



# Supervised Machine Learning For Detecting Drop Attack in UAV Ad-hoc Network

Said NECIRI<sup>1</sup>, Nouredine CHAIB<sup>2,\*</sup>, and Chabane DJEDDI<sup>3</sup>

<sup>1</sup> Computer Science and Mathematics Laboratory (LIM), Laghouat University, Laghouat, Algeria.

<sup>2</sup> Amar Telidji University, Laghouat 03000, Algeria [n.chaib@lagh-univ.dz](mailto:n.chaib@lagh-univ.dz)

<sup>3</sup> National school of artificial intelligence, Algeria  
[chabane.djeddi@univ-constantine2.dz](mailto:chabane.djeddi@univ-constantine2.dz)

\* Corresponding author

**Abstract.** UAV Ad hoc Networks (UANETs) play a critical role in applications that necessitate secure and resilient communication, including data collection and surveillance. UANETs encounter substantial security challenges as a result of their decentralized and dynamic characteristics. One such challenge is the potential for malicious nodes to disrupt operations through the discarding of packets. The Drop Attack Detection Algorithm (DADA-UANET), which utilises supervised machine learning to improve network security, is the subject of this research. A combination of Logistic Regression (LR), Decision Tree (DT), and K-Nearest Neighbours (KNN) is utilised to differentiate between normal and malicious nodes efficiently. Our methodology incorporates an original implementation of linear regression to evaluate the credibility of nodes on a periodic basis by analysing their past actions. The experimental findings derived from a comparative analysis demonstrate that our approach attains an enhanced level of performance, surpassing established methodologies by as much as 92% in classification accuracy when LR and KNN are employed. The integration of DADA-UANET substantially enhances the robustness of unmanned aerial vehicle (UAV) communication in the face of advanced cyber threats, thereby guaranteeing more dependable functioning of vital applications.

**Keywords:** UAV Ad-hoc Network (UANET) · Supervised Machine Learning · Path Credibility Matrix · Node Credibility Matrix · Node Presence Matrix.

## 1 Introduction

Unmanned Aerial Vehicles (UAVs) have gained significant prominence in various applications, ranging from surveillance and reconnaissance to disaster response and environmental monitoring. In the context of UAV operations, the establishment of efficient and secure communication networks is crucial for ensuring reliable data transfer and coordination among UAVs[4]. UAV Ad-hoc Networks (UANETs) have emerged as a viable solution, allowing UAVs to communicate

© The Author(s) 2024

C. A. Kerrache et al. (eds.), *Proceedings of the International Conference on Emerging Intelligent Systems for Sustainable Development (ICEIS 2024)*, Advances in Intelligent Systems Research 184,

[https://doi.org/10.2991/978-94-6463-496-9\\_22](https://doi.org/10.2991/978-94-6463-496-9_22)

with each other in a decentralized manner. However, the open and dynamic nature of UANETs makes them susceptible to various security threats, including the presence of Malicious nodes. Malicious nodes can compromise the integrity, confidentiality, and availability of data, leading to potential disruptions in UAV operations[12]. Therefore, there is a pressing need to develop robust security mechanisms for identifying and mitigating Malicious nodes within UANETs. Such networks can be secured using a variety of protocols and techniques [6]. Furthermore, by identifying whether a hostile node or an intruder is present in the network, this research presents an efficient technique for securing communication in UANET. Owing to numerous complicating circumstances, some of the currently in use techniques for determining if an intruder has entered the network are unreliable. Euclidean Distance (ED) and clustering are the foundations of an existing technique that finds intruders in a MANET [7]. The DPAA-AODV methodology is used in [14] as a way to lessen Black hole and Grey hole attacks, however both approaches take a lot of time. [2] a quantitative intrusion detection technique for the identification of hostile nodes. Approaches based on anomaly detection have been suggested by [3][10]. [9] Unsupervised technique based on statistical, spectral, model-based clustering, classification, and clustering is proposed for anomalous detection. The [16] technique is predicated on the extraction of features, followed by clustering and analysis of auto encoders. [5] Employing a supervised algorithm for intrusion detection. [14][11] represents the less accurate detection of an intrusion depending on the node's trust value. As the current approaches aren't accurate or effective enough, therefore, there is a possibility that unauthorized equipment or persons could hack the message. we provide a methodology in this study for safeguarding communication in UANET to determine whether a Malicious node is present in any communication network in UANETs. A Malicious node is defined as one that drops packets. To locate this malevolent node within the network, we can utilize multiple pre-existing machine-learning algorithms. First, we use linear regression algorithms to evaluate a node's credibility based on its behavior over time. Subsequently, nodes are classified using Logistic Regression (LR), Decision Tree (DT), and K-Nearest Neighbors (KNN) based on the derived trust values, distinguishing between malicious and normal nodes effectively. We will examine related work in section II. We describe The proposed system in section III. while Section IV presents the Detection Method, The Principale Of DADA-UNET is shown in Section V. Result And Analysis are presented in Section VI. Finally, Section VII concludes the paper.

