Baghdad Science Journal

Volume 22 | Issue 8 Article 28

8-27-2025

A Comparative of Detecting Physical and Cyber Attacks on Drones Using Machine Learning and Deep Learning Techniques

Khattab M Ali Alheeti
Department of Computer Networking Systems, College of Computer and Information Technology, University of Anbar, Anbar, Iraq, co.khattab.alheeti@uoanbar.edu.iq

Sara Abbas Rafa
Department of Law, College of law and political science, University of Anbar, Ramadi, Iraq, Sara.abbas@uoanbar.edu.iq

Maha Mahmood
Department of Artificial Intelligence, College of Computer Science and IT, University of Anbar, Ramadi, Iraq, maha-mahmood@uoanbar.edu.iq

Aythem Khairi Kareem
Department of Heet Education, General Directorate of Education in Anbar, Ministry of Education, Anbar, Iraq, ayt19c1004@uoanbar.edu.iq

Mohammad Aljanabi
Imam Ja'afar Al-Sadiq University, Baghdad, Iraq, mohammad.cs88@gmail.com

See next page for additional authors

How to Cite this Article

Alheeti, Khattab M Ali; Rafa, Sara Abbas; Mahmood, Maha; Kareem, Aythem Khairi; Aljanabi, Mohammad; and Nafea, Ahmed Adil (2025) "A Comparative of Detecting Physical and Cyber Attacks on Drones Using Machine Learning and Deep Learning Techniques," *Baghdad Science Journal*: Vol. 22: Iss. 8, Article 28.
DOI: https://doi.org/10.21123/2411-7986.5039

A Comparative of Detecting Physical and Cyber Attacks on Drones Using Machine Learning and Deep Learning Techniques

Authors

Khattab M Ali Alheeti, Sara Abbas Rafa, Maha Mahmood, Aythem Khairi Kareem, Mohammad Aljanabi, and Ahmed Adil Nafea

BAGHDAD SCIENCE JOURNAL 2025;22(8):2800–2812

RESEARCH ARTICLE

A Comparative of Detecting Physical and Cyber Attacks on Drones Using Machine Learning and Deep Learning Techniques

Khattab M Ali Alheeti [1], Sara Abbas Rafa [2], Maha Mahmood [3], Aythem Khairi Kareem [4], Mohammad Aljanabi [5], Ahmed Adil Nafea [3,*]

[1] Department of Computer Networking Systems, College of Computer and Information Technology, University of Anbar, Anbar, Iraq
[2] Department of Law, College of Law and Political Science, University of Anbar, Ramadi, Iraq
[3] Department of Artificial Intelligence, College of Computer Science and IT, University of Anbar, Ramadi, Iraq
[4] Department of Heet Education, General Directorate of Education in Anbar, Ministry of Education, Anbar, Iraq
[5] Imam Ja'afar Al-Sadiq University, Baghdad, Iraq

ABSTRACT

Multitudes of Unmanned Aerial Vehicles (UAVs) are generally embraced in military and civilian applications. Yet, this physical-cyber method is intimidated by cyber-attacks. Recently, Machine Learning (ML) based attacks detection approaches have been effectively embraced to detect cyber-attacks. This paper presented the Intrusion Detection Security (IDS) approach. The proposed approach investigates UAVs' cyber and physical attributes under normal process and attack circumstances. Two types of cyber-attacks have been classified: Denial-of-service (DoS) and replay. This study developed IDS approaches established on ML and Deep Learning (DL) prototypes, including Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Naive Bayes (NB), and One Dimensional Convolutional Neural Networks (1DCNN). The produced approach is trained using physical and cyber attributes individually. The finding results indicate that the 1D-CNN model achieved higher accuracy (99.79%) compared to the machine learning algorithms. The experimental results show the efficiency of the proposed method's performance.

