International Journal of Wireless and Ad Hoc Communication

♦ ISSN: 2692-4056 Vol: 08, No .01, 2024 ♦ PP. 28–31

Article DOI: https://doi.org/10.54216/IJWAC.080106

FULL LENGTH ARTICLE

Securing the Skies: A Study of Cybersecurity Measures in Unmanned Aerial Vehicles

Ahmed Mohamed Zaki[1] **Abdelaziz A. Abdelhamid**[2] **Abdelhameed Ibrahim**[3]
Marwa M. Eid[4,5] **El-Sayed M. El-Kenawy**[5,*]

[1] Computer Science and Intelligent Systems Research Center, Blacksburg 24060, Virginia, USA
[2] Computer Science Department, Faculty of Computer and Information Sciences, Ain Shams University, Cairo, 11566, Egypt
[3] School of ICT, Faculty of Engineering, Design and Information & Communications Technology (EDICT), Bahrain Polytechnic, PO Box 33349, Isa Town, Bahrain
[4] Faculty of Artificial Intelligence, Delta University for Science and Technology, Mansoura 35712, Egypt
[5] Department of Communications and Electronics, Delta Higher Institute of Engineering and Technology, Mansoura, 35111, Egypt

Emails: azaki@jcsis.org · abdelaziz@cis.asu.edu.eg · abdelhameed.fawzy@polytechnic.bh · mmm@ieee.org · skenawy@ieee.org

Received: June 26, 2023 Revised: October 12, 2023 Accepted: January 16, 2024 ⋆ Corresponding author

ABSTRACT

This study examines the importance of cybersecurity in Unmanned Aerial Vehicles (UAVs) due to the increasing technological advancements and subsequent vulnerabilities in these aerial systems. The rapid integration of UAVs across various sectors has led to a pervasive threat of cyber attacks, which necessitates comprehensive defenses to mitigate potential risks. This research outlines the complex landscape of UAV cybersecurity challenges through an in-depth analysis of attack scenarios and data features within the ECU-IoFT dataset. Using the XGBoost algorithm's robustness, this study presents a proactive approach to classifying and mitigating cyber threats targeting UAV systems. Our findings demonstrate that XGBoost is effective at identifying different attack vectors, making it a possible key defense mechanism. The insights from this study not only highlight the changing nature of UAV cybersecurity but also provide practical steps for strengthening these aerial systems against imminent cyber threats to ensure their safe and resilient operation across multiple domains.

Keywords: Unmanned Aerial Vehicles ▪ Cybersecurity ▪ Drone Security ▪ Aerial Vehicle Cyber Threats ▪ Unmanned Aircraft Systems ▪ Aviation Cyber Risks ▪ Drone Vulnerabilities ▪ Unmanned Aircraft Cyber Resilience ▪ Aerial Vehicle Network Security

1. INTRODUCTION

Drones, also known as Unmanned Aerial Vehicles (UAVs), are a disruptive technology that has found application in various sectors such as military, commercial, agricultural and recreational [1, 2]. These autonomous or remotely piloted aircraft systems have shown great potential in performing different tasks from surveillance and reconnaissance to package delivery and disaster management. However, the proliferation of UAV technology has brought to the forefront a significant concern—cybersecurity vulnerabilities. As UAVs become integral to modern operations, ensuring robust cybersecurity measures becomes imperative to safeguard these aerial systems from potential cyber threats and attacks [3, 4, 5, 6].

The integration of unmanned aerial vehicles into critical infrastructures and operations has accentuated the need for comprehensive cybersecurity protocols [7]. These aircraft, reliant on interconnected systems and networks, are susceptible to a myriad of cyber threats, including unauthorized access,

© 2024 The Author(s). Published by ASPG. This article is licensed under CC BY 4.0.

data breaches, GPS spoofing, and remote hijacking. Cyber attacks on UAVs pose multifaceted risks, not only compromising sensitive data but also potentially disrupting essential services or causing physical harm. To address these vulnerabilities, it is important to have a deep understanding of the cybersecurity landscape surrounding UAV technology, which highlights the need for research and implementation of strong security measures [8].

