Grenze International Journal of Engineering and Technology, January Issue

An Intelligent Intrusion Detection System (IDS) for Internet of Drones (IOD) using Improved Deep Learning Framework

Ch. Chandra Sekhar[1], Ch. Sri Devi[2], Ramesh Naidu Balaka[3], J. Sai Kamal[4], B. Shanmukh[5] and K. Guna[6]
[1-6]Aditya Institute of Technology and Management, Dept. of IT, Tekkali, AP, India
Email: dlaxmics@gmail.com, sridevi.ch2003@gmail.com, ramesshnaiidu5@gmail.com, jsaikamal@gmail.com, buddepushanmukh124@gmail.com, gunarithwick@gmail.com

***Abstract*— The enlargement of the Internet of Things into numerous domain names has paved the manner for the advent of the Internet of Drones (IOD) as a crucial subset, gaining massive attention due to its essential programs. However, IoD networks are incredibly liable to security threats due to their decentralized and dynamic nature. To address the ones demanding conditions, Intrusion Detection systems (IDS) are used to have a study and evaluate information site traffic among linked nodes, efficaciously figuring out wonderful types of cyber-attacks in the IoD environment. The Flying ad hoc network (FANET) further complicates intrusion detection due to its complex architecture and evolving protection threats to mitigate those risks, FANET makes use of real-time statistics analytics powered by way of an improved Deep learning Framework, which includes a Recurrent Neural network (RNN), The framework typically is predicated on RNNs for intrusion detection at the same time as integrating massive information analytics to hit upon anomalies, it employs Long Short-Term Memory (LSTM), a variation of RNN, to decorate accuracy and improve safety hazard detection.**

***Index Terms*— IDS, IOD, LSTM, RNN, FANET, DEEP LEARNING.**

I. INTRODUCTION

The Internet of Drones (IoD) are more and more applied in several IoT programs, yet its networks, in particular Flying Ad Hoc Networks (FANETs), continue to be fairly liable to protection threats. Their decentralized nature makes them prone to cyber-attacks and unauthorized intrusions, highlighting the need for strong safety mechanisms. To counter those challenges, an Intrusion Detection System (IDS) performs a vital role in reading network traffic and detecting capability threats. This observe provides a smart IDS specifically designed for IoD, incorporating a complicated Deep gaining knowledge of Framework that leverages RNN and LSTM fashions.
The internet of Drones (IoD) has several packages across specific sectors. Its miles utilized in surveillance for monitoring big regions, in delivery offerings to move items like scientific substances, and in agriculture for duties like crop tracking and spraying. In environmental tracking, they tune conditions like air quality and natural world [1] [2]. The army uses IoD for surveillance and reconnaissance, at the same time as drones also are used for visitors monitoring to enhance avenue safety. These programs show how IoD is remodeling industries but additionally create the want for strong protection systems to cope with rising threats [3].

Grenze ID: 01.GIJET.12.1.69

An Intrusion Detection system is a vital cybersecurity degree that helps discover capacity threats by way of constantly reading network site visitors and device activities. IDS can be classified into two number one sorts: Network-based Intrusion Detection System (NIDS), which scrutinizes records waft across networks to hit upon anomalies, and Host-based Intrusion Detection System (HIDS), which video display unit's activities on character devices. The detection techniques contain signature-based detection, which identifies recognized assault patterns, and anomaly-primarily based detection, which detects deviations from everyday conduct. Which identifies deviations from traditional behavior that would recommend security risks [4]. Enforcing IDS complements protection with the aid of way of permitting early threat detection, fast reaction to attacks, and precise activity logging for forensic investigations and compliance functions [5].

Problem Statement: Despite the growing importance of IoD, most existing security frameworks are inadequate in handling multi-vector, time-dependent attacks. Conventional IDS models exhibit limitations such as high false positive rates, poor scalability, and an inability to generalize to unseen attack types. There is a critical need for an intelligent IDS capable of processing sequential network and telemetry data, detecting subtle anomalies, and adapting to new threat vectors.

II. Related Works

This section examines existing studies at the IoD to discover gaps and demonstrate the contributions of the proposed framework. Gamal et al. [1] used RNN-LSTM with SMOTE and one-hot encoding on CICIDS2017 data, and reported the accuracy of over 99%. Jose et al. [2] presented the STFA-HDLID model, which combined Sea Turtle Foraging Algorithm with Deep Belief Networks. Waheed et al. [4] proposed a hybrid ABC-DA via ANN, outperforming in classification over several benchmark datasets.

