Journal of Cyber Security

Tech Science Press

DOI: 10.32604/jcs.2023.042486
Article

Improving Intrusion Detection in UAV Communication Using an LSTM-SMOTE Classification Method

Abdulrahman M. Abdulghani, Mokhles M. Abdulghani, Wilbur L. Walters and Khalid H. Abed*

Department of Electrical & Computer Engineering and Computer Science, Jackson State University (JSU), Jackson, 39217, USA

*Corresponding Author: Khalid H. Abed. Email: khalid.h.abed@jsums.edu

Received: 31 May 2023; Accepted: 10 July 2023; Published: 10 August 2023

Abstract: Unmanned Aerial Vehicles (UAVs) proliferate quickly and play a significant part in crucial tasks, so it is important to protect the security and integrity of UAV communication channels. Intrusion Detection Systems (IDSs) are required to protect the UAV communication infrastructure from unauthorized access and harmful actions. In this paper, we examine a new approach for enhancing intrusion detection in UAV communication channels by utilizing the Long Short-Term Memory network (LSTM) combined with the Synthetic Minority Oversampling Technique (SMOTE) algorithm, and this integration is the binary classification method (LSTM-SMOTE). We successfully achieved 99.83% detection accuracy by using the proposed approach and the Canadian Institute for Cybersecurity Intrusion Detection Evaluation Dataset 2017 (CICIDS2017) dataset. We demonstrated the efficiency of LSTM-SMOTE in defending UAV communication channels against possible attacks and bolstering the overall security posture through the use of a real-world scenario.

Keywords: Intrusion detection systems; IDS; unmanned aerial vehicles; UAV communication; binary classification; LSTM-SMOTE; CICIDS2017; network security

1 Introduction

Unmanned Aerial Vehicles (UAVs) have become effective in recent years for a variety of tasks in military and commercial applications, such as reconnaissance and surveillance, package delivery, and disaster response. UAV integration has revolutionized industries by bringing previously unheard-of benefits and capabilities. However, as UAVs are used more often for vital tasks, protecting the security and integrity of their communication networks becomes of the utmost importance [1] and [2]. Due to their wireless nature and the transfer of sensitive data, UAV communication networks, like any other wireless networks, are vulnerable to a number of security threats. Unauthorized entry, eavesdropping, data alteration, and denial-of-service assaults are among the dangers that might negatively affect the availability, confidentiality, and integrity of UAV communication channels. Strong

security measures are thus urgently required to safeguard UAV communication infrastructure and guarantee the continued and secure execution of UAV operations [3] and [4]. In [5], we demonstrated that the detection and mitigation of security risks inside networks is greatly aided by the use of Intrusion Detection System (IDS), and we also demonstrated that our hybrid machine learning technique uses random forest and support vector machine classification to reach a positive detection rate with a small false alarm rate. In [6], our IDS keeps track of network activity, examines trends and abnormalities, and spots any harmful or intrusive activity during a variety of uses. IDS offers prompt reactions and preventative steps to safeguard the UAV communication infrastructure by identifying and warning network administrators about such situations [7]. This research study will examine the application of IDS in UAV communication networks in order to improve security, improve detection precision, and guarantee the continuous operation of UAV missions. The main goals are to assess the state-of-the-art in IDS for UAV communication, compare various detection strategies, examine their performance metrics, and pinpoint any potential drawbacks. By focusing on these goals, our research intends to increase the security of UAV communication and enable the effective use of UAVs in important tasks. To accomplish these goals, a thorough analysis of the body of knowledge will be carried out to acquire information on the most recent developments in IDS for UAV communication networks. The efficacy, efficiency, and applicability of various IDS strategies, including anomaly-based detection, machine learning methods, hybrid systems, and signature-based detection, will be examined and assessed. Furthermore, to verify the effectiveness and usability of particular IDS methodologies, real-world case studies and experimental assessments will be carried out. Ultimately, the goal of this research is to offer insightful analysis and suggestions for improving the security and robustness of UAV communication networks through the efficient application of IDS as shown in Fig. 1. This research contributes to the larger objectives of ensuring the secure operation of UAV missions in critical applications, fostering public trust, and facilitating the widespread adoption of UAV technology in a variety of industries by addressing the difficulties and limitations related to UAV communication security.

