I. J. Mathematical Sciences and Computing, **2024, 2, 32-48**
Published Online on June 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2024.02.04

Comparative Analysis of Threat Detection Techniques in Drone Networks

Syed Golam Abid*
Department of Computer Science and Engineering, Faculty of science and technology, American International University-Bangladesh(AIUB), Dhaka, Bangladesh
E-mail: sg.abid@hotmail.com
ORCID iD: https://orcid.org/0009-0007-8018-7088
*Corresponding author

Muntezar Rabbani
Department of Computer Science and Engineering, Faculty of science and technology, American International University-Bangladesh(AIUB), Dhaka, Bangladesh
E-mail: muntezar88@gmail.com
ORCID iD: https://orcid.org/0009-0008-6875-9298

Arpita Sarker
Department of Computer Science and Engineering, Faculty of science and technology, American International University-Bangladesh(AIUB), Dhaka, Bangladesh
E-mail: sarkerarpita4@gmail.com
ORCID iD: https://orcid.org/0009-0005-9891-4939

Tasfiq Ahmed Rafi
Department of Computer Science and Engineering, Faculty of science and technology, American International University-Bangladesh(AIUB), Dhaka, Bangladesh
E-mail: tasfiqahmedrafi@gmail.com
ORCID iD: https://orcid.org/0009-0002-8493-5171

Dip Nandi
Faculty of Science and Technology, American International University-Bangladesh (AIUB), Dhaka, Bangladesh
E-mail: dip.nandi@aiub.edu
ORCID iD: https://orcid.org/0000-0002-9019-9740

Received: 21 December, 2023; Revised: 24 January, 2024; Accepted: 18 February, 2024; Published: 08 June, 2024

Abstract: With the rapid proliferation of drones and drone networks across various application domains, ensuring their security against cyber threats has become imperative. This paper presents a comprehensive analysis and comparative analysis of the state-of-the-art techniques for detecting cyber threats in drone networks. The background provides a primer on drones, networks, drone network architectures, communication mechanisms, and enabling technologies like wireless protocols, satellite navigation, onboard computers, sensors, and flight control systems. The landscape of emerging technologies including blockchain, software-defined networking, machine learning, fog computing, ad-hoc networks, and swarm intelligence is reviewed in the context of transforming drone network capabilities while also introducing potential vulnerabilities. The paper delves into common cyber threats faced by drone networks such as hacking, DoS attacks, data breaches, and GPS spoofing. A detailed literature review of proposed threat detection techniques is provided, categorized into machine learning, multi-agent systems, blockchain, intrusion detection systems, software solutions, and miscellaneous methods. A key gap identified is handling increasingly sophisticated attacks, complex environments, and resource limitations in aerial platforms. The analysis highlights accuracy, overhead and real-time trade-offs between techniques, while factors like model optimization can influence efficacy. A comparative analysis highlights the advantages and limitations of each approach considering metrics like accuracy, scalability, flexibility, and overhead. Key observations include the trade-offs between computational complexity and real-time performance, the challenges in handling evolving attack techniques, and the dependencies between detection accuracy and factors like model selection and training data quality. The analysis provides a comprehensive reference for cyber threat detection in drone networks, benefiting researchers and practitioners aiming to advance this crucial area of drone

security through robust detection systems tailored for resource-constrained aerial environments.

Index Terms: Drone networks, Cybersecurity, Intrusion detection systems, Anomaly detection, Machine learning, Deep learning, Blockchain, Vulnerabilities, Cyber threats, Security protocols, Satellite navigation systems, Flight control systems, Swarm intelligence, Fog Computing Security, Comparative analysis.

1. Introduction

Drones, also recognized as unmanned aerial vehicles (UAVs), have transformed industries and applications across diverse domains. Ranging in size and configuration from small quadcopters to larger fixed-wing aircraft [1], these aircraft can fly autonomously or be remotely controlled without an onboard human pilot. The capabilities of drones, facilitated by sensors, communication devices, and navigation systems, encompass tasks such as surveillance, aerial photography, package delivery, and inspections. The benefits of drones include cost-effectiveness, accessibility, flexibility, and the ability to access remote or hazardous regions [2]. They excel at capturing high-resolution imagery, efficiently collecting data, and performing tasks with precision. In the context of interconnected systems, drone networks bring a revolutionary aspect. Drone networks encompass interconnected drones capable of communication, coordination, and collaboration. These networks, established through networking technologies, enable drones to interact, exchange data, and collectively execute tasks. Specific applications, such as surveillance operations, swarm-based tasks, or search and rescue missions, can prompt the formation of drone networks. Equipped with communication devices and protocols, drones in these networks establish connections with fellow drones, ground control systems, navigation satellite systems, and air traffic control systems [3]. This communication framework allows drones to share vital information, coordinate their actions, and work towards common objectives. For reliable communication and data exchange, drone networks incorporate network infrastructure and protocols. Utilizing wireless communication technologies, such as radio frequency (RF) or cellular networks [4], alongside ad-hoc networking protocols, these networks establish connections among drones. The control, monitoring, and coordination of drones within the network are facilitated by network management systems and protocols. The integration of drones with networks within drone networks yields advanced capabilities and applications. This integration supports autonomous flight, real-time monitoring, data sharing, and efficient mission planning among drones. The result is an enhancement in the scalability, adaptability, and effectiveness of unmanned aerial systems across various domains.

While drones and drone networks enable transformative capabilities across diverse applications, their security vulnerabilities can facilitate malicious exploits. Existing literature has extensively analyzed threats and detection techniques in traditional IT environments. However, cyber threat detection frameworks customized for decentralized, aerial drone networks remain relatively underexplored despite their growing prevalence. Most analyses focus on generic networks or lack comparative assessments tailored to resource constraints, transient topologies, limited oversight, and tight real-time constraints intrinsic to drones. The explosions of drones from hobbyist quadcopters to commercial delivery fleets urgently necessitate such applied security insights to guide threat detection innovations for this nascent ecosystem. This paper addresses this gap by providing the first comprehensive analysis and comparative study specialized for cyber threat detection in drone networks considering their unique architectures, objectives, and constraints. A rigorous evaluation of detection techniques based on machine learning, blockchain, intrusion detection systems and multi-agent systems is conducted weighing accuracy, overhead, flexibility and other metrics crucial for security with limited onboard capabilities. Observations on optimizing future detection frameworks like balancing computational complexity and timely response, boosting resilience against evolving attacks through adaptive methods, and tweaking solutions to training data availability and quality constraints offer actionable insights tailored to drone network environments.

By bridging security research specialized for traditional systems with the emerging landscape of drone-based solutions, this study contributes guidance for practitioners and a foundation for scholars to advance innovations at the intersection of drone systems and security. The detailed comparative analysis distils observations from dispersed literature to inform detection capabilities catering to the scale, diversity and criticality of expanding commercial and government drone networks while constrained by weight, space, power and cost.

2. Background

The literature review section has been divided into four subsections. The first subsection discusses how drone networks works. The next subsection highlights the technologies and also the emerging technologies that are being highly used and researched in Drone Networks. The third subsection discusses about the issues and vulnerabilities within drone networks. Finally, the last subsection shows the threat detection techniques used to address various cyber threats. The last subsection by collecting the motivation from the previous two subsections highlights formulated hypotheses.

2.1. Working Principle of Drone Networks

Drone/UAS networks comprise unmanned aerial systems, commonly known as drones, equipped with diverse sensors, communication devices, and navigation systems. These networks are designed to facilitate communication with ground control systems, enable navigation via satellite systems, and ensure compliance with air traffic control regulations. Communication between drones and ground control systems involves receiving commands, transmitting telemetry data, and establishing a reliable control link. This interaction is typically facilitated through dedicated datalinks, such as radio frequency (RF) or wireless communication protocols [5]. The central control point for monitoring and managing multiple drones concurrently is the ground control system (GCS) [6]. Additionally, drones rely heavily on navigation satellite systems like GPS to precisely determine their location, altitude, and velocity [5,6]. Moreover, drones operating within controlled airspace adhere to communication requirements with air traffic control systems, ensuring safe integration, coordination with other aircraft, and regulation compliance. Air traffic control (ATC) systems provide essential flight information, airspace restrictions, and real-time traffic updates to drone operators [7].

