# Airspace Security: Challenges and Innovations in Drone Technology for Transportation, Military and Industrial Applications. A Brief Review

Vivian Ukamaka Ihekoronye, Urslla Uchechi Izuazu, Jae Min Lee, Dong-Seong Kim
*Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea*
*Kumoh National Institute of Technology* Gumi, South Korea
ihekoronyevivian@gmail.com, (uursla8, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—This study conducts a brief review emphasizing the significance of drone technology across various sectors, including military, logistics, and industrial surveillance. The paper explores the evolution of drone technology and highlights the susceptibility of drones to diverse attacks, buttressing the importance of robust anti-drone systems for airspace security. Based on state-of-the-art literature, the integration of blockchain technology and artificial intelligence are reliable and robust solution to mitigate airspace accidents resulting from inappropriate drone usage.**

***Index Terms*—Airspace Security, Artificial Intelligence, Blockchain technology, Drone technology.**

## I. Introduction

Drone technology has revolutionized various sectors in today's technological-driven world, including military defense, transportation systems, industrial surveillance, etc. As drones have evolved into sophisticated Internet of Things (IoT) devices with multiple uses, they have transcended their original functionality as recreational gadgets. However, drones have a heightened need for security, precision, and efficiency, to minimize airspace accidents due to their misusage by attackers and amateurs.

In this study, the significant roles of drone technology are highlighted. Also, the corresponding security issues associated with its adoption for military applications and transportation in smart cities, are unraveled for airspace security. Specifically, the contributions of state-of-the-art literature and the innovative strategies implemented using artificial intelligence and blockchain technologies to provide security, precision, and efficiency for airspace security are presented.

The rest of the paper goes thus: Section II analyzes the potential threats associated with the adoption of drones. In Section III, the threat mitigation strategies implemented in recent works are discussed, and Section IV concludes the brief review.

## II. THREAT ANALYSIS

The proliferation and benefits of drones are not without challenges. Some of the crucial issues faced in smart cities corresponding to drone applications revolve around ensuring the security, precision, and reliability of the deployment of drones for national security and airspace safety.

- **Security Challenges in Internet of Military Things (IoMT):**

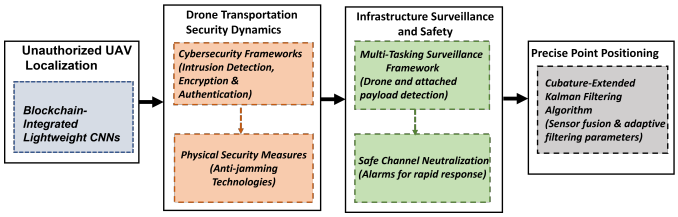


Fig. 1. Drone Threat Mitigation Techniques

IoMT is an interconnected military network consisting of various IoT devices (with drones inclusive) and communication technologies, deployed to collect and exchange data during military operations. Drones significantly contribute to military operations through their capabilities to operate in hard-to-reach environments. They are mostly deployed for intelligence, reconnaissance, and surveillance operations, capturing vast amounts of data in real-time; enhancing military situational awareness. The IoMT network is highly susceptible to cyberattacks launched by adversaries to compromise the confidentiality, availability, and integrity of sensitive data conveyed by drones during operations. Therefore, it is imperative to safeguard against unauthorized data interceptions and the injection of falsified data to ensure the security of the IoMT network. Also, localization attacks, such as interference with navigational and positional signals via GPS spoofing and jamming attacks, are threats to the IoMT network.

- **Security Dynamics in Smart Mobility Systems:** The prevalent utilization of drones for priority-based logistics in smart cities can be attributed to the technological convergence of advanced drone capabilities and AI. Undoubtedly, the ubiquitous usage of logistics drones can potentially violate smart cities' aerial security. Attackers can exploit drones for the illicit transportation of hazardous weapons or explosives across national borders, escalating the risk of conflicts. Such threats can be devastating when there are incongruent drone detection techniques or insufficient authentication mechanisms to distinguish between legitimate and rogue drones [1].
- **Adversarial Profiling in Real-Time Infrastructure Surveillance:** The rise in civilian drone applications,

particularly for logistics, poses a challenge in redefining the anti-drone strategy. Currently, attackers exploit drones equipped with stealth technologies to spy on industrial facilities. Stealth technologies reduce the drone's visibility, making it difficult for anti-drone systems to detect the presence of the rogue drone. Since attackers have become more innovative in their attack strategies, there also should be a corresponding advancement of anti-drone systems for robust illegal drone detection. The anti-drone systems should be capable of detecting drones in real-time amidst the drone's altitude and the weather conditions in which it was flown [2].