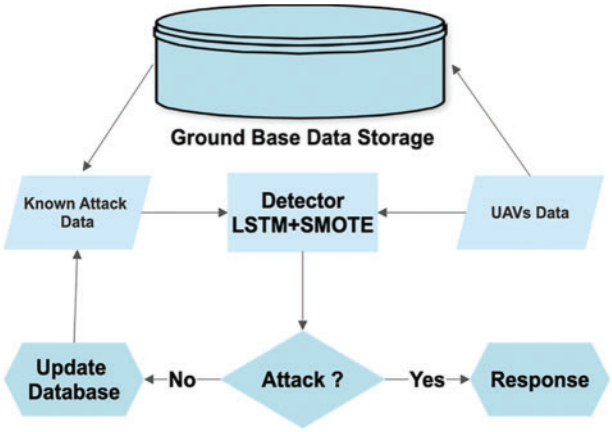

Figure 1: The UAVs-based IDS engine

The rest of this article is organized as follows: In Section 2, we review the related works of IDS in the field of UAVs. In Section 3, we present the proposed SMOTE-LSTM intrusion detection method. Section 4 discusses the results, and we provide a conclusion and future perspective in Section 5.

2 Related Work

UAVs have received a lot of attention recently and are being used in a variety of fields, such as surveillance, infrastructure assessment, and disaster response. As UAVs are used increasingly often in crucial missions, it is crucial to protect the confidentiality and integrity of their communication systems [1]. UAVs extensively rely on wireless communication networks to send private information like video feeds, sensor readings, and command and control information [2] and [3]. These lines of communication are nonetheless vulnerable to a number of security risks, such as denial-of-service attacks, unauthorized access, and data manipulation [4]. We demonstrated in [5] and [6] that the detection and mitigation of security risks inside networks is greatly aided by the use of IDS. Through the detection and mitigation of possible breaches, IDS are essential for protecting UAV communication networks [7]. A survey of current research publications on IDS for UAV communication applications that were published is given in this part. These papers illustrate the efficacy and performance of various strategies and techniques used for intrusion detection in UAV communication. The findings and types of datasets included in these researches provide insight into the developments achieved in UAV communication network security.

The CICIDS2017 dataset was used by the authors in [8] to assess the effectiveness of the Long Short-Term Memory Recurrent Neural Networks (LSTM-RNN) algorithm for intrusion detection in UAV communication. Both binary and multiclass classification operations were included in their study. Notably, the LSTM-RNN method showed the best performance in the three algorithms examined. However, it is important to note that while obtaining an average accuracy of 81%, all three algorithms had difficulty correctly diagnosing Grayhole attacks. A grayhole attack refers to a type of cyber-attack where a malicious entity selectively drops or modifies network packets rather than blocking them entirely. This manipulation of data can disrupt the communication flow and compromise the integrity of the system. These results highlight how challenging it is to accurately identify and categorize this specific form of assault in UAV communication networks. To overcome the drawbacks of Grayhole attacks and improve the precision of intrusion detection systems in such circumstances, more study and development are required.

In [9], the researchers proposed a Timed Probabilistic Automaton (TPA)-based IDS to solve the security issues brought on by drone swarms. The IDS was created to simulate the typical drone swarm behavior and identify any variations that could point to intrusion attempts. The technology successfully protected drone swarms from malicious assaults thanks to a high detection accuracy of 98.65%. The suggested IDS has proven to be a useful tool in assuring the integrity, dependability, and security of drone swarm operations by using TPA and its flexibility to change attack patterns. To enhance the system's performance and investigate its application in actual drone swarm deployments, more studies and real-world validations are suggested.

In [10], the authors introduced the University Kebangsaan Malaysia Intrusion Detection System 20 (UKM-IDS20) dataset, which was created particularly for intrusion detection in UAVs to solve security issues around UAVs. Their research examines the effect of feature selection on IDS for UAV networks in light of the significance of feature selection in improving the effectiveness of IDS. The Incremental Grid Classification (IGC) and Multilayer Perceptron (MLP) techniques combined as (IGC-MLP) algorithm is suggested by the authors to achieve this goal. The approach adds the best collection of features to the MLP classification model by means of feature selection algorithms. The effectiveness of the suggested method is assessed in two situations using 15 and 20 chosen characteristics. According to the examination, the suggested model obtains a remarkable accuracy of 99.93%. In addition, fewer characteristics demand less memory and CPU time, which increases

the effectiveness of intrusion detection in UAV networks while simultaneously improving accuracy. These results demonstrate the IGC-MLP algorithm's capability to efficiently secure UAV systems while maximizing resource utilization.