2.2. Existing Technologies

Drone networks leverage a variety of technologies to enable communication, coordination, and collaboration among drones. Here are some of the key technologies used in drone networks:

Table 1. Existing Technologies in Drone Networks

Technologies	Description
Communication Technologies	Drones use wireless technologies like RF, Wi-Fi, Bluetooth, cellular networks to communicate with each other and ground systems [8,9]. They can also use satellite systems for long-range communication.
Navigation and Positioning Technologies	Drones use GNSS like GPS and IMUs with sensors like accelerometers and gyroscopes to determine position, orientation, velocity for navigation [10,11,12]. Computer vision is also used for navigation.
Data Processing and Storage Technologies	Drones have onboard computers for data processing, decision-making and storage devices like SSDs to store collected data [13,14].
Sensor Technologies	Drones have cameras and other imaging sensors like thermal, multispectral for aerial data collection. Specialized sensors used for environment monitoring [15].
Control Systems and Autonomy	Drones have flight controllers for flight stabilization, navigation. AI and ML used to enhance autonomy [16,17].

2.3. Emerging Technologies

Drone networks are rapidly evolving to leverage new innovations that enhance capabilities and open up new applications. Here are some key emerging technologies for drone networks:

Table 2. Emerging Technologies in Drone Networks

Technologies	Description
Blockchain Technology	Provides security, efficiency through decentralization, tamper-proof ledgers, identity verification, smart contracts for drones [18-24].
Software-defined networking (SDN)	Enables centralized control, dynamic reconfiguration, optimized routing, virtualization, security through controller managing all network resources [25-29].
Machine learning	Provides intelligent data analysis, anomaly detection, computer vision, autonomous navigation, performance optimization, security for drones [30-35].
Ad-hoc Networking	Enables decentralized collaboration, mesh networking, dynamic routing, redundancy, rapid deployment for drones [36,37,38].
Swarm Technology	Facilitates coordinated, distributed operations through formation control, distributed decision-making, load balancing, communication protocols [39-42].
Fog Computing	Provides real-time analytics, efficiency, resilience through localized processing, computation offloading, encryption at network edge [43-46].

2.4 Issues and Vulnerabilities

Issues related to Drone Network Infrastructure: Drone networks face various vulnerabilities including wireless attacks like spoofing and jamming [47,48], compromised onboard systems through unauthorized access [49], malware injection in storage devices [49], inefficient encryption methods [50], manipulation of visual sensors, breaches of ground infrastructure [51], and vulnerabilities in blockchain-based systems like flawed smart contracts. These vulnerabilities arising from communication technologies, onboard systems, sensors, and emerging technologies can be exploited to disrupt operations, gain unauthorized control, and compromise security.

Vulnerabilities related to the Emerging Technologies in Drone Networks: Communication technologies in drone networks face various vulnerabilities that can be exploited by attackers. Weak encryption protocols and insecure wireless network configurations expose sensitive data to unauthorized access through insecure channels, enabling adversaries to gain external access and control over drones [51]. Additionally, unsecured Wi-Fi connections used by smart device-enabled drones make them susceptible to communication disruption and physical damage [52].

Furthermore, Software Defined Networking (SDN) introduces vulnerabilities due to lack of multi-layered protection. SDN controllers can be disrupted by attacks, enabling unauthorized access and spyware integration. Weak authentication leads to information disclosure [53]. The centralized architecture makes SDN controllers critical targets for attacks that can cause single point of failure [53,54]. Complex application interactions also create conflicts in flow rules [54].

Although blockchain provides decentralization and immutability, it still faces threats like smart contract flaws, consensus algorithm attacks, and resource constraints that allow unauthorized transactions, data tampering, and theft. Transaction limits, high energy consumption, and latency impact real-time performance. Both public and private blockchains can be tampered with, causing losses and unauthorized actions. Hardware requirements also affect drone payloads.

Additionally, machine learning and deep learning models used in drones can be manipulated through adversarial attacks to generate biased results [55]. Model performance also varies based on resource availability. Further, insufficient and inaccurate training data reduces model effectiveness and reliability [55]. Large datasets required for mapping environments strain drone storage capacities [55].

At the edge, fog computing introduces vulnerabilities through insecure fog nodes and devices leading to unauthorized access, requiring robust authentication protocols. Weak security measures and inadequate updates also pose threats. Fog computing offers limited computing resources versus centralized clouds. Failed fog nodes in disasters disrupt operations.

Furthermore, ad-hoc networks lack centralized control and consistent security enforcement, making them susceptible to various attacks exploiting their constraints [56,57]. Swarm technologies are challenged by vulnerabilities in mesh protocols, intermittent connections, security protocols, and manufacturing costs [57].

2.5 Types of Detection

Threat detection involves recognizing potential security breaches by monitoring indicators, behaviors, and patterns in a system. Utilizing techniques like Intrusion Detection Systems (IDS), SIEM systems, and behavioral analytics, it identifies unauthorized access, vulnerabilities, and malicious activities. Various tools analyze network traffic, system logs, user behavior, and threat intelligence to detect anomalies or patterns indicating threats [58]. The primary goal is swift response to mitigate damage, bolster security, and safeguard assets and information.

Detection of Cyber Threats in Drone Networks: A multifaceted approach is required to monitor drone operations and communications for cyber threats. Experts utilize real-time monitoring, network traffic analysis, anomaly detection algorithms, and machine learning to identify malicious patterns [59].

Network Traffic Analysis inspects protocols, headers, payloads, frequencies, volumes, and patterns to detect anomalies indicating potential exploitation [60]. Deploying intrusion detection systems (IDS) at the host and network levels analyzes traffic and logs to identify attack signatures, behavioral deviations, and suspicious activities [61].

Signature-based detection quickly flags known threats by matching observed patterns against databases of attack signatures [62]. However, this method struggles with novel threats lacking known signatures. Strong encryption algorithms and authentication mechanisms prevent unauthorized access and tampering of drone communications [63].

Continuous monitoring to identify breach attempts maintains operational integrity. Analyzing drone behavior identifies anomalies in flight, power, sensors, or performance indicating system compromises [64]. Comparing against baselines flags abnormal activities.

As research progresses, engaging with latest academic publications, industry reports, and conferences is imperative to stay updated on evolving techniques and insights [65]. A proactive approach ensures comprehensive understanding aligned with cutting-edge threat detection strategies enabling effective responses to emerging challenges.

Overall, a combination of traffic analysis, IDS, behavioral monitoring, authentication, encryption, signature matching, and machine learning is required for robust cyber threat detection. Continuously updating domain knowledge is key to tackling threats against the rapidly advancing drone ecosystem.

Detection of Physical Threats in Drone Networks: Advanced sensors like proximity, collision detection, and thermal cameras enable drones to perceive the environment and swiftly respond to imminent physical threats through evasive actions [66].

GPS spoofing detection involves analyzing signal attributes to identify anomalies and deviations from expected behavior [67]. Comparing received signals with trusted baseline flags spoofing attempts. Algorithms can also detect threats by identifying patterns and abnormalities in historical flight and sensor data [68]. Machine learning techniques automate and improve this analysis.

Deploying cameras and visual sensors allows real-time surveillance to identify approaching objects or tampering [69]. Object detection algorithms recognize and classify potential threats. By continuously analyzing flight parameters and integrating external data like weather forecasts, algorithms detect anomalies indicating external hazards.

Furthermore, leveraging machine learning algorithms enables intelligent data interpretation. Analyzing speed, altitude, orientation, and other physical attributes identifies deviations possibly signaling interception attempts or unauthorized access. Integrating drone data with external sources provides early warning of risks like adverse weather or restricted airspace.

Overall, a combination of advanced sensors, GPS spoofing detection algorithms, machine learning-based pattern recognition, visual surveillance, flight data analysis, and data integration with external sources provides a

comprehensive approach to safeguard drones from physical threats. The intelligent fusion of internal and external data equips drones with the tools to perceive hazards and navigate safely through complex environments.

3. Comparative Analysis of Techniques

3.1 Threat Detection Techniques

From the literature review, a comparative discussion of the technologies emerging in drone networks has been showcased. Each table describes about the methods used and also the detection techniques that are followed to detect threats and anomalies.

Table 3. Machine Learning Methods

Methods	Detection Technique
Jamming detection in drone networks using Multi-layer Perceptrons and Decision Trees:	Multi-layer Perceptron and Decision Tree [70]. These techniques are incorporated into the framework along with the selected measures to enhance the detection of jamming attacks.
Predicting Application Layer DDoS Attacks Using Machine Learning Algorithms	This paper introduces a new approach for identifying Distributed Denial of Service (DDoS) attacks in network traffic flow data. The method involves analysing the traffic traces and creating an access matrix. By applying Principal Component Analysis (PCA), the method reduces the number of attributes used for detection [71].
Distributed Denial of Service Attacks based on Machine Learning Algorithms	In this article we are shown that can be used to detect Distributed Denial of Service (DDoS) attacks.

Table 4. Deep Learning Methods

Methods	Detection Technique
Autonomous Detection of Malicious Events using Machine Learning Models in Drone Networks	The authors gathered a comprehensive dataset from a drone network, comprising a wide range of normal and attack scenarios.

