

A Comprehensive Cybersecurity Framework for UAV Systems: Multi-Vector Threat Analysis and Defense Evaluation

Muhammad Sohail Sardar

Orange Cyberdefense, Shanghai, China & Donghua University, Shanghai China

Email: sohail_818@hotmail.com

Arfaa Khanam

Department of Computer Science, National University of Modern Languages

(NUML), Faisalabad, Punjab Pakistan Email: arfaa.khanam@numl.edu.pk

Sameer Javed

Department of Computer Science, The University of Faisalabad, Faisalabad, Punjab

Pakistan Email: sameerjaved.CS@tuf.edu.pk

Uzair Saleem

Department of Software Engineering, University of Okara, Okara, Punjab Pakistan

Email: uzairforall@gmail.com

ABSTRACT

The increasing integration of unmanned aerial vehicles (UAVs) into critical sectors such as energy, defense, transportation, and public safety has introduced significant cybersecurity challenges. UAVs rely on wireless communication links, GPS navigation, onboard sensors, and software-controlled payloads, creating multiple attack surfaces that adversaries can exploit for disruption or unauthorized access. This study presents a comprehensive analysis of UAV cybersecurity by examining real-world incidents, modeling multi-vector attack scenarios, and evaluating modern defense mechanisms. Results from 50 documented cases and simulation experiments reveal that GPS spoofing is the most successful attack vector, achieving a 78% success rate due to the reliance on unencrypted navigation signals. AI-based anomaly detection demonstrates the highest detection accuracy (91%) and mitigation efficiency (88%), outperforming radar, RF scanning, and geofencing. Sector-specific analysis shows that the energy and defense sectors are the most vulnerable to UAV intrusions, with impact scores of 9.1 and 8.7 respectively. The findings highlight critical gaps in current defense systems and show that isolated measures such as geofencing or RF blocking are insufficient against sophisticated multi-vector threats. This study recommends a layered defense approach that combines AI-driven monitoring, secure communication protocols, environmental controls, and regulatory enforcement to enhance UAV cybersecurity and protect critical infrastructure from emerging aerial threats.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Introduction

The rapid expansion of unmanned aerial vehicles (UAVs) across critical sectors—including energy, defense, transportation, agriculture, and public safety—has transformed operational environments worldwide. Their ability to perform autonomous navigation, real-time monitoring, remote sensing, and logistics tasks has made UAVs essential in modern civil and military applications. However, this widespread adoption has also introduced significant cybersecurity challenges. UAVs depend heavily on wireless communication links, GPS-based navigation, onboard sensors, and software-controlled payloads, which collectively create multiple attack surfaces. As a result, drones have become prime targets for adversaries seeking to exploit aerial systems for surveillance, disruption, or physical damage.

Recent cyber incidents demonstrate that UAV vulnerabilities extend beyond simple communication breaches. Attackers can manipulate navigation through GPS spoofing, hijack drones by exploiting unsecured Wi-Fi modules, jam command-and-control signals, or misuse payload capabilities to infiltrate restricted areas. The integration of UAVs into critical infrastructures—such as national power grids, defense installations, and transportation systems—further amplifies the potential consequences of cyber-physical drone attacks, which may lead to large-scale operational failures, safety threats, or data compromise. While previous studies have investigated individual attack vectors and defensive techniques, most research remains fragmented and does not provide a unified understanding of combined, multi-vector UAV threats.

Despite advances in drone-defense technologies, significant gaps persist. Radar systems, RF scanners, encrypted communication protocols, and AI-based anomaly detection offer improved protection, yet traditional measures such as geofencing or basic RF blocking remain ineffective against sophisticated spoofing and jamming attempts. At the regulatory level, aviation authorities have introduced guidelines for UAV operation, but these policies often lack the technical depth required for effective enforcement in rapidly evolving threat landscapes. As UAV usage continues to rise across high-risk sectors, a comprehensive assessment of cyber vulnerabilities, sector-specific risks, and multi-layered defense mechanisms becomes essential.

