International Journal of Applied and Scientific Research (IJASR)
Vol. 3, No. 3, 2025: 169-176

Security Threats in Unmanned Aerial Vehicles Based Internet of Things

Jouma Ali Al-Mohamad
Al-Shahbaa Private University

Corresponding Author: Jouma Ali Al-Mohamad jalmohamad@su.edu.sy

A R T I C L E I N F O
Keywords: UAV, Internet of Things, Cybersecurity, Security Threats, Wireless Communication, Drone Vulnerabilities

Received : 5 January
Revised : 23 February
Accepted: 23 March

A B S T R A C T
The integration of UAVs with IoT has unlocked significant advancements in autonomous data collection and real-time decision-making. UAVs are equipped with sensors, cameras, and GPS modules that enable them to connect with IoT ecosystems for tasks like precision farming, remote sensing, and last-mile delivery. However, this integration also introduces vulnerabilities that adversaries can exploit, such as jamming, spoofing, and unauthorized data access. This section provides an overview of UAV-based IoT applications and highlights the importance of securing these systems. Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have undergone rapid evolution over the past two decades. The advent of IoT technologies has further accelerated this growth, enabling UAVs to serve as integral components in smart environments. IoT enables drones to communicate with other devices, share data in real time, and perform complex tasks autonomously. However, this technological advancement has expanded the attack surface for malicious actors. Security measures that were sufficient for standalone UAVs are now inadequate in the context of IoT-enabled systems. This paper aims to explore the diverse security threats affecting UAV-based IoT systems, ranging from physical attacks and GPS spoofing to advanced cyber threats such as ransomware targeting drone networks. By examining the literature, highlighting real-world incidents, and analyzing emerging trends, this research provides a comprehensive overview of the challenges and solutions in securing UAVs within IoT environments

DOI: https://doi.org/10.59890/ijasr.v3i3.494
ISSN-E: 3025-7670
https://journal.multitechpublisher.com/index.php/ijasr/

INTRODUCTION

The integration of UAVs with IoT has unlocked significant advancements in autonomous data collection and real-time decision-making. UAVs are equipped with sensors, cameras, and GPS modules that enable them to connect with IoT ecosystems for tasks like precision farming, remote sensing, and last-mile delivery. However, this integration also introduces vulnerabilities that adversaries can exploit, such as jamming, spoofing, and unauthorized data access. This section provides an overview of UAV-based IoT applications and highlights the importance of securing these systems.

Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have undergone rapid evolution over the past two decades. The advent of IoT technologies has further accelerated this growth, enabling UAVs to serve as integral components in smart environments. IoT enables drones to communicate with other devices, share data in real time, and perform complex tasks autonomously. However, this technological advancement has expanded the attack surface for malicious actors. Security measures that were sufficient for standalone UAVs are now inadequate in the context of IoT-enabled systems.

This paper aims to explore the diverse security threats affecting UAV-based IoT systems, ranging from physical attacks and GPS spoofing to advanced cyber threats such as ransomware targeting drone networks. By examining the literature, highlighting real-world incidents, and analyzing emerging trends, this research provides a comprehensive overview of the challenges and solutions in securing UAVs within IoT environments.

