Analysis for Multi-UAV-Based Reconnaissance Mobility Models. Drones. 2023 Feb 25, 7(3):161.

[74] Ahmad S, Hassan MA. Secure communication routing in fanets: A survey. InComputational Intelligence for Unmanned Aerial Vehicles Communication Networks 2022 Mar 30 (pp. 97-110). Cham: Springer International Publishing.

[75] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[76] Abdelmaboud A. The internet of drones: Requirements, taxonomy, recent advances, and challenges of research trends. Sensors. 2021 Aug 25, 21(17):5718.

[77] Yang W, Wang S, Yin X, Wang X, Hu J. A review on security issues and solutions of the Internet of Drones. IEEE Open Journal of the Computer Society. 2022 Jun 14.

[78] Wazid M, Das AK, Rodrigues JJ, Shetty S, Park Y. IoMT malware detection approaches: analysis and research challenges. IEEE access. 2019 Dec 17, 7:182459-76.

[79] Jahanbakht M, Xiang W, Hanzo L, Azghadi MR. Internet of underwater things and big marine data analytics—a comprehensive survey. IEEE Communications Surveys & Tutorials. 2021 Jan 20, 23(2):904-56.

[80] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan, 13(2):691.

[81] Bas J, Dowhuszko AA. End-to-end performance of an uplink NB-IoT transmission relayed on a low-altitude UAV platform with non-orthogonal single-carrier FDMA in the optical wireless backhaul link. Mobile Networks and Applications. 2023 Feb, 28(1):49-64.

[82] Zhang M, Xiong Y, Ng SX, El-Hajjar M. Content-Aware Transmission in UAV-Assisted Multicast Communication. IEEE Transactions on Wireless Communications. 2023 Mar 1.

[83] Donateo T, Ficarella A, Spedicato L, Arista A, Ferraro M. A new approach to calculating endurance in electric flight and comparing fuel cells and batteries. Applied energy. 2017 Feb 1, 187:807-19.

[84] Sepulveda Palacios E, Smith H. Impact of mission requirements on the design of low observable UCAV configurations. Aircraft Engineering and Aerospace Technology. 2019 Oct 21, 91(10):1295-307.

[85] Sziroczak D, Rohacs D, Rohacs J. Review of using small UAV based meteorological measurements for road weather management. Progress in Aerospace Sciences. 2022 Oct 1, 134:100859.

[86] Arafat MY, Alam MM, Moh S. Vision-based navigation techniques for unmanned aerial vehicles: Review and challenges. Drones. 2023 Jan 27, 7(2):89.

[87] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[88] Müller H, Niculescu V, Polonelli T, Magno M, Benini L. Robust and efficient depth-based obstacle avoidance for autonomous miniaturized uavs. IEEE Transactions on Robotics. 2023 Oct 5.

[89] Ma Z, Wang Z, Ma A, Liu Y, Niu Y. A Low-Altitude Obstacle Avoidance Method for UAVs Based on Polyhedral Flight Corridor. Drones. 2023 Sep 19, 7(9):588.

[90] Besada JA, Bergesio L, Campaña I, Vaquero-Melchor D, López-Araquistain J, Bernardos AM, Casar JR. Drone mission definition and implementation for automated infrastructure inspection using airborne sensors. Sensors. 2018 Apr 11, 18(4):1170.

[91] Agarwal A, Mohanta C, Mehta SN. Drone Technologies: State-of-the-Art, Challenges, and Future Scope. Drone Technology: Future Trends and Practical Applications. 2023 May 22:1-9.

[92] Javed F, Khan HZ, Anjum R. Communication capacity maximization in drone swarms. Drone Systems and Applications. 2023 May 5, 11:1-2.

[93] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[94] Zhang JZ, Srivastava PR, Eachempati P. Evaluating the effectiveness of drones in emergency situations: a hybrid multi-criteria approach. Industrial Management & Data Systems. 2023 Feb 3, 123(1):302-23.

[95] Gugan G, Haque A. Path Planning for Autonomous Drones: Challenges and Future Directions. Drones. 2023 Feb 28, 7(3):169.

[96] Jacobsen RH, Matlekovic L, Shi L, Malle N, Ayoub N, Hageman K, Hansen S, Nyboe FF, Ebeid E. Design of an Autonomous Cooperative Drone Swarm for Inspections of Safety Critical Infrastructure. Applied Sciences. 2023 Jan 17, 13(3):1256.