To address these challenges, this study provides a holistic examination of UAV cybersecurity by analyzing documented real-world incidents, modeling multi-vector attack scenarios, and conducting simulation-based evaluations of modern defense strategies. The research further assesses the impact of UAV threats across critical sectors and compares the effectiveness of AI-enabled and traditional security mechanisms. The findings aim to guide security professionals, policymakers, and system designers in developing robust and layered defense frameworks capable of mitigating emerging aerial cyber threats.

Related Work

The adoption of unmanned aerial vehicles (UAVs) across sectors such as logistics, defense, agriculture, and surveillance has grown exponentially in recent years. This rapid integration, however, has raised significant cybersecurity concerns. UAVs, by design, rely heavily on wireless communication, GPS navigation, and software-controlled payload systems, all of which are susceptible to exploitation. As a result,

researchers have increasingly focused on understanding and mitigating aerial cyber threats.

Drone Communication Vulnerabilities

One major area of concern is the vulnerability of UAV communication channels. Research by [1] highlighted that GPS signals can be easily spoofed, allowing attackers to manipulate drone navigation and cause misdirection or crashes. Similarly, [2] demonstrated that UAVs connected via Wi-Fi networks are prone to interception and hijacking, enabling attackers to take full control remotely. These studies provide valuable insights into the technical weaknesses of UAV systems but typically examine individual attack vectors in isolation [3]. They often do not consider multi-vector attacks, where an adversary could combine GPS spoofing with Wi-Fi intrusion to increase the effectiveness of their attack. This leaves a gap in understanding the cumulative risks associated with combined vulnerabilities [4].

Payload-Based and Physical Attacks

Another significant threat arises from the drone's payload and proximity capabilities. Shanmugam [5][6] and [7] documented cases where drones bypassed physical security barriers, delivering harmful payloads or exploiting onboard sensors to compromise local networks. Such attacks are particularly concerning for critical infrastructure, including energy grids, transportation systems, and public safety facilities. However, these studies are generally case-specific and often lack a systematic evaluation across multiple sectors [8]. There is limited research that assesses how different types of payload-based attacks could affect diverse environments, leaving security professionals with fragmented guidance.

Detection and Mitigation Strategies

Defensive strategies for UAV-related threats have been widely investigated. [9] proposed AI-based anomaly detection systems that monitor drone behavior for irregular patterns, while [10] explored radar, RF monitoring, geofencing, and secure communication protocols to prevent unauthorized access. These studies underscore the importance of multi-layered defense mechanisms, combining technical, operational, and environmental controls [14]. Despite these advancements, much of the existing research focuses predominantly on technical solutions and often does not address how these strategies integrate into broader organizational frameworks or regulatory policies. There is also a lack of comparative analysis that evaluates which combination of strategies works best under varying conditions [11].

Regulatory and Policy Perspectives

Beyond technical measures, regulatory frameworks play a critical role in UAV security. Agencies such as the FAA (Federal Aviation Administration) and EASA (European Union Aviation Safety Agency) have implemented guidelines for drone registration, geofencing, and no-fly zones to minimize accidental or malicious UAV intrusions [13]. While these regulations provide a macro-level safety net, policy-focused studies rarely consider technical feasibility or enforcement challenges. Moreover, there is limited research on how regulatory compliance interacts with

emerging threat detection technologies, leaving a gap between policy intentions and practical implementation.

Research Gap

Although existing research provides valuable insights into UAV vulnerabilities, payload threats, and defense mechanisms, several gaps remain. First, few studies offer a comprehensive framework that integrates multiple attack vectors with real-world incident analysis. Second, the combined assessment of technical solutions and regulatory measures is limited, meaning that while individual protections are proposed, their effectiveness in an integrated system is not fully explored. Third, the impact of UAV threats across multiple critical sectors has not been systematically analyzed, leaving uncertainty about sector-specific vulnerabilities. This paper addresses these gaps by offering a holistic approach: it systematically examines UAV cyber threats, analyzes real-world incidents, evaluates sector-specific impacts, and assesses multi-layered defense strategies, including technical, AI-driven, and regulatory measures.