Table 5. Multi-Agenting Methods

Methods	Detection Technique
A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks	The primary focus of the system is to identify the most dangerous cyber-attacks that can target UAV networks, such as the dissemination of false information, GPS spoofing, jamming, black hole attacks, and gray hole attacks.
Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications	The authors demonstrate that the true positive rate approaches one while bounding the false positive rate to below 0.05% for reckless attackers, below 7% for random attackers with attack probability as low as 0.2, and below 6% for opportunistic attackers when the error of monitoring due to environment noise is at 1%.
A Multiagent and Machine Learning Based Denial of Service Intrusion Detection System for Drone Networks	The goal is to detect Denial-of-Service (DoS) attacks more effectively. By using a combination of these machine learning methods and a multi-agent approach [72], they aim to strengthen the drones' defences and make them more resilient against cyber threats.

Table 6. Blockchain Methods

Methods	Detection Technique
Blockchain based peer to peer communication in autonomous drone operation	The approach we're considering involves using a blockchain ledger to register all the components involved in aerospace operations [73]. This ledger will hold essential information related to communication, making it secure and tamper-proof.

Table 7. IDS Solutions

Methods	Detection Technique
Signal Spoofing and Jamming Attacks in UAV Networks using a Lightweight IDS	The UAV comes equipped with a cutting-edge autopilot system and incorporates smart security measures to ensure its safety. Even in challenging situations like signal loss or potential hacking attempts, the system can safely guide the UAV back home. One remarkable feature is the UAV's ability to distinguish between fake and authentic signals, providing an extra layer of protection.
Specification Based Intrusion Detection for Unmanned Aircraft Systems	The system focuses on protecting sensors and actuators embedded in the UAS and addresses the challenge of detecting sophisticated and hidden attackers while ensuring a high level of security [74]. The researchers use behavior-rule specifications and transform them into state machines to create lightweight, efficient rules for each component.

Table 8. Software Solutions

Methods	Detection Technique
An Amateur Drone Surveillance System Based on Cognitive Internet of Things	The system consists of various active and passive surveillance devices such as cameras, sensors, radars, and drones, or a crowd of people that serve as local fog computing platforms to sense the environment and locally warn the presence of amateur drones. The system has four key fundamental cognitive tasks, sequentially: 1) sensing; 2) data analytics; 3) semantic derivation and knowledge discovery; and 4) intelligent decision-making.
A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework	The algorithm uses cosine similarity to distinguish between DDoS attack flows [75] and normal flows, with a threshold value of cosine similarity used to determine if a port is under attack.

Table 9. Miscellaneous

Methods	Detection Technique
Intrusion Detection System and Threat Estimation with Wireless Networks	The paper proposes a Mahalanobis distance-based detection policy [76] to counter cyber-attacks against data integrity and a distribution of signal strength-based detection policy to counter GPS spoofing attacks that target the GPS coordinates of drones. The paper evaluates the performances of the cyber security system using the NS3 simulator [76] and provides simulation results in Section 4 of the paper.
Intrusion Detection and Ejection Framework Against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology	The framework is based on Bayesian games [76] and aims to detect and deter lethal attacks with high accuracy while incurring low overhead. The simulation results show that the proposed SGF incurs a low overhead [76] to detect and deter lethal attacks with high accuracy.
A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing	The system proposed here is an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) for Man in the Middle (MitM) attack at the fog layer [77]. The authors discuss the need for low resource demanding, yet strong security systems that will protect the fog layer from being attacked [77].
Dynamic Authentication for Threat Mitigation	The dynamic authentication and secure channels approach [78] enables trust establishment and verified identities, which helps mitigate against injection attacks, data breaches, and unauthorized access threats. It is a blockchain and fog computing enabled security architecture that operates on fog nodes to facilitate equipment authentication and secure communication between equipment and cloud. The architecture uses dynamic ECQV certificates, ECIES, and Diffie-Hellman key exchange to establish trust, ensure anonymity, and enable secure channels.
Blockchain-based Threat Monitoring	The blockchain-based trust mechanisms discussed provide transparency, accountability, and access control that aid in detecting threats like data tampering, spoofing, rogue nodes through transaction validation rules and consensus protocols. Discuss using blockchain technology in fog computing to enhance security, transparency, and trust through features like distributed smart contracts, immutable ledgers, and accountability of transactions. Blockchain aids services like access control, identity management, and forensics.
Layered Intrusion Detection Systems	The layered security model [79] incorporates dedicated intrusion detection systems for threat monitoring at the network, data, and device levels. These can employ AI/ML for anomaly detection against threats. Putting forth a layered security model for fog computing consisting of network, data processing, and device privacy categories. They survey authentication, access control, intrusion detection, trust management, and privacy preservation techniques. Encryption, differential privacy, identity obfuscation are some privacy solutions.
Predictive Caching and ML for Threat Detection	The caching and machine learning techniques can enable predictive caching to secure against denial-of-service attacks by caching anticipated popular content. ML also aids in detecting outlier access patterns [80]. By reviewing caching techniques like Steiner tree caching, application-based caching, smart collaborative caching, and deep learning-based content caching that aim to improve efficiency, scalability, throughput, and disaster recovery in fog computing. Machine learning methods for cache optimization are also explored.
Auditing and Threat Attribution using Blockchain	The analysis of security threats and blockchain solutions looks at using blockchain features like immutability, transparency, and decentralization for auditing and threat attribution after detection by other systems. A comprehensive analysis of security threats, issues and blockchain-based solutions in the context of IoT and industrial IoT systems connected via fog computing. Attacks like DDoS, malware, ransomware and solutions like access control, authentication, encryption are covered.
Threat Detection in Fog Computing	Connecting trust establishment, authentication protocols, confidentiality mechanisms, attack detection systems, and privacy preservation techniques to threat detection in fog computing [81]. Specifically, trust validation allows identifying unauthorized and insider attacks, authentication verifies spoofing attempts, encryption breach anomalies indicate data theft attacks. Dedicated detection systems like decoys and malware monitors proactively hunt threats, while privacy tools prevent exposure of data that can enable attacks. The distributed and decentralized infrastructure poses challenges that require decentralized security methodologies tailored to fog computing infrastructure. The study recommends authentication and policy coordination between nodes along with usage control to deal with various threats and attacks.

3.2 Limitation:

Flaws and limitations in a thesis paper refer to inherent weaknesses or constraints that can affect the quality and reliability of the research findings. These can include issues such as narrow scope, inadequate data, biased assumptions, limited generalizability, ethical oversights, lack of replication, and the potential for subjective interpretation.

Table 10. Machine Learning Techniques

Methods	Flaws / Limitations
Multi-layer Perceptrons and Decision Trees	MLP classifiers reach precision values between about 70% and 75%. This indicates that the models may have difficulty accurately distinguishing between normal instances and jamming instances. Accuracy drops as the window size increases. This suggests that the performance of the detection techniques might deteriorate when analyzing a larger context or timeframe. Overfitting on noisy drone data, lack of balanced training datasets, hardware constraints, and sensitivity to small input changes limit the reliability of machine learning approaches. For instance, the low 75% precision of Multi-Layer Perceptrons and Decision Trees specifically for jamming attack detection highlight the difficulty in distinguishing between legitimate and malicious drone behaviors. These flaws need to be addressed for machine learning to be dependable for drone threat detection.
Detection of DDoS Attacks Using Machine Learning Algorithms	Machine learning techniques proposed for detecting distributed denial-of-service (DDoS) intrusions on drones grapple with efficiency and robustness challenges. As highlighted, support vector machines (SVM) tend to have high training and testing times due to complex optimization computations classifying data in hyperspace. This hampers real-time attack prevention capabilities given onboard processing limitations. Additionally, SVMs may mislabel legitimate behaviors as anomalous fairly often, resulting in excessive false alarms. While simpler Bayes classifiers alleviate efficiency issues, their detection accuracy can significantly lag sophisticated models. Naive Bayes made the highest number of classification errors identifying DDoS attacks. Its assumptions of inter-feature independence limit suitability for precisely modeling multi-factor attack vectors. Thus, balancing computational complexity, detection precision, and generalizability remains an open challenge in countering evolving drone threat landscapes using machine learning.