- **False Positioning Estimations:** Signal interference by attackers can compromise the intended flight path of drones, resulting in flight accidents. Attackers can also employ signal jammers to disrupt the drone's GPS signals, causing it to lose its satellite connection. As a result, the drone will rely on falsely injected positioning data sent by the attacker. Once the spoofing or jamming attack is successfully launched, the attacker gains unauthorized access and disrupts the drone's functionality [3].

## III. THREATS MITIGATION STRATEGIES

Recent mitigation strategies for the drone system encompass both AI and blockchain technology for robust airspace security. Based on current literature the following techniques highlighted in Fig. 1 are mostly employed to mitigate both the attacks on drones and the attacks exploited by the use of drones. These techniques are briefly discussed in this section and are subject to enhancement for more effective drone usage.

- **Integrated Blockchain and AI Framework:** The authors in [4] designed an integrated blockchain and centralized deep learning framework to detect and identify unauthorized UAV nodes in the IoMT network. The blockchain system authenticates users to control unauthorized access, while the CNN model analyzes the radio frequency signal sent by the drones' antenna array element to determine the direction of arrival for the localization of any illegal UAV in the network. The absence of evaluating the robustness of the CNN model to adversarial attacks should preempt further research on the assessment of the framework to adversaries.
- **Cybersecurity Frameworks:** In [1], they proposed the design of intrusion detection, encryption, and authentication techniques as viable means of securing cyberspace. These techniques utilized evolutionary AI algorithms such as self-supervised learning, federated learning, reinforcement learning, and explainable AI to create models that can detect anomalous data in drone communication channels. In addition, the integration of functional NFT and blockchain technology into the drone network and model designs helps validate the AI-model source of data, maintain integrity, and establish edge-to-edge connectivity in the network. Nevertheless, the investigation of a decentralized federated learning scheme will enhance the scalability and robustness of attack detection models.
- **Multi-Tasking Surveillance Framework:** The design of a vision-based multi-tasking anti-drone framework for real-time detection of drones in varying weather scenarios while identifying the harmful status of the drones in the airspace was designed in [2]. The authors also integrated a safe-channel neutralization model to counter rogue drones with harmful attached payloads. Future directions in this area should be on the model's optimization with considerations to efficiency and reliability. Furthermore, there is a need for the evaluation of the model's robustness for real-world deployment and testing.
- **Precise Point Positioning (PPP) Optimization:** PPP inaccuracies are the major challenge of the global navigation satellite system units providing positional data for the navigation of drones. To ensure efficient drone navigation and eliminate PPP errors and complexity, authors in [3] proposed an intelligent hybrid cubature extended Kalman filter computation model that can be integrated into the drones' GPS-IMU. Thereby, improving the drone's ability to navigate, communicate, and execute predefined tasks in any given environment. Future works should explore adaptive learning mechanisms that allow the navigation system to continuously improve and adapt to changing environments, for optimal drone operations.

## IV. CONCLUSION

This work presents current innovative mitigation strategies that leverage artificial intelligence (AI) and blockchain technologies to fortify airspace security caused by the misusage of drones. Although the state-of-the-art literature reviewed in this work proposed efficient and effective drone defense strategies, there is still the need for further advancement. Future works should focus on assessing the robustness of existing models against adversarial attacks, optimizing real-time deployment, and addressing emerging challenges in this dynamic landscape. Which were overlooked in the literature.


## ACKNOWLEDGMENT

This research was supported by the MSIT, Korea, under the Innovative Human Resource Development for Local Intellectualization support program (IITP-2024-2020-0-01612) supervised by the IITP and by Priority Research Centers Program through the NRF of Korea funded by the MEST(2018R1A6A1A03024003)


## REFERENCES


[1] S. O. Ajakwe, D.-S. Kim, and J.-M. Lee, "Drone transportation system: Systematic review of security dynamics for smart mobility," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14 462–14 482, 2023.

[2] S. O. Ajakwe, V. U. Ihekoronye, D.-S. Kim, and J. M. Lee, "Dronet: Multi-tasking framework for real-time industrial facility aerial surveillance and safety," *Drones*, vol. 6, no. 2, 2022. [Online]. Available: https://www.mdpi.com/2504-446X/6/2/46

[3] W.-P. Nwadiugwu, S.-H. Kim, and D.-S. Kim, "Precise-point-positioning estimations for recreational drones using optimized cubature-extended kalman filtering," *IEEE Access*, vol. 9, pp. 134 369–134 383, 2021.

[4] R. Akter, M. Golam, V.-S. Doan, J.-M. Lee, and D.-S. Kim, "Iomt-net: Blockchain-integrated unauthorized uav localization using lightweight convolution neural network for internet of military things," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6634–6651, 2023.