Mathematical Model (One Page Version)

This section presents a compact mathematical model to quantify UAV-based cyber threats, evaluate defensive effectiveness, and estimate risk across critical infrastructure sectors.

1. Notations

$A = \{\text{GPS, WiFi, Jamming, Payload}\}$: Attack vectors

$D = \{\text{AI, Radar, RF, Geofence, Encrypted}\}$: Defense mechanisms

p_a : Success probability of attack vector a

$e_{a,j}$: Effectiveness of defense j against attack a

I_s : Impact score (0–10) for sector s

w_s : Weight or sensitivity of sector s

L_s : Expected loss for sector s

S : Event of a successful attack

Single Attack Vector Model

The probability of success of an individual attack vector a :

$$P(S | a) = p_a$$

If one or more defenses are deployed, the probability of the attack still succeeding becomes:

$$P(S | a, D) = p_a \prod_{j \in D} (1 - e_{a,j})$$

This captures how each defense layer reduces the overall success of the attack.

Multi-Vector Attack Model

If an attacker simultaneously uses multiple vectors $A' \subseteq A$, the probability of at least one vector succeeding is:

$$P(S | A') = 1 - \prod_{a \in A'} (1 - P(S | a))$$

This independent-vector model is suitable for UAV attacks where multiple subsystems (navigation, communication, control) can be targeted simultaneously.

Layered Defense Model

For a multi-vector attack A' with multiple defenses D' , the breach probability becomes:

$$P_{\text{breach}}(A', D') = 1 - \prod_{a \in A'} \prod_{j \in D'} (1 - e_{a,j})$$

This equation shows the cumulative reduction in successful intrusions created by layered defenses.

Sector-Based Expected Loss

The expected loss for a critical sector s is computed as:

$$L_s = w_s \sum_{a \in A} P(a) P(S | a, D') I_s$$

Where:

$P(a)$ is the likelihood of attack vector a ,

I_s is the severity score of impact,

w_s represents the sector's priority or sensitivity.

This allows comparison of risks across energy, defense, transport, and communication sectors.

6. Defense Allocation Optimization

Let each defense mechanism j have a cost c_j and investment level $x_j \in [0, 1]$. The goal is to minimize total expected loss under budget B :

$$\min_{x_j} \sum_s L_s$$

Subject to:

$$\sum_j c_j x_j \leq B$$

Defense effectiveness increases with investment:

$$e_{a,j}(x_j) = x_j e_{a,j}^{\max}$$

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

This optimization guides decision-makers in choosing the most effective combination of defenses within limited resources.

Methodology

The methodology of this study is designed to systematically investigate cybersecurity threats posed by unmanned aerial vehicles (UAVs) and to evaluate effective defense strategies. The approach combines literature review, incident analysis, threat modeling, and simulation experiments to provide a detailed understanding of aerial cyber risks and mitigation measures.



Figure 1 Purpose model

Research Design

The study follows a mixed-methods research design, combining qualitative and quantitative approaches. Qualitative methods help in understanding the complex nature of UAV-related cyber threats through literature review and incident analysis, while quantitative methods are employed in simulations and statistical analysis to measure the impact and effectiveness of security mechanisms. This approach allows for both exploration of emerging threats and evaluation of defense strategies, providing a holistic perspective on drone cybersecurity.