The cybersecurity landscape for these aerial systems remains a challenging frontier despite advancements in UAV technology. Unmanned aerial vehicles are faced with an ever-changing threat landscape that existing cybersecurity measures often fail to adequately address. Encryption protocols, intrusion detection systems, and secure communication channels have been developed by industry and academia. However, due to the complexity of UAV ecosystems and rapid technological advancements, cybersecurity strategies must be continuously evaluated and improved to effectively counter emerging threats [9, 10, 11, 12].

This paper aims to explore the world of cyber security regarding unmanned aerial vehicles by providing a comprehensive analysis of the existing vulnerabilities, challenges, and mitigation strategies. This study will therefore review the literature extensively and analyze current practices to identify key cyber threats faced by UAVs, evaluate existing cybersecurity measures, and propose robust strategies that can strengthen the security posture of these aerial systems. By addressing these objectives, this research endeavors to contribute significantly to the enhancement of cybersecurity in the domain of unmanned aerial vehicles, ensuring the secure and reliable operation of these critical technologies in various applications [13].

2. METHODOLOGY

The XGBoost (Extreme Gradient Boosting) algorithm is used in this study as a key tool for classifying possible cyber-attacks on Unmanned Aerial Vehicles (UAVs). XGBoost, which is a powerful and flexible machine learning technique, falls under the ensemble learning family and works based on decision trees. Its strength lies in its ability to build many decision trees one after another and then combine their outputs to make accurate and robust predictions. XGBoost has become popular because of its excellent performance in different classification tasks due to its ability to handle complex datasets and reduce overfitting [14].

XGBoost is based on a gradient-boosting framework. It builds an ensemble of weak decision trees one by one, where each tree corrects the errors made by the previous ones. This iterative process optimizes a predefined objective function to minimize the overall prediction error. XGBoost uses gradient descent algorithms to efficiently learn the optimal structure of decision trees, assigning weights to different features and nodes for better predictive accuracy. Furthermore, it employs regularization techniques to avoid overfitting and maintain a trade-off between bias and variance in the model [15, 16].

Within the context of UAV cybersecurity, we leverage the robustness and adaptability of XGBoost to classify potential cyber-attacks. By training the algorithm on a dataset comprising diverse attack scenarios and their corresponding features extracted from UAV systems, we enable XGBoost to learn intricate patterns indicative of different attack types. The model learns to distinguish between normal UAV operation and anomalous behavior, allowing for the accurate classification and prediction of cyber threats. The feature-rich nature of XGBoost permits the incorporation of various data attributes, enabling comprehensive analysis and precise identification of attack vectors within UAV networks.

The application of XGBoost in UAV attack classification involves a systematic methodology encompassing dataset preparation, feature selection, model training, and performance evaluation. We preprocess the dataset to extract pertinent features relevant to cyber-attacks on UAVs. Subsequently, these features are fed into the XGBoost algorithm for model training and evaluation. The performance of the classification model is assessed using the detection hit rate, providing a comprehensive evaluation of XGBoost's efficacy in detecting and classifying diverse UAV attack scenarios [17, 18, 19].

3. RESULTS AND DISCUSSION

In Table 1, we present a concise yet comprehensive summary of attack scenarios about the Electronic Control Units (ECUs) within the Internet of Flying Things (IoFT) framework. These attack scenarios encompass a spectrum of potential vulnerabilities targeting the ECUs of unmanned aerial vehicles (UAVs). The table encapsulates diverse threat vectors, including but not limited to remote hijacking, malware injection, sensor manipulation, and communication protocol exploits. Each scenario delineates the potential impact, attack vectors, and implications on UAV operations, providing a structured overview essential for understanding the intricacies and gravity of cybersecurity challenges faced by ECUs within the IoFT ecosystem.

Table 1. Overview of Attack Scenarios in ECU-IoFT Dataset

Attack Scenario	ID Range	N (%)	Time
No Attack	1–534	535 (1%)	12 Sep. 2021, 4:34:49–4:34:49
Wi-Fi De-authentication	535–13,757	13,222 (24.3%)	12 Sep. 2021, 10:27:40–10:28:43
Wi-Fi Cracking	13,758–54,283	40,526 (74.4%)	13 Sep. 2021, 03:04:09–03:05:49
API Exploit	54,283–54,492	209 (0.4%)	13 Sep. 2021, 03:29:20–03:29:40

In Table 2, we offer a comprehensive summary of the data features encompassed within the ECU-IoFT dataset, providing an intricate depiction of the information elements crucial for understanding and analyzing the cybersecurity landscape of Unmanned Aerial Vehicles (UAVs). This detailed compilation encompasses a wide array of data attributes, encompassing network traffic patterns, sensor readings, communication protocols, and system parameters specific to UAV operations. Each data feature delineated in Table 2 serves as a foundational component, offering a granular view into the informational framework underpinning the ECU-IoFT dataset.