Table 11. Multi-Agenting Methods

Methods	Flaws / Limitations
Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule	Behavior rules are directly derived from threats: The limitations arise from the direct dependency of behavior rules on the defined threats. New threats require adding behavior rules: When new threats are discovered and introduced to the threat model, new behavior rules corresponding to these threats must be added to the rule set. While deriving behavior rules directly from known threats enables precise attack signatures, this tight coupling impedes detecting new and evolving attacks against drones. As adversarial techniques grow more sophisticated, unprecedented zero-day exploits can bypass rules crafted for existing threats. Updating rule sets is an error-prone process requiring extensive expertise and may still fail to capture future attack vectors. Additionally, frequent manual rule additions introduce significant overhead in maintaining robust detection capabilities. The reliance on pre-defined rules renders such intrusion detection systems ineffective against novel threats with unfamiliar patterns.
Multiagent and Machine Learning Based Denial of Service Intrusion Detection System for Drone Networks	The Naive Bayes algorithm cannot be used due to its low accuracy, which does not exceed 68.7%. The scalability of the detection schemes becomes an issue when the number of UAVs increases, particularly in the presence of a high number of attackers. Ensuring consistent detection rates across larger networks and higher attack volumes is crucial for comprehensive security. The low accuracy of the Naive Bayes algorithm in the used technique indicates the need for alternative machine learning algorithms with higher accuracy.

Table 12. Blockchain Methods

Methods	Flaws / Limitations
Blockchain based peer to peer communication in autonomous drone operation	Balancing block size and security can be challenging. In blockchain-based cyber threat and cyber-attack detection, finding the right balance between block size and security is crucial. Blockchain-based cyber threat and cyber-attack detection techniques offer advantages such as decentralization, immutability, and transparency. However, they also face certain flaws and limitations (Kumar et al., 2021). Furthermore, the growth of the blockchain over time leads to increased memory consumption.

Table 13. IDS Solution

Methods	Flaws / Limitations
Detecting Signal Spoofing and Jamming Attacks in UAV Networks using a Lightweight IDS	As the random attack probability decreases, the attacker becomes more hidden and insidious. This indicates a limitation in the detection capability of the Specification IDS.
Specification Based Intrusion Detection for Unmanned Aircraft Systems	This poses a challenge for the Specification IDS in detecting jamming attacks. The Specification IDS shows limitations in detecting signal spoofing and jamming attacks when the random attack probability decreases.

Table 14. Software Solutions

Methods	Flaws / Limitations
DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework	The number of packet-in messages sent by SD-IoT switch S3 to the SD-IoT controller increases with time. This limitation suggests that the detection techniques implemented in the Drone Surveillance System and SD-IoT may suffer from scalability issues. The increase in the number of packet-in messages sent by the SD-IoT switch S3 to the SD-IoT controller over time indicates a scalability limitation.

Table 15. Miscellaneous

Methods	Flaws / Limitations
Intrusion Detection System and Threat Estimation with Wireless Networks	Trade-off between Time Slots and Accuracy: One limitation observed is the trade-off between the number of time slots used for threat estimation and the accuracy of detection [82]. Decreased Accuracy with Increasing Number of UAVs: Another limitation identified is that the accuracy rate of the system decreases as the number of UAVs increases [82]. Lack of Bayesian Game-Theoretic Approach: In the case of this system, a limitation is mentioned regarding the absence of a Bayesian game-theoretic approach [82].
Intrusion Detection and Ejection Framework in Bayesian Game-Theoretic Methodology	Inapplicability of Traditional Techniques: One limitation identified is that traditional techniques for preventing intrusion may not be applicable at the fog level [82]. Need for Low Resource-Demanding Security: Another limitation highlighted is the need for a low resource-demanding, yet strong security system to protect the fog layer from being attacked [82].

4. Analysis and Discussion

From the literature review, a comparative analysis of the technologies showcasing the advantages and disadvantages are as follows,

Table 16. Comparative Analysis of the Technologies

Names	Advantages	Disadvantages
Jamming detection at the edge of drone networks using Multi-layer Perceptron and Decision Trees	**Non-linearity:** This allows them to capture intricate patterns and make accurate predictions for a wide range of tasks. **Feature Learning:** This eliminates the need for manual feature engineering and allows the network to adapt to the problem at hand. **Wide Range of Applications**: MLPs are widely used in diverse areas, including image recognition, natural language processing, time series analysis, and more. **Interpretability:** Decision Trees offer a transparent and easy-to-understand decision-making process. **Efficiency:** Decision Trees have relatively fast training and prediction time, making them efficient for both small and large datasets.	**Overfitting:** Overfitting occurs when the model learns noise in the training data rather than general patterns, leading to poor performance on unseen data. **Data Requirements:** Insufficient data can lead to poor performance. **Instability to Small Changes:** Decision Trees are sensitive to small changes in the training data, leading to different tree structures.

Predicting Application Layer DDoS Attacks Using Machine Learning Algorithms	**Simplicity and Speed:** Naive Bayes is a simple and computationally efficient algorithm. It can be trained quickly and is suitable for large datasets. **Low Data Requirements:** Naive Bayes can perform well even with a small amount of training data. It is particularly useful when the dataset is limited. **No Training Phase:** KNN is a lazy learning algorithm, which means it does not explicitly build a model during the training phase. Instead, it stores the training data and uses it directly for predictions. **Adapts to Local Patterns:** KNN can adapt to local patterns and variations in the data, which makes it robust to changes in the data distribution.	**Sensitive to Irrelevant Features:** While Naive Bayes can handle irrelevant features to some extent, highly irrelevant features can negatively impact its performance. **Zero Probability Issue:** Naive Bayes assigns zero probabilities to features not seen in the training data, which can cause problems during prediction. To mitigate this issue, techniques like Laplace smoothing can be used, but it may introduce some bias. **Memory Intensive:** KNN stores the entire training dataset, which can lead to high memory usage for large datasets. **Sensitive to Noise and Outliers:** Outliers and noisy data can significantly impact the performance of KNN, as they may dominate the decision-making process for nearby points. **Imbalanced Data:** KNN can be biased towards the majority class in imbalanced datasets, leading to poor performance in minority classes.
Detection of Distributed Denial of Service Attacks based on Machine Learning Algorithms	**Works Well with Limited Data**: SVM can perform well even with a small amount of training data, making it suitable for applications with limited labeled samples. **Effective in Small Sample Size:** SVM can handle datasets with a small number of samples effectively.	**Memory Intensive:** SVM needs to store support vectors and their associated weights, which can consume significant memory for large datasets. **Sensitivity to Noise:** SVM may be sensitive to noisy data, as noisy points can become support vectors and affect the decision boundary.
Autonomous Detection of Malicious Events using Machine Learning Models in Drone Networks	**Automatic Feature Selection**: Decision trees can automatically select important features, reducing the need for extensive feature engineering. **Fast Training**: Decision tree algorithms have relatively fast training times compared to some other complex algorithms. **Low Data Requirements:** Naive Bayes can work well even with limited training data. **Effective with Limited Data:** SVM can perform well even with a small amount of training data.	**Difficulty in Handling Continuous Data:** Decision trees may not handle continuous data well, as they work best with discrete features. **Memory Intensive:** KNN needs to store the entire training dataset, which can lead to high memory usage for large datasets. **Sensitive to Irrelevant Features:** KNN may be affected by irrelevant or noisy features, leading to suboptimal performance. **Noisy Data:** Outliers and noisy data points can negatively impact KNN's classification accuracy. **Imbalanced Data:** Naive Bayes can be biased towards dominant classes in imbalanced datasets, affecting its performance on minority classes. **Data Preprocessing:** Deep learning models are sensitive to data preprocessing, and poor data preparation can negatively impact performance.
A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks	Rules-based detection efficiently detects known attacks based on attack signatures. Anomaly detection using SVM can detect new unknown attacks by modeling normal behavior. Combination of rules-based and anomaly detection improves accuracy. Hierarchical system with ground station verification reduces false positives/negatives. Prompt attack detection achieved through UDA monitoring. Node assessment improves decisions and allows node categorization.	Rules require frequent manual updates to detect new attacks. SVM anomaly detection has high computational cost. Monitoring by multiple UDA agents increases communication overhead.

Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behaviour Rule Specifications	Behaviour rules directly linked to threats, so new threats can be incorporated. Adapts detection strength by adjusting compliance threshold based on attacker type and environment noise. Can trade higher false positives for lower false negatives to handle sophisticated attackers. True positive rate approaches 100% while bounding false positive rate below 0.05% for reckless attackers. Outperforms benchmark IDS in accuracy. Can identify emerging attacks through anomaly detection. Balance coverage, accuracy and adaptability over standalone techniques Generalize better across new attacks with adversarial data and evolving normalcy models. Allows customization and tuning for particular environments and threats when implemented.	Requires comprehensive threat model to derive complete behaviour rules. Must add new behaviour rules when new threats identified. Determining attacker type and environment noise precisely is challenging. Anomaly detection techniques have high false alarm rates requiring careful tuning. Integrating specification rules and anomaly detection is an open, complex challenge. Lack of complete situational awareness for unknown attack vectors. Substantial testing and customization needed for each deployment scenario. Requires diversity and volume of adversarial data which may be difficult to obtain. Changes in flight parameters can accidentally trigger false alarms. Resource constraints of drones may impede complex model deployments.
A Multiagent and Machine Learning Based Denial of Service Intrusion Detection System for Drone Networks	Multi-agent system provides modular design, eliminating single point of failure. Distributed storage enables real-time processing. Machine learning enables high attack detection accuracy. Specifically: • Decision Tree gave 100% accuracy on known DoS attacks. • Random Forest, SVM, PNN also had 99.9% accuracy.	Naive Bayes had poor 68.7% accuracy on known DoS attacks. Unknown attack detection mechanism still needs implementation. System was not evaluated on UAV-specific network traffic datasets.
Blockchain based peer to peer communication in autonomous drone	Decentralization, tamper-proof, confidentiality and data integrity are ensured by using hashing algorithms are core concepts of blockchain. The smart contracts provide an extended layer to set condition on policy and set cryptographic rules based on the requirements of UAV infrastructure. By utilizing Blockchain for UAV position data, spoofing attacks are prevented because any unauthorized attempt to modify or manipulate the position information would be detectable. The approval time of block is faster based on the ether fee payment than other application of blockchain technology. The proposed design outperformed the exiting design by minimizing drift errors, reducing integrity risk and vulnerability to cyber-attacks. The proposed method is demonstrated without additional hardware which makes it more feasible for real-time application usage. The platform usage ensures energy efficiency.	Blockchain networks can face scalability challenges when handling many transactions, which may impact the real-time communication requirements of drone swarms. Implementation of blockchain in a UAV system may require additional computational resources and increase complexity which could increase system overhead. Blockchain-based communication may introduce some latency due to the chained process which could impact time-sensitive drone operations.

Detecting Signal Spoofing and Jamming Attacks in UAV Networks using a Lightweight IDS	Multiclass SVM classifies different types of attacks in UAV and increases accuracy of the classification process. Deep-Q network is used for reverse routing after an attacker is identified. STL deep learning is used for identifying strong features and multicast SVM for classification by using location tracker normal and attacked UAV is observed and represented by graph. As accuracy of attack detection range from 92% to 94%, deep learning-based IDS is more efficient than machine learning based IDS accuracy is 72% to 82%	Hierarchical nature increases complexity of computation. The multiclass SVM approach may face challenges when dealing with imbalanced datasets as distribution samples of Dataset value is equally balanced. The lightweight design may compromise the accuracy of the IDS compared to more complex and resource-intensive IDS solutions. The vulnerability detection Of UAV auto-pilot requires embedded software in on-board system could increase system latency causing degraded system performance.
Specification Based Intrusion Detection for Unmanned Aircraft Systems	The state machine is used to collect compliance degree data for testing and debugging phase. The specification-based approach allows for precise detection of unknown attacks based on deviations from expected behavior, making it effective in identifying intrusion attempts with high accuracy. The IDS is designed to balance value of minimum compliance threshold for trade higher false positives rate. Off for lower false negatives rate minimizes the risk of detecting sophisticated and hidden attackers. IDS ensures a high detection probability of attackers while limiting the false alarm probability to below 5% for reckless attackers and below 20% for random attackers.	Anomaly based technique has high false positives. The IDS design requires more sensitive sensors due to functionality requirements which potentially could increase complexity and overall cost for the infrastructure. The external entity for monitoring the behaviours introduces communication overhead impacting real time response and increases vulnerability of the networking system. Defining accurate behavior rules for each sensor or actuator component in a UAV can be complex and time-consuming and requires expert evaluation while configuration. The IDS relies on compliance degree data which may be subject to noise and unreliable wireless communication, potentially impacting the accuracy of intrusion detection.
An Amateur Drone Surveillance System Based on Cognitive Internet of Things	CIoT technology integrated surveillance system of amateur drone gains high-level intelligence, enabling more real-time feedback for surveillance decision-making capabilities. The context-free feature provides better accuracy of location tracking for continuous switching between surveillance system and environment. Mobile crowd sensing (MCS) allows for large-scale data collection across diverse geographic locations and timeframes. It enables the collection of real-time, dynamic, and fine-grained data that may not be feasible through traditional sensing methods which require powerful sensors and dedicated sensing network. Heterogenous data fusion uses copula theory instead of product model or multivariate Gaussian model to mitigate suboptimal fusion result and enhance the performance.	Amateur drones are harder to detect because of the size of the done. The detection performance increases based on the number of samples which increases detection delay. The detection classification and performance improved at a marginal rate with both additional sensors and detection delay that may not be cost effective.
A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework	Centralized control of SD-IoT improves manageability, flexibility and security. Controller pool provides load balancing and avoids single point of failure. Cosine similarity metric effectively identifies DDoS attack patterns. Blocks attacks by adding drop rules once detected, reducing impact. Simulation demonstrates lower resource usage compared to baseline	Additional complexity of deploying SDN controllers for IoT systems Overhead of controller communications and packet encapsulation/decapsulation Setting optimal threshold for cosine similarity can require tuning. Detection time depends on sampling window size, which may cause some delay. Simulation uses simplified topology, real-world conditions may differ

How to Detect Cyber-attacks in Unmanned Aerial Vehicles Network?	Detection policies are tailored to identify common UAV network attacks. Belief model accounts for uncertainty in IDS observations to improve accuracy. Achieves high attack detection rates with low false positives in simulations. Scales well even with increasing UAVs and attackers in network Collaborative approach allows detecting compromised insider UAVs. Provides detection framework extensible to other UAV network attacks	Requires time and data to train optimal belief model thresholds. Dependent on attack behaviors matching expected patterns. Simulation may differ from real-world conditions with noise and errors. Communication overhead for collaborative monitoring between UAVs Increased computation load for detection policies on resource-limited UAVs Unable to prevent attacks before they occur, only detect them.
Intrusion Detection and Ejection Framework Against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology	Bayesian games provide an optimized tradeoff between security and overhead. Belief model reduces false positives/negatives by estimating threat levels. High detection accuracy (>90%) even with many attackers. Lower communication overhead than specification-based systems. Handles insider misbehavior attacks and scales well as nodes increase. Flexible framework applicable to different UAV network architectures.	High computational complexity of game theoretic approach. Requirement for nodes to actively participate in monitoring and ejection. Detection dependent on attack behaviors matching expected patterns. Delay between detecting attacks and ejecting malicious nodes. Simulated environments may differ from real-world conditions. Increased energy consumption for monitoring and communications.
A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing	Specifically designed for resource-constrained fog computing environments. Low overhead suspicion level calculation to detect MITM attacks. Prevents session hijacking unlike authentication-only approaches. Lightweight AES encryption has minimal impact on latency and energy. Achieves high attack detection accuracy with low false positives. Reduces reliance on computationally intensive cryptography.	Accuracy dependent on setting optimal suspicion level thresholds. Increased latency and energy consumption versus no security. Effectiveness relies on active participation of nodes in monitoring. Suspicion levels may be circumvented by sophisticated attackers. Lack of preventive measures before attack detection. Limited evaluation in simulated environments only.

The comparative analysis reveals that various threat detection techniques like machine learning, multi-agent systems, blockchain, intrusion detection systems (IDS), and software security solutions each offer distinct trade-offs between their advantages and disadvantages for detecting threats in drone networks.

Machine learning techniques like neural networks, support vector machines, and ensemble methods can automatically learn and extract complex features from drone telemetry data to identify anomalies and cyberattack patterns. The algorithms self-improve through training on datasets, avoiding reliance on manual feature engineering. However, machine learning models are prone to overfitting on noise in drone data, reducing detection accuracy on new samples. They require large, balanced training sets that capture diverse drone flight behaviours and threats, which are challenging to obtain. The computational complexity of training complex models on resource-constrained drone hardware can also limit real-time detection capability.

In contrast, multi-agent systems distribute threat analysis across networks of lightweight software agents installed on individual drones. This provides decentralized detection and response without a single point of failure. However, optimally combining and coordinating detections from heterogeneous agents relies on accurate threat modelling and mapping of drone interactions. Limited views of individual agents increase vulnerability to coordinated attacks. Lack of central control also complicates aggregating responses and enforcing consistent security policies.

Blockchain offers tamper-proofing of drone flight logs and distributed consensus mechanisms for validating detections between drones. However, the computational overhead of cryptography and distributed ledger replication incurs significant scaling challenges for large drone fleets. Latency issues from proof-of-work consensus protocols also limit blockchain's ability to detect and respond to threats in real-time.