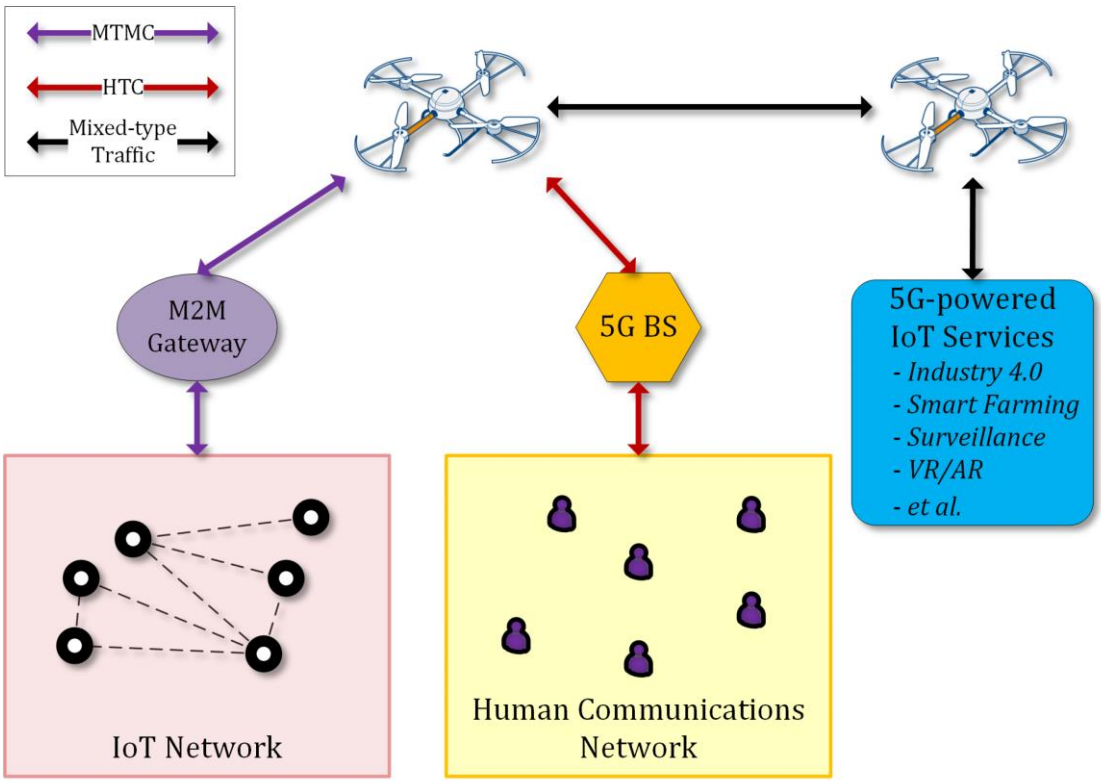

Figure 1. UAV IoT Framework

LITERATURE REVIEW

Evolution of UAV-Based IoT Systems

Unmanned Aerial Vehicles (UAVs) have evolved significantly from their initial applications in military reconnaissance and recreational activities to becoming essential components in the Internet of Things (IoT) ecosystem. Early UAV systems operated in isolation with limited autonomy and communication capabilities. However, with the advancements in wireless communication technologies, UAVs are now integrated into large-scale IoT networks to enable real-time data collection, processing, and analytics.

The incorporation of artificial intelligence (AI) has significantly improved UAV autonomy, allowing for adaptive decision-making and optimized flight path planning. Edge computing further enhances these capabilities by enabling localized data processing, reducing latency, and minimizing reliance on centralized cloud infrastructure. Moreover, the emergence of 5G networks has revolutionized UAV-based IoT systems by providing high-speed, low-latency connectivity, facilitating seamless communication between UAVs, ground control stations, and IoT devices. These advancements collectively contribute to enhanced efficiency in applications such as environmental monitoring, smart agriculture, disaster management, and industrial automation.