[97] Ihor K. Drones as elements of remote control of the state of geophysical objects. InIOP Conference Series: Earth and Environmental Science 2023 Apr 1 (Vol. 1156, No. 1, p. 012023). IOP Publishing.

[98] Kang KM, Ko YS, Lee YS, Yi J, Won CY. The Operation Method of Hybrid Power Supply System Combining Lithium Polymer Battery and Supercapacitor for Industrial Drones. Energies. 2023 Nov 13, 16(22):7552.

[99] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[100] Yu H, Zhang K, Zhao X, Zhang Y, Cui B, Sun S, Liu G, Yu B, Ma C, Liu Y, Gao W. Research on Data Link Channel Decoding Optimization Scheme for Drone Power Inspection Scenarios. Drones. 2023 Nov 6, 7(11):662.

[101] Yigit Y, Nguyen LD, Ozdem M, Kinaci OK, Hoang T, Canberk B, Duong TQ. TwinPort: 5G drone-assisted data collection with digital twin for smart seaports. Scientific Reports. 2023 Jul 29, 13(1):12310.

[102] Hein D, Gessner M, Kraft T, Gonschorek J. Real-time Distribution of an Airborne Situational Picture into Command and Control Systems.

[103] Ahmadian N, Lim GJ, Torabbeigi M, Kim SJ. Smart border patrol using drones and wireless charging system under budget limitation. Computers & Industrial Engineering. 2022 Feb 1, 164:107891.

[104] Johannessen KA. A conceptual approach to time savings and cost competitiveness assessments for drone transport of biologic samples with unmanned aerial systems (Drones). Drones. 2022 Feb 27, 6(3):62.

[105] Nyangaresi VO, Jasim HM, Mutlaq KA, Abduljabbar ZA, Ma J, Abduljaleel IQ, Honi DG. A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles. Electronics. 2023 Aug 31, 12(17):3688.

[106] Fakhraian E, Semanjski I, Semanjski S, Aghezzaf EH. Towards Safe and Efficient Unmanned Aircraft System Operations: Literature Review of Digital Twins' Applications and European Union Regulatory Compliance. Drones. 2023 Jul 20, 7(7):478.

[107] Rani SS, Deshmukh VM, Pradeep S, Dinesh RM, Prabhu SG. Securing technology enabled services using unmanned aerial vehicles. In2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) 2022 Jan 20 (pp. 234-240). IEEE.

[108] El Adawy M, Abdelhalim EH, Mahmoud M, Mohamed IH, Othman MM, ElGamal GS, ElShabasy YH. Design and fabrication of a fixed-wing Unmanned Aerial Vehicle (UAV). Ain Shams Engineering Journal. 2023 Sep 1, 14(9):102094.

[109] Shah AS. Architecture of emergency communication systems in disasters through UAVs in 5G and beyond. Drones. 2022 Dec 29, 7(1):25.

[110] Müller W, Reinert F, Pallmer D. Open architecture of a counter UAV system. InOpen Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2018 2018 May 9 (Vol. 10651, pp. 34-41). SPIE.

[111] Xu Z, Liu T, Lv H, Shan Y. Hierarchical System Architecture Design of UAV Cluster Based on Mission Requirements. InInternational Conference on 5G for Future Wireless Networks 2022 Dec 17 (pp. 230-239). Cham: Springer Nature Switzerland.

[112] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[113] Adoni WY, Lorenz S, Fareedh JS, Gloaguen R, Bussmann M. Investigation of Autonomous Multi-UAV Systems for Target Detection in Distributed Environment: Current Developments and Open Challenges. Drones. 2023 Apr 12, 7(4):263.

[114] Mademlis I, Torres-González A, Capitán J, Montagnuolo M, Messina A, Negro F, Le Barz C, Gonçalves T, Cunha R, Guerreiro B, Zhang F. A multiple-UAV architecture for autonomous media production. Multimedia Tools and Applications. 2023 Jan, 82(2):1905-34.

[115] Benaya AM, Ismail MH, Ibrahim AS, Salem AA. Physical Layer Security Enhancement via Intelligent Omni-Surfaces and UAV-Friendly Jamming. IEEE Access. 2023 Jan 3, 11:2531-44.

[116] Asim A, Cada M. Enhancement of Physical Layer Security in Flying Ad-hoc Networks by Intelligent Reflecting Metasurfaces. International Journal Of Intelligent Systems And Applications In Engineering. 2023 Jan 16, 11(1s):46-50.

[117] Javaid S, Saeed N, Qadir Z, Fahim H, He B, Song H, Bilal M. Communication and Control in Collaborative UAVs: Recent Advances and Future Trends. IEEE Transactions on Intelligent Transportation Systems. 2023 Mar 20.