The authors of [11] mentioned the topological situation of Flying Ad-Hoc Networks (FANETs), where IoT nodes are accessible on the ground and UAVs gather data. UAVs' high mobility patterns lead to disruptions where intruders may quickly launch Denial of Service (DoS) or Distributed Denial of Service (DDoS) assaults. UAVs, satellites, and base stations used to be part of the physical infrastructure of flying ad hoc networks. Applications for IoT-based UAV networks include agriculture, search and rescue, tracking, and surveillance. On the other hand, DoS/DDoS assaults disrupt the behavior of the entire FANET and cause energy imbalance, end-to-end latency, and packet loss. This research study focuses on a detailed analysis of IDS that uses machine learning. Additionally, the University of New South Wales (UNSW-NB 15) dataset is used to model the cognitive lightweight LR technique. Machine learning is used to develop an IoT-based UAV network that can identify potential security intrusions. In the context of an IoT-based UAV network, the queuing and data traffic model is applied to implement Decision Tree, Random Forest, XGBoost, AdaBoost, Bagging, and Logistic Regression. The suggested method for estimating statistical probability is logistic regression. Overall, the binomial distribution is the foundation of exploration. Logistic regression uses a linear association technique. The cost and weight of logistic regression behaviors are cheap as compared to other methods. In comparison to other strategies, the simulation results show that logistic regression produces better outcomes (80%). Additionally, a great precision is matched perfectly and optimally.

The authors of [12] acknowledged the growing importance of Internet of Things (IoT) networks made up of UAVs in a range of civilian and military applications. However, UAV networks have severe network security challenges, making IDS essential for their defense. Traditional IDSs frequently fall short of meeting the high bandwidth and data traffic demands of contemporary computer networks. In order to improve intrusion detection effectiveness and lower false alarms, researchers have resorted to machine learning and deep learning techniques. The Deep Reinforcement Learning and Black Widow Optimization (DRL-BWO) method is used to optimize deep reinforcement learning for UAV networks in this research report. The method uses a Deep Belief Network (DBN) for intrusion detection that is based on better reinforcement learning. The DRL approach is parameter optimized using the BWO algorithm, which enhances the performance of intrusion detection in UAV networks. The suggested model is effective, as shown by extensive experimental analysis, which produced high accuracy of 98.9%. The results show how well-suited and effective the suggested solution is, making it a potential strategy for protecting UAV networks.

The literature review emphasizes ongoing research in the area of IDS for UAV communication networks in its conclusion. The research covers a range of approaches and techniques, such as reinforcement learning, timed probabilistic automata, deep learning, and machine learning. The outcomes provide remarkable detection accuracies, ranging from 98.6% to 99.6%, demonstrating the efficacy of these strategies in protecting UAV communication systems. Additionally, the research stresses the significance of tackling certain issues like categorizing Grayhole attacks and lowering false alerts. The performance of the suggested IDS approaches has been examined using a variety of datasets, such as CICIDS2017, UKM-IDS20, and UAV swarm datasets. The results emphasize the importance of feature selection for enhancing IDS performance, as fewer features not only increase accuracy but also need less memory and CPU time. Additionally, the incorporation of cutting-edge algorithms like LSTM-RNN, and DRL-BWO shows the capability of sophisticated methods in providing resilient and adaptable intrusion detection for UAV communication networks. It is clear that improvements in IDS for UAV communication have the potential to improve the security,

dependability, and integrity of UAV operations in important applications. To address new security issues, assess performance in practical situations, and improve the effectiveness of intrusion detection systems in the changing UAV communication environment, further study is nonetheless required.

We will expand on the knowledge gathered from the examined literature in the subsequent sections as we provide our proposed approach for intrusion detection in UAV communication networks. To accomplish precise and effective intrusion detection, the technique uses cutting-edge algorithms for a large dataset. Through our study, we expect to advance the field of UAV communication security and promote the safe and dependable use of UAVs across a range of applications.

3 The Proposed Method

The methodological approach described in this part is used to improve the efficacy of intrusion detection in UAV communication networks. By detecting and reducing possible security risks, intrusion detection is essential for protecting the UAV communication infrastructure. The very unbalanced structure of UAV transmission data, however, makes it difficult to do reliable detection. To solve this problem, we suggest combining Synthetic Minority Over-sampling Technique (SMOTE) with Long Short-Term Memory (LSTM) networks to enhance the detection of minority class incursions while preserving a balanced dataset representation. With the use of this combined strategy, the LSTM-SMOTE algorithm is better able to distinguish between intrusions in UAV communication data by learning from both the majority and minority class cases. With the use of our technology, we hope to significantly enhance intrusion detection performance while also enhancing the security and dependability of UAV communication networks.