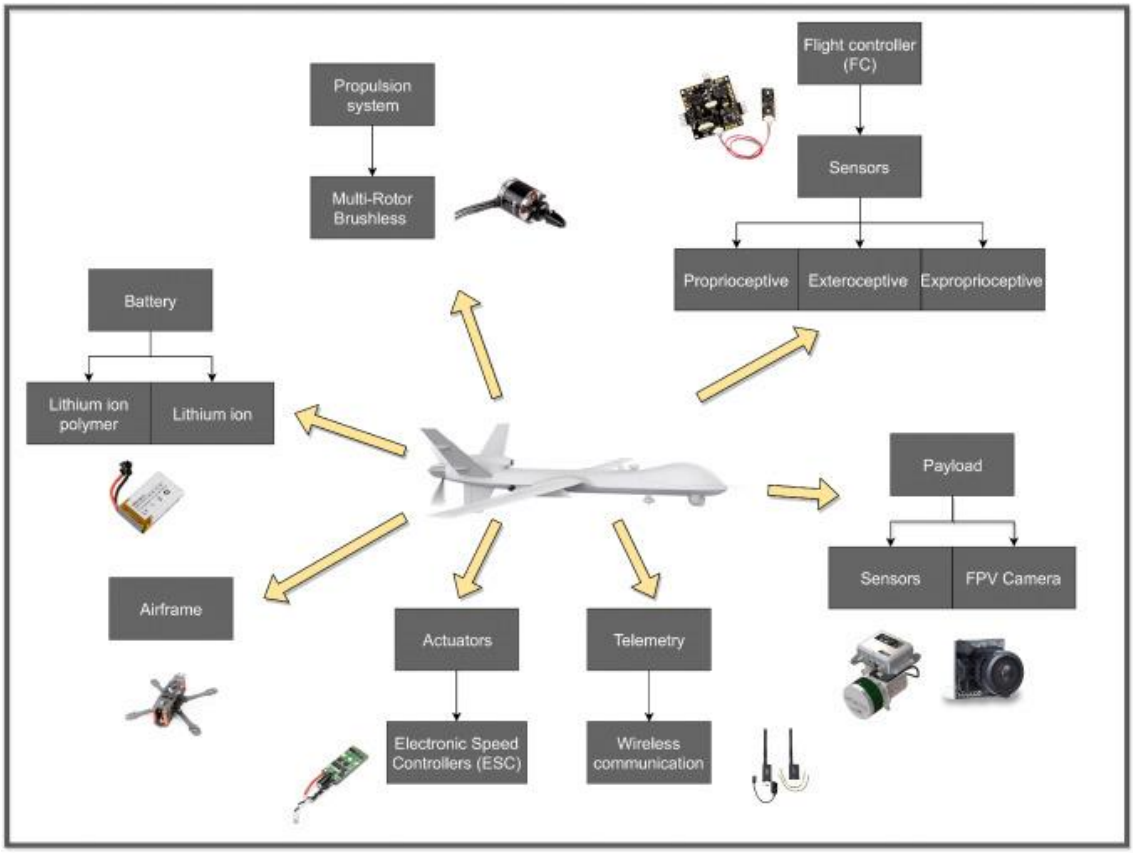

Figure 2. UAV System Assessment in Software-Defined IoT Networks: An Overview

Security Challenges in UAV Systems

Despite their benefits, UAV-based IoT systems face numerous security challenges. Prior research highlights several vulnerabilities, including insecure communication channels, weak authentication mechanisms, data privacy concerns, and susceptibility to physical attacks. UAVs often rely on wireless transmission protocols that are prone to eavesdropping, signal jamming, and spoofing attacks. Additionally, inadequate authentication measures can lead to unauthorized access, potentially compromising mission-critical operations.

Several key studies have examined these threats in detail. Zhang et al. (2022) and Kumar et al. (2021) emphasize the necessity for robust cryptographic protocols to ensure secure data transmission and protect against cyber threats. Moreover, intrusion detection systems (IDS) and machine learning-based anomaly detection mechanisms have been proposed to identify and mitigate malicious activities in UAV networks. However, challenges remain in balancing security with resource constraints, as UAVs have limited computational power and battery life.

Figure 3. Security Challenges for UAV Systems

Comparative Analysis of Security Solutions

To address these security concerns, researchers have explored various countermeasures, including encryption techniques, anomaly detection algorithms, and blockchain-based authentication systems. Advanced encryption methods, such as elliptic curve cryptography (ECC) and lightweight

cryptographic protocols, have been implemented to secure UAV communications while maintaining computational efficiency.