Moreover, Heba et al. [7] applied meta-heuristic algorithms with stacked autoencoders used a Crystal Structure Optimization approach for feature selection and hyperparameter optimization. However, almost all related work presented to date considers offline processing, or it is unable to deal with real-time environments. And not many models take into account the learning process that allows automatic systems to adjust to changes in the threat landscape.

Khalid et al. [5] CSODAE-id model become designed to enhance net of Drones (IoD) protection by using efficiently detecting intrusions. This technique contains feature selection through a modified Deer searching Optimization approach (MDHO-FS) to refine enter statistics AE used for the class. Additionally, Crystal shape Optimization (CSO) is hired for hyperparameter tuning, similarly optimizing detection performance in the Table 1 provides the information to the related work.

Table I. Recent Comparative IDS Approaches

Study	Model	Dataset	Accuracy	Limitation
Gamal et al. [1]	RNN-LSTM + SMOTE	CICIDS2017	99.84%	Limited real-time capability
Jose et al. [2]	STFA + DBN	UNSW-NB15	98.60%	High computational cost
Waheed et al. [4]	ABC-DA +ANN	NSL-KDD	96.75%	Inefficient on large-scale networks
Heba et al. [7]	MFOFS + SAE	UNSW-NB15	98.92%	Requires pre-processed features

III. The Proposed IDS in the Real Environment

Looking into the Fig. 1 represents the workflow of an IDS for the IoD the usage of a deep learning framework. It starts with facts series, in which facts consisting of drone telemetry, network communication logs, and sensor information is collected. This raw data is then subjected to facts labelling and annotation, wherein it's far classified into regular or anomalous behaviors, imparting a foundation for supervised learning. Next, the records undergo preprocessing, which involves cleaning, normalizing, and transforming it into an everyday layout suitable for evaluation [6][7]. The function extraction step identifies important patterns, collectively with community utilization anomalies or uncommon drone movement, which is probably indicative of ability protection threats.

Information collection: Statistics is accumulated from drones, consisting of telemetry, network verbal exchange logs, and sensor information. The ones datasets offer insights into drone movements, network behaviours, and feasible assault patterns. Accumulated information consists of timestamps, IP addresses, packet sizes, and connection attempts, which may be vital for in addition assessment.

Pre-processing: The raw accrued statistics is wiped smooth and normalized to take away noise and inconsistencies. Duplicates and irrelevant facts are filtered out to maintain security. Information is formatted into

primarily based totally actually logs to ensure compatibility with deep learning models, permitting inexperienced processing and evaluation.

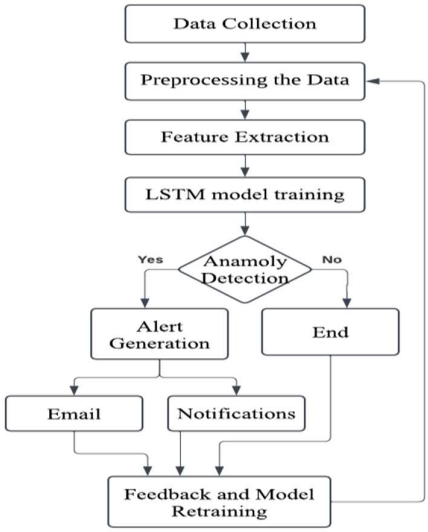

Figure 1. Workflow for the proposed IDS

Feature Extraction: Important network parameters which includes packet transmission price, latency, supply IP, and unauthorized get right of entry to attempts are extracted. This step allows in figuring out anomalous conduct by using detecting deviations from everyday community operations. Extracted functions are then converted into numerical representations suitable for device gaining knowledge.

Training LSTM model: The pre-processed information is hired to educate an LSTM model, which learns sequential styles of ordinary and ordinary network sports activities. Ancient attack datasets are used to help the version understand awesome intrusion types. Hyper-parameter tuning is achieved to decorate the model's performance and detection accuracy.

Anomaly Detection: The educated LSTM version constantly video display devices incoming information in real-time. If it detects deviations from discovered normal styles, it flags the occasion as an anomaly. The model assesses each anomaly primarily based totally on predefined thresholds, classifying it as a potential cyber-assault or a fake alarm.