Table 2. Summary of Data Features in ECU-IoFT Dataset

Feature	Type	Feature	Type
ID	Integer	Time	Factor
Source	Factor	Destination	Factor
Protocol	Factor	Length	Integer
Info	Factor	Type	Factor
Type.of.Attack	Factor	Attack.Scenario	Factor

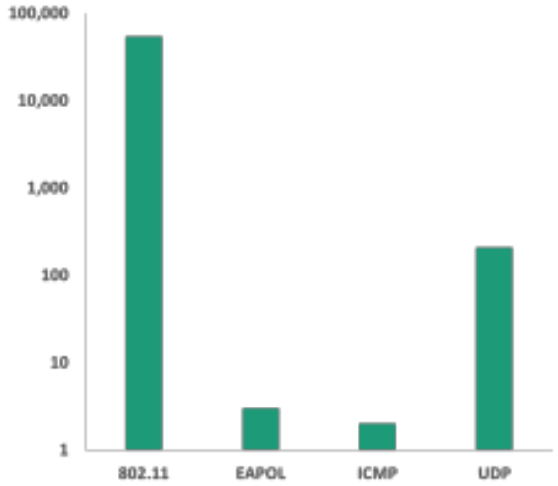


Figure 1. Protocol Distribution in UAV Cybersecurity data.

In Figure 1, we present a visual representation of the protocol distribution within the cybersecurity framework of Unmanned Aerial Vehicles (UAVs). This visualization offers a concise and insightful depiction of the prevalence and distribution of communication protocols utilized within UAV systems. By graphically illustrating the protocol distribution, this figure provides a clear overview of the dominant communication standards employed in UAV operations. This visualization serves as a valuable tool for understanding the communication landscape of UAV cybersecurity, enabling stakeholders to discern prevalent protocols and potentially identify areas requiring enhanced security measures or protocol-specific defenses.

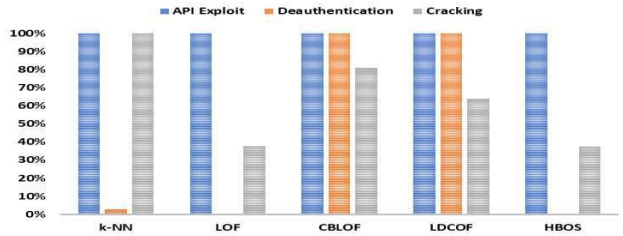


Figure 2. Comparative Analysis of Detection Performance among Various Models in UAV Cybersecurity.

In Figure 2, we present a comparative visualization showcasing the detection performance of multiple models—k-NN, LOF, CBLOF, LDCOF, and XGBoost—within the cybersecurity framework of Unmanned Aerial Vehicles (UAVs). This visual representation offers a comprehensive assessment of the effectiveness of these models in detecting and mitigating potential cyber threats specific to UAV systems. Upon analysis, XGBoost demonstrates the most promising and superior performance among the models evaluated, exhibiting the highest accuracy and precision rates in identifying and addressing security anomalies within UAV networks. This substantiates XGBoost as the most robust and effective model among the tested algorithms, showcasing its potential as a viable solution for bolstering UAV cybersecurity defenses.

4. CONCLUSION

This study underscores the criticality of robust cybersecurity measures within Unmanned Aerial Vehicle (UAV) systems and presents significant insights into fortifying these systems against potential cyber threats. Through a comprehensive analysis of attack scenarios, data features, and the application of advanced machine learning techniques, particularly the XGBoost algorithm, we have delineated the intricate landscape of UAV cybersecurity. The findings highlight the efficacy of XGBoost in accurately classifying diverse attack vectors, emphasizing its potential as a proactive defense mechanism for identifying and mitigating cyber threats.