## 2 Related Work

We examined numerous articles about the identification of intrusions and their resolutions to provide a quick overview of the techniques currently in use for the Flying Ad-Hoc Networks (FANETs). The authors of [4] highlight the growing need for security in these networks as they provide a machine-learning technique to identify Sybil attacks in the Internet of Flying Things (IoFT). The authors

have suggested improving network integrity and evaluating the effectiveness of a clustering technique to identify and remove rogue nodes in Mobile Ad hoc Networks (MANET) [7]. Discuss how quantitative intrusion detection techniques can be used to identify hostile nodes in MANETs, hence enhancing the security and dependability of these networks [2]. Utilizing data mining principles to increase detection accuracy, [3] develops a novel clustering strategy combined with an adaptive SVM classifier for intrusion detection in wireless sensor networks. [9] describes unsupervised anomaly detection methods for unmanned aerial vehicles to have the technology recognize anomalies on its own that might point to system malfunctions or security risks. To improve the security of UAV operations, [16] presents a unique method for identifying sensor attacks on unmanned aerial vehicles. [14] investigates the application of clustering methods and supervised learning to identify malicious nodes in drone ad-hoc networks to protect these networks against internal threats. Perform a security study of drone systems in [17], addressing several attack vectors, recognizing constraints, and making suggestions to improve drone security. To increase the resilience and adaptability of these systems, [8] proposes the use of software-defined networking in conjunction with machine learning to secure communications in drone swarms. To improve the security and dependability of automotive networks, [1] describes an incremental online machine-learning strategy for identifying hostile nodes in vehicular communications. This approach makes use of real-time monitoring.

### 3 The proposed system

In this section, we provide the DADA-UNET details of our solution. We start by providing the environment details, then we present the attacker model, and finally, we present our technique.

