Sci

MDPI

*Review*

# Detecting Denial of Service Attacks (DoS) over the Internet of Drones (IoD) Based on Machine Learning

**Albandari Alsumayt [1], Naya Nagy [2,*], Shatha Alsharyofi [2], Noor Al Ibrahim [2], Renad Al-Rabie [2], Resal Alahmadi [2], Roaa Ali Alesse [2] and Amal A. Alahmadi [2]**

[1] Computer Science Department, Applied College, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; afaalsumayt@iau.edu.sa

[2] Department of Networks and Communications, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; 2200002971@iau.edu.sa (S.A.); 2200004369@iau.edu.sa (N.A.I.); 2200005412@iau.edu.sa (R.A.-R.); 2200005337@iau.edu.sa (R.A.); 2190000554@iau.edu.sa (R.A.A.); aaalahmadi@iau.edu.sa (A.A.A.)

* Correspondence: nmnagy@iau.edu.sa

**Abstract:** The use of Unmanned Aerial Vehicles (UAVs) or drones has increased lately. This phenomenon is due to UAVs' wide range of applications in fields such as agriculture, delivery, security and surveillance, and construction. In this context, the security and the continuity of UAV operations becomes a crucial issue. Spoofing, jamming, hijacking, and Denial of Service (DoS) attacks are just a few categories of attacks that threaten drones. The present paper is focused on the security of UAVs against DoS attacks. It illustrates the pros and cons of existing methods and resulting challenges. From here, we develop a novel method to detect DoS attacks in UAV environments. DoS attacks themselves have many sub-categories and can be executed using many techniques. Consequently, there is a need for robust protection and mitigation systems to shield UAVs from DoS attacks. One promising security solution is intrusion detection systems (IDSs). IDs paired with machine learning (ML) techniques provide the ability to greatly reduce the risk, as attacks can be detected before they happen. ML plays an important part in improving the performance of IDSs. The many existing ML models that detect DoS attacks on UAVs each carry their own strengths and limitations.

**Keywords:** Denial of Service (DoS); intrusion detection system (IDS); Internet of Drones (IoD); machine learning (ML); Unmanned Aerial Vehicle (UAV)

check for updates

**Citation:** Alsumayt, A.; Nagy, N.; Alsharyofi, S.; Al Ibrahim, N.; Al-Rabie, R.; Alahmadi, R.; Alesse, R.A.; Alahmadi, A.A. Detecting Denial of Service Attacks (DoS) over the Internet of Drones (IoD) Based on Machine Learning. *Sci* **2024**, *6*, 56. https://doi.org/10.3390/sci6030056

Academic Editors: Ki-Hyun Jung and Luis Javier García Villalba

Received: 17 July 2024
Revised: 7 September 2024
Accepted: 9 September 2024
Published: 20 September 2024

**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

Our future is heading towards an exciting era of technological improvement, where the latest innovations, such as sensors, cloud computing, and drones, are becoming an important part of our lives [1]. As such, the need to secure drones or Unmanned Aerial Vehicles (UAVs) is unquestionable. The concept of the Internet of Drones (IoDs) refers to the common practice of integrating drones within the Internet of Things (IoT). IoD is made of UAVs, connected over the internet, that are able to communicate with each other and with other controllers and devices [2]. This paper is focused on the security of IoDs. Many attacks could happen to UAVs in the IoD environment. Among these attacks, Denial of Service (DOS) can be considered the most prominent one. In the context of the wide range of UAV abilities and the ensuing security challenges, DoS remains the most common attack on drones, easily rendering them unfunctional [3]. When DoS happens, the attacker sends a large load of packets. As a result, the connection between the drone and the controller becomes de-authenticated, and the UAV malfunctions [4]. Possible solutions that mitigate DoS attacks are access controls, firewalls, and cryptographic algorithms [5]. However, this paper focuses on one particular solution, namely the intrusion detection system (IDS). An IDS will work as a protection mechanism and as a proactive solution that will identify DoS attacks as and while they happen. The IDS aims to secure UAVs and decrease the chance of

malfunctions [6]. IDSs with good performance can be developed by using machine learning techniques [7].

### *1.1. Contribution*

This paper addresses the critical issue of detecting Denial of Service (DoS) attacks within the Internet of Drones (IoD). It starts by evaluating and reviewing various machine learning techniques currently applied in drone technology. Our primary contribution is a comprehensive analysis of these algorithms, highlighting their strengths, limitations, and applicability in securing UAV networks against DoS attacks. Additionally, we identify key challenges in the existing approaches and propose potential directions for enhancing these techniques to develop more effective and resilient security solutions for drone networks.

### *1.2. Paper Organization*

Section 2 reviews UAV security, highlighting the different security, privacy, and safety concerns and discussing existing threats and cyberattacks on UAVs. Section 3 talks about DoS attacks in particular, the different DoS attack categories, and compares real attacks on drones to attacks on other IoT devices. Section 4 is a review of the different ML models for detecting DoS attacks on UAVs. After that, Section 5 shows current UAV security solutions related to our work, and compares the results of these. Next is Section 6, includes comparisons and results.. Section 7 presents the gap analysis. In Section 8, the discussion of our solution and future research directions are presented. Finally, Section 9 concludes the paper. Figure 1 shows the sections of this study.

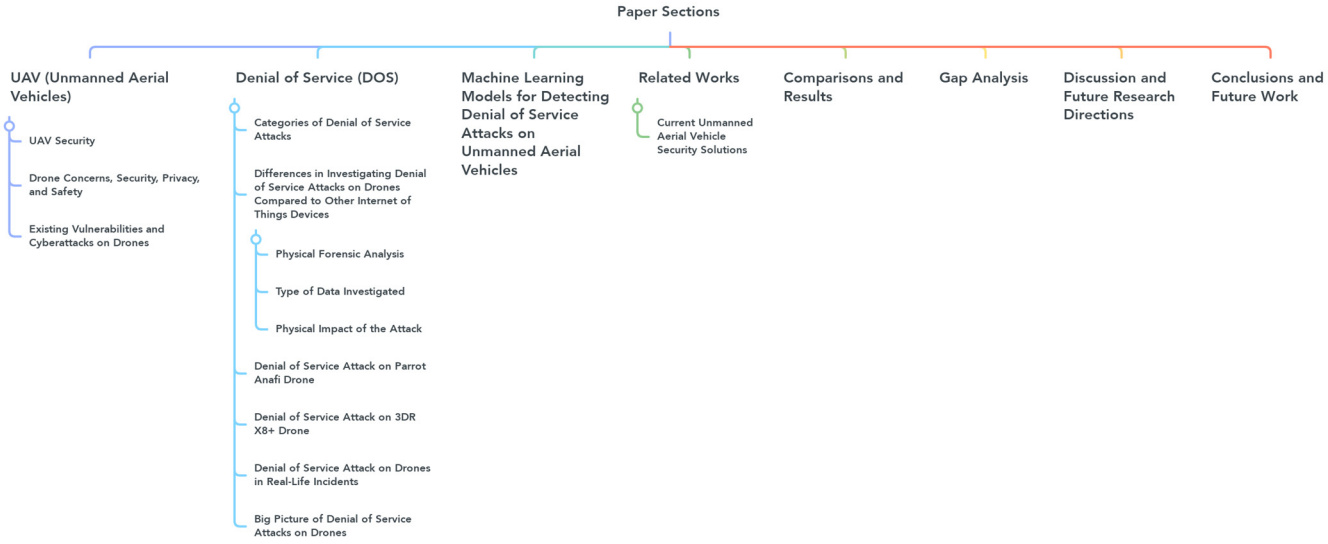



**Figure 1.** Paper sections.

## 2. UAVs (Unmanned Aerial Vehicles)

### *2.1. UAV Security*

It is well established that unmanned aerial vehicles are extensively used in many fields and in many areas of life. They perform critical tasks or sensitive operations and require extreme precision. For instance, the military domain relies on drones for recording terrorist activities, marking targets, precision shelling, and more. In addition, the police can make use of drones for monitoring traffic, conducting forensics search and rescue, and tracking escapees from prisons and crime scenes. Other applications of drones include crisis management in the case of natural disasters or terrorist attacks. Drones can also be found in environmental management applications, such as pollution measurements and agricultural projects [8].