3.1 Dataset

In order to evaluate the performance and efficiency of IDS in the field of network security, it is essential to have access to extensive and trustworthy datasets. In recent years, the CICIDS2017 dataset has been a well-known source for assessing IDS algorithms. The CICIDS2017 dataset, created by the Canadian Institute for Cybersecurity (CIC), provides a broad and comprehensive collection of network traffic data that includes both legitimate and criminal operations. This dataset offers a realistic picture of network settings by incorporating multiple attack scenarios, network protocols, and traffic patterns. We present our methodology for intrusion detection and compare its performance and effectiveness against the CICIDS2017 dataset. We hope to use this standardized dataset to show how well our suggested strategy works for identifying and thwarting different kinds of network intrusions. The CICIDS2017 dataset was used as the basis for our study, ensuring that our suggested technique is subjected to a thorough review and comparison with existing methodologies, advancing the area of intrusion detection and boosting the security of network infrastructures.

3.2 Feature Selection

To create a reliable intrusion detection technique, we carefully analyze the pertinent classes from the dataset throughout the feature selection stage of our study. We concentrate on many attack types in particular, such as PortScan, Web Attack, Brute Force, DDoS, Bot, Infiltration, DoS, and Heartbleed. These attack classes stand for a variety of hostile actions that endanger the network. Additionally, we define a distinct class called "BENIGN," which includes examples of safe data flow exhibiting typical network behavior. The classifications we prioritize for categorization in our suggested strategy are clearly illustrated in Fig. 2 with a focus on separating attack occurrences from the secure data flow.

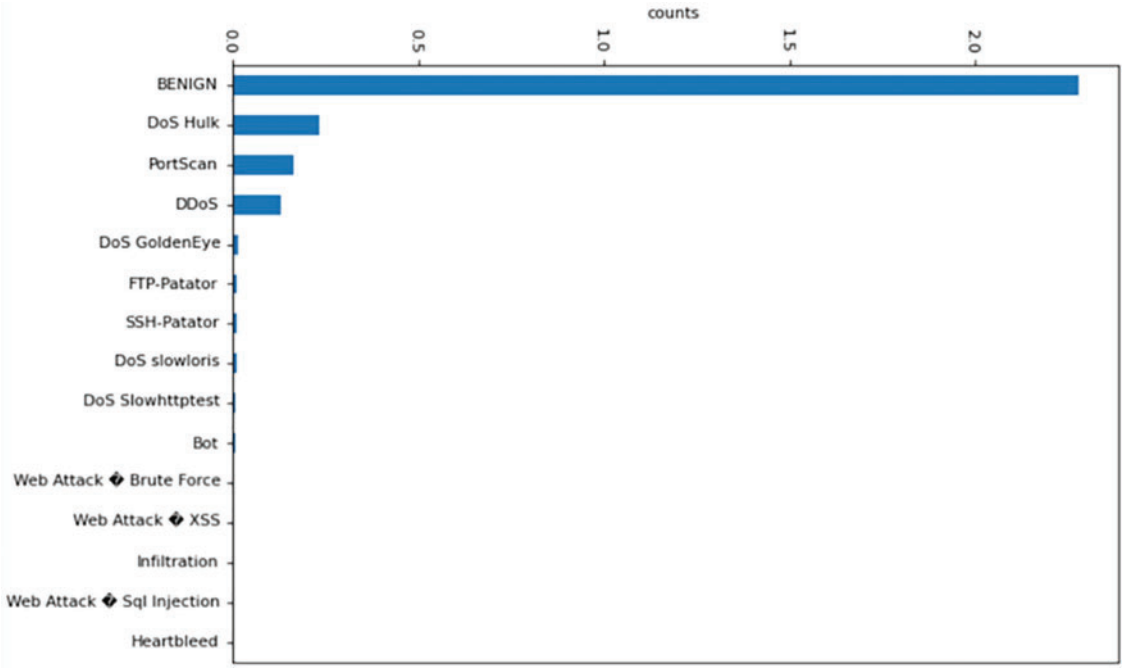

Figure 2: The features chosen to be used as inputs for our methodology

The focus of our intrusion detection system is on precisely detecting and categorizing the important attack classes while distinguishing them from innocuous network traffic due to our feature selection technique. We prioritize these particular classes in an effort to provide an accurate and effective intrusion detection system that successfully handles the security issues brought on by the identified attack vectors.