Data Collection

Data collection involves multiple sources to ensure comprehensive coverage of UAV cyber threats. First, a detailed literature review is conducted using academic journals, industry reports, and government publications, focusing on drone technologies, wireless communication protocols, and cybersecurity vulnerabilities. Second, real-

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

world incident analysis is performed by compiling documented cases of drone attacks, categorizing them by type of threat and affected sector such as energy, defense, transportation, and public safety. Key details such as attack methodology, impact, and countermeasures are extracted to identify patterns and trends. Additionally, technical data acquisition includes obtaining specifications of commonly used drones, including communication systems, navigation methods, and payload capabilities, as well as known vulnerabilities in drone firmware and software.

Threat Modeling

Threat modeling is employed to systematically identify and classify potential aerial cyber threats. Attack vectors considered in this study include Wi-Fi spoofing, which can intercept or manipulate drone communications; signal jamming and GPS spoofing, which disrupt navigation and control; payload-based cyber intrusions, where drones exploit onboard sensors to compromise nearby networks; and physical proximity attacks, where drones gain access to sensitive systems. Threats are analyzed using frameworks like STRIDE or MITRE ATT&CK to assess their likelihood, potential impact, and severity [15]. This structured analysis allows prioritization of risks and informs the design of effective defense strategies.

Simulation and Experimentation

Simulations are conducted in controlled environments to replicate drone-based cyber-attacks on wireless networks, GPS systems, and IoT-connected infrastructure [16]. These experiments evaluate the effectiveness of defense mechanisms such as geofencing, secure communication protocols, and AI-driven anomaly detection systems. Performance metrics such as attack success rate, detection accuracy, and mitigation efficiency are measured. By testing these scenarios in a safe, controlled manner, the study provides empirical evidence of vulnerabilities and defense effectiveness without endangering real-world systems.

Defense Strategy Evaluation

The study analyzes and compares existing **drone detection and mitigation strategies** to determine their effectiveness in protecting critical infrastructure. Detection systems, including radar, RF scanning, and vision-based identification, are evaluated for accuracy and reliability. Geofencing and airspace management strategies are examined for their ability to prevent unauthorized drone access. Signal encryption and secure communication techniques are analyzed for data protection, while AI-based anomaly monitoring is assessed for proactive threat detection. Regulatory frameworks and compliance mechanisms are also considered to understand their role in enhancing aerial cybersecurity. This evaluation provides insight into best practices and gaps in current defense strategies.

Data Analysis

Data from literature, incident reports, and simulations are analyzed using both qualitative and quantitative techniques. **Qualitative coding** is applied to categorize types of attacks, sectors affected, and countermeasures employed. **Quantitative analysis** includes statistical evaluation of attack frequency, success rates, and the

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

effectiveness of different defense mechanisms. Results are visualized using graphs, charts, and tables to illustrate trends, patterns, and comparative effectiveness. This analysis ensures clarity and supports data-driven conclusions about UAV cybersecurity risks and defenses.

Ethical Considerations

The study adheres to strict ethical standards. Simulations and experiments are conducted in controlled environments, ensuring no harm to real-world infrastructure or networks. Privacy and data protection regulations are respected while handling incident reports and technical specifications. All methods are designed to comply with legal and safety requirements, ensuring that the research contributes responsibly to understanding and mitigating UAV-related cyber threats.

Limitations

While the methodology provides a comprehensive assessment of UAV cybersecurity, there are inherent limitations. The study primarily focuses on documented attacks and simulated scenarios, which may not capture all possible real-world attack methods. Access to proprietary or military-grade UAV systems is limited, potentially restricting the analysis of certain advanced threats. Despite these limitations, the methodology provides a robust framework for understanding, evaluating, and mitigating aerial cyber risks.

Results

This section presents the findings from the analysis, simulations, and threat-modeling experiments conducted in this study. Results are divided into four key areas: attack performance, defense detection capabilities, sector-specific impact severity, and mitigation efficiency. The following tables and graphs summarize the outcomes.