Classic intrusion detection systems (IDS) leverage hand-coded rules and signatures to identify known threat behaviours. This enables rapid detection of predefined attacks with low false positives. But unknown zero-day threats readily bypass rules-based IDS, requiring constant rule updates. Behavioural IDS address this by modelling normal drone traffic patterns to flag anomalies but are prone to false alarms due to the diversity of legitimate drone behaviours. Running IDS on individual drones also faces hardware constraints.

Unified software security platforms consolidate various detection capabilities into centralized servers or cloud frameworks. This simplifies managing policies and configurations across multiple drones. However centralized approaches create single points of failure with limited resilience. Bandwidth and latency bottlenecks from funnelling large volumes of drone data to a centralized system delay threat response time.

In summary, while each threat detection technique has merits, their limitations pose challenges for comprehensive and efficient drone threat monitoring. Machine learning excels at feature extraction but faces accuracy and scalability issues. Multi-agent systems enable decentralized detection but rely heavily on threat modelling. Blockchain provides tamper-proofing at the cost of performance overhead. Signature-based IDS enables rapid known threat detection while behavioural IDS catches novel threats but risks false alarms. Centralized software platforms ease drone fleet security management but concentrate risk and constrain performance.

As drone networks grow in scale and criticality for applications from delivery to surveillance, enhancing threat detection capabilities is crucial but finding optimal solutions remains challenging. The diversity of drone hardware, environments, applications and threats rules out a one-size-fits-all approach. Combining complementary detection techniques may potentially overcome individual limitations, for instance blending machine learning with multi-agent systems or IDS rules. But tightly integrating diverse methods is complex.

Finding the right hybrid balance to maximize detection accuracy and coverage while minimizing resource demands and false positives is not straightforward. This requires extensive testing and tuning tailored to particular drone fleet architectures, applications and threat landscapes. Lightweight optimization of multiple detection engines competing for tight resource budgets on drones presents engineering hurdles. So does securely integrating and coordinating detections from distributed, heterogeneous systems.

To address these challenges, further research is needed to develop robust, adaptive and tightly integrated threat detection frameworks specialized for diverse drone environments. Key focus areas include distributed machine learning algorithms that enable collaborative learning without central data concentration. Hybrid behavioural learning techniques can combine learned anomaly detection with expert system rules to improve accuracy and reduce false alarms. Hardware-optimized implementations of encrypted distributed ledgers may overcome blockchain scaling hurdles. Adaptive multi-agent systems could monitor drone interactions to adjust coordination strategies and agent responsibilities.

A key challenge in deploying threat detection systems for large-scale drone networks is the potential for substantial memory consumption, especially over extended operation periods. Machine learning models used for anomaly detection require large, labelled datasets encompassing diverse drone behavior for effective training, which demands significant storage capacity that can constrain resource-limited drones. Additionally, retaining historical flight and system data over months and years to continually improve threat models incurs major memory overhead. However, optimizations in model architecture, dimensionality reduction of drone flight telemetry, and leveraging edge computing can alleviate resource strains. Compact deep neural networks with pruning and compression techniques extract efficient data representations to minimize memory footprints. Storing raw historical data distributed across edge nodes rather than drones enables centralized model re-training without overloading individual drones. Such strategies to streamline memory consumption on drones coupled with edge-powered AI can make comprehensive, large-scale threat analysis sustainable. However, the resource-accuracy tradeoffs require extensive empirical evaluation through simulations and test deployments.

Testing across simulated and real-world drone trial environments is essential to evaluate detection performance, overhead tradeoffs and integration efficacy. This can guide the development of tailored solutions balancing comprehensive threat coverage, accuracy, resilience, and lightweight overhead for sustainable long-term drone fleet security. With careful optimization of hybrid techniques, emerging drone networks can reap the benefits of ubiquitous connectivity without substantially increasing attack surfaces. Robust integrated threat detection creates a crucial shield against abuse, helping build trust in drone technology across commercial, government and civilian domains.

5. Conclusion

In this paper, a comprehensive literature review on threat detection techniques for drone networks was conducted. Background information on drones, networks, and drone networks was provided to establish context. An overview was provided on how drone networks function, communicate, and leverage various technologies like wireless communication, satellite systems, onboard computers, sensors, and flight controllers. The paper then delved into emerging technologies including blockchain, software-defined networking, machine learning, fog computing, ad-hoc networking, and swarm intelligence that are transforming drone network capabilities. However, these same technologies also introduce potential security issues and vulnerabilities. Common cyber threats faced by drone networks were outlined.

The paper thoroughly reviewed and analysed various threat detection techniques proposed in literature, spanning methods based on machine learning, multi-agent systems, blockchain, intrusion detection systems, software solutions, and miscellaneous approaches. A comparative analysis was conducted contrasting the advantages and disadvantages of these techniques. As seen in the analysis, each method has its merits but also limitations in aspects like accuracy, scalability, flexibility, and resource utilization. Trade-offs exist between computational complexity, real-time performance, overhead, and detection accuracy. The comparative assessment provides insights into the maturity and applicability of these detection techniques for securing drone networks against evolving cyber threats.

This study can serve as a knowledge base for stakeholders aiming to develop and deploy robust threat detection systems for drone networks. While intrusion detection systems have been extensively studied in traditional environments, developing robust frameworks tailored to decentralized fog computing architectures remains an open challenge. Innovations in lightweight cryptography, adaptive suspicion propagation protocols and privacy-preserving analytics aligned to transient fog topologies offer future interdisciplinary research directions. Similarly, advanced machine learning techniques based on ensembles, deep learning and reinforcement learning can mitigate limitations like overfitting, high false positives and generalizability that constrain current drone threat detectors. Systematically benchmarking and tight integration of ML algorithms best suited to in-situ objectives could enable optimized implementations meeting the scale, diversity and resource constraints of next-generation unmanned fleets. Between customizable intrusion detection and adaptive cyber threat modeling, the convergence of security guarantees with complex edge computing ecosystems provides promising opportunities for specialized innovation. Future directions include exploring techniques tailored to resource-constrained drone environments, lightweight algorithms optimized for real-time detection, combinations of diverse detection methods, implementation and testing of techniques through simulations and testbeds, and standardization of performance metrics. As drone networks grow in scale and criticality across various domains, advancing and implementing cyber threat detection capabilities is crucial. This paper contributes a detailed reference on state-of-the-art detection techniques and analysis to aid these future efforts in securing drone networks.

References

[1] Lutkevich B, (2021). Drone (UAV). Available at https://www.techtarget.com/iotagenda/definition/drone#:~:text=Essentially%2C%20a%20drone%20is%20a,often%20associated%20with%20the%20military. Accessed on 7 July 2023.

[2] Daley S, (2023). Drone Technology: What Is a Drone? Available at https://builtin.com/drones. Accessed on 7 July 2023.

[3] Manesh, M. R., & Kaabouch, N. (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Computers & Security*, *85*, 386-401.

[4] Gharibi, M., Boutaba, R., & Waslander, S. L. (2016). Internet of drones. *IEEE Access*, *4*, 1148-1162.

[5] Hassija, V., Chamola, V., Agrawal, A., Goyal, A., Luong, N. C., Niyato, D., ... & Guizani, M. (2021). Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *23*(4), 2802-2832.

[6] Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intelligent Service Robotics*, *16*(1), 109-137.

[7] Zhou, Z., Chen, J., & Liu, Y. (2020). Optimized landing of drones in the context of congested air traffic and limited vertiports. *IEEE Transactions on Intelligent Transportation Systems*, *22*(9), 6007-6017.

[8] Chang, S. Y., Park, K., Kim, J., & Kim, J. (2023). Securing UAV Flying Base Station for Mobile Networking: A Review. *Future Internet*, *15*(5), 176.

[9] Noor, F., Khan, M. A., Al-Zahrani, A., Ullah, I., & Al-Dhlan, K. A. (2020). A review on communications perspective of flying ad-hoc networks: key enabling wireless technologies, applications, challenges and open research topics. *Drones*, *4*(4), 65.

[10] Sheridan, I. (2020). Drones and global navigation satellite systems: Current evidence from polar scientists. *Royal Society open science*, *7*(3), 191494.

[11] Buggiani, V., Ortega, J. C. Ú., Silva, G., Rodr ǵuez-Molina, J., & Vilca, D. (2023). An Inexpensive Unmanned Aerial Vehicle-Based Tool for Mobile Network Output Analysis and Visualization. *Sensors*, *23*(3), 1285.

[12] Tlili, F., Fourati, L. C., Ayed, S., & Ouni, B. (2022). Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures. *Ad Hoc Networks*, *129*, 102805.