Alert: If an anomaly is classed as a safety threat, an alert is gentrified alerts are classified based on severity stages low, mild, or crucial. Notifications are dispatched to administrators through e-mail, SMS, or dashboard indicators. The device moreover logs precise critiques for future analysis and forensic studies.

Feedback Loop: The device consists of feedback from safety professionals to beautify version accuracy. Fake positives and negatives are reviewed, and changes are made to refine detection thresholds. Over time, the version adapts to new and evolving cyber threats, constantly enhancing its detection competencies.

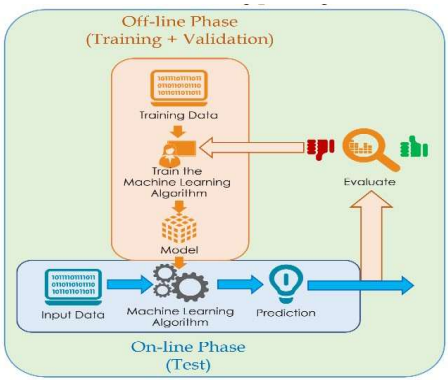

Figure 2. The proposed IDS model

The intrusion detection machine for the IoD works in two fundamental phases from Fig. 3. The offline segment and the online segment, inside the offline segment, the IDS learning version is trained the use of categorized information to apprehend both regular and unusual behaviours. This educated model is then used within the on-line phase, in which it analyses actual-time enter from drones to find out capability threats [8]. The machine collects information via a huge router, filters it, and sends it to a number one hub for assessment the use of deep reading models like RNN and LSTM. If any unusual interest is detected, the machine immediately increases alerts to prevent feasible attacks. This setup permits at ease drone verbal exchange and ensures secure operation [9][10].

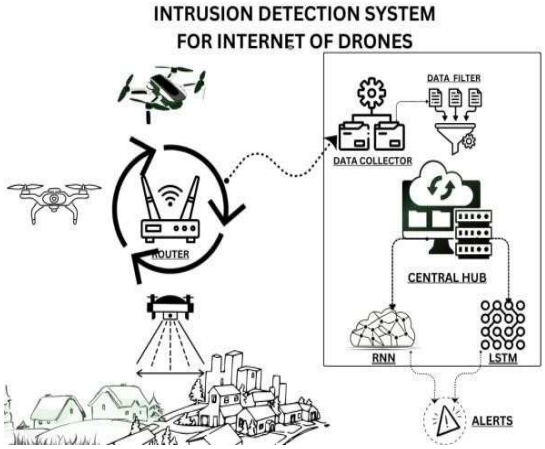

Figure 3. Architecture of IDS

A. Dataset used-CICIDS2017

The dataset used in this study was obtained from wellestablished cybersecurity repositories containing realworld and simulated attack scenarios. The dataset includes network traffic logs, drone telemetry data, and attack simulation records. The data in the Table 2. Characteristics of the CICIDS2017 Dataset represents the characteristics of the CICIDS2017 dataset like type, releasing year, instances, features, class and the data in the Table 3. represents the distribution of instances by class for the CICIDS2017 dataset, include different class names such as benign, port scan, Dos, Bot, Brute force attack, XSS, infiltration, SQL injection attack [11].

TABLE II. CICIDS2017 DATASET CHARACTERISTICS

Property Name	CICIDS2017
Type	Multi-class
Releasing Year	2017
No. of Instances	2,830,540
Total Features	83
No. of Classes	15

TABLE III. CICIDS2017 DATASET DISTRIBUTION OF INSTANCES BY CLASS

Class Name	Total No. of instances
Benign	9891,074
port scan	5158,930
DoS	2128,027
Bot	1,966
Brute Force attack	1,507
XSS	5652
Infiltration	636
WSQL Injection attack	121

B. Drone Intrusion Detection using RNN Model

RNN is a device getting to know model mainly designed for processing sequential information. It achieves this by using preserving hidden states which is shown in Fig. 4. That maintain statistics from previous time steps, permitting it to recognize styles and dependencies through the years, their capacity to apprehend temporal

relationships makes them mainly beneficial for drones, particularly in analyzing timecollection statistics to detect network anomalies or protection threats [12]. By using education on labeled datasets, RNNs can identify suspicious patterns and deviations in network site visitors.