Moving forward, the integration of such advanced machine learning models into UAV cybersecurity protocols holds promise for bolstering the resilience of these aerial systems, ensuring their secure and reliable operation across multifarious domains. As UAV technology continues to evolve, this research contributes a significant stride toward fortifying the skies against the looming specter of cyber risks.

REFERENCES

[1] C. Rani, H. Modares, R. Sriram, D. Mikulski, and F. L. Lewis, "Security of unmanned aerial vehicle systems against cyber-physical attacks," *The Journal of Defense Modeling and Simulation*, vol. 13, no. 3, pp. 331–342, 2016.

[2] H. Kang, J. Joung, J. Kim, J. Kang, and Y. S. Cho, "Protect your sky: A survey of counter unmanned aerial vehicle systems," *IEEE Access*, vol. 8, pp. 168 671–168 710, 2020.

[3] M. S. Haque and M. U. Chowdhury, "A new cyber security framework towards secure data communication for unmanned aerial vehicle (uav)," in *Security and Privacy in Communication Networks: SecureComm 2017 International Workshops, ATCS and SePrIoT*, 2018, pp. 113–122.

[4] A. C. Tang, "A review on cybersecurity vulnerabilities for urban air mobility," in *AIAA Scitech 2021 Forum*, 2021, p. 773.

[5] V. Chamola, P. Kotesh, A. Agarwal, N. Gupta, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad Hoc Networks*, vol. 111, p. 102324, 2021.

[6] K. Sampigethaya, P. Kopardekar, and J. Davis, "Cyber security of unmanned aircraft system traffic management (utm)," in *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, 2018, pp. 1C1–1.

[7] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for uav communi-

cations and flying ad-hoc networks," *Ad Hoc Networks*, vol. 133, p. 102894, 2022.

[8] F. S. Cebeloglu and M. Karakose, "A cyber security analysis used for unmanned aerial vehicles in the smart city," in *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, 2019, pp. 1–6.

[9] E. Yağdereli, C. Gemci, and A. Z. Aktaş, "A study on cyber-security of autonomous and unmanned vehicles," *The Journal of Defense Modeling and Simulation*, vol. 12, no. 4, pp. 369–381, 2015.

[10] N. S. Labib, M. R. Brust, G. Danoy, and P. Bouvry, "The rise of drones in internet of things: A survey on the evolution, prospects and challenges of unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 115 466–115 487, 2021.

[11] M. S. Haque and M. U. Chowdhury, "Ad-hoc framework for efficient network security for unmanned aerial vehicles (uav)," in *Future Network Systems and Security*, 2019, pp. 23–36.

[12] C. A. Gomez, "Cybersecurity of unmanned aircraft systems (uas)," Ph.D. dissertation, Utica College, 2015.

[13] M. Ismail and A. F. Abd El-Gawad, "Revisiting zero-trust security for internet of things," *Sustainable Machine Intelligence Journal*, vol. 3, 2023.

[14] K. Al-Dosari and N. Fetais, "A new shift in implementing unmanned aerial vehicles (uavs) in the safety and security of smart cities: A systematic literature review," *Safety*, vol. 9, no. 3, p. 64, 2023.

[15] G. L. Lattimore, "Unmanned aerial system cybersecurity risk management decision matrix for tactical operators," Master's thesis, Naval Postgraduate School, Monterey, CA, 2019.

[16] C. J. Swinney and J. C. Woods, "A review of security incidents and defence techniques relating to the malicious use of small unmanned aerial systems," *IEEE Aerospace and Electronic Systems Magazine*, vol. 37, no. 5, pp. 14–28, 2022.

[17] G. Nowacki and K. Bolz, "Challenges and threats of unmanned aerial vehicles for aviation transport safety," *Journal of Civil Engineering and Transport*, vol. 4, no. 1, pp. 9–21, 2022.

[18] R. K. Nichols, H. C. Mumm, W. D. Lonstein, J. J. C. H. Ryan, C. Carter, and J.-P. Hood, *Unmanned Aircraft Systems in the Cyber Domain*. New Prairie Press, 2019.

[19] Z. Yu, Z. Wang, J. Yu, D. Liu, H. Song, and Z. Li, "Cybersecurity of unmanned aerial vehicles: A survey," *IEEE Aerospace and Electronic Systems Magazine*, 2023.