[13] Vasconcelos, G., Carrijo, G., Miani, R., Souza, J., & Guizilini, V. (2016, October). The impact of DoS attacks on the AR. Drone 2.0. In *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR)* (pp. 127-132). IEEE.

[14] Singh, N. K., Muthukrishnan, P., Sanpini, S. (2019), "Industrial System Engineering for Drones: A Guide with Best Practices for Designing", Apress.

[15] Aeronautics. Unmanned Ariel Vehicles and System: Revolutionizing the future of Aviation .Available at :https://aeronautics-sys.com/unmanned-aerial-vehicles-and-systems-revolutionizing-the-future-of-aviation/ Accessed on 11 July 11, 2023.

[16] Unmanned System Technology. Flight Control Systems for UAV & Drones. Available at :https://www.unmannedsystemstechnology.com/expo/flight-control systems/#:~:text=What%20are%20flight%20control%20systems,autonomously%20by%20an%20onboard%20computer.Accessed on 11 July 11, 2023.

[17] Lahmeri, M. A., Kishk, M. A., & Alouini, M. S. (2021). Artificial intelligence for UAV-enabled wireless networks: A survey. *IEEE Open Journal of the Communications Society*, *2*, 1015-1040.

[18] Ossamah, "Blockchain as a solution to Drone Cybersecurity," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp. 1-9, doi: 10.1109/WF-IoT48130.2020.9221466.

[19] Harbi, Y., Medani, K., Gherbi, C., Senouci, O., Aliouat, Z., & Harous, S. (2023). A Systematic Literature Review of Blockchain Technology for Internet of Drones Security. *Arabian Journal for Science and Engineering*, *48*(2), 1053-1074.
[20] Han, P., Sui, A., & Wu, J. (2022). Identity Management and Authentication of a UAV Swarm Based on a Blockchain. *Applied Sciences*, *12*(20), 10524.
[21] Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of network and computer applications*, *177*, 102857.
[22] Alladi, T., Chamola, V., Sahu, N., & Guizani, M. (2020). Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications*, *23*, 100249.
[23] Allouch, A., Cheikhrouhou, O., Koubâa, A., Toumi, K., Khalgui, M., & Nguyen Gia, T. (2021). Utm-chain: blockchain-based secure unmanned traffic management for internet of drones. *Sensors*, *21*(9), 3049.
[24] B. Rawat, D., Chaudhary, V., & Doku, R. (2020). Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems. *Journal of Cybersecurity and Privacy*, *1*(1), 4-18.
[25] Hu, N., Tian, Z., Sun, Y., Yin, L., Zhao, B., Du, X., & Guizani, N. (2021). Building agile and resilient UAV networks based on SDN and blockchain. *IEEE Network*, *35*(1), 57-63.
[26] Gupta, L., Jain, R., & Vaszkun, G. (2015). Survey of important issues in UAV communication networks. *IEEE communications surveys & tutorials*, *18*(2), 1123-1152.
[27] McCoy, J., & Rawat, D. B. (2019). Software-defined networking for unmanned aerial vehicular networking and security: A survey. Electronics, 8(12), 1468.
[28] Alharthi, M., Taha, A. E. M., & Hassanein, H. S. (2019, May). An architecture for software defined drone networks. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)* (pp. 1-5). IEEE.
[29] Jiang, J., Lin, C., Han, G., Abu-Mahfouz, A. M., Shah, S. B. H., & Martínez-García, M. (2022). How AI-enabled SDN technologies improve the security and functionality of industrial IoT network: Architectures, enabling technologies, and opportunities. Digital Communications and Networks.
[30] Baig, B., Shahzad, A.Q. (2022). Machine Learning and AI Approach to Improve UAV Communication and Networking. In: Ouaissa, M., Khan, I.U., Ouaissa, M., Boulouard, Z., Hussain Shah, S.B. (eds) Computational Intelligence for Unmanned Aerial Vehicles Communication Networks. Studies in Computational Intelligence, vol 1033. Springer, Cham. https://doi.org/10.1007/978-3-030-97113-7_1
[31] Bithas, P. S., Michailidis, E. T., Nomikos, N., Vouyioukas, D., & Kanatas, A. G. (2019). A survey on machine-learning techniques for UAV-based communications. Sensors, 19(23), 5170.
[32] Pi, Y., Nath, N. D., & Behzadan, A. H. (2020). Convolutional neural networks for object detection in aerial imagery for disaster response and recovery. *Advanced Engineering Informatics*, *43*, 101009.
[33] Şengönül, E., Samet, R., Abu Al-Haija, Q., Alqahtani, A., Alturki, B., & Alsulami, A. A. (2023). An Analysis of Artificial Intelligence Techniques in Surveillance Video Anomaly Detection: A Comprehensive Survey. *Applied Sciences*, *13*(8), 4956.
[34] Duc Bui, V., Shirakawa, T., & Sato, H. (2022). Autonomous unmanned aerial vehicle flight control using multi-task deep neural network for exploring indoor environments. *SICE Journal of Control, Measurement, and System Integration*, *15*(2), 130-144.
[35] Yazid, Y., Ez-Zazi, I., Guerrero-Gonzalez, A., El Oualkadi, A., & Arioua, M. (2021). UAV-enabled mobile edge-computing for IoT based on AI: A comprehensive review. *Drones*, *5*(4), 148.
[36] Sumeyra, M. U. T. İ., & Ülkü, E. E. (2022). A Review on Machine Learning Techniques Used in VANET and FANET Networks. *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi*, *9*(2), 1150-1165.
[37] Bekmezci, I., Sahingoz, O. K., & Temel, Ş. (2013). Flying ad-hoc networks (FANETs): A survey. *Ad Hoc Networks*, *11*(3), 1254-1270.
[38] Agrawal, R., Faujdar, N., Romero, C. A. T., Sharma, O., Abdulsahib, G. M., Khalaf, O. I., ... & Ghoneim, O. A. (2022). Classification and comparison of ad hoc networks: A review. *Egyptian Informatics Journal*.
[39] Campion, M., Ranganathan, P., & Faruque, S. (2018). UAV swarm communication and control architectures: a review. *Journal of Unmanned Vehicle Systems*, *7*(2), 93-106.
[40] Lopez, M. A., Baddeley, M., Lunardi, W. T., Pandey, A., & Giacalone, J. P. (2021, July). Towards secure wireless mesh networks for UAV swarm connectivity: Current threats, research, and opportunities. In *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (pp. 319-326). IEEE.
[41] Asaamoning, G., Mendes, P., Rosário, D., & Cerqueira, E. (2021). Drone swarms as networked control systems by integration of networking and computing. *Sensors*, *21*(8), 2642.
[42] Zhou, Y., Rao, B., & Wang, W. (2020). UAV swarm intelligence: Recent advances and future trends. *Ieee Access*, *8*, 183856-183878.
[43] Tank, B., & Gandhi, V. (2023). A Comparative Study on Cloud Computing, Edge Computing and Fog Computing.
[44] Gupta, A., & Gupta, S. K. (2022). A survey on green unmanned aerial vehicles‐based fog computing: Challenges and future perspective. *Transactions on Emerging Telecommunications Technologies*, *33*(11), e4603.
[45] Baktyan, A., & Zahary, A. (2018). A review on cloud and fog computing integration for iot: Platforms perspective. *EAI Endorsed Transactions on Internet of Things*, *4*(14).
[46] Al-Khafajiy, M., Baker, T., Hussien, A., & Cotgrave, A. (2020). UAV and fog computing for IoE-based systems: A case study on environment disasters prediction and recovery plans. *Unmanned Aerial Vehicles in Smart Cities*, 133-152.
[47] Shafique, A., Mehmood, A., & Elhadef, M. (2021). Survey of security protocols and vulnerabilities in unmanned aerial vehicles. *IEEE Access*, *9*, 46927-46948.
[48] Sathyamoorthy, D., Fitry, Z., Selamat, E., Hassan, S., Firdaus, A., & Zaimy, Z. (2020). Evaluation of the vulnerabilities of unmanned aerial vehicles (uavs) to global positioning system (GPS) jamming and spoofing. *Defence S and T Technical Bulletin*, *13*, 333-343.
[49] Nguyen, H. P. D., & Nguyen, D. D. (2021). Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication. *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*, 185-210.
[50] Siddiqi, M. A., Iwendi, C., Jaroslava, K., & Anumbe, N. (2022). Analysis on security-related concerns of unmanned aerial vehicle: Attacks, limitations, and recommendations. *Mathematical biosciences and engineering*, *19*(3), 2641-2670.