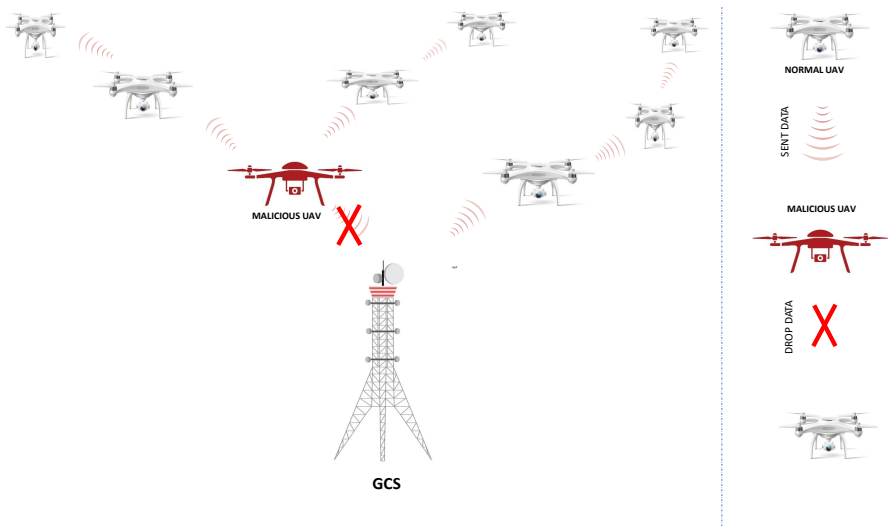
#### 3.1 System environment

Our system comprises of a ground station and an ensemble of UAVs nodes. The UAVs play the role of mobile nodes in setting up a communication network where the ground station acts as the ultimate recipient for data that is sent across by the UAVs. This model is illustrated as a directed graph with the UAV representing nodes while edges are created between them based on their communication proximity. Each flying UAV maintains its own geographic location consisting of latitude, longitude, altitude, direction and speed. Every searching UAV is allocated a stationary region which delineates the area it will survey and collect information from; this UAV graph model can support any typical route transmission mechanism.

#### 3.2 Attacker Model

The Model attacker is depicted in Figure 1, where the malicious nodes would not pass any data packets they receive to the destination as required but rather drop

them, which would result in a loss of information. The effect of drop attacks can be very drastic because they can cripple communication between the network nodes entirely. This means that some important information might not reach where it was intended, hence failure in mission-critical applications (commonly supported by FANETs) due to lack of data[1].



**Fig. 1.** Attacker model.

### 3.3 System model

There are UAV nodes with varying degrees of power. Strong nodes provide as reliable sources that aid in locating dangerous components within the network. Next, at the ground station, we gather packets sent across every routing path after injecting packets into the source UAV nodes. To see if any packets have been discarded. The ground station can obtain all the path information of the packet transmission because the routing protocol employed in the UAV ad-hoc network includes the addition of the relay nodes to the packet content. First, the packet drop rate on each path is equal to the credibility value of that path. Next, based on the credibility value of the path, we compute each UAV's credibility value using the linear regression machine learning algorithm. Eventually, the UAVs will be located using supervised machine learning techniques, Logistic Regression (LR), Decision Tree (DT), and K-Nearest Neighbors (KNN). The system model is represented in Figure 2.

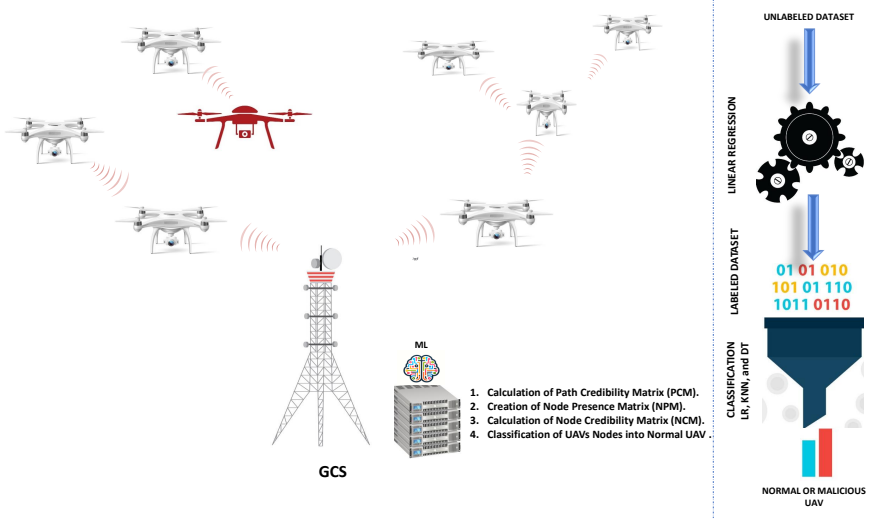


Fig. 2. System model.