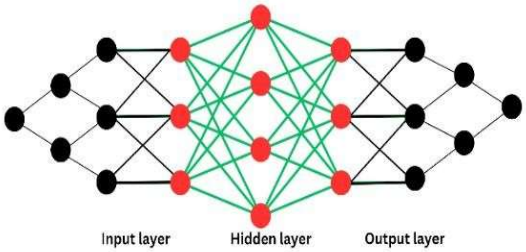

Figure 4. The RNN cell architecture

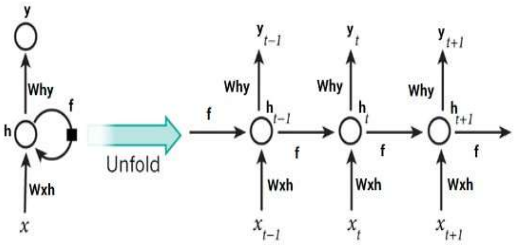

Figure 5. The RNN cell architecture

Hidden State Update

$$h_t = (W_h x_t + U_h h_{t-1} + b_h) \qquad (1)$$

From Fig. 5 represents the shape consists of interconnected nodes, in which: x_t represents the input at a particular time step, y represents output produced through the model, Wxh represents the weights used to convert the enter into the hidden nation, Why represents the weights that convert the hidden state into a final prediction, h_t denotes the hidden state,at the same time as the circle represents the RNN mobile, b_h for bias time period, and f is activation function (commonly tanh or ReLU).

Output Calculation:

$$y_t = W_{hy} h_t + b_y \qquad (2)$$

Where: y_t for output at time, W_{hy} for hidden-to-output weight matrix and b_y for output bias.

C. Drone Intrusion Detection using LSTM Model

LSTM networks are a specialized version of RNN especially engineered to method sequential records, greater correctly by way of mitigating the gradient issue. Traditional RNNs conflict to preserve statistics over long sequences, while LSTMs use a completely unique memory mobile shape with gating mechanisms to modify facts float. This permits them to seize long-time period dependencies, rendering them noticeably suitable for applications like time collection forecasting, herbal language processing, and anomaly detection [13]. LSTMs incorporate a memory mobile that lets in them to save and control lengthy-term dependencies. This makes them particularly powerful for programs that require the retention of beyond information, which include time collection, forecasting, anomaly detection, and predictive modelling [14].

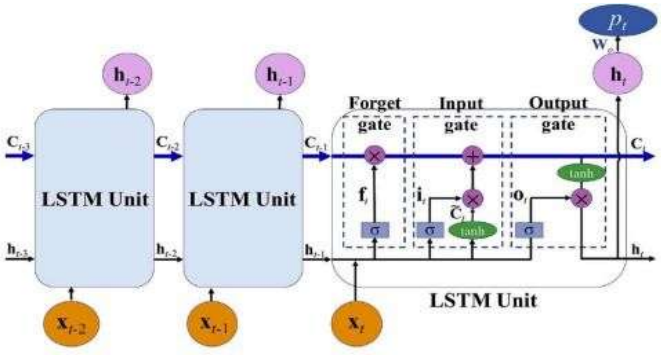

Figure 6. The LSTM cell architecture

LSTMs manage information drift via three number one gates, from the above Fig. 6. The forget Gate (ft), which gets rid of unneeded statistics, the input Gate, and the Output Gate, which determines what records is passed earlier [15]. The ones gates work together to maintain and update important records, permitting LSTMs to correctly analyze from sequential styles.

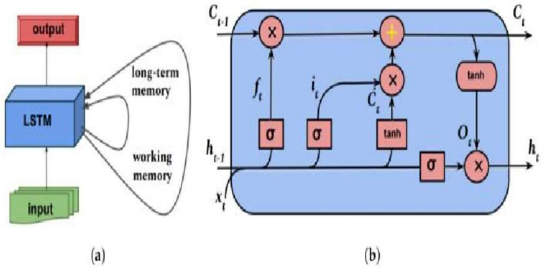

Figure 7. LSTM Internal Structure

Forget Gate

$$ft = (Wfxt + Ufht{-}1 + bf) \qquad (3)$$

Fig. 7 represents the shape consists of interconnected nodes, where: f_t for forget gate activation, W_f, U_f for weight matrices, b_f for Bias term and σ for Sigmoid activation function.