Despite all the beneficial and promising uses of drones, having this technology available attracts malicious users. This can develop to serious security concerns that potentially

endanger public safety. The papers in [8,9] identified two main categories of malicious users. The first category includes criminals who employ drones to conduct physical attacks and break through geo-boundaries. Their purpose is to seize people's sensitive data, such as IDs, passwords, and credit card information, thus violating the privacy of others. These attacks are in the category of logical attacks, often including the setting up of a free Wi-Fi network. The second category of malicious users includes terrorists responsible for attacks such as propaganda, UAV surveillance, cyberattacks, etc. Figure 2 illustrates the usage of UAVs in different domains and for different purposes.

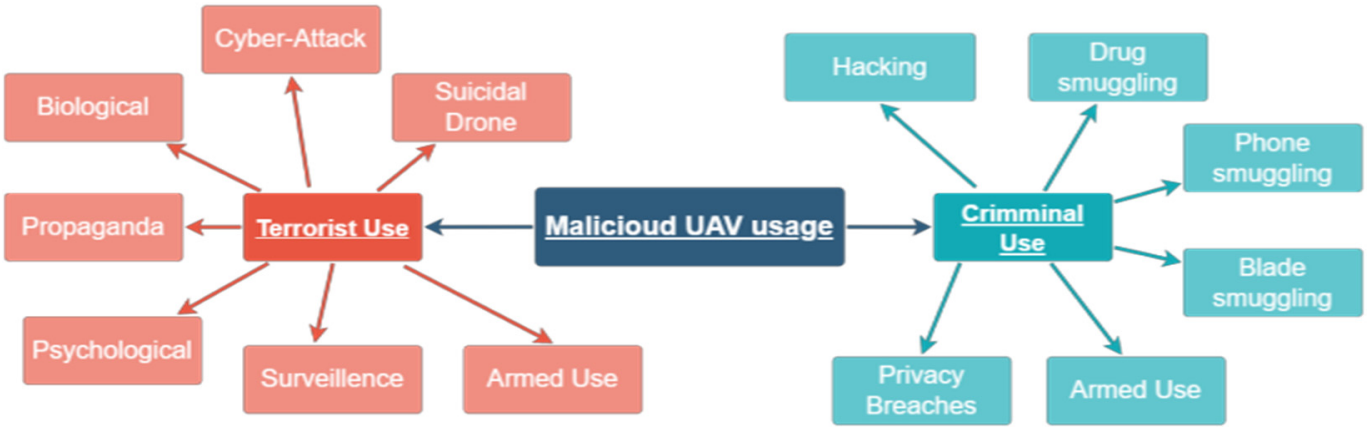



**Figure 2.** Malicious uses of drones.

### 2.2. Drone Concerns, Security, Privacy, and Safety

As mentioned previously, drones are used in critical operations and make use of sensitive information in order to provide high-quality services to users. As such, they can be used maliciously and cause serious issues and damages and they must be protected against attacks. Security requirements, including confidentiality, integrity, availability, authentication, and non-repudiation, must be taken into consideration from the beginning and during the UAV design process [9].

The characteristics of drones, including their small size and low cost, present a major security concern, as they are becoming a preferred tool for malicious users to carry out their criminal and terrorist attacks [8]. In addition, safety concerns are exacerbated by the reality that safety features are not integrated in the design process of drones. This could cause the drone to malfunction and go out of control, leading to severe material damage and injuries. Missing operational and technical standards regarding crash avoidance mechanisms make it difficult for drones to recognize objects and avoid them. Moreover, in situations where the UAV's command and control center is prone to unauthorized access and exploitation, cyber-criminals can hack/hijack the UAV, putting the safety of operations in danger [8]. Another serious concern regarding drones is the possibility of invading individuals' physical location and behavioral privacy by utilizing drones to capture images and record peoples' movements without their knowledge or consent [8].

### 2.3. Existing Vulnerabilities and Cyberattacks on Drones

Drones are correctly perceived as a great threat to data protection, and many UAVs are designed without considering security measures [8]. This leads to drones being prone to many physical attacks and cyberattacks [8–10]. The impacts of such attacks include the unavailability of the UAV, the exposure of confidential information, the interruption of UAV operations, the reduction in UAV performance, the malfunction and misbehavior of the UAV, or infrastructure damage [11]. Current security vulnerabilities and attacks on drones include the following:

1. Malware attacks: UAVs are mainly controlled and connected through remote devices. This technique is considered unsafe, as the automatic installation of malware over UAVs can easily be accomplished by injecting a reverse-shell TCP payload into the drone's memory (hacking the UAV, then installing malware) [8,10].
2. Spoofing/jamming attacks: These are considered sensor-based attacks that involve GPS (easiest), motion sensors, and UAV spoofing [9]. Such attacks are related to the communication methods and telemetry links transporting data to/from drones via serial ports that lack secure encryption measures. This data link vulnerability enables access and modification to the information associated with the GPS [10,11] and gives hackers full control over the targeted drones [8]. Signal congestion and signal loss methods are also used by attackers to transfer the control of a drone to a third party and spoof drones [9].
3. Unauthorized Manipulations: Altering the pre-defined and pre-programmed UAV flying routes is a possible attack and can lead to serious consequences, ranging from the theft of high-value shipments to the redirection of drones to deliver explosives and terrorist payloads [8,10].
4. Data interception and interference: UAV monitoring and data transfers are performed using telemetry feeds through non-secure, open transmissions. This makes the vehicles vulnerable to attacks such as malicious data injection, interception, and alteration, allowing attackers to inject infected image/video files from the UAV to the ground station [8].
5. DoS attacks: During this attack, the attacker floods the UAV communication links with large volumes of unnecessary requests to overwhelm the resources of the target, causing extreme degradation of the performance of the drone and/or making it inaccessible to legitimate users [11,12].
6. Skyjack-based attacks: A skyjack is a malicious software that the attacker installs on the targeted UAVs to detect the wireless networks within the region of the target. After that, the attacker can conduct de-authentication attacks and disable any client connected to the infected UAV through the wireless network, including the navigation controller [10,12].

The following Table 1 summarizes cyberattacks targeting drones:

**Table 1.** Drone cyberattacks.

| Security Target | Attack Type | Attack Nature |
|---|---|---|
| Confidentiality | • Malware Backdoor Access<br>• Baiting<br>• Social Engineering<br>• Reconnaissance Scanning<br>• Eavesdropping<br>• Man-in-the-Middle | • Exploitation<br>• Infection<br>• Exploitation<br>• Infection<br>• Data gathering<br>• Data gathering<br>• Interception<br>• Authentication |
| Privacy | • Malware<br>• Backdoor Access<br>• Baiting<br>• Social Engineering<br>• Injection/Modification<br>• Fabrication<br>• Reconnaissance<br>• Scanning<br>• Eavesdropping<br>• Traffic Analysis<br>• Man-in-the-Middle | • Infection<br>• Infection<br>• Exploitation<br>• Exploitation<br>• Exploitation<br>• Exploitation<br>• Data gathering<br>• Data gathering<br>• Interception<br>• Interception<br>• Authentication |

**Table 1.** *Cont.*

| Security Target | Attack Type | Attack Nature |
|---|---|---|
| Integrity | • Malware<br>• Backdoor Access<br>• Baiting<br>• Injection/Modification<br>• Fabrication<br>• Scanning<br>• Man-in-the-Middle | • Infection<br>• Infection<br>• Exploitation<br>• Exploitation<br>• Exploitation<br>• Data gathering<br>• Authentication |
| Availability | • Malware<br>• Backdoor Access<br>• Three-Way Handshake<br>• DoS | • Infection<br>• Infection<br>• Interception<br>• Jamming |
| Authentication | • Malware<br>• Backdoor Access<br>• Baiting<br>• Social Engineering<br>• Fabrication<br>• Three-Way Handshake<br>• Password breaking<br>• Wi-Fi Air-Crack<br>• Wi-Fi Jamming<br>• De-Authentication<br>• Replay<br>• Buffer Overflow<br>• DoS<br>• ARP Cache Poison<br>• GPS Spoofing<br>• Ping of death | • Infection<br>• Infection<br>• Exploitation<br>• Exploitation<br>• Exploitation<br>• Interception<br>• Cracking<br>• Cracking<br>• Jamming<br>• Jamming<br>• Jamming<br>• Jamming<br>• Jamming<br>• Jamming<br>• Jamming<br>• Jamming |

## 3. Denial of Service (DOS)

A Denial of Service (DoS) attack occurs when a server or network resource is inundated with an excessive number of requests, rendering the system incapable of handling them effectively. This assault can exploit vulnerabilities in applications or networking protocols, or it can simply overpower a target by generating an immense volume of requests.