Keywords: Cyber attacks, Deep learning, Internet of Things, Intrusion Detection Security, Machine learning, Physical attacks, Unmanned aerial vehicles

Introduction

The appearance of Internet of Things (IoT) technology with intelligent Intrusion Detection Security (IDS) approach has strengthened the Vehicular Ad-hoc Networks (VANETs) for present an additional delightful and more effective driving knowledge. [1–3] But, because of the extraordinarily dynamical environment of community topologies, VANETs regularly recognize the task of alternating link interruption. To come upon this challenge, UAVs may be applied as the maximum recommended contender to decorate the connectedness of VANETs. For instance, UAV can offer help to the floor car at some stage in the facts transmission thru Storage Carry Forward (SCF) approach that can safely decrease the end-to-end put off as well as decorate the letter delivery rate. [4]

UAVs also are named drones which have declared their hopeful skills in numerous real-time programs such observation system, health-care system, disaster management, data collection, rescue system, localization, traffic surveillance systems in the smart city, environmental monitoring. Drones are the current development because the flying IoT things that faux

Received 12 February 2024; revised 31 May 2024; accepted 2 June 2024.
Available online 27 August 2025

* Corresponding author.
E-mail addresses: co.khattab.alheeti@uoanbar.edu.iq (K. M. A. Alheeti), Sara.abbas@uoanbar.edu.iq (S. A. Rafa), maha-mahmood@uoanbar.edu.iq (M. Mahmood), ayt19c1004@uoanbar.edu.iq (A. K. Kareem), mohammad.cs88@gmail.com (M. Aljanabi), ahmed.a.n@uoanbar.edu.iq (A. A. Nafea).

https://doi.org/10.21123/2411-7986.5039

to be detecting devices.[5] The remote-control center manages the drone's communication with the user.[6] The built-in sensors in every drone transmit the collected data from its surrounding environment to the remote-control server through some form of wireless communication. The drones are being supported all over the world, and it's largely because they've learned how to reach remote locations with minimal effort, time, resources, and manpower. Of course, these features allow the end user, but it's also expected to be essential because directly access benefits can lead to other serious security risks.[7]

Internet of Drones (IoD) leverages Internet of Things (IoT) technologies to achieve its acute operational needs.[8] The main requirements of the IoD network associated with cost-effective operations include localization, authorization, trajectory planning, unmanned aerial vehicle (UAV) monitoring, and security. Even though technology has come a long way and there are lots of solutions out there, privacy and security are still a major concern in the open-source world. IoD designs are resource limited since a drone has controlled computation, storage sources, and power.[9]

Unmanned Aerial Vehicles (UAVs) have gained significant popularity and widespread adoption in both military and civilian applications. The increasing need for UAVs also gives about troubles about their weakness to cyber-attacks. In recent year researchers have focused on ML based intrusion detection methods as a means to detect and mitigate these cyber-attacks. This paper proposed an Intrusion Detection Security (IDS) approach specifically designed for UAVs.[10,11] The IDS method studies the cyber and physical attributes of UAVs under normal operational conditions and through attack states. There are two types of cyber-attacks as a Denial-of-Service (DoS) and replay attacks with examining these attack types, the IDS approach aims to develop effective methods for detecting threats.[12,13]

This study utilized several ML and Deep Learning (DL) techniques as the organization for the IDS methods. The algorithms are SVM, KNN, NB, and 1D-CNN. The IDS methods are trained utilizing both physical and cyber attributes independently, allowing the models to learn and identify differences in UAV behavior. This highlights the higher performance of the 1D-CNN model in detecting and classifying cyber and physical attacks on UAVs. The contribution of this work to the field of UAV security via proposed an IDS method utilized ML and DL techniques by focusing on both the physical and cyber attributes of UAVs, the proposed method shown a comprehensive solution to detect cyber-attacks. The experimental results support the efficiency of the approach, paving the way for further advancements in securing UAVs beside evolving cyber threats.