3.3 Binary Classification SMOTE

In order to overcome the class imbalance problem in our dataset, we use the Synthetic Minority Over-sampling Technique (SMOTE) as a binary classification approach in our research. A popular strategy called SMOTE oversamples the minority class in an effort to address the problems caused by unbalanced data [9]. In our example, we classify different assaults such as PortScan, Web Attack, Brute Force, DDoS, Bot, Infiltration, DoS, and Heartbleed under a single class called "ATTACK," whereas examples denoting typical and legal actions are referred to as "BENIGN." SMOTE works by creating synthetic instances for the minority class based on the already available data points. It locates each minority class sample's closest neighbours and generates synthetic samples along the line segments spanning the minority class instance and those neighbours. By expanding the representation of the "ATTACK" class, we can balance the distribution of classes throughout the dataset. We try to lessen the training process' bias towards the majority class by utilizing SMOTE. Oversampling the minority class makes it possible for both classes to be represented fairly, which improves the effectiveness and precision of our intrusion detection system. With the use of this method, the model is better able to recognize and categorize different sorts of assaults inside UAV communication networks by efficiently learning from examples that fall under the "ATTACK" class. Instances marked as "BENIGN" continue to display themselves just as they do now. To provide a balanced dataset that includes both attack and benign events by oversampling the minority class. We train our intrusion

detection system using this expanded dataset and the LSTM method, which is excellent at identifying sequential patterns.

3.4 LSTM Detection

We introduce the LSTM algorithm as a deep classifier in this part of the method we have selected for training and evaluating the SMOTE output in our intrusion detection system. Recurrent Neural Networks (RNNs) of the LSTM variety excel at catching and learning long-term relationships in sequential data, making them ideally suited for studying network traffic patterns [13]. Here, we discuss the LSTM's workings and describe how we will apply them to our technique. The LSTM model is trained using this supplemented dataset as its input. The LSTM algorithm examines the sequential network traffic data during the training phase, learning to identify complicated temporal patterns linked to attacks and safe activities. It improves the classification and differentiation of various kinds of network traffic by iteratively updating internal parameters based on backpropagation over time. Table 1 shows the hyperparameters for LSTM. The input sequences of network traffic examples are fed into the LSTM model during training, which trains it to recognize relationships and patterns. The model successfully processes lengthy sequences and alleviates the vanishing gradient problem by using its internal memory cells and gating mechanisms to selectively preserve or delete information. The LSTM model improves at identifying and categorizing intrusions in UAV communication networks by learning from the expanded dataset, which now provides a balanced representation of attack and benign cases. We move on to the testing step after the LSTM model has been trained. In this step, we make use of a different testing dataset made up of fictitious examples of network traffic. These sequences are processed by the trained LSTM model, which creates predictions for each occurrence and categorizes them as either "ATTACK" or "BENIGN" based on previously discovered patterns. We assess the accuracy, precision, recall, and other performance parameters of our intrusion detection system by comparing the model's predictions with the ground truth labels of the testing dataset. Our intrusion detection method shows promise for successfully identifying and mitigating attacks in real-time settings by utilizing LSTM's capacity to capture long-term dependencies and learn from the balanced dataset provided by SMOTE.

Table 1: The highlighted hyperparameters for LSTM

No.	Hyperparameter	Value
1	Activation function	SoftMax
2	Number of epochs	100
3	Dropout	0.2
4	Units	30
5	Optimizer	Adam

The LSTM-based intrusion detection system's training phase includes a comparison of loss and validation loss that acts as a gauge of its generalizability and convergence. While the validation loss predicts the model's performance on unobserved data, the training loss measures the model's capacity to match the patterns in the training data. We can spot indications of overfitting or underfitting by keeping an eye on the loss and validation loss as shown in Fig. 3. A low training loss but a large validation loss point to overfitting and signal the model cannot generalize. On the other hand, high training and validation losses indicate underfitting and show that the model is unable to capture

the underlying patterns. We can guarantee the LSTM model learns and simplifies well by balancing training and validation loss.