### *3.1. Categories of Denial of Service Attacks*

A DoS attack, which includes techniques like jamming and flooding, has the objective of disrupting a network or system, rendering its resources inaccessible to intended users. In reference to [13], the paper introduces two primary categories of DoS attacks: logic attacks and flooding attacks.

A logic attack is defined as exploiting vulnerabilities in the logical aspect of a system in order to crash or degrade the performance of its operations. It targets bugs or flaws in the design or implementation of the system to make it unavailable to the use of authorized users. Ping of death, an example of a logical attack, sends a packet larger than 65,535 bytes to the target computer. Despite the potential mitigation through software updates, logic attacks remain a significant concern today.

The second approach, a flooding attack, overwhelms the resources of the target device, including the central processing unit (CPU), memory, and network resources, by inundating it with numerous unauthorized requests. Given the characteristics of request messages, distinguishing between legitimate and unauthorized requests becomes a challenging task. An illustrative example is the SYN-flood attack, wherein an attacker dispatches a substantial number of synchronized (SYN) packets to the transmission control protocol (TCP) port of the target device, initiating a connection but failing to provide final confirmation.

Consequently, the target expends resources while awaiting the connection, rendering it unavailable for legitimate communications.

### *3.2. Differences in Investigating Denial of Service Attacks on Drones Compared to Other Internet of Things Devices*

DoS attacks on UAVs can share similarities with DoS on other Internet of Things (IoT) devices, but there are differences relating to the characteristics of UAVs. The following is a description of such differences.

#### 3.2.1. Physical Forensic Analysis

Investigating attacks such as DoS attacks on a UAV usually involves accessing the physical drone resources, like the flight controller chip, the CPU, and the sensors [14]. By contrast, other IoT devices do not require physical evidence as much as drone forensics do, because they often operate in a controlled environment. An example of a forensic framework that relied on the physical acquisition of drones [15] highlights the different physical resources that can be used in an investigation and proposes their forensics framework, which involves acquiring both hardware and digital forensics. The approach was tested on two drone types, the DJI Phantom 4 drone and the Yuneec Typhoon H drone. They concluded that hardware forensics helped them identify the user and analyze the components, while digital forensics helped them analyze the drone's flight. Meanwhile, forensic analysis on other IoT devices does not rely on physical access to resources as much as UAVs do. This is because they mostly rely on analyzing the network traffic to gain insight into potential security breaches.

#### 3.2.2. Type of Data Investigated

The type of data to be investigated after a DoS attack is similar in both UAVs and other IoT devices, except for the flight data and the telemetry data found in UAVs. Ahn [16] performed validation of anomaly detection of UAVs by utilizing real flight data. The anomaly detection scheme is created by analyzing real flight data and making decisions based on observing the sensor data from a drone over time. The flight data were gathered through a set of flight tests, and in order to investigate the issues in the machine, signals obtained from the INS were used. In their model, a separate anomaly classification learning model is developed for each UAV. When flight data are input, the subsystem to be observed is evaluated by computing its anomaly score. The condition of the subsystem is then decided based on a predefined threshold value. Kulp and Mei [17] utilized telemetry data in the detection of attacks on drones. The authors proposed a framework to detect attacks on drones and implement proactive measures against them. In the proposed framework, a pre-processing engine has the task of absorbing telemetry data from sensors in order to standardize the diverse data sources into a unified form. The data are then forwarded to a rules engine where events are tagged using signatures. The data are further processed by the analytics engine, which keeps contextual information about the events in order to assess the necessity for taking action or implementing countermeasures.

#### 3.2.3. Physical Impact of the Attack

As Guo et al. [18] suggested, UAVs are considered a Cyber-Physical System (CPS), meaning that they integrate physical components like sensors with computational elements. A DoS-like attack poses a great danger to UAVs since the attack and the harm can extend to the physical domain and cause destructive consequences. UAVs can crash or become uncontrollable, rendering the attacked UAV useless. When it comes to other IoT devices, a large percentage of them are stationary, which means that they will not have the same impact on the physical domain as the UAVs when subjected to a DoS attack.

### 3.3. Denial of Service Attack on Parrot Anafi Drone

Feng [19] analyzes and explains how vulnerable Parrot ANAFI drones are to various forms of Denial of Service (DoS) attacks. The Parrot ANAFI drone, also referred to as an Unmanned Aerial Vehicle (UAV), is a remotely controllable aircraft that operates without an onboard pilot. They define the assets in their drone, and some of these assets include Wi-Fi Wireless Access Point (used to establish a connection between the drone and a smartphone and controller). In their research, they initiated an SYN-flood attack by employing tools like the low-orbit ion cannon (LOIC) 1.0.8, Netwox 7.2, and Hping3 (20051105). These tools are used for issuing a TCP SYN-flooding attack. First, they established a connection between their computer and the drone's wireless access point and executed specific commands to carry out the attack on port 554, which is responsible for video streaming. The findings of the study indicated that when a Parrot ANAFI drone is subjected to a SYN-flood attack, it substantially impacts the frame rate of video streaming. This is a crucial aspect for a pilot operating a cell phone and utilizing the onboard camera, and the experience is a significant disruption.

### 3.4. Denial of Service Attack on 3DR X8+ Drone

Kwon et al. [20] employed the hping3 tool to carry out an ICMP flooding attack on a 3DR X8+ drone that operates on the MAVLink protocol. MAVLink, short for Micro Air Vehicle Link, is a messaging protocol utilized for exchanging mission commands between Unmanned Aerial Vehicles (UAVs) and ground control stations (GCSs). In the context of ICMP flooding, this technique involves the transmission of ICMP request messages to the target drone (UAV), intending to elicit a response from the recipient. When an adversary dispatches a substantial volume of ICMP request messages at a high frequency, it overwhelms the target system, forcing it to use up significant resources for processing and responding to these messages. This then qualifies as a successful DoS attack.

### 3.5. Denial of Service Attack on Drones in Real-Life Incidents

In recent years, Denial of Service (DoS) attacks have been employed to target drone networks and various other systems. Elkhider et al. [21] mention some of the incidents. For example, in 2017, hackers successfully executed a DoS attack on the Colombian drone manufacturer DJI in China. This recent surge in cyberattacks against drones has created substantial challenges for ensuring the secure operation of these aerial devices. To illustrate further, in 2017, the Federal Aviation Administration (FAA) reported an incident where a multitude of drones disrupted air traffic control operations in the vicinity of New York City's JFK airport for approximately an hour. This incident is considered an example of a DoS attack.

### 3.6. Big Picture of Denial of Service Attacks on Drones

Virupakshar et al. [22] highlighted the weight of DoS attacks on drones while mentioning a real-life demonstration of DoS attacks and hijacking of drones. A DoS attack arises when an attacker renders the service or network of a drone incapable of providing its expected services, either temporarily or permanently [23]. When a service is not accessible, the attacker can manipulate the situation and insert malicious code into the system of the drone before fully restoring it. This creates a temporary DoS with the purpose of a big security breach that even may persist if a backdoor is established. The hijacked drones, instead of fulfilling their intended purpose, are weaponized to mal-perform, potentially causing hidden damages, before being returned to their original administrators, who are oblivious of the change. To illustrate the broader impact of DoS attacks on drones, a possible scenario that could happen is when an attacker detours a drone meant to carry medical supplies in a remote area, denying access to critically needed resources. Demonstration of drone hijacking was performed by Samy Kamkar, in his program, skyjack (9250), in which a threat actor has the ability to disturb a drone using radio signals, reprogram its onboard

software, and take control by manipulating GPS coordinates [24]. This showcases how signals and data can be manipulated to alter a drone's intended destination.