[118] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[119] Alkhalifah ES, Almalki FA. Developing an Intelligent Cellular Structure Design for a UAV Wireless Communication Topology. Axioms. 2023 Jan 28, 12(2):129.

[120] Choutri K, Lagha M, Dala L. Multi-layered optimal navigation system for quadrotor UAV. Aircraft Engineering and Aerospace Technology. 2020 Jan 22, 92(2):145-55.

[121] Song Y, Romero A, Müller M, Koltun V, Scaramuzza D. Reaching the limit in autonomous racing: Optimal control versus reinforcement learning. Science Robotics. 2023 Sep 13, 8(82):eadg1462.

[122] Kurunathan H, Huang H, Li K, Ni W, Hossain E. Machine learning-aided operations and communications of unmanned aerial vehicles: A contemporary survey. IEEE Communications Surveys & Tutorials. 2023 Sep 11.

[123] Mademlis I, Symeonidis C, Tefas A, Pitas I. Vision-based drone control for autonomous UAV cinematography. Multimedia Tools and Applications. 2023 Aug 15:1-29.

[124] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11, 2(3):399-406.

[125] Kharchenko V, Grekhov A. Traffic simulation and losses estimation in stratospheric drone network. Peer-to-Peer Networking and Applications. 2023 Jan, 16(1):57-70.

[126] Kim TW, Moon SY, Shin IC, Park JS. A Research on Quantum Repeater Platform Using Drone: Utilization Methods and Considerations. InInternational Conference on Computer Science and its Applications and the International Conference on Ubiquitous Information Technologies and Applications 2022 Dec 19 (pp. 117-123). Singapore: Springer Nature Singapore.

[127] Raivi AM, Huda SA, Alam MM, Moh S. Drone Routing for Drone-Based Delivery Systems: A Review of Trajectory Planning, Charging, and Security. Sensors. 2023 Jan 28, 23(3):1463.

[128] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[129] Lai KT, Chung YT, Su JJ, Lai CH, Huang YH. AI wings: an AIoT drone system for commanding ArduPilot UAVs. IEEE Systems Journal. 2022 Jul 21.

[130] Veerappan CS, Loh PK, Chennattu RJ. Smart Drone Controller Framework—Toward an Internet of Drones. AI and IoT for Smart City Applications. 2022:1-4.

[131] Silva M, Reis A, Sargento S. A Mission Planning Framework for Fleets of Connected UAVs. Journal of Intelligent & Robotic Systems. 2023 May, 108(1):2.

[132] Kumar A, Krishnamurthi R, Nayyar A, Luhach AK, Khan MS, Singh A. A novel Software-Defined Drone Network (SDDN)-based collision avoidance strategies for on-road traffic monitoring and management. Vehicular Communications. 2021 Apr 1, 28:100313.

[133] Erunkulu OO, Zungeru AM, Lebekwe CK, Mosalaosi M, Chuma JM. 5G mobile communication applications: A survey and comparison of use cases. IEEE Access. 2021 Jun 28, 9:97251-95.

[134] Umran, S. M., Lu, S., Abduljabbar, Z. A., & Nyangaresi, V. O. (2023). Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things, 100969.

[135] Lyu X, Li X, Dang D, Dou H, Wang K, Lou A. Unmanned aerial vehicle (uav) remote sensing in grassland ecosystem monitoring: A systematic review. Remote Sensing. 2022 Feb 23, 14(5):1096.

[136] Ma H, Li X, Ji J, Cui H, Shi Y, Li N, Yang C. Monitoring Indicators for Comprehensive Growth of Summer Maize Based on UAV Remote Sensing. Agronomy. 2023 Nov 24, 13(12):2888.

[137] Bao W, Zhu Z, Hu G, Zhou X, Zhang D, Yang X. UAV remote sensing detection of tea leaf blight based on DDMA-YOLO. Computers and Electronics in Agriculture. 2023 Feb 1, 205:107637.

[138] Yamamoto S, Nomoto S, Hashimoto N, Maki M, Hongo C, Shiraiwa T, Homma K. Monitoring spatial and time-series variations in red crown rot damage of soybean in farmer fields based on UAV remote sensing. Plant Production Science. 2023 Jan 2, 26(1):36-47.

[139] Nyangaresi VO, Ibrahim A, Abduljabbar ZA, Hussain MA, Al Sibahee MA, Hussien ZA, Ghrabat MJ. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) 2021 Dec 9 (pp. 1-6). IEEE.