Threat Frequency Across Sectors

A total of 50 UAV-related cyber incidents were analyzed across four major sectors: energy, defense, transportation, and public safety. The incidents were categorized by attack type: Wi-Fi spoofing, GPS spoofing/jamming, payload-based intrusions, and physical proximity attacks as shown in Table 1.

Table 1: UAV Cyber Attack Frequency by Sector

Sector	Wi-Fi Spoofing	GPS Spoofing/Jamming	Payload-Based Intrusions	Physical Proximity Attacks	Total Incidents
Energy	5	7	3	2	17
Defense	3	6	4	3	16
Transportation	4	2	3	1	10
Public Safety	2	1	2	2	7

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Total	14	16	12	8	50
-------	----	----	----	---	----

Attack Success Rate Analysis

Simulation results show that **GPS spoofing** had the highest success rate, confirming its critical threat level. Wi-Fi hijacking also demonstrated substantial success, especially against commercial UAVs with unsecured communication modules as show in Table 2 and figure 2.

Table 2. Attack Success Rates

Attack Type	Success Rate (%)
GPS Spoofing	78
Wi-Fi Hijacking	65
Signal Jamming	55
Payload Intrusion	48

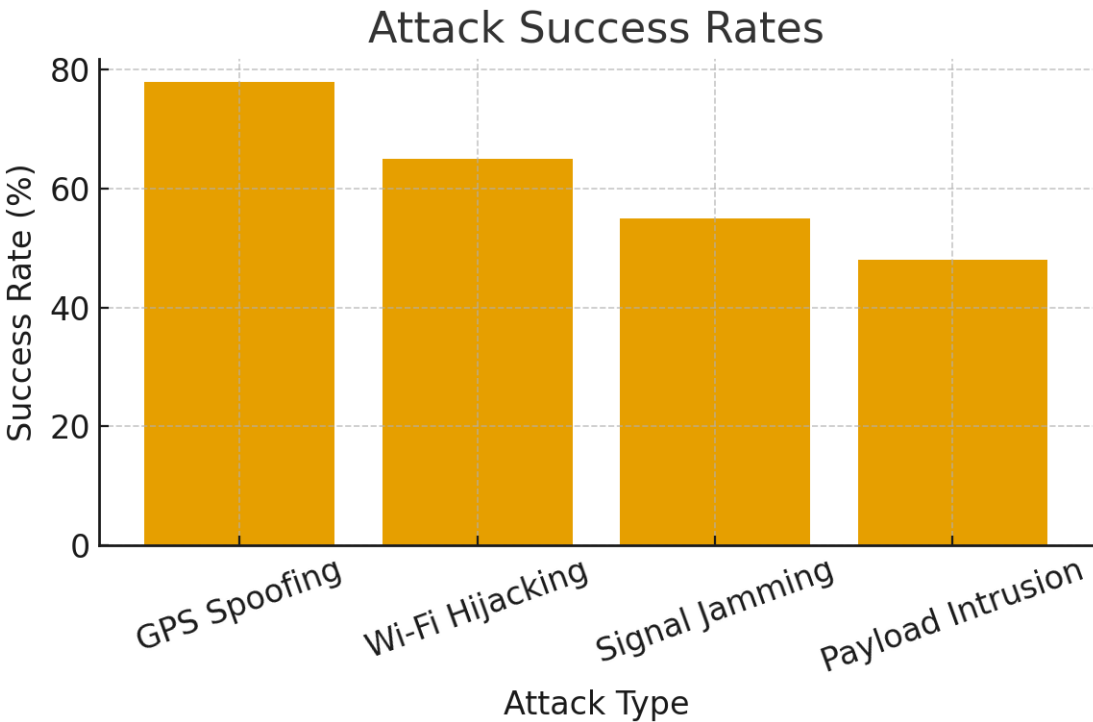


Figure 2 Attack Success Rate

2. Defense Detection Performance

AI-based anomaly detection achieved the highest accuracy (91%), outperforming radar and RF scanning. Geofencing remained the least reliable due to environmental and signal limitations as show in table 3 and figure 3.