## 4. Machine Learning Models for Detecting Denial of Service Attacks on Unmanned Aerial Vehicles

As UAVs are employed more frequently for important tasks, it is essential to safeguard the integrity and secrecy of their communication systems. An overview of recent studies on IDS for UAV communication applications is given in this section. IDS is crucial for the defense of UAV networks because of the serious network security issues they face [25]. Modern computer networks have significant bandwidth and data traffic requirements, which traditional IDSs frequently cannot keep up with [26]. Researchers have used machine learning to increase intrusion detection performance and decrease false alarms. An enormous benefit is that the ML algorithms learn from the training data and improve themselves to achieve higher accuracy and better outcomes without the need for human interaction. By identifying the existence of malevolent drones within the network, machine learning techniques can be utilized to prevent attacks such as Denial of Service attacks. With additional experience, these algorithms continue to become more advanced and produce more precise outcomes [27–30]. Additionally, the models can be trained to automatically identify flaws and repair them. Furthermore, multidimensional and heterogeneous data may be handled by ML algorithms. These algorithms are very well suited for usage in drone applications because of all these factors [3]. In these studies, Naive Bayes, Long Short-Term Memory (LSTM), Random Forest (RF), Multilayer Perceptron (MLP), K-nearest Neighbor (KNN), Decision Tree (DT), K-means (KM), Logistic regression (LR), and support vector machines (SVMs) are used to demonstrate the effectiveness and performance of several common machine learning classifiers for drone applications. Table 2 shows the result comparison of ML algorithms. The findings of this research provide insight into developments in the security of UAV communication networks.

**Table 2.** ML comparison result.

| Ref. | ML Algorithms | Accuracy | Precision | Recall | F1 | Open Issue |
|---|---|---|---|---|---|---|
| [25] | LR | 82.54% | NM | NM | NM | Has problems with relations effects among variables |
| [31,32] | LSTM-SMOTE | 99.71% Benign 99.83% Attack | 99.95% Benign 97.95% Attack | 99.44% Benign 99.79% Attack | 99.89% Benign 98.96% Attack | Work on increasing the efficiency of the model is much needed |
| [33] | RF | 99.09% | NM | NM | NM | Work on decreasing the latency is needed |
| [34] | MLP | 99.93% | | | | The efficient detection of a variety of vulnerable drones can be worked upon in the future |
| [35,36] | SVM | 99.07% | 95.6% | 96% | 95.8% | Need to improve the inconsistent results |
| [37] | DT | 99.99% | 1 | 1 | 1 | Lack of real-time adaption, scalability issue |
| [37] | KNN | 99.94% | 0.999 | 1 | 0.999 | Scalability issue, sensitive to noise. |
| [37] | K-M | 37.67% | 0.331 | 0.982 | 0.496 | Needs an improvement in terms of accuracy |
| [38] | LR&RF | 98.58% | 0.9768 | 0.9859 | 0.9901 | High cost |
| [39] | Tree Ensemble | 99.98% | 0.997 | 0.995 | NM | NM |

**Table 2.** *Cont.*

| Ref. | ML Algorithms | Accuracy | Precision | Recall | F1 | Open Issue |
|---|---|---|---|---|---|---|
| [40] | ANN | 90.79% | 0.9961 | NM | NM | prone to overfitting |
| [40] | DNN | 91.36% | 0.9960 | NM | NM | need a big amount of training data to learn the complex patterns and features in the data |
| [40] | PSO-DBN | 92.44% | 0.9982 | NM | NM | NM |

The authors of this paper analyze the Long Short-Term Memory Recurrent Neural Network (LSTM) method for intrusion detection in UAV communication [31]. Sequential data can be captured and learned to have long-term associations through the LSTM variety. The models are perfectly suited for analyzing network traffic patterns because they can process extended sequences through the utilization of their embedded storage cells and gating systems to deliberately safeguard or erase information. The LSTM-SMOTE algorithm analyzes sequential network traffic data to spot intricate temporal patterns associated with assaults and safe activities. It generates predictions for every instance and classifies them as either "ATTACK" or "BENIGN" by referencing patterns discovered previously [32]. This method managed to achieve a high detection accuracy of 99.83% on the CICIDS2017 dataset. However, the unique challenges of UAV networks, such as dynamic environments and real-time requirements, necessitate continued research and innovation in this area.

Baig et al. [11] presented a Random Forest method that would be used to categorize data packets as benign or DoS-affected. Using a bootstrap approach, a decision tree is created as the first step in the categorization process. The remaining data samples are utilized for the trained random forest decision tree model's inner cross-validation. Decision Tree [33] represents a widely employed machine learning model or classifying text that relies on various variables. It categorizes data parameters into branch-like components which are subsequently employed to construct an inverted tree including a root node, internal nodes, and leaf nodes. Using decision trees as a basis for classification, Random Forest falls under the category of ensemble learning classifiers. To obtain better results, votes are used to combine the output of different trees. The important discovery of [33] is that the Weka tool offers more accurate and efficient categorization methods than Scikit-learn. However, one significant weakness of the study is the lack of data on the algorithm's precision, recall, and F1 score, which would have offered a more comprehensive assessment of their effectiveness. Without these critical measures, the different algorithms' effectiveness cannot be completely assessed, which is a limitation that the authors should address in future studies.

Mohammed et al. [34] propose the Multilayer Perceptron (MLP) algorithm. The nonlinear Multilayer Perceptron (MLP) model can classify data. With an input layer and a hidden layer to process the input data and pass them on to the output layer, it is a layered model. The dataset consisted of information about DoS assaults in pcap format, and the authors devised and built a Multilayer Perceptron technique [rapid]. The MLP algorithm looks for and validates certain obvious chains that it finds in the gathered data. The detection method counts the number of moving items in the first place and then determines the kind of moving object by looking at its identification [34]. The drone's incoming data traffic is divided into benign and impacted packets. The analysis shows that the suggested model achieves a remarkable accuracy of 99.93%. The efficiency with which the MLP algorithm can protect UAV systems while maximizing resource efficiency is shown by these results. Support vector machines (SVMs) are supervised ML techniques that fall under the category of linear classifiers [35]. It has been extensively utilized to detect intrusions by examining data and spotting trends. SVM models are built using training data that have been divided into categories. Any information that does not fall into one of those categories is regarded as untrue. This is advantageous for drones since the SVM will spot an anomaly

in the pattern if there are any anomalies, which normally indicate that an assault has taken place [36].

Shrestha et al. [37] explore many ML algorithms that are used to detect attacks. The algorithms are trained to classify incoming packets into one of two categories: normal or attack. The algorithm models are known as classifiers. The project discusses several classifiers, including Logistics Regression (LR), Linear Discriminant Analysis (LDA), K-nearest Neighbor (KNN), Decision Tree (DT), Gaussian Naive Bayes (GNB), Stochastic Gradient Descent (SGD), and K-means (KM). The comparison involved evaluating their accuracy, precision, F1 Score, and false negative rate, and the experiment was conducted using a dataset containing records of DoS attacks. The results show that the DT and the KNN imply a high degree of accuracy with the highest correctly classified data. The DT also possesses a 0 FNR, which represents the portion of attacks classified as normal packets. Conversely, the LDA shows a 99.02% rate of accuracy and a 0.014 FNR, which is an impressive ratio when compared to DT and KNN. The K-means model exhibits the least accurate performance at 37.67% and a high FNR of 0.897. The high accuracy demonstrates the effectiveness in improving the security of UAV networks. However, the paper does not provide a detailed analysis of the system's computational complexity and resource requirements, nor does it address the challenges of long-term real-world deployment and maintenance, implying that more research is required to ensure the solution's practical viability.

Aldaej et al. [38] present a seven-module framework to preserve the security and privacy of drones. The seven modules include the drone module, the edge computational module, the security module, the transmission module, the processing module, the storage module, and the visualization module. Each module is responsible for implementing a specific task, in addition to the normal operations. The proposed technique explores important details using machine learning. The study deals with a probabilistic ranking classifier, which is an ML approach of hybrid LR and RF. The data of the drone module are protected in the security module using ML models before being transferred to the transmission module. The proposed technique achieved a 98.58% accuracy, which is considered a high score. This indicates that the technique is capable of detecting data instances that are vulnerable to DoS attacks. The result shows that the suggested strategy effectively improves the security of IoT-enabled drone networks. The framework performs well across a wide range of evaluation parameters, including precision, accuracy, dependability, and stability. The study does not, however, go into detail on the suggested framework's limitations. The approach's scalability, ability to handle different threat scenarios, and computing overhead are not fully addressed. As drone networks and IoT systems become more complex, there may be a need for more adaptive and dynamic security solutions that can proactively detect and respond to emerging threats. A complete architecture that incorporates modern techniques such as deep learning, federated learning, and blockchain may be necessary to overcome the dynamic security concerns in future IoT–drone ecosystems.