Input Gate:

$$i_t = (W_i x_t + U_i h_{t-1} + b_i) \qquad (4)$$

$$C_t = \tan \mathrm{h}(W_c x_t + U_c h_t - 1 + b_c) \qquad (5)$$

$$C_t = f_t \odot C_{t-1} + i_t \odot C_t \qquad (6)$$

Where: i_t for Input gate activation, C_t for Cell state, $\tilde{C}_t$ for Candidate memory content, and $\odot$ for Element-wise multiplication.

Output Gate:

$$o_t = (W_o x_t + U_o h_{t-1} + b_o) \qquad (7)$$

Hidden State:

$$h_t = o_t \odot \tan \mathrm{h}(C_t) \qquad (8)$$

Where: o_t for Output gate activation, h_t for Hidden state.

D. Drone Data Collector

The system integrates an RNN-LSTM module that efficiently handles data collection and analysis. This module identifies key parameters from the incoming packets—such as reception rate, source and destination IP addresses, transmission rate, transmission-to-reception ratio, duration of activity, and transmission mode. To facilitate both batch and real-time processing, the design incorporates two data collection units, one embedded in each drone and another situated at the base station. This offers continuous monitoring, making sure dependable intrusion detection. The amassed statistics is then transmitted to the valuable RNN-LSTM module at the bottom station, wherein it is very well analyzed to. Not like conventional networks, UAV networks require nonstop verbal exchange with floor base stations whilst dynamically adjusting their places primarily based on operational needs [16]. To address this task, the proposed framework capabilities a twin-issue structure, which includes an onboard drone module and a base station module. Each drone is ready with an independent LSTMRNN module designed to hit upon protection threats autonomously. This distributed method enhances the accuracy of intrusion detection and enables real-time threat evaluation, thereby reinforcing the overall security of UAV networks.

E. Alerting and Response

RNN-LSTM models can be used to trigger various alert moves based on their predictions of anomalous community site visitor's internet of Drones (IoD) Intrusion Detection structures (IDS). The ones move can help mitigate protection dangers and guard the IoD machine.

- Log the occasion: hold the facts in a database or log document.
- trigger an Alert: ship an e mail, SMS, or a notification to the network administrator.
- Take automatic action: Block the source IP, terminate the session, etc.

IV. Findings And Analysis

The data in the Table 4, we evaluated the IDS on the CICIDS2017 dataset, a standard for intrusion detection benchmarks. The performance was compared against traditional Machine Learning models like Logistic Regression (LR), K-Nearest Neighbors (KNN), and Support Vector Machines (SVM).

Table IV. Performance Metrics

Model	Accuracy	Precision	Recall	F1-Score
LSTM-RNN (Proposed)	99.82%	99.77%	99.89%	99.83%
Logistic Regression	95.2%	94.8%	94.5%	94.6%
KNN	92.1%	91.3%	90.8%	91.0%
SVM	94.7%	93.6%	93.9%	93.7%

The proposed system showed remarkable generalization capability, effectively reducing both false positives and negatives. The use of LSTM cells enabled the model to capture long-term dependencies, which are essential in sequential network traffic analysis.

V. Conclusion

The IDS evolved for the IoD employs deep mastering techniques, those are RNN and LSTM, to decorate network safety. This efficaciously identifies anomalies in drone communique, supplying strong safety towards cyber threats. Experimental consequences show excessive detection accuracy while decreasing fake positives and negatives, making sure a reliable security mechanism for IoD networks. The findings highlight the effectiveness of Deep Learning-based IDS solutions in securing drone networks and permitting safe operations across numerous applications.

Future advancements can focus on integrating real-time data processing to enhance response times and deploying IDS on edge computing devices to improve scalability and efficiency. Enforcing Blockchain generation can in addition at ease drone verbal exchange with the aid of preventing unauthorized get right of entry to and making sure facts integrity.. Those enhancements will make contributions to a extra intelligent, scalable, and resilient IDS for future IoD packages.

References

[1] Gamal, M., Elhamahmy, M., Taha, S., & Elmahdy, H. (2024). Improving intrusion detection using LSTM-RNN to protect drones' networks. Egyptian Informatics Journal, 27, 100501.

[2] Jose, A., & et al. (202x). Statistical flow features analysis (STFA) with deep belief network (DBN) for intrusion detection.