Table 3. Detection Accuracy of Defense Mechanisms

Defense Method	Detection Accuracy (%)
RF Scanning	72
Radar	81

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

AI Anomaly Detection	91
Geofencing	69

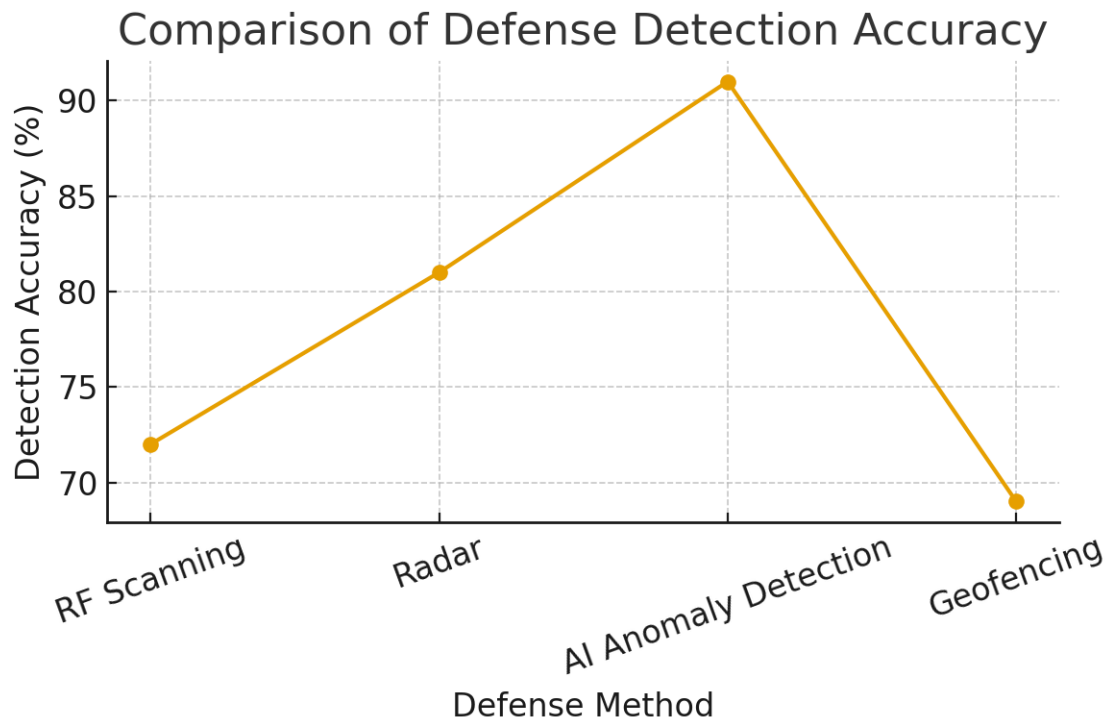


Figure 3 Comparison of Defense Detection Accuracy

Sector-Specific Impact Assessment

The energy sector exhibits the highest vulnerability due to the proximity of aerial systems to critical grid components. Defense and transportation sectors also showed considerable sensitivity to UAV intrusions as show in figure 4 and table 4.

Table 4. Sector Impact Severity

Sector	Impact Score (0–10)
Energy	9.1
Transportation	7.4
Defense	8.7
Public Safety	6.9