## 4 The Principle of DADA-UNET

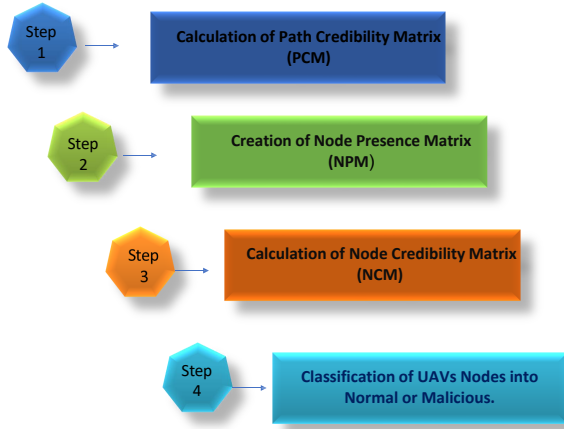
The DADA-UNET uses a combination of Supervised Machine Learning algorithms to detect malicious nodes in UNET. The DADA-UNET detection steps is represented in Figure 3

Table 1. List Of Terminologies.

Vocabulary	Meaning
Path Credibility Matrix (PCM)	Reputation or Trust value of the message path.
Node Presence Matrix (NPM)	An indication that a node exists along a path.
Node Credibility Matrix (NCM)	Trust or Reputation value of the node in the path.
Node Set	A list of nodes in a network.
Sent Packets	packets that the source's node sends to the grand station.
Received Packets	packets that the ground station receives from the source's node.
DR	Drop ratio

**Calculation of Path Credibility Matrix (PCM)** Path Credibility (PC) refers to a message's path's reputation or trust value. The value of this reputation is floating-point normalized. Appended in the PCM is the PC value for every path. Below is the calculation for path credibility.

$$DR = \frac{\text{len}[\text{SentPacket}] - \text{len}[\text{ReceivedPacket}]}{\text{len}[\text{SentPacket}]}$$



**Fig. 3.** DADA-UNET detection steps.

**Creation of Node Presence Matrix (NPM)** This matrix indicates whether a particular node of the node set is present in a particular path. Rows are paths in this matrix, and columns are nodes. The array is appended with the value 1 if a node from the set of nodes is found on a given path, and the value 0 otherwise.

$$A = \begin{vmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ u_{21} & u_{22} & \dots & u_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{m1} & u_{m2} & \dots & u_{mn} \end{vmatrix}$$

$$u_{ij} = \begin{cases} 0 & , \text{if } u_i \text{ is not in } PA_j. \\ 1 & , \text{if } u_i \text{ is in } PA_j. \end{cases}$$

Where  $u_i$  is  $i$ -th UAV node, for  $i=(1, 2, 3...n)$  and  $PA_j$  is  $j$ -th path, for  $j=(1, 2, 3...m)$ .

**Calculation of node credibility (NCM)** Once we obtain the path credibility matrix (PCM) and the node presence matrix (NPM), we solve the calculation of the node credibility matrix (NCM) by transforming the NCM problem into a multiple linear regression problem.

$$y = bx + a$$

where  $b$  is the slope of the line and  $a$  is the intercept. To train the algorithm, the

variables  $y$  and  $x$  are substituted by PCM and NPM, respectively, to determine the regression line that aids in calculating the NCM value.

**Classification of UAVs Nodes into Normal or Malicious** A node's normal or Malicious nature can be determined by looking at its NCM values. To categorize the NCM data into two labels "Normal" and "Malicious" we employ LR, DT, and KNN classification algorithms.

---

**Algorithm 1:** Drop Attack Detection Algorithm in UAV Ad-hoc Network (DADA-UNET)

---

```

1 Input: SentPackets, ReceivedPackets, NodeSet, PathSet
2 Output: Normal Node, Malicious Node.
3 START
4  $PCM = [];$ 
5  $i = 0;$ 
6 for Any Path in PathSet do
7    $PC = (len[SentPacket] - len[ReceivedPacket])/len[SentPacket];$ 
8    $PCM.append(PC);$ 
9 end
10 while  $i \leq (len(PathSet))$  do
11    $j = 0;$ 
12    $NPMi = [];$ 
13   while  $j \leq (len(NodeSet))$  do
14     if node[j] exists in PathSet[i] then
15        $NPMi.append(1);$ 
16     else
17        $NPMi.append(0);$ 
18     end
19      $j+ = 1;$ 
20   end
21    $NPM.append(NPMi);$ 
22    $i+ = 1;$ 
23 end
24  $NCM = LinearRegression(NPM, PCM);$ 
25    $label = SML(LabeledDataset);$ 
26 Return Label;
```