[140] Debauche O, Mahmoudi S, Guttadauria A. A new edge computing architecture for IoT and multimedia data management. Information. 2022 Feb 14, 13(2):89.

[141] Periola AA, Alonge AA, Ogudo KA. Edge computing for big data processing in underwater applications. Wireless Networks. 2022 Jul, 28(5):2255-71.

[142] Bourechak A, Zedadra O, Kouahla MN, Guerrieri A, Seridi H, Fortino G. At the Confluence of Artificial Intelligence and Edge Computing in IoT-Based Applications: A Review and New Perspectives. Sensors. 2023 Feb 2, 23(3):1639.

[143] Khanh QV, Nguyen VH, Minh QN, Van AD, Le Anh N, Chehri A. An efficient edge computing management mechanism for sustainable smart cities. Sustainable Computing: Informatics and Systems. 2023 Apr 1, 38:100867.

[144] Hussein WN, Hussain HN, Hussain HN, Mallah AQ. A deployment model for IoT devices based on fog computing for data management and analysis. Wireless Personal Communications. 2023 Feb 20:1-3.

[145] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149).

[146] Tang J, Duan H, Lao S. Swarm intelligence algorithms for multiple unmanned aerial vehicles collaboration: A comprehensive review. Artificial Intelligence Review. 2023 May, 56(5):4295-327.

[147] Liu HY, Chen J, Huang KH, Cheng GQ, Wang R. UAV swarm collaborative coverage control using GV division and planning algorithm. The Aeronautical Journal. 2023 Mar, 127(1309):446-65.

[148] Alam MM, Moh S. Q-learning-based routing inspired by adaptive flocking control for collaborative unmanned aerial vehicle swarms. Vehicular Communications. 2023 Apr 1, 40:100572.

[149] Murdan AP. Internet of Things for enhancing stability and reliability in power systems. Journal of Electrical Engineering, Electronics, Control and Computer Science. 2023 Jul 13, 9(3):1-8.

[150] Nyangaresi VO, Al Sibahee MA, Abduljabbar ZA, Ma J, Khalefa MS. Biometric-Based Packet Validation Scheme for Body Area Network Smart Healthcare Devices. In2022 IEEE 21st Mediterranean Electrotechnical Conference (MELECON) 2022 Jun 14 (pp. 726-731). IEEE.

[151] Xiao P. A reliability and security enhanced framework for cloud-based storage systems. International Journal of Information Technology and Management. 2023, 22(1-2):160-74.

[152] Wu Q, Xu J, Zeng Y, Ng DW, Al-Dhahir N, Schober R, Swindlehurst AL. A comprehensive overview on 5G-and-beyond networks with UAVs: From communications to sensing and intelligence. IEEE Journal on Selected Areas in Communications. 2021 Jun 15, 39(10):2912-45.

[153] Meng K, Wu Q, Xu J, Chen W, Feng Z, Schober R, Swindlehurst AL. UAV-enabled integrated sensing and communication: Opportunities and challenges. IEEE Wireless Communications. 2023 Apr 10.

[154] Marchese M, Moheddine A, Patrone F. IoT and UAV integration in 5G hybrid terrestrial-satellite networks. Sensors. 2019 Aug 26, 19(17):3704.

[155] Mu J, Zhang R, Cui Y, Gao N, Jing X. UAV meets integrated sensing and communication: challenges and future directions. IEEE Communications Magazine. 2023 Jan 2.

[156] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1, 13(1).

[157] Samanth S, KV P, Balachandra M. Security in internet of drones: a comprehensive review. Cogent Engineering. 2022 Dec 31, 9(1):2029080.

[158] Tanveer M, Nguyen T, Ahmad M, Abdei-Latif A. Towards a secure and computational framework for internet of drones enabled aerial computing. IEEE Transactions on Network Science and Engineering. 2022 Feb 15.

[159] Yu S, Das AK, Park Y, Lorenz P. SLAP-IoD: Secure and lightweight authentication protocol using physical unclonable functions for internet of drones in smart city environments. IEEE Transactions on Vehicular Technology. 2022 Jul 6, 71(10):10374-88.

[160] Jan SU, Abbasi IA, Algarni F. A mutual authentication and cross verification protocol for securing Internet-of-Drones (IoD). Computers, Materials & Continua. 2022 Jan 1, 72(3):5845-69.

[161] Pu C, Wall A, Choo KK, Ahmed I, Lim S. A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of Drones environment. IEEE Internet of Things Journal. 2022 Mar 30, 9(12):9918-33.