Rahman et al. [25] explained how machine learning is being used to create an Internet of Things-based UAV network that can identify possible security threats. The great mobility of UAVs causes disturbances where trespassers could easily conduct DoS attacks. This research project focuses on a thorough examination of machine learning-based IDS. Logistic regression is the recommended technique for calculating statistical probability. The binomial distribution serves as the basis for all exploration. Logistic regression uses a linear association approach. Logistic regression behaviors are less expensive in weight and cost when compared to alternative methods.

Ouiazzane et al. [39] propose a NIDS model that uses AI techniques such as multi-agent systems and multiple ML algorithms, including RF, DT, and Tree ensemble, to detect known and unknown DoS and DDoS attacks on drone networks. The authors used the CICIDS2017 dataset to assess the performance of their NIDS technique, emphasizing the importance of the geographical and computing data that drones retain and communicate, making drone networks an appealing target for malicious actors. The paper lacks detailed information about the limitations of the proposed solution and the potential technical and

operational challenges that may arise during its implementation, such as computational and resource constraints, real-time detection and response requirements, scalability and adaptability concerns, and privacy protection measures to discuss the potential privacy concerns of intrusion detection technologies. Incorporating these concerns into the research methodology and proposed NIDS solution would result in a more comprehensive and practical approach to protecting drone networks from cyber threats.

Tan et al. [40] describe an intrusion detection method for UAV networks that uses a Deep Belief Network (DBN) optimized using Particle Swarm Optimization (PSO) to tackle the difficulty of recognizing complex and developing cyber threats in these dynamic and resource-constrained environments. The researchers create a DBN classification model and then apply the PSO algorithm to maximize the number of hidden layer nodes, resulting in the ideal DBN structure for intrusion detection. The authors evaluate the proposed PSO-DBN approach on a benchmark intrusion dataset and show that it achieves an accuracy of 92.44%, surpassing various machine learning approaches such as SVM, ANN, DNN, and Adaboost. The method's main strength is the employment of a deep learning-based model to capture complicated and nonlinear patterns in incursion data, as well as effectively optimize the model architecture with the PSO method. However, the paper provides insufficient information about the limitations of the proposed model and the dataset's characteristics and fails to address important practical considerations for deploying the intrusion detection system in real-world UAV network environments, such as computational complexity, resource constraints, and integration with other security mechanisms. Future research should overcome these constraints, test the approach on a broader range of UAV network datasets, and investigate the holistic integration of the intrusion detection system to provide a full security solution for increasingly critical UAV applications.

Previous research has emphasized the ongoing difficulties with IDSs for UAV communication networks. These include the need to address growing security threats, evaluate the real-world performance of IDS solutions, and improve the overall effectiveness of IDS in the always-changing UAV communication environment. Further study and development are required to address these issues, as the efficiency gains shown by ML algorithms in previous studies may have far-reaching consequences. For example, faster and more accurate malware categorization, as demonstrated in IoT botnet detection, can result in faster response and remediation, lowering the potential impact of botnet-driven attacks on IoT devices and networks. This is especially important in time-sensitive and mission-critical applications such as autonomous vehicle control and critical infrastructure monitoring, where early identification, preventing IoT botnet incursions, can make the difference between successful and compromised operations. Furthermore, improved cybersecurity in IoT-powered drone networks can enable a variety of drone-based services and capabilities, such as rapid deployment for disaster response, while boosting privacy and reliability. However, addressing the privacy implications of the suggested intrusion detection and mitigation strategies is also critical, as drone users have a fair expectation of privacy regarding the data collected and communicated by their drone systems. To balance better cybersecurity and strong privacy protection, the framework should include comprehensive data anonymization, encryption, and user privacy controls. Furthermore, implementing these methods in real-world UAV systems presents additional obstacles, such as guaranteeing compatibility with existing hardware and software, as well as the capacity to scale and adapt to a variety of operational contexts. Overcoming these practical implementation challenges will be critical for moving the proposed cybersecurity framework from theoretical notions to effective and widely adopted solutions in the UAV arena.

## 5. Related Works

*Current Unmanned Aerial Vehicle Security Solutions*

To resolve the security issues arising from the various attacks mentioned in the previous section, and to aid researchers in identifying the areas of search and contributing to solutions, it is necessary to classify them first. Figure 3 demonstrates attack classifications as perceived by Abro et al. [10]

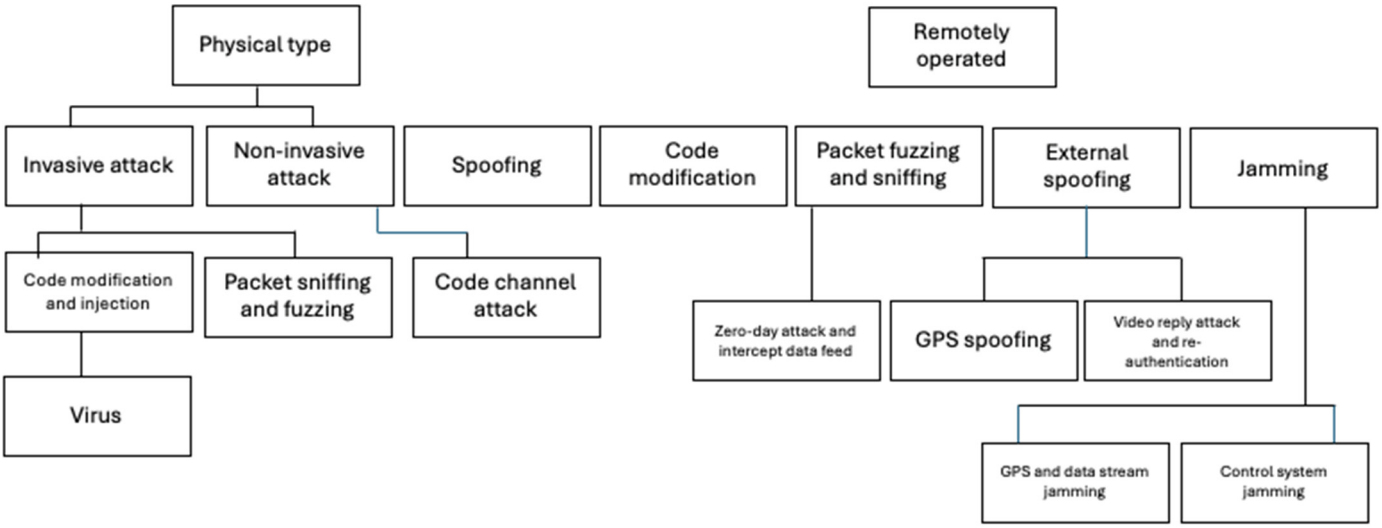



**Figure 3.** UAV attack classification.

One of the most recent and effective techniques for improving UAV network security is relying on ML-based IDS to detect threats to UAVs and notify the responsible personnel in the ground control room (GCR) [8,9]. Authors of [10] categorized ML-based IDS systems into three main types: rule-based, signature-based, and anomaly-based IDS. The rule-based IDS is more dependent on technology and artificial intelligence than manual interactions. On the other hand, signature-based IDS makes use of a list of predefined and pre-programmed threats along with their indicators of compromise (IOCs). These IOCs are stored in a database and used by the IDS to compare with the network packets to detect malicious behavior in the UAV's network. The anomaly-based IDS relies on machine learning to educate itself and define a normalized baseline used to compare the network traffic against, and therefore identify unusual behavior in the network; its only limitation is the immense number of resources required to be effective. The research in [10] also mentioned studies that made use of rule-based IDS to target the signal strength between the GCR and the UAV and identify false data injection attacks.

Despite the effective uses of the IDS approach in enhancing UAV security, it is not the best for complex attacks that are difficult to identify. For that, another scientific solution that involves the use of forensic methods is suggested. With the help of forensics analysis and monitoring schemes, both the attack method and the attacker can be identified [9,10]. After identifying the attack, the appropriate countermeasure can be applied to prevent and avoid any further attack attempts. Yaacoub et al. [8] mentioned several studies that implemented forensics methods for securing drones, including one that introduced a generic framework for network forensics, which includes the analysis of network data transmitting through IDSs and firewalls and implements a six-phased chain of custody to track and trace back the attack source. Securing UAV data and communication is crucial to protect against attacks such as interception and eavesdropping. However, since data on drones must be aggregated and transformed into data packets to minimize network traffic [9], aggregating encrypted data produces many challenges. Unfortunately, the work in [8] states that current symmetric and asymmetric homomorphic encryption solutions suffer from performance and security concerns.