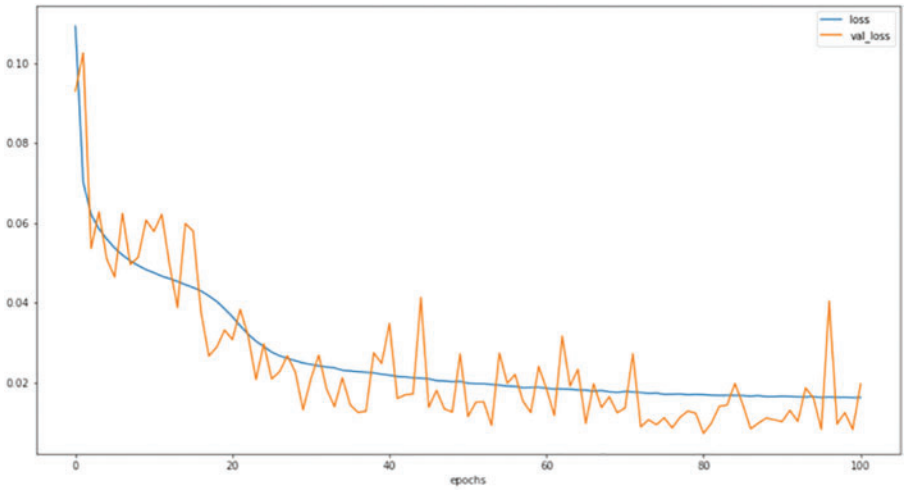

Figure 3: The loss and validation loss values

3.5 Model Deployment

In our comprehensive approach to ensuring the security of UAV operations, we have deployed the IDS both onboard the UAV and at the Ground Control Station (GCS). This dual deployment strategy offers a layered defense mechanism against potential attacks. The IDS onboard the UAV plays a crucial role in preserving the integrity and security of the UAV itself. Acting as the first line of defense, it continuously monitors the data collected from the onboard sensors. The intrusion detection algorithm analyzes this data by comparing it against a knowledge database, which includes information gathered from prior instances of assaults and typical behaviors. By leveraging this database, the system can identify and flag any recognized attacks or anomalies. These incidents are then recorded and added to the blacklist stored in the ground-based data storage. Simultaneously, at the GCS, an additional intrusion detection mechanism is employed to monitor the communication channels between the UAV and the GCS. This system utilizes the LSTM-SMOTE method, which allows for real-time analysis of the communication data. By centralizing the monitoring and analysis process at the GCS, we can ensure the timely detection of intrusions and the implementation of appropriate countermeasures. To maintain an up-to-date knowledge base and protect the entire fleet of UAVs, including those on the ground or in the air, a synchronization process is performed. When a UAV returns to the ground control base, the primary database is updated with the most recent data from its flight. This updated information, including the latest knowledge of attacks and typical behaviors, is then shared with the rest of the fleet. This synchronized approach enhances the overall security posture and enables proactive threat detection in future UAV operations. Fig. 4 illustrates the interconnected components and information flow within our system, showcasing the collaborative role of the onboard and ground-based intrusion detection mechanisms.

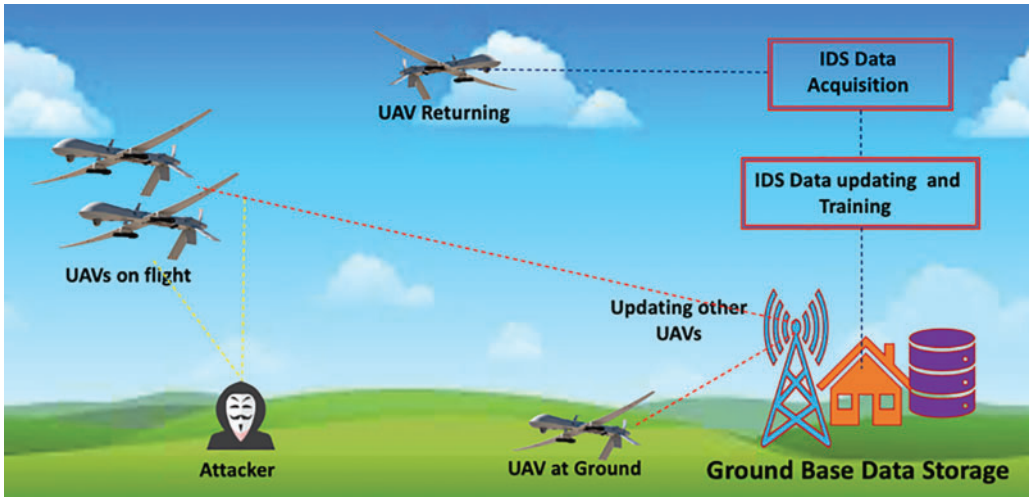

Figure 4: The IDS model deployment scenario

By using this strategy, our IDS integrates both onboard and main databases while using each UAV's past flight data. By doing this, the system is kept up to date and is able to recognize any new attack patterns or abnormalities. The UAV communication network's overall security and resilience are improved by the seamless integration of the IDS with UAV operations, which creates a proactive defense mechanism against intrusions. The deployment of models and data flow throughout the IDS system are depicted in Fig. 1 with particular emphasis placed on the ongoing updates and knowledge exchange between the onboard and ground-based components. The UAV fleet is given the ability to defend against prospective assaults collectively due to this deployment approach, which ensures that the IDS stays flexible to changing threats.

The LSTM-SMOTE approach is a powerful technique that enhances intrusion detection in UAV communication channels. By combining the capabilities of the LSTM network with the SMOTE algorithm, it effectively analyzes network traffic data to identify potential intrusions and malicious activities. What sets this approach apart is its versatility, as it can be applied to any type of communication channel, irrespective of the underlying technology or protocol used for UAV-GCS communication. Whether the communication is based on Radio Frequency (RF), satellite communication, or any other wireless technology, the LSTM-SMOTE approach remains agnostic to the specific communication technology employed. It is also independent of any particular communication protocol, be it TCP/IP, UDP, or proprietary protocols. This flexibility allows the method to operate on network traffic data, regardless of the communication type or protocol, enabling it to effectively identify patterns and anomalies indicative of intrusion attempts.