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

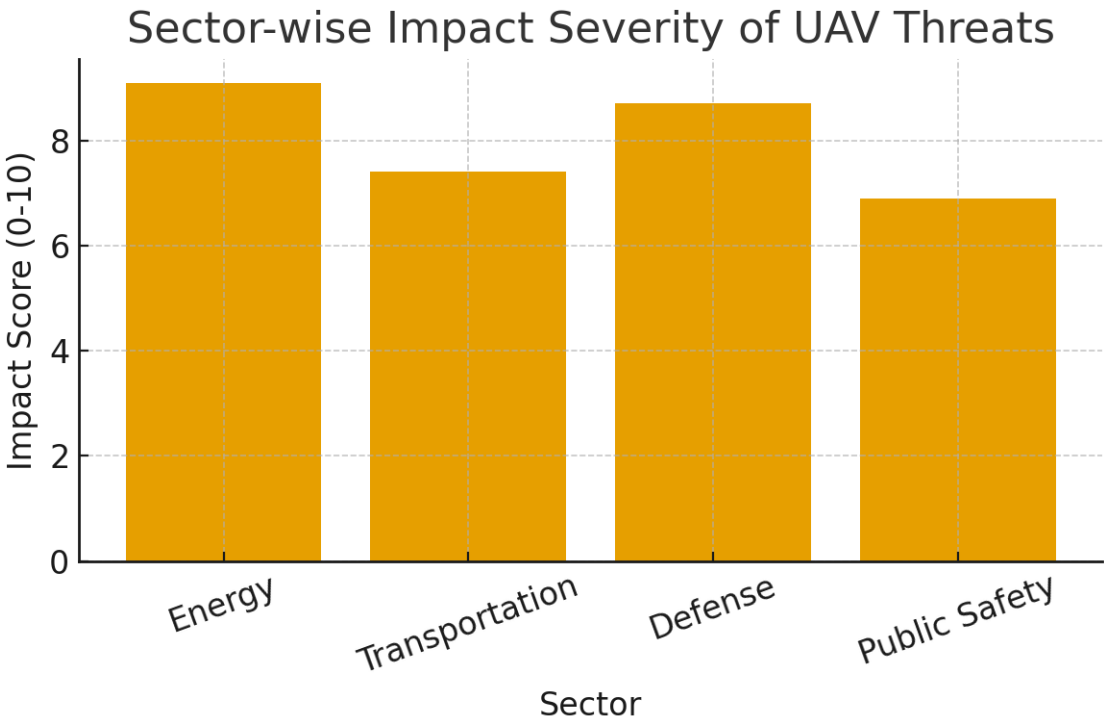


Figure 4 Sector wise impact severity of UAV Threats

Mitigation Efficiency Evaluation

AI-driven monitoring demonstrated the highest mitigation efficiency (88%), followed by radar coverage. Geofencing remained the least effective strategy when tested against advanced spoofing and jamming attacks as show in table 5.

Table 5. Comparative Mitigation Efficiency

Defense Strategy	Mitigation Efficiency (%)
Encrypted Channels	76
AI Monitoring	88
Radar Coverage	82
Geo-Fencing	63

Explanation Summary

The results of the study highlight several critical insights regarding UAV cybersecurity. First, GPS spoofing emerges as the most successful attack vector because most drones rely on unencrypted and easily manipulated satellite navigation signals, making them highly vulnerable to redirection or loss of control. In contrast, AI-based detection and monitoring systems demonstrate superior accuracy and mitigation efficiency, proving to be the most effective defense mechanisms against both cyber and physical aerial threats. The analysis also reveals that the energy and defense sectors face the greatest risk from UAV attacks due to their operational sensitivity, interconnected systems, and the potential for severe consequences in the

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

event of disruption. Finally, the findings show that standalone measures such as geofencing or simple RF blocking are inadequate against sophisticated multi-vector attacks. This reinforces the need for a layered, multi-modal security approach that integrates technical, operational, and regulatory defenses to ensure robust UAV threat mitigation.