Recently, blockchain technology has been considered among the most powerful approaches for achieving security, and many researchers have utilized it to improve the privacy and security of drones [10]. Authors of [41] presented a BCT-based security solution in which the main information regarding the drone's instructions, responses, reliability, and authenticity are all stored on a cloud platform that applies secure hashing algorithms (SHAs) and an elliptic curve cryptography to ensure data privacy. The data are kept on an Ethereum-based public blockchain to make BCT transactions easier. However, experimental results of blockchain solutions show that implementing BCT reduces performance due to the increase in processing and time consumption caused by blockchain integration [42].

Blockchain offers strong security for UAVs, but with performance challenges. In smart agriculture, where UAVs are essential for data collection, DL-based IDS provides a more efficient solution. These IDSs are designed to protect against threats like DDoS attacks, ensuring real-time security in edge computing environments without the latency issues associated with blockchain. The authors of [43] suggested a DL-based IDS for smart agriculture (SA) environments, which addresses the issues that IoT devices experience when working in severe conditions. By combining BiGRU and LSTM with a Softmax classifier, the IDS identifies network edge threats efficiently. The use of truncated backpropagation through time (TBPTT) improves training by removing the need for full data retrace. The design comprises an attack scenario and deployment architecture that is specifically targeted to extreme SA conditions. The system outperforms baseline and cutting-edge approaches, obtaining accuracy rates of 99.82%, 99.55%, and 98.32% for the CIC-IDS2018, ToN-IoT, and Edge-IIoTset datasets, respectively, while dramatically lowering false positive rates.

While the DL-based IDS for smart agriculture has made tremendous progress in threat identification, with high accuracy rates and fewer false positives, recent improvements have enhanced these techniques for larger industrial applications. The authors of [44] describe an improved and explainable threat detection system designed specifically for Industrial Internet of Things (IIoT) networks. This system extends the ideas of DL by combining explainable AI with a BiLSTM architecture, a self-adaptive attention mechanism, and a Softmax classifier. Using the SHAP mechanism, this IDS not only achieves a high detection accuracy of 99.92% and 96.54%, but it also provides transparent decision-making procedures that allow security analysts to have a better understanding. Compared to traditional and current frameworks, this suggested IDS shows improved performance.

UAVs may differ in size from small devices to large military aircrafts, and they can be grouped into remotely piloted vehicles (RPVs), multi-rotor drones (also called rotary-wing drones), fixed-wing drones, mixed fixed/rotary-wing drones, machine aircraft, and pilotless aircrafts, based on how they fly. Additionally, the size, battery life, and flight time of UAVs are directly influenced by their payloads, which can range from tens of grams to several hundred kilograms and include communication equipment, recording devices, radars, and sensors. Due to their special qualities, UAVs can ensure rapid setup and mobility while offering ubiquitous and affordable wireless access over wide areas of coverage at high elevation angles and low altitudes with a high probability of line-of-sight (LoS) connectivity with ground-based nodes.

Even with the advancements, research to date emphasizes how difficult it still is to identify DDoS attacks because of their dynamic and unexpected character. All of these challenges are made worse by UAV systems' intrinsic limitations. Deep learning models also face challenges associated with the intricacy of training on large datasets and the prolonged performance durations necessary. As such, an upgraded model that accurately recognizes DDoS attacks across these demanding contexts is still desperately needed. Numerous problems plague present studies on DDoS mitigation in UAV networks, such as excessive latency, inconsistent model accuracy, and difficult resource management. The thorough examination of the literature makes it abundantly evident that ensemble learning, in which several models work together to address a single problem, is an effective tactic. By enabling every classifier to handle the information being supplied separately, our suggested methodology improves the detection of attacker data and produces integrated outcomes

that result in better performance indicators, such as greater reliability and lower rates of false alarms.

## 6. Comparisons and Results

The list of algorithms was explained in the preceding section. In this section, the results obtained from the comparative analysis of classifiers performed on the drone dataset are discussed. The classifiers used in this research include support vector machines (SVMs), K-nearest Neighbor (KNN), Decision Tree (DT), K-means (KM), Random Forest (RF), Naive Bayes (NB), Long Short-Term Memory (LSTM), K-means (KM), and Random Forest (RF). The task yielded an accuracy rate of 99.99%, the highest for the cybersecurity controlling procedure. Table 2 demonstrates that K-means produces the least accurate findings. Next, a 99.71% accurate LSTM was used. MLP and LR&RF, on the other hand, have somewhat higher accuracy at 98%. Random Forest, KNN, LR, and SVM also attain a value higher than 99%. Decision Tree produces accurate and reliable findings, with accuracy levels of 99.99%. Additionally, the paper reports the performance of other ML models, including ANN at 90.79% accuracy, DNN at 91.36% accuracy, and PSO-DBN at 92.44% accuracy. Other measures also affect the result; just as Table 2 shows, the LSTM-SMOTE model's precision for the Benign class is 99.95%, while its recall is 97.95%. This shows that while the model is fairly good at identifying Benign cases, it may miss some of them. The precision for the Attack class is 99.44%, and the recall is 99.79%, showing that the model is extremely good at detecting and properly classifying Attack instances. The SVM model has a precision of 95.6% and a recall of 96%, which is good overall but somewhat lower than the LSTM-SMOTE model. The DT classifier has perfect precision and recall of 1.0, indicating that it is extremely accurate at both identifying and accurately categorizing cases. The KNN model also performs well, with a precision of 0.999 and a recall of 1.0. The K-M model has a poor precision of 0.331 but a high recall of 0.982, meaning that while it can detect many true positives, it also produces a high number of false positives. As for the LR and LR&RF models, precision and recall metrics are not provided. The Tree Ensemble model performs quite well, with a precision of 0.997 and a recall of 0.995. The ANN, DNN, and PSO-DBN models all have high precision values of 0.9961, 0.9960, and 0.9982, respectively; however, recall numbers are not supplied. In conclusion, while accuracy is a significant parameter, precision and recall provide a more complete picture of the model's performance in correctly recognizing both positive and negative instances, which is critical for effective intrusion detection in drone networks. However, these indicators alone are not enough to decide which ML model to use in an IDS, measures such as the nature of data to be classified, Model Complexity and Interpretability, and robustness and resilience of the model.

## 7. Gap Analysis

This study's research on machine learning (ML) methods for UAV intrusion detection highlights important advancements, but there are still several gaps. Although Long Short-Term Memory Recurrent Neural Nets (LSTM) are effective in capturing temporal patterns, further research and development are necessary to address some shortcomings. Despite its robustness, the Random Forest method's applicability in dynamic UAV communication situations has not been thoroughly explored. Although the Multilayer Perceptron (MLP) algorithm is very accurate, there should be some discussion about its scalability and resource efficiency. Furthermore, a more thorough assessment of the various ML algorithms' usefulness in various threat scenarios—taking into account their real-world applicability—is necessary for the comparative analysis of these algorithms [37]. The seven-module architecture that is suggested in [38] achieves great accuracy; however, a more thorough comprehension of its actual use and possible obstacles is required. On the other hand, while the comparative analysis of other methodologies is limited, the preference for logistic regression in [31] warrants closer examination.

Transitioning to UAV security solutions, the research project recognizes the importance of ML-based intrusion detection systems (IDSs) in augmenting security. The division of IDSs into rule-based, signature-based, and anomaly-based categories, however, does not provide a thorough analysis of each category's advantages and disadvantages. Although rule-based intrusion detection systems (IDSs) exhibit a reliance on technology, further research is needed to determine the efficacy of signature- and anomaly-based IDSs while taking resource needs into account. Identifying attack tactics and attackers with the inclusion of forensic methods is a respectable solution. However, there is still a great deal of research to be conducted on the necessity of thorough forensic investigation and monitoring plans for sophisticated attacks. The limitations of existing encryption systems are illustrated by the difficulties in aggregating encrypted data for UAVs, as noted in [8]. Although blockchain technology is positioned as a promising security solution, its use in UAV contexts needs to be carefully considered due to the trade-off between increased security and decreased performance, as demonstrated by testing results [42]. To sum up, these gaps highlight the necessity for more sophisticated machine learning algorithms and comprehensive security plans that incorporate cutting-edge technology in order to protect UAVs against changing threats in practical applications.