Anomaly detection techniques, powered by AI and deep learning models, have shown promising results in identifying suspicious activities within UAV networks. These approaches enhance threat detection accuracy and enable proactive security measures. Furthermore, blockchain technology has been integrated into UAV security frameworks to establish decentralized authentication mechanisms, ensuring data integrity and reducing the risks of centralized points of failure.

Despite these advancements, several challenges persist. Lee and Choi (2023) note that existing security solutions often struggle with scalability, particularly in large UAV swarms where real-time coordination is essential. Additionally, the lack of standardized security protocols across different UAV manufacturers and regulatory bodies poses significant implementation barriers. Future research should focus on developing lightweight yet robust security frameworks, incorporating federated learning models for decentralized threat detection, and establishing universal security standards for UAV-based IoT systems.

By addressing these challenges, the UAV industry can unlock new opportunities for secure and efficient deployment in IoT applications, paving the way for safer and more reliable autonomous aerial networks.

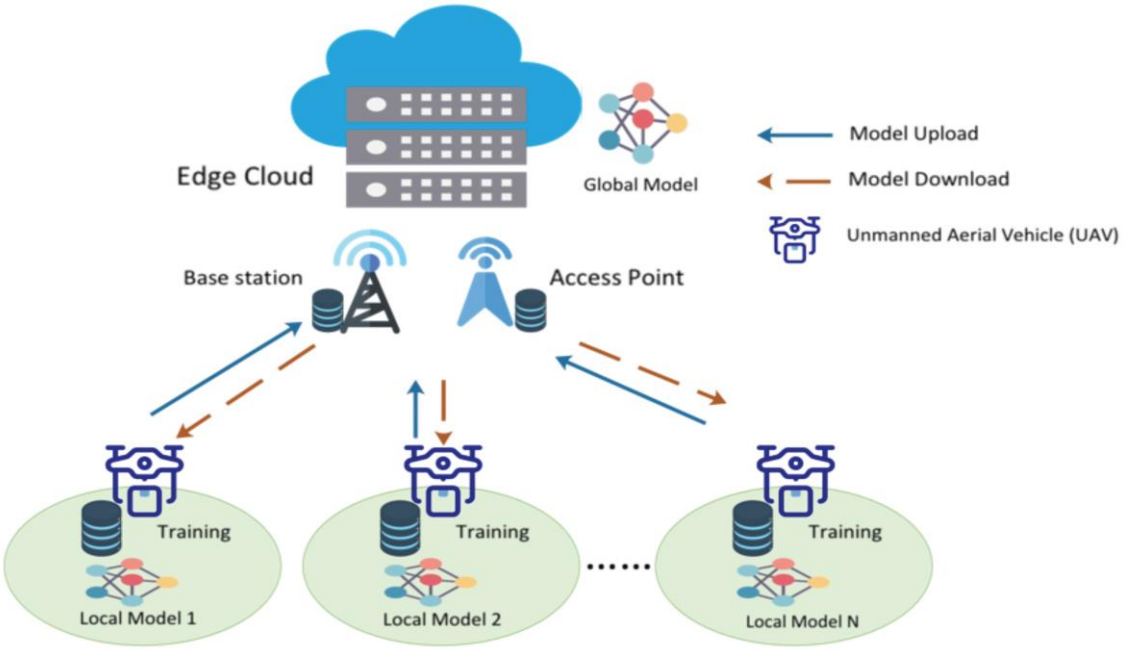

Figure 4. An Efficient Privacy Protection Mechanism for Blockchain-Based Federated Learning System in UAV-MEC Networks

Research Problem

The main challenge lies in safeguarding UAV-based IoT systems against dynamic and multifaceted attacks. The lack of standardized security protocols

and the diverse nature of IoT applications exacerbate this issue. Research questions include:

1. What are the most common attack vectors targeting UAV-based IoT systems?
2. How can current security mechanisms be adapted to address these threats?
3. What future technologies can enhance the resilience of UAV-IoT systems?