---

## 5 Result And Analysis

In this study, we use Accuracy, Precision, Recall, and F1-score metrics computed according to the following equations:

$$Accuracy = (tp + tn)/(tp + fp + fn + tn)$$

$$Precision = tp/((tp + fp))$$

$$Recall = tp / (tp + fn)$$

$$F1score = 2((PrecisionRecall) / (Precision + Recall))$$

Where  $tp$ ,  $fp$ ,  $fn$ , and  $tn$  are, respectively, the number of instances correctly classified as positive, the number of instances incorrectly classified as positive, the number of instances incorrectly classified as negative, and the number of instances correctly classified as negative. Experiments are performed on Jupyter notebook, and Python 3.11.5 is used along with the Matplotlib 3.5.2, NumPy 1.20.0, and pandas 1.4.4 libraries. DADA-UNET is implemented using Python libraries like scikit-learn, Numpy, and pandas. In the subsequent section, we will exhibit and discuss the results of evaluating the overall performance of the LR, KNN and, DT classifiers.

### 5.1 Training and Testing Score

Figure-4 displays the performance of the classifiers DT, KNN, and LR. The training scores for DT and KNN are above 94%, while LR has a perfect score of 100%. A high training score indicates that the model has been able to fit the training data well. However, the ultimate goal is to have a model that performs well on new, unseen data, as indicated by the testing score. In this case, all classifiers - LR, DT, and KNN - achieved a testing score of 92%. It's worth noting that while a high training score is desirable, the model's true performance is determined by the testing score on unseen data.

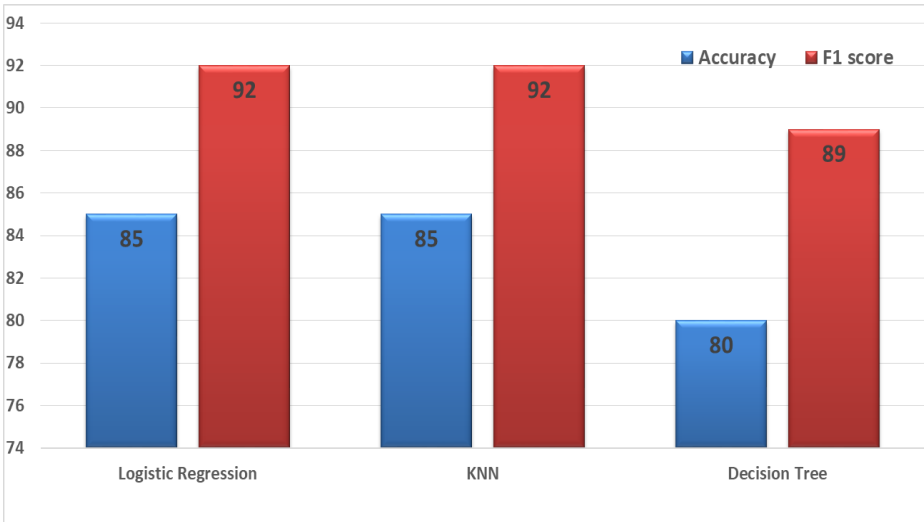
Model	Train Score	Test Score
KNN	0.925	0.85
Logistic Regression	1	1
Decision Tree	1	0.9

Fig. 4. Training and Testing score.