During the data processing stage, the intrusion detection algorithm carefully examines the incoming data collected from onboard sensors. Leveraging knowledge from prior instances of attacks and typical behaviors, the algorithm identifies any detected attacks or anomalies. Subsequently, the identified data is marked and added to the ground-based data storage's blacklist. This blacklist acts as a comprehensive database of attack signatures and abnormalities, empowering the system to remain vigilant and effectively identify potential dangers in future UAV operations. By associating the data, itself with the blacklist, our system focuses on the inherent characteristics of the data rather than labelling specific data sources as unreliable. This approach significantly enhances the overall

security and integrity of the system, ensuring a robust defense against intrusions and preserving the trustworthiness of UAV operations.

4 Results and Analysis

Based on the evaluation of our output, we give the performance metrics of our IDS in the research outcomes analysis section. The important metrics for both the "BENIGN" (representing typical activities) and "ATTACK" classes are shown in the table below, including accuracy, precision, recall, and F1-score. The tests were carried out in the Anaconda-Python environments on a Windows 10 PC with an Intel Core i7 4210H processor running at 2.90 GHz and 16 GB of RAM. Our IDS's accuracy for the "BENIGN" class was 99.71%, demonstrating its capacity to categorize typical occurrences. The precision number of 99.95% emphasizes the system's accuracy in recognizing normal activities by denoting the high proportion of genuine positive predictions compared to false positives. The IDS's capacity to efficiently capture a sizeable fraction of genuine positive cases while reducing the false negative rate is demonstrated by the recall value of 99.44%. The F1-score of 99.89% provides a thorough evaluation of the IDS's performance for the "BENIGN" class by reflecting the overall balance between precision and recall. The results are shown in Table 2. The analyses of both BENIGN & ATTACK show that the proposed technique performed better.

Table 2: The IDS accuracy for the proposed algorithm

Class	Accuracy	Precision	Recall	F1-score
BENIGN	99.71%	99.95%	99.44%	99.89%
ATTACK	99.83%	97.95%	99.79%	98.96%

Nevertheless, Our IDS's high accuracy of 99.83% for the "ATTACK" class demonstrates its capacity to accurately identify occurrences that constitute attacks. With a precision rating of 97.95%, it is clear that the majority of occurrences that were correctly identified as assaults were detected, reducing the number of false positives. The IDS is effective in capturing the bulk of true positive events, as seen by the recall score of 99.79%, which also suggests a low false negative rate. The F1-score of 98.96% provides an overall assessment of the IDS's performance for the "ATTACK" class by acting as a harmonic mean between accuracy and recall. These data show how well our IDS performs in correctly identifying situations as "BENIGN" or "ATTACK".

The robustness of our technique in recognizing and differentiating between legitimate and harmful actions inside UAV communication networks is validated by the excellent accuracy, precision, recall, and F1-score values. These findings demonstrate our IDS's capacity to protect UAV operations and uphold the security of crucial missions as a strong defensive tool.

5 Conclusion and Future Work

A substantial improvement in strengthening the security and integrity of crucial missions is represented by the implementation of LSTM-SMOTE in intrusion detection for UAV communication. The LSTM-SMOTE IDS demonstrates its effectiveness in recognizing and preventing possible threats inside UAV communication channels with a detection accuracy of 99.83% using the CICIDS2017 dataset. This new method adds to the overall resilience and dependability of UAV operations in sensitive situations by strengthening the security of UAV communication. In order to guarantee the

security, dependability, and efficiency of UAV missions in the face of changing security challenges, and ongoing research and development in the field of intrusion detection techniques, particularly those utilizing cutting-edge machine learning algorithms like LSTM-SMOTE are essential. In summary, the proposed LSTM-SMOTE method is designed to be independent of the communication type and communication protocol between the UAV and the GCS, making it versatile and adaptable to different UAV communication environments. It is necessary to keep investigating and creating intrusion detection methods for future communication networks. The performance of the method might be improved by more research into other architectures, hyperparameter optimization, and testing the system against various and changing attack scenarios. The intrusion detection system may also be made more effective and assure prompt threat mitigation by integrating real-time monitoring and adaptive response methods. The efficiency of LSTM-SMOTE in real-world circumstances may also be confirmed by performing field tests and case studies in real-world UAV flights. Future studies will contribute to the ongoing enhancement of UAV communication security such as encrypted communications, detection time from the start of an attack, and the general accomplishment of UAV missions by focusing on these areas.