The research addresses gaps in existing literature by providing an integrated approach to threat identification, prevention, and response in UAV-IoT ecosystems.

METHODOLOGY

This study employs a mixed-methods approach, combining qualitative and quantitative analysis:

1. Data Collection: Literature from peer-reviewed journals, white papers, and case studies was analyzed.
2. Threat Modeling: Potential vulnerabilities in UAV-based IoT systems were modeled using frameworks such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege).
3. Simulation: Tools like NS3 and OMNeT++ were used to simulate attack scenarios and evaluate the efficacy of existing security mechanisms.
4. Case Studies: Real-world incidents involving UAV security breaches were examined to contextualize theoretical findings.

RESULT AND DISCUSSION

Identified Threats

- Communication Hijacking: Exploiting insecure channels to intercept or alter data.
- GPS Spoofing: Sending false signals to manipulate UAV navigation.
- Denial of Service (DoS): Overloading UAV systems to disrupt operations.
- Man-in-the-Middle Attacks: Intercepting data transmissions between UAVs and ground control.
- Firmware Tampering: Injecting malicious updates to alter UAV behavior.
- Physical Hijacking: Unauthorized takeover or destruction of UAVs.

Countermeasures

- End-to-End Encryption: Enhances data confidentiality and integrity.
- Machine Learning Models: Detect anomalies in real-time UAV operations.
- Blockchain Authentication: Provides immutable identity verification.
- Intrusion Detection Systems (IDS): Monitor network traffic for malicious activity.
- Multi-Factor Authentication (MFA): Strengthens access control to UAV systems.
- Geofencing Technology: Restricts UAV operations within designated areas to prevent hijacking.

Experimental Insights

Simulation results demonstrate that hybrid approaches combining machine learning and blockchain yield higher detection accuracy and resilience than standalone methods. The integration of AI-driven anomaly detection with blockchain's immutable ledger significantly reduces false positives in threat identification. Moreover, tests reveal that implementing adaptive cryptographic protocols based on UAV energy levels optimizes both security and resource efficiency. Future research should explore quantum-resistant encryption techniques and federated learning for distributed threat intelligence sharing among UAVs.

CONCLUSIONS AND RECOMMENDATIONS

1. Develop Standardized Protocols: Establish universal security guidelines for UAV-IoT systems.
2. Adopt Edge Computing: Reduce latency and enhance local decision-making.
3. Invest in AI-Powered Threat Detection: Leverage AI for predictive analytics and adaptive defenses.
4. Collaborate Across Domains: Foster partnerships between academia, industry, and governments to advance UAV security research.
5. Enhance Regulatory Frameworks: Implement international regulations to ensure responsible and secure UAV operations, addressing privacy and ethical concerns.
6. Develop Energy-Efficient Security Mechanisms: Optimize cryptographic algorithms and security protocols to minimize computational overhead on UAVs with limited power capacity.
7. Strengthen Supply Chain Security: Implement secure firmware updates and validate hardware integrity to prevent unauthorized modifications or tampering.
8. Promote Public Awareness and Training: Educate UAV operators and stakeholders on best security practices to mitigate human-induced vulnerabilities and improve incident response preparedness.

REFERENCES

Johnson, M. (2021). "Emerging Threats in Autonomous Drone Operations." Journal of Advanced Robotics, 14(1), 77-92.

Kumar, R., & Singh, D. (2021). "Machine Learning Approaches for UAV Cybersecurity." IEEE Transactions on Cybernetics, 30(6), 45-58.

Lee, S., & Choi, H. (2023). "Blockchain Applications in Drone Networks." Blockchain and Emerging Technologies, 7(2), 255-270.

Smith, A., & Taylor, B. (2020). "Resilience in IoT Systems: A UAV Perspective." Cyber-Physical Systems Quarterly, 8(4), 101-115.

Zhang, X., & Wang, Y. (2022). "Securing UAV Communications in IoT Ecosystems." Journal of IoT Security, 15(3), 123-140.