[162] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[163] Gorrepati RR, Guntur SR. DroneMap: an IoT network security in internet of drones. Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead. 2021:251-68.

[164] Lv Z. The security of Internet of drones. Computer Communications. 2019 Dec 15, 148:208-14.

[165] Ali OM, Mahmood AF. Edge Computing Towards Smart Applications: A Survey. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science). 2023 Jan 1, 16(1):55-72.

[166] Cox JH, Clark R, Owen H. Leveraging SDN and WebRTC for rogue access point security. IEEE Transactions on Network and Service Management. 2017 Jun 5, 14(3):756-70.

[167] Kuo EC, Chang MS, Kao DY. User-side evil twin attack detection using time-delay statistics of TCP connection termination. In2018 20th International Conference on Advanced Communication Technology (ICACT) 2018 Feb 11 (pp. 211-216). IEEE.

[168] Choudhary G, Sharma V, Gupta T, Kim J, You I. Internet of drones (iod): Threats, vulnerability, and security perspectives. arXiv preprint arXiv:1808.00203. 2018 Aug 1.

[169] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec, 11(4):66.

[170] Deebak BD, Hwang SO. Intelligent drone-assisted robust lightweight multi-factor authentication for military zone surveillance in the 6G era. Computer Networks. 2023 Apr 1, 225:109664.

[171] Perumalla S, Chatterjee S, Siva Kumar AP. Secure communication using multilevel authentication strategy in Internet of Drones. Concurrency and Computation: Practice and Experience. 2023 May 30, 35(12):e7667.

[172] Berini AD, Ferrag MA, Farou B, Seridi H. HCALA: Hyperelliptic curve-based anonymous lightweight authentication scheme for Internet of Drones. Pervasive and Mobile Computing. 2023 May 1, 92:101798.

[173] Hassija V, Chamola V, Agrawal A, Goyal A, Luong NC, Niyato D, Yu FR, Guizani M. Fast, reliable, and secure drone communication: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2021 Jul 16, 23(4):2802-32.

[174] Mishra D, Singh M, Reval P, Pursharthi K, Kumar N, Barnawi A, Rathore R. Quantum-safe Secure and Authorized Communication Protocol for Internet of Drones. IEEE Transactions on Vehicular Technology. 2023 Jul 6.

[175] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[176] Mekdad Y, Aris A, Babun L, El Fergougui A, Conti M, Lazzeretti R, Uluagac AS. A survey on security and privacy issues of UAVs. Computer Networks. 2023 Apr 1, 224:109626.

[177] Tedeschi P, Al Nuaimi FA, Awad AI, Natalizio E. Privacy-Aware Remote Identification for Unmanned Aerial Vehicles: Current Solutions, Potential Threats, and Future Directions. IEEE Transactions on Industrial Informatics. 2023 Jun 5.

[178] Akram J, Umair M, Jhaveri RH, Riaz MN, Chi H, Malebary S. Chained-Drones: Blockchain-based privacy-preserving framework for secure and intelligent service provisioning in Internet of Drone Things. Computers and Electrical Engineering. 2023 Sep 1, 110:108772.

[179] Alsamhi SH, Curry E, Hawbani A, Kumar S, Hassan UU, Rajput NS. DataSpace in the Sky: A Novel Decentralized Framework to Secure Drones Data Sharing in B5G for Industry 4.0 toward Industry 5.0.

[180] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2(4):608-13.

[181] Lounis K, Ding SH, Zulkernine M. D2D-MAP: A Drone to Drone Authentication Protocol Using Physical Unclonable Functions. IEEE Transactions on Vehicular Technology. 2022 Nov 24, 72(4):5079-93.

[182] Lykou G, Moustakas D, Gritzalis D. Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. Sensors. 2020 Jun 22, 20(12):3537.

[183] Westbrooke V, Lucock X, Greenhalgh I. Drone Use in On-Farm Environmental Compliance: An Investigation of Regulators' Perspectives. Sustainability. 2023 Jan 23, 15(3):2153.

[184] Alhussan AA, Al-Dhaqm A, Yafooz WM, Razak SB, Emara AH, Khafaga DS. Towards Development of a High Abstract Model for Drone Forensic Domain. Electronics. 2022 Apr 7, 11(8):1168.

[185] Studiawan H, Grispos G, Choo KK. Unmanned Aerial Vehicle (UAV) Forensics: The Good, The Bad, and the Unaddressed. Computers & Security. 2023 Jun 18:103340.