[51] Krichen, M., Adoni, W. Y. H., Mihoub, A., Alzahrani, M. Y., & Nahhal, T. (2022, May). Security challenges for drone communications: Possible threats, attacks and countermeasures. In *2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH)* (pp. 184-189). IEEE.
[52] Pradhan, A., & Mathew, R. (2020). Solutions to vulnerabilities and threats in software defined networking (SDN). *Procedia Computer Science*, *171*, 2581-2589.
[53] Y. Liu, B. Zhao, P. Zhao, P. Fan and H. Liu, "A survey: Typical security issues of software-defined networking," in *China Communications*, vol. 16, no. 7, pp. 13-31, July 2019, doi: 10.23919/JCC.2019.07.002.
[54] Oren, C., & Verity, A. (2020). Artificial Intelligence (AI) Applied to Unmanned Aerial Vehicles (UAVs) and its Impact on Humanitarian Action. *Digital Humanitarian Network, May*.
[55] Tanwar, S., & Prema, K. V. (2013). Threats & security issues in ad hoc network: a survey report. *International Journal of Soft Computing and Engineering*, *2*(6), 138-143.
[56] Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, *133*, 102894.
[57] Jensen, I. J., Selvaraj, D. F., & Ranganathan, P. (2019, June). Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs). In *2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)* (pp. 1-7). IEEE.
[58] Choudhary, G., Sharma, V., Gupta, T., Kim, J., & You, I. (2018). Internet of drones (iod): Threats, vulnerability, and security perspectives. *arXiv preprint arXiv:1808.00203*.
[59] Best, K. L., Schmid, J., Tierney, S., Awan, J., Beyene, N. M., Holliday, M. A., ... & Lee, K. (2020). *How to analyze the cyber threat from drones: Background, analysis frameworks, and analysis tools* (p. 96). RAND.
[60] Rahman, M. A. (2020). Detection of distributed denial of service attacks based on machine learning algorithms. *International Journal of Smart Home*, *14*(2), 15-24.
[61] Arthur, M. P. (2019, August). Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS. In *2019 international conference on computer, information and telecommunication systems (CITS)* (pp. 1-5). IEEE.
[62] Choudhary, G., Sharma, V., You, I., Yim, K., Chen, R., & Cho, J. H. (2018, June). Intrusion detection systems for networked unmanned aerial vehicles: a survey. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 560-565). IEEE.
[63] Jabbar, R., Dhib, E., Said, A. B., Krichen, M., Fetais, N., Zaidan, E., & Barkaoui, K. (2022). Blockchain technology for intelligent transportation systems: A systematic literature review. *IEEE Access*, *10*, 20995-21031.
[64] Mitchell, R., & Chen, R. (2013). Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. *IEEE transactions on systems, man, and cybernetics: systems*, *44*(5), 593-604.
[65] Kumar, C. R. S., & Mohanty, S. (2021, October). Current trends in cyber security for drones. In *2021 International Carnahan Conference on Security Technology (ICCST)* (pp. 1-5). IEEE.
[66] Yağdereli, E., Gemci, C., & Aktaş, A. Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation*, *12*(4), 369-381.
[67] Sedjelmaci, H., Senouci, S. M., & Messous, M. A. (2016, December). How to detect cyber-attacks in unmanned aerial vehicles network?. In *2016 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE.
[68] Moustafa, N., & Jolfaei, A. (2020, September). Autonomous detection of malicious events using machine learning models in drone networks. In *Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and beyond* (pp. 61-66).
[69] Ding, G., Wu, Q., Zhang, L., Lin, Y., Tsiftsis, T. A., & Yao, Y. D. (2018). An amateur drone surveillance system based on the cognitive Internet of Things. *IEEE Communications Magazine*, *56*(1), 29-35.
[70] Greco, C., Pace, P., Basagni, S., & Fortino, G. (2021). Jamming detection at the edge of drone networks using multi-layer perceptrons and decision trees. *Applied Soft Computing*, *111*, 107806.
[71] Umarani, S., & Sharmila, D. (2015). Predicting application layer DDoS attacks using machine learning algorithms. *International Journal of Computer and Systems Engineering*, *8*(10), 1912-1917.
[72] Ouiazzane, S., Addou, M., & Barramou, F. (2022). A multiagent and machine learning based denial of service intrusion detection system for drone networks. *Geospatial Intelligence: Applications and Future Trends*, 51-65.
[73] Kumar, M. S., Vimal, S., Jhanjhi, N. Z., Dhanabalan, S. S., & Alhumyani, H. A. (2021). Blockchain based peer to peer communication in autonomous drone operation. *Energy Reports*, *7*, 7925-7939.
[74] Mitchell, R., & Chen, I. R. (2012, June). Specification based intrusion detection for unmanned aircraft systems. In *Proceedings of the first ACM MobiHoc workshop on Airborne Networks and Communications* (pp. 31-36).
[75] Yin, D., Zhang, L., & Yang, K. (2018). A DDoS attack detection and mitigation with software-defined Internet of Things framework. *IEEE Access*, *6*, 24694-24705.
[76] Sedjelmaci, H., Senouci, S. M., & Ansari, N. (2016). Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A Bayesian game-theoretic methodology. *IEEE Transactions on Intelligent Transportation Systems*, *18*(5), 1143-1153.
[77] Aliyu, F., Sheltami, T., & Shakshuki, E. M. (2018). A detection and prevention technique for man in the middle attack in fog computing. *Procedia computer science*, *141*, 24-31.
[78] Hewa, T., Braeken, A., Liyanage, M., & Ylianttila, M. (2022). Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing. *IEEE transactions on industrial informatics*, 18(10), 7174-7185.
[79] Alzoubi, Y. I., Osmanaj, V. H., Jaradat, A., & Al‐Ahmad, A. (2021). Fog computing security and privacy for the Internet of Thing applications: State‐of‐the‐art. *Security and Privacy*, *4*(2), e145.
[80] Naeem, M. A., Zikria, Y. B., Ali, R., Tariq, U., Meng, Y., & Bashir, A. K. (2023). Cache in fog computing design, concepts, contributions, and security issues in machine learning prospective. *Digital Communications and Networks*, 9(5), 1033-1052.
[81] Ashi, Z., Al-Fawa'reh, M., & Al-Fayoumi, M. (2020). Fog computing: security challenges and countermeasures. *Int. J. Comput. Appl*, 175(15), 30-36.
[82] Sedjelmaci, H., Senouci, S. M., & Ansari, N. (2017). A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *48*(9), 1594-1606.

Authors' Profiles

Syed Golam Abid completed his Bachelor of Science in Computer Science and Engineering from American International University – Bangladesh (AIUB). He has done his major in Computer Engineering covering Operating Systems, Computer Network and Network Security. Now, he is currently pursuing his Master of Science in Cyber Security at Bangladesh University of Professionals (BUP). Besides, he is also currently working as a Security Operations Center (SOC) Analyst at GenNext Technologies Limited and also as one the Security Infrastructure Architects of Meghna Cloud. Furthermore, his research interest is in Cybersecurity, Information, Network and IoT Security.

Muntezar Rabbani is currently pursuing a Master of Science degree in the Computer Science program from American International University – Bangladesh (AIUB). With research interests and experience in the emerging fields of Data Science and Artificial Intelligence, he contributes his knowledge and passion for these subjects through his role as an Instructor at AIUB.

Arpita Sarker is an undergraduate student pursuing a degree in Computer Science and Engineering (CSE) at American International University – Bangladesh (AIUB). She has specialized in Computer Engineering and studied subjects including Computer Networks and Network Security. Her research interests lie in the fields of Computer Networks and Network Security.

Tasfiq Ahmed Rafi is an undergraduate at American International University-Bangladesh (AIUB), is studying Computer Science and Engineering (CSE) with a focus on Computer Engineering. His coursework has covered core topics like Computer Networks and Network Security. Moreover, He aims to contribute to the fields of Cybersecurity and Offensive Security through penetratiobn testing initiatives that probe system security vulnerabilities. Rafi leveraged his background in Computer Engineering and Networks to pursue research in responsible offense-oriented security assessment.

Dr. Dip Nandi currently works as a Professor and the Associate Dean of Faculty of Science and Technology in American International University-Bangladesh (AIUB). Dr. Nandi achieved his Doctor of Philosophy (PhD) degree from RMIT, Australia and MSc degree from The University of Melbourne, Australia. His research area includes Software Engineering, E-Learning Technologies, Data Mining, and Information systems. He has supervised more than 70 students as thesis supervisor. Dr. Nandi is associated with several organizations such as IEEE, ACM. He has published several peer-reviewed journal articles.

How to cite this paper: Syed Golam Abid, Muntezar Rabbani, Arpita Sarker, Tasfiq Ahmed Rafi, Dip Nandi, "Comparative Analysis of Threat Detection Techniques in Drone Networks", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.10, No.2, pp. 32-48, 2024. DOI: 10.5815/ijmsc.2024.02.04