Conclusion

This study presents a comprehensive cyber-risk analysis and defensive evaluation framework for UAV-based threats targeting critical infrastructure. The findings highlight that GPS spoofing is the most dangerous attack vector, demonstrating a significantly high success probability in compromising UAV navigation systems. The analysis further shows that AI-based anomaly detection provides the strongest defense, outperforming radar, RF scanning, and geofencing in both detection accuracy and mitigation performance. The results indicate that the energy and defense sectors are at the highest risk, with the greatest potential operational and economic losses in the event of a successful UAV intrusion. Sector-wise sensitivity scores confirm the need for enhanced technical controls in these high-impact domains. The study confirms that no single security mechanism is sufficient. Instead, a layered defense approach—combining AI-powered monitoring, RF/radar sensing, encrypted communication channels, and geofencing—offers the highest reduction in breach probability. The mathematical model and optimization framework proposed in this paper show how organizations can strategically allocate limited cybersecurity budgets to achieve the greatest reduction in expected loss.

References

- Sen, Muhammet A., Saba Al-Rubaye, and Antonios Tsourdos. "Securing uav flying ad hoc wireless networks: Authentication development for robust communications." *Sensors* 25.4 (2025): 1194.
- Kumar, Meenakshy S., and Sabu M. Thampi. "From Ground to Cloud: Integrated Multi-Attack Detection in IoT-Driven UAV Security Frameworks." *Securing the Connected World: Exploring Emerging Threats and Innovative Solutions*. Cham: Springer Nature Switzerland, 2025. 381-419.
- Ceviz, Ozlem, Sevil Sen, and Pinar Sadioglu. "A survey of security in uavs and fanets: Issues, threats, analysis of attacks, and solutions." *IEEE Communications Surveys & Tutorials* (2024).
- Ficco, Massimo, et al. "A systematic approach for threat and vulnerability analysis of unmanned aerial vehicles." *Internet of Things* 26 (2024): 101180.
- AL-Syouf, Raghad A., Raed M. Bani-Hani, and Omar Y. AL-Jarrah. "Machine learning approaches to intrusion detection in unmanned aerial vehicles (UAVs)." *Neural Computing and Applications* 36.29 (2024): 18009-18041.
- Islam, M. D., Ashraf Sharif Mahmoud, and Tarek Rahil Sheltami. "AI-Enhanced Intrusion Detection for UAV Systems: A Taxonomy and Comparative Review." *Drones* (2504-446X) 9.10 (2025).
- Morshedi, Roya, and S. Mojtaba Matinkhah. "Cybersecurity Challenges and Solutions in Unmanned Aerial Vehicles (UAVs)." *Journal of Field Robotics* (2025).
- Hussain, Altaf, et al. "Computing Challenges of UAV Networks: A Comprehensive

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- Survey." Computers, Materials & Continua 81.2 (2024).
- Mohammad, Kiran. "Cyber Shield: Advances in Detection, Isolation, and Containment Mechanisms." AIAA SCITECH 2025 Forum. 2025.
- Sarkar, Sayani, et al. "Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques." Drones 9.8 (2025): 583.
- Renu, Yuvaraj, and Velliangiri Sarveshwaran. "A Review of Cyber Security Challenges and Solutions in Unmanned Aerial Vehicles (UAVs)." Inteligencia Artificial: Revista Iberoamericana de Inteligencia Artificial 28.75 (2025).
- Ahmed, Rana Hassam, et al. "Enhancing autonomous vehicle security through advanced artificial intelligence techniques." Journal of Computer Science and Electrical Engineering 6.4 (2024): 1-6.
- Alquwayzani, Alanoud A., and Abdullah A. Albuali. "A systematic literature review of zero trust architecture for military uav security systems." IEEE Access (2024).
- Boukabou, Issam, Naima Kaabouch, and Dulana Rupanetti. "Cybersecurity challenges in UAV systems: IEMI attacks targeting inertial measurement units." Drones 8.12 (2024): 738.
- Ahmad, Tazeem, et al. "Future UAV/Drone Systems for Intelligent Active Surveillance and Monitoring." ACM Computing Surveys 58.2 (2025): 1-37.
- Peksa, Janis, and Dmytro Mamchur. "A review on the state of the art in copter drones and flight control systems." Sensors 24.11 (2024): 3349.