After evaluating our work and comparing it to other works, we have concluded two points. Firstly, we found that an ML-based IDS as a security solution for UAVs was an ideal choice as a security solution for DoS attacks, as it successfully supports the security of UAVs by mitigating the attacks that threaten UAVs, with ML helping the effectiveness of the IDS. It also is a cost-effective solution, as it reduces the manual monitoring of the UAV operations, and unlike traditional IDSs, ML-based IDSs reduce false positive alerts. On the other hand, other solutions, like the seven-module architecture suggested by [38], have high computational costs that could be improved by using more efficient methods. We also think that the RF ML model was a good choice for the IDS to utilize due to its many advantages, such as its effectiveness in identifying anomalies and potential intrusions, its ability to manage big datasets, and its robustness and ability to learn a big amount of information, which helps with the dynamic nature of network traffic data. Other models, like the logistic regression used in [25], may face some issues, like not being able to handle complex relationships that are present in the data it consumes. Other models, like the LSTM model used in [31], also suffer from issues, like the need to acquire a large amount of training data in order to have good and effective performance, unlike the RF model, which can be effective even with a small amount of data.

## 8. Discussion and Future Research Directions

Regarding the nature of the IoD network and how the devices are connected, it is clear that several limitations made the IoD vulnerable to security breaches. Drone capture attacks, impersonation attacks, reply attacks, and man-in-the-middle attacks are examples of DoS attacks that can occur in IoD. While the special specifications of drones, such as constraints on energy and mobility, allow vulnerabilities to be exploited, threats are regarded as crucial elements. Because most of the data in these systems are extremely sensitive, these threats are compared to those of a standard Internet of Devices system. Using IoD, the sensitive data are collected or processed while being categorized for their appropriate activities. These kinds of data leaks might result in significant losses of confidence and privacy. The reliability and accessibility of communication transmission are compromised by adversarial behavior in the propagation spectrum's natural environment. Criminals can utilize off-the-shelf technology that takes advantage of open-air communication to neutralize and imitate or jam UAV signals throughout the operation. One of the risky threat attack methods used to interfere with UAVs' ability to communicate with other authorized entities via their network is jammer assault. It seeks to purposefully break radio communication's physical layer of security (PHY) or media access control protocol (MAC) rules in order to impede data transfers and deteriorate system performance [18]. It happens when attackers use the radio frequency to broadcast a noise signal.

After conducting our research on the security issues regarding drones and analyzing the current ML-based solutions for mitigating DoS attacks targeting UAVs, we noticed the need for the following improvements:

- Proposing an ML-based IDS model with a better accuracy rate through the implementation of continuous model training, regular collection of new high-quality data, and employing feedback from network administrators and security professionals. This contributes to the overall performance of the IDS and ensures its effectiveness in managing such attacks. Model optimization techniques should also be implemented to increase ML model scalability for identifying a different type of DoS attack.
- Developing scalable solutions, because drone platforms come with inherent resource limits. As the drone ecosystem grows, these solutions should function effectively with the limited computing and energy resources of drones.
- Lowering the cost of machine learning methods for Denial of Service (DoS) attacks. In order to reduce costs, we can develop computational resource-efficient, lightweight machine learning models that can be used in edge contexts or on devices with limited resources.
- Implementing strategies to provide better latency for the ML-IDS. Such strategies include using ML algorithms like conventional neural networks (CNNs). Another strategy can be to use cache memory techniques to store the results of operations and avoid the redundant calculation of those operations.
- Current IDS systems are missing adequate mechanisms to respond to the detected attacks. Integrating this feature enables network administrators and security personnel responsible for dealing with security to gain more control and aid in decisions regarding the recovery and later prevention of such incidents. Training the IDS to not only detect intrusions to the UAV network but also determine the appropriate responses to them based on certain factors and information the IDS collects ensures a high-quality security service that contributes to the overall safety of the UAV system and data.
- Developing robust defense mechanisms capable of identifying and mitigating adversarial attempts aimed at circumventing machine learning-based security systems.
- Adapting anomaly detection methodologies to accommodate diverse environmental conditions and operational contexts within drone networks for ensuring the sustained effectiveness of detection mechanisms across varied scenarios.
- Applying chaos engineering methods to evaluate the robustness of drone swarms. Chaos engineering is an emerging technology that tests the versatility of an interconnected system by arbitrarily causing unexpected events. In this way, the robustness of a swarm of drones can be tested for arbitrary attacks.
- Considering timestamps to detect different types of DoS attacks in real-time networks.
- Subsequent investigations ought to concentrate on collaborative UAV tactics, optimizing latency and incorporating more extensive spectrum-sharing protocols. These developments would support the creation of more robust and flexible UAV anti-jamming technologies.

## 9. Conclusions and Future Work

In summary, existing approaches to mitigate DoS attacks on drones exhibit limitations such as latency, real-time adaptability, scalability challenges, and inadequate response strategies. To overcome these shortcomings and bolster UAV security, this proposal recommends the creation of an intrusion detection system (IDS) enriched with machine learning capabilities to enable early detection and effective mitigation of DoS attacks. By integrating IDS technology with machine learning models, it becomes possible to promptly identify and counteract DoS attacks, thereby safeguarding the security, reliability, and integrity of UAV operations, particularly in critical applications. This proposal underscores the significance of developing robust IDS solutions to shield UAVs from DoS attacks and other potential security vulnerabilities. Through the enhancement of detection and mitigation

methods, the integration of machine learning, and the resolution of current limitations, this research proposal aspires to fortify the security, dependability, and performance of UAV operations across diverse domains. For future work, a novel method will be proposed to detect DoS attacks in UAVs based on machine learning and identify anomalies such as drop packets. However, it is important to differentiate between the normal dropping of packets regarding network failure or congestion and DoS attacks. It takes into account the advantages of the existing methods and avoids the limitations of the existing studies.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Zeng, Y.; Wu, Q.; Zhang, R. Accessing from the Sky: A Tutorial on UAV Communications for 5G and beyond. *Proc. IEEE* **2019**, *107*, 2327–2375. [CrossRef]
2. Jamil, S.; Rahman, M.; Fawad. A Comprehensive Survey of Digital Twins and Federated Learning for Industrial Internet of Things (IIoT), Internet of Vehicles (IoV) and Internet of Drones (IoD). *Appl. Syst. Innov.* **2022**, *5*, 56. [CrossRef]
3. Hassija, V.; Chamola, V.; Agrawal, A.; Goyal, A.; Luong, N.C.; Niyato, D.; Yu, F.R.; Guizani, M. Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2802–2832. [CrossRef]
4. IEEE Computer Society. Technical Council on Test Technology, IEEE Solid-State Circuits Society, International Federation for Information Processing, and EDA Association. In Proceedings of the 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, 25–29 March 2019.
5. Tsao, K.-Y.; Girdler, T.; Vassilakis, V.G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Netw.* **2022**, *133*, 102894. [CrossRef]
6. Prasad, R.; Rohokale, V.; Prasad, R.; Rohokale, V. Artificial intelligence and machine learning in cyber security. In *Cyber Security: The Lifeline of Information and Communication Technology*; Springer: Cham, Switzerland, 2020; pp. 231–247.
7. Ramadan, R.A.; Emara, A.-H.M.; Al-Sarem, M.; Elhamahmy, M. Internet of Drones Intrusion Detection Using Deep Learning. *Electronics* **2021**, *10*, 2633. [CrossRef]
8. Yaacoub, J.P.; Noura, H.; Salman, O.; Chehab, A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things* **2020**, *11*, 100218. [CrossRef]
9. Majeed, R.; Abdullah, N.A.; Mushtaq, M.F.; Kazmi, R. Drone Security: Issues and Challenges. Available online: www.ijacsa.thesai.org (accessed on 2 February 2024).
10. Abro, G.E.M.; Zulkifli, S.A.B.M.; Masood, R.J.; Asirvadam, V.S.; Laouti, A. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats. *Drones* **2022**, *6*, 284. [CrossRef]
11. Baig, Z.; Syed, N.; Mohammad, N. Securing the Smart City Airspace: Drone Cyber Attack Detection through Machine Learning. *Future Internet* **2022**, *14*, 205. [CrossRef]
12. Yahuza, M.; Idris, M.Y.I.; Bin Ahmedy, I.; Wahab, A.W.B.A.; Nandy, T.; Noor, N.M.; Bala, A. Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges. *IEEE Access* **2021**, *9*, 57243–57270. [CrossRef]
13. Hsu, W.C. Lightweight Cyberattack Intrusion Detection System for Unmanned Aerial Vehicles Using Recurrent Neural Networks. Master's Thesis, Purdue University, West Lafayette, IN, USA, 2021.
14. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [CrossRef]
15. Renduchintala, A.; Jahan, F.; Khanna, R.; Javaid, A.Y. A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework. *Digit. Investig.* **2019**, *30*, 52–72. [CrossRef]
16. Ahn, H. Deep Learning Based Anomaly Detection for a Vehicle in Swarm Drone System. In Proceedings of the 2020 International Conference on Unmanned Aircraft Systems (ICUAS), Athens, Greece, 1–4 September 2020.
17. Kulp, P.; Mei, N. A Framework for Sensing Radio Frequency Spectrum Attacks on Medical Delivery Drones. In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Toronto, ON, Canada, 11–14 October 2020; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2020; pp. 408–413. [CrossRef]
18. Guo, R.; Tian, J.; Wang, B.; Shang, F. Cyber-Physical Attack Threats Analysis for UAVs from CPS Perspective. In Proceedings of the 2020 International Conference on Computer Engineering and Application, ICCEA 2020, Guangzhou, China, 18–20 March 2020; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2020; pp. 259–263. [CrossRef]
19. Feng, J.; Tornert, J. *Denial-of-Service Attacks against the Parrot ANAFI Drone*; KTH Royal Institute of Technology: Stockholm, Sweden, 2021.