### 5.2 Performance Evaluation of Classifiers

This section evaluates the machine learning models of the Drop Attack Detection Algorithm through the utilization of F1 scores and accuracy metrics. In contrast to Logistic Regression, which attains an impeccable training accuracy of 100%,

Decision Tree and K-Nearest Neighbours both surpass 94%. The evaluation accuracy of 92% for each model indicates strong performance when applied to new data. The graphs emphasize F1 scores, which serve as indicators of both precision and recall, in cases where LR and KNN outperform DT, effectively managing false positives while optimizing recall. By graphically representing the strengths and weaknesses of each model, graphical analyses shed light on their operational effectiveness in the detection of malicious nodes within UAV networks. as shown in Figures 5



**Fig. 5.** Accuracy and F1 score of KNN, LR, and DT

Graphical analysis of precision and recall metrics for the Logistic Regression (LR), Decision Tree (DT), and K-Nearest Neighbours (KNN) models was also incorporated into the DADA-UNET performance evaluation. The graphs depicted in Figure 6 demonstrate that LR and KNN demonstrate significantly greater precision in predicting malevolent nodes than DT. This suggests that these models have a greater likelihood of accurately classifying a node as malicious. With fewer false negatives, the recall graph demonstrates that LR and KNN also outperform DT in identifying the actual malicious nodes present. In security applications where failure to detect a malicious entity can result in severe repercussions, this high recall is crucial. The graphical depiction of these metrics offers an instantaneous comprehension of the efficacy with which each model differentiates between benign and malicious nodes. LR and KNN demonstrate an exceptional equilibrium between precision and recall, thereby bolstering the dependability of network security protocols for unmanned aerial vehicles.

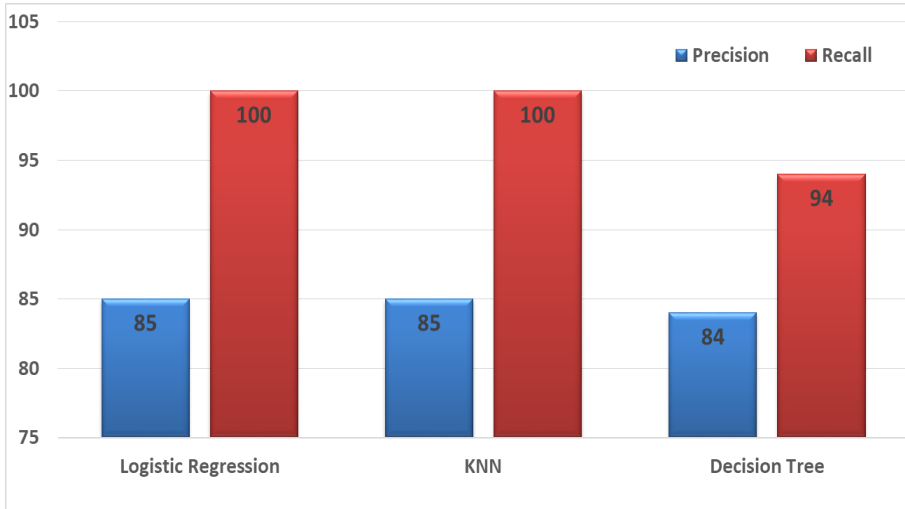


Fig. 6. Precision and Recall of KNN, LR, and DT

## 6 Conclusion

The paper presents the DADA-UANET, a novel supervised machine learning technique that combines logistic regression, decision trees, and K-nearest neighbours to identify malicious nodes in UAV ad-hoc networks accurately. The results of our study show that this approach not only improves the accuracy of classification by up to 92% compared to current methods [13][15] but also demonstrates a high level of adaptability when applied to various testing situations. The DADA-UANET improves the security and reliability of UAV communications by accurately identifying legitimate and malicious nodes. This is crucial for the effectiveness of key applications like military operations and disaster response. Implementing this strategy could greatly enhance the ability of UAV networks to withstand complex cyber assaults, guaranteeing strong and dependable communication in crucial deployment situations. Future improvements will prioritise the fine-tuning of these algorithms by conducting thorough real-world testing and investigating sophisticated machine learning frameworks to address upcoming security concerns in UAV networks.