Acknowledgement: The authors acknowledge the contribution and the support of the Department of Electrical & Computer Engineering and Computer Science at Jackson State University (JSU).

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: A. Abdulghani, M. Abdulghani, W. Walters, K. Abed; data collection: A. Abdulghani; analysis and interpretation of results: A. Abdulghani, M. Abdulghani, W. Walters, K. Abed; draft manuscript preparation: A. Abdulghani, M. Abdulghani, K. Abed. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The dataset used in this work is available online and can be accessed freely on https://doi.org/10.3390/electronics10212633. The code used and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. J. Hadi, Y. Cao, K. U. Nisa, A. M. Jamil and Q. Ni, "A comprehensive survey on security, privacy issues and emerging defense technologies for uavs," *Journal of Network and Computer Applications*, vol. 213, pp. 103607, 2023. https://doi.org/10.1016/j.jnca.2023.103607

[2] A. M. Abdulghani, M. M. Abdulghani, W. L. Walters and K. H. Abed, "Cyber-physical system based data mining and processing toward autonomous agricultural system," in *2022 Int. Conf. on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, USA, pp. 720–724, 2022. https://doi.org/10.1109/CSCI58124.2022.00214

[3] Z. Wang, W. Li, S. Wu, Y. Zhou, L. Yang *et al.,* "A survey on cybersecurity attacks and defenses for unmanned aerial systems," *Journal of Systems Architecture*, vol. 138, pp. 102870, 2023. https://doi.org/10.1016/j.sysarc.2023.102870

[4] A. O. Hashesh, S. Hashima, R. M. Zaki, M. M. Fouda, K. Hatano *et al.,* "AI-enabled UAV communications: Challenges and future directions," *IEEE Access*, vol. 10, pp. 92048–92066, 2022. https://doi.org/10.1109/ACCESS.2022.3202956

[5] E. A. Alareqi and K. H. Abed, "Predictive hybrid machine learning model for network intrusion detection," in *The 2018 Int. Conf. on Data Science (ICDATA'18)*, Las Vegas, Nevada, pp. 258–262, 2018.
[6] M. M. Abdulghani, A. Harden and K. H. Abed, "A drone flight control using brain-computer interface and artificial intelligence," in *Int. Conf. on Computational Science and Computational Intelligence—Artificial Intelligence (CSCI'22-AI)*, Las Vegas, NV, USA, pp. 1–6, 2022.
[7] R. Hamadi, H. Ghazzai and Y. Massoud, "Reinforcement learning based intrusion detection systems for drones: A brief survey," in *2023 IEEE Int. Conf. on Smart Mobility (SM)*, Thuwal, Saudi Arabia, pp. 104–109, 2023. https://doi.org/10.1109/sm57895.2023.10112557
[8] R. A. Ramadan, A. H. Emara, M. Al-Sarem and M. Elhamahmy, "Internet of drones intrusion detection using deep learning," *Electronics*, vol. 10, no. 21, pp. 2633, 2021. https://doi.org/10.3390/electronics10212633
[9] V. Subbarayalu and M. A. Vensuslaus, "An intrusion detection system for drone swarming utilizing timed probabilistic automata," *Drones*, vol. 7, no. 4, pp. 248, 2023. https://doi.org/10.3390/drones7040248
[10] A. B. Mohammed, L. Chaari Fourati and A. M. Fakhrudeen, "A comparative study of attribute selection algorithms on intrusion detection system in UAVs: A case study of UKM-IDS20 dataset," in *Lecture Notes in Computer Science*, vol. 13, pp. 34–46, 2023.
[11] K. Rahman, M. Aziz, N. Usman, T. Kiren, T. Cheema *et al.,* "Cognitive lightweight logistic regression-based ids for IoT-enabled FANET to detect cyberattacks," *Mobile Information Systems*, vol. 2023, pp. 1–11, 2023. https://doi.org/10.1155/2023/7690322
[12] V. Vargas, J. Aranda, R. Costa, P. Pereira and J. Barbosa, "Imbalanced data preprocessing techniques for machine learning: A systematic mapping study," *Knowledge and Information Systems*, vol. 65, no. 1, pp. 31–57, 2022. https://doi.org/10.1007/s10115-022-01772-8
[13] J. Rezaeenour, M. Ahmadi, H. Jelodar and R. Shahrooei, "Systematic review of content analysis algorithms based on deep neural networks," *Multimedia Tools and Applications*, vol. 82, no. 12, pp. 17879–17903, 2022. https://doi.org/10.1007/s11042-022-14043-z