20. Kwon, Y.M.; Yu, J.; Cho, B.M.; Eun, Y.; Park, K.J. Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles. *IEEE Access* **2018**, *6*, 43203–43212. [CrossRef]
21. Elkhider, S.M.; El-Ferik, S.; Saif, A.W.A. Containment Control of Multiagent Systems Subject to Denial of Service Attacks. *IEEE Access* **2022**, *10*, 48102–48111. [CrossRef]
22. Virupakshar, K.B.; Asundi, M.; Channal, K.; Shettar, P.; Patil, S.; Narayan, D.G. Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud. *Procedia Comput. Sci.* **2020**, *167*, 2297–2307. [CrossRef]
23. Masys, A.J. Advanced Sciences and Technologies for Security Applications. 2021. Available online: http://www.springer.com/series/5540 (accessed on 30 January 2024).
24. Dey, V.; Pudi, V.; Chattopadhyay, A.; Elovici, Y. Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study. In Proceedings of the IEEE International Conference on VLSI Design, Pune, India, 6–10 January 2018; IEEE Computer Society: Washington, DC, USA, 2019; pp. 398–403. [CrossRef]
25. Rahman, K.; Aziz, M.A.; Usman, N.; Kiren, T.; Cheema, T.A.; Shoukat, H.; Bhatia, T.K.; Abdollahi, A.; Sajid, A. Cognitive Lightweight Logistic Regression-Based IDS for IoT-Enabled FANET to Detect Cyberattacks. *Mob. Inf. Syst.* **2023**, *2023*, 7690322. [CrossRef]
26. Majeed, R.; Abdullah, N.A.; Mushtaq, M.F.; Umer, M.; Nappi, M. Intelligent cyber-security system for iot-aided drones using voting classifier. *Electronics* **2021**, *10*, 2926. [CrossRef]
27. Mihoub, A.; Fredj, O.B.; Cheikhrouhou, O.; Derhab, A.; Krichen, M. Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. *Comput. Electr. Eng.* **2022**, *98*, 107716. [CrossRef]
28. Fredj, O.B.; Mihoub, A.; Krichen, M.; Cheikhrouhou, O.; Derhab, A. CyberSecurity Attack Prediction: A Deep Learning Approach. In Proceedings of the SIN 2020: 13th International Conference on Security of Information and Networks, Merkez, Turkey, 4–7 November 2020; ACM International Conference Proceeding Series. Association for Computing Machinery: New York, NY, USA, 2020. [CrossRef]
29. Mihoub, A.; Snoun, H.; Krichen, M.; Kahia, M.; Salah, R.B.H.; Predicting, R.B.H.S. Predicting COVID-19 Spread Level using Socio-Economic Indicators and Machine Learning Techniques. In Proceedings of the 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 3–5 November 2020. [CrossRef]
30. Qaisar, S.M.; Alyamani, N.; Waqar, A.; Krichen, M. Machine Learning with Adaptive Rate Processing for Power Quality Disturbances Identification. *SN Comput. Sci.* **2022**, *3*, 14. [CrossRef]
31. Abdulghani, A.M.; Abdulghani, M.M.; Walters, W.L.; Abed, K.H. Improving Intrusion Detection in UAV Communication Using an LSTM-SMOTE Classification Method. *J. Cyber Secur.* **2022**, *4*, 287–298. [CrossRef]
32. Rezaeenour, J.; Ahmadi, M.; Jelodar, H.; Shahrooei, R. Systematic review of content analysis algorithms based on deep neural networks. *Multimed. Tools Appl.* **2023**, *82*, 17879–17903. [CrossRef]
33. Susanto; Stiawan, D.; Arifin, M.A.S.; Idris, M.Y.; Budiarto, R. IoT botnet malware classification using weka tool and scikit-learn machine learning. In Proceedings of the International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Institute of Advanced Engineering and Science, Yogyakarta, Indonesia, 1–2 October 2020; pp. 15–20. [CrossRef]
34. Mohammed, A.B.; Fourati, L.C.; Fakhrudeen, A.M. A Comparative Study of Attribute Selection Algorithms on Intrusion Detection System in UAVs: A Case Study of UKM-IDS20 Dataset. *Lect. Notes Comput. Sci. (Incl. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinform.)* **2023**, *13857*, 34–46. [CrossRef]
35. Karimibiuki, M.; Aibin, M.; Lai, Y.; Khan, R.; Norfield, R.; Hunter, A. Drones' Face off: Authentication by Machine Learning in Autonomous IoT Systems. In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2019, New York, NY, USA, 10–12 October 2019; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2019; pp. 0329–0333. [CrossRef]
36. Ribeiro, A.A.; Sachine, M. On the optimal separating hyperplane for arbitrary sets: A generalization of the SVM formulation and a convex hull approach. *Optimization* **2022**, *71*, 213–226. [CrossRef]
37. Shrestha, R.; Omidkar, A.; Roudi, S.A.; Abbas, R.; Kim, S. Machine-learning-enabled intrusion detection system for cellular connected uav networks. *Electronics* **2021**, *10*, 1549. [CrossRef]
38. Aldaej, A.; Ahanger, T.A.; Atiquzzaman, M.; Ullah, I.; Yousufudin, M. Smart Cybersecurity Framework for IoT-Empowered Drones: Machine Learning Perspective. *Sensors* **2022**, *22*, 2630. [CrossRef]
39. Ouiazzane, S.; Addou, M.; Barramou, F. DoS and DDoS Cyberthreats Detection in Drone Networks. In *Advances in Intelligent System and Smart Technologies*; Lecture Notes in Networks and Systems; Springer: Cham, Switzerland, 2024; pp. 109–119. [CrossRef]
40. Tan, X.; Su, S.; Zuo, Z.; Guo, X.; Sun, X. Intrusion Detection of UAVs Based on the Deep Belief Network Optimized by PSO. *Sensors* **2019**, *19*, 5529. [CrossRef]
41. Ch, R.; Srivastava, G.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. Security and privacy of UAV data using blockchain technology. *J. Inf. Secur. Appl.* **2020**, *55*, 102670. [CrossRef]
42. Abualsauod, E.H. A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network. *Comput. Electr. Eng.* **2022**, *99*, 107847. [CrossRef]

43. Javeed, D.; Gao, T.; Saeed, M.S.; Kumar, P. An Intrusion Detection System for Edge-Envisioned Smart Agriculture in Extreme Environment. *IEEE Internet Things J.* **2024**, *11*, 26866–26876. [CrossRef]
44. Attique, D.; Hao, W.; Ping, W.; Javeed, D.; Kumar, P. Explainable and Data-Efficient Deep Learning for Enhanced Attack Detection in IIoT Ecosystem. *IEEE Internet Things J.* **2024**, *1*, 1. [CrossRef]

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.