## References

1. Souad Ajjaj, Souad El Houssaini, Mustapha Hain, and Mohammed-Alamine El Houssaini. Incremental online machine learning for detecting malicious nodes in vehicular communications using real-time monitoring. In *Telecom*, volume 4, pages 629–648. MDPI, 2023.

2. M Arul Selvan and S Selvakumar. Malicious node identification using quantitative intrusion detection techniques in manet. *Cluster computing*, 22(Suppl 3):7069–7077, 2019.
3. Gautam M Borkar, Leena H Patil, Dilip Dalgade, and Ankush Hutke. A novel clustering approach and adaptive svm classifier for intrusion detection in wsn: A data mining concept. *Sustainable Computing: Informatics and Systems*, 23:120–135, 2019.
4. Donpiti Chulerttiyawong and Abbas Jamalipour. Sybil attack detection in internet of flying things-ioft: A machine learning approach. *IEEE Internet of Things Journal*, 2023.
5. Anurag Das, Samuel A Ajila, and Chung-Horng Lung. A comprehensive analysis of accuracies of machine learning algorithms for network intrusion detection. In *Machine Learning for Networking: Second IFIP TC 6 International Conference, MLN 2019, Paris, France, December 3–5, 2019, Revised Selected Papers 2*, pages 40–57. Springer, 2020.
6. Abdelouahid Derhab, Omar Cheikhrouhou, Azza Allouch, Anis Koubaa, Basit Qureshi, Mohamed Amine Ferrag, Leandros Maglaras, and Farrukh Aslam Khan. Internet of drones security: Taxonomies, open issues, and future directions.  *Vehicular Communications*, 39:100552, 2023.
7. S Gopalakrishnan et al. Performance analysis of malicious node detection and elimination using clustering approach on manet. *Circuits and Systems*, 7(06):748, 2016.
8. Christophe Guerber, Mickaël Royer, and Nicolas Larrieu. Machine learning and software defined network to secure communications in a swarm of drones. *Journal of information security and applications*, 61:102940, 2021.
9. Samir Khan, Chun Fui Liew, Takehisa Yairi, and Richard McWilliam. Unsupervised anomaly detection in unmanned aerial vehicles. *Applied Soft Computing*, 83:105650, 2019.
10. Duc C Le and Nur Zincir-Heywood. Exploring anomalous behaviour detection and classification for insider threat identification. *International Journal of Network Management*, 31(4):e2109, 2021.
11. Xin Liu, Mai Abdelhakim, Prashant Krishnamurthy, and David Tipper. Identifying malicious nodes in multihop iot networks using diversity and unsupervised learning. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2018.
12. Thi Ngoc Diep Pham and Chai Kiat Yeo. Detecting colluding blackhole and grey-hole attacks in delay tolerant networks. *IEEE Transactions on Mobile Computing*, 15(5):1116–1129, 2015.
13. Shanshan Sun, Zuchao Ma, Liang Liu, Hang Gao, and Jianfei Peng. Detection of malicious nodes in drone ad-hoc network based on supervised learning and clustering algorithms. In *2020 16th International Conference on Mobility, Sensing and Networking (MSN)*, pages 145–152. IEEE, 2020.
14. Sebastin Suresh, V Prabhu, V Parthasarathy, Rajasekhar Boddu, Yadala Sucharitha, and Gemmachis Teshite. A novel routing protocol for low-energy wireless sensor networks. *Journal of Sensors*, 2022:1–8, 2022.
15. Shrikant Tangade, R Arun Kumaar, S Malavika, S Monisha, and Farooque Azam. Detection of malicious nodes in flying ad-hoc network with supervised machine learning. In *2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*, pages 1–5. IEEE, 2022.

16. Jason Whelan, Thanigajan Sangarapillai, Omar Minawi, Abdulaziz Almeahmadi, and Khalil El-Khatib. Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles. In *Proceedings of the 16th ACM symposium on QoS and security for wireless and mobile networks*, pages 23–28, 2020.
17. Jean-Paul Yaacoub, Hassan Noura, Ola Salman, and Ali Chehab. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, 11:100218, 2020.

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