[3] Ramadan,R. A., Emara, A.-H., Al Sarem, M., & Elhamahmy, M. (2024).Internet of Drones Intrusion Detection Using Deep Learning. Electronics, 10(21), 2633.

[4] Waheed, G., & Ghanem, A. (2020). Metaheuristic-based neural network training and feature selector for intrusion detection in large-scale networks.

[5] Rose, J. B. R., Arulmozhinathan, T., Gopinathan, V. T., & Benifa, J. B. (2023). Internet of drones: applications, challenges, opportunities. Internet of Drones, 1-18.

[6] Gueriani et al. (2024) provide a survey on Deep Reinforcement Learning (DRL) for IoT IDS, relevant to drone environments since drones are part of IoT ecosystems

[7] Heba, A., & et al. (202x). Multi-Objective Feature Selection (MFOFS) with Stacked Autoencoder (SAE) for intrusion detection.

[8] Xu et al. (Apr 2025) offer a comprehensive survey on DL-IDS, covering architectures like CNN, LSTM, GNN, transfer/few-shot learning—useful for drone IDS design.

[9] Elhamahmy, M., et al. (2024), Improving intrusion detection using LSTM RNN to protect drones' networks. Egyptian Informatics Journal, 27(4), 100501

[10] lzahrani, A. (2024) Novel Approach for Intrusion Detection Attacks on Small Drones Using ConvLSTM Model. IEEE Access, 12, 149238–149253.

[11] Escorcia-Gutierrez, J., Gamarra, M., Leal, E., Madera, N., Soto, C., Mansour, R. F., ... & Gupta, D. (2023). Sea turtle foraging algorithm with hybrid deep learning-based intrusion detection for the internet of drones environment. Computers and Electrical Engineering, 108, 108704.

[12] Ghanem, W. A. H., Jantan, A., Ghaleb, S. A. A., & Nasser, A. B. (2020). An efficient intrusion detection model based on hybridization of artificial bee colony and dragonfly algorithms for training multilayer perceptrons. IEEE Access, 8, 130452-130475.

[13] Mohamed, H. G., Alotaibi, S. S., Eltahir, M. M., Mohsen, H., Ahmed Hamza, M., & Sarwar Zamani, A. (2022). Feature selection with stacked autoencoder based intrusion detection in drones environment. Computers Mater Continua, 73(3), 5441-58.
[14] Alissa, K. A., Alotaibi, S. S., Alrayes, F. S., Aljebreen, M., Alazwari, S., Alshahrani, H., ... & Motwakel, A. (2022). Crystal structure optimization with deep-autoencoder-based intrusion detection for secure internet of drones environment. Drones, 6(10), 297.
[15] Abdelmaboud, A. (2021). The internet of drones: Requirements, taxonomy, recent advances, and challenges of research trends. Sensors, 21(17), 5718.
[16] Boccadoro, P., Striccoli, D., & Grieco, L. A. (2021). An extensive survey on the Internet of Drones. Ad Hoc Networks, 122, 102600.
[17] Chamola, V., Kotesh, P., Agarwal, A., Gupta, N., &Guizani, M. (2021). A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. Ad hoc networks, 111, 102324.
[18] Labib, N. S., Brust, M. R., Danoy, G., &Bouvry, P. (2021). The rise of drones in internet of things: A survey on the evolution, prospects and challenges of unmanned aerial vehicles. IEEE Access, 9, 115466-115487.
[19] Nguyen, H. P. D., & Nguyen, D. D. (2021). Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication. Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead, 185-210.
[20] Abualigah, L., Diabat, A., Sumari, P., &Gandomi, A. H. (2021). Applications, deployments, and integration of internet of drones (iod): a review. IEEE Sensors Journal, 21(22), 25532-25546.
[21] Menssouri, S., Delamou, M., Ibrahimi, K., & Amhoud, E. (2024) Enhanced Intrusion Detection System for Multiclass Classification in UAV Networks. arXiv preprint arXiv:2406.10417.
[22] Zhi, Y., Fu, Z., Sun, X., & Yu, J. (2020). Security and privacy issues of UAV: A survey. Mobile Networks and Applications, 25(1), 95101. Ilgi, G. S., & Ever, Y. K. (2020). Critical analysis of security and privacy challenges for the Internet of drones: A survey. In Drones in smart-cities (pp. 207-214). Elsevier.