Related works

RFID-based authentication methods are easy to use, however securing RFID-based techniques is a difficult project because to the very limited computational capabilities of RFID identifies.[14,15] To solve this problem of RFID established verification systems, the theory of physical unclonable function (PUF) tools was introduced.[16] PUF is a purpose obtained as of a physical property and utilized to generate a device specific production for several input, such as an identification. Including PUF and RFID could ensure hardware security. These approaches can solve challenges linked to one-to-one verification but cannot keep answers for large-scale and dynamic networks.[17]

Drone safety includes various modes and levels depending on their utilized, control and size methods. In highest issues, drones use the Wi-Fi (IEEE 802.11) protocol communication.[18] The drone chassis contains a Wi-Fi network and linking field stations, which are exposed to cybersecurity dangers. The lack of encoding technique on their chip could advance to drones of hijacking.[19]

Thomas Hickling et al.[20] proposed an innovative approach that utilizes the interpretability of DL models to create an effective detector capable of protecting DL models and the UAVs that utilize them from attacks. The approach employs a Deep Reinforcement Learning (DRL) strategy for planning and is trained using a Deep Deterministic Policy Gradient (DDPG) with Prioritized Experience Replay (PER) DRL method. To enhance training duration and obstacle performance, an Artificial Potential Field (APF) is incorporated. A simulated environment is established to facilitate UAV planning using explainable DRL, which includes adversarial and obstacle attacks. Adversarial attacks, generated using the Basic Iterative Method (BIM), reduce obstacle detection rates from 97% to 35%. To counteract this reduction, two malicious attack detectors are proposed. The first is a Convolutional Neural Network Adversarial Detector (CNN-AD) that achieves an 80% accuracy in detection. The second detector utilizes a Long Short-Term Memory (LSTM) network and achieves 91% accuracy, with faster computation times compared to the CNN-AD, making it suitable for real-time malicious detection.

Jiaping Xiao et al.[21] presented an altered sliding invention series approach established on the comprehensive Kalman filter optimal condition estimate for an involved quadrotor method to predict real-time

cyber-attacks imposed on its sensors and actuators. These cyber-attacks contain random attacks, denial-of-service (DoS) attacks, and false data injection (FDI) attacks. This approach predicts and calculates the operative mean of the standardized invention series inside a sliding period window and initiates the alarm if the value exceeds the preset edge. The detector surveys a decreased false alarm rate corresponding to more condition estimation-based detectors. To manage the initial estimate error issue, this approach implements an iteration strategy to create and calibrate the detector. The proposed approach can isolate cyber-attacks by estimating the model covariance of the normalized creation series. Finally, results of a quadrotor in an occasional, complicated trajectory flying are supplied to confirm the efficacy of the proposed method.

Another attacks, such as man-in-the central attack, often span up to 2 km and are also responsible for robberies.[22] IoD is developing actual common in the military industry.[23] Small drones have gained public attention in the past decades due to their small size, light weight and wingspan. Small drones also pose a threat to the security of public and government data.[24] By using a probabilistic approach, authors in[25] presented a method for detection and controlling an actuation attack in a constrained cyber-physical. In,[26] Blockchain is being used to make sure data is safe when being sent over 5G and using drones that are connected to the internet of things. This system relies on people being able to identify potential threats. Before, people had to use keys to authenticate their devices, but that wasn't good enough for an IoT-connected drone network.

According to the literature review, many researchers have used machine learning models to address cyberattacks in cellular networks[27] and sensor-driven wireless networks. The authors in[28] exploited a supervised learning method with a self-learning model through LSTM (autoencoder) and RF for detection DDoS attacks utilizing two features. An intelligent intrusion detection system is necessary for drone identification and defense due to the rise in drone threats. A unique one-class classifier-based approach for drone intrusion detection was presented in.[29] The model performed well on a variety of UAV platforms, achieving platform-specific F1 scores for malicious and benign sensor readings of 99.56% and 99.73%. A methodology for recognizing malevolent assaults on the sensors of tiny unmanned aerial vehicles was introduced in.[30] By identifying a spoofing attack on the global positioning system (GPS), they demonstrate the suggested paradigm. Using a simulated dataset and this model, many results were reached. In order to safeguard the environment of medical delivery drones with active capability, delivery dependability, and other medical applications,[31] proposed a framework for attack detection.

Research methodology

In this section, the design an Intrusion Detection Security (IDS) approach for a swarm of UAVs First, and after that discuss the UAV dataset description. Then, discuss PCA feature selection and data preprocessing and review Ml and DL techniques applied in the proposed approach. As shown in Fig. 1, the general structure of the proposed ML techniques are SVM, NB, and KNN, while Fig. 2 shows the DL model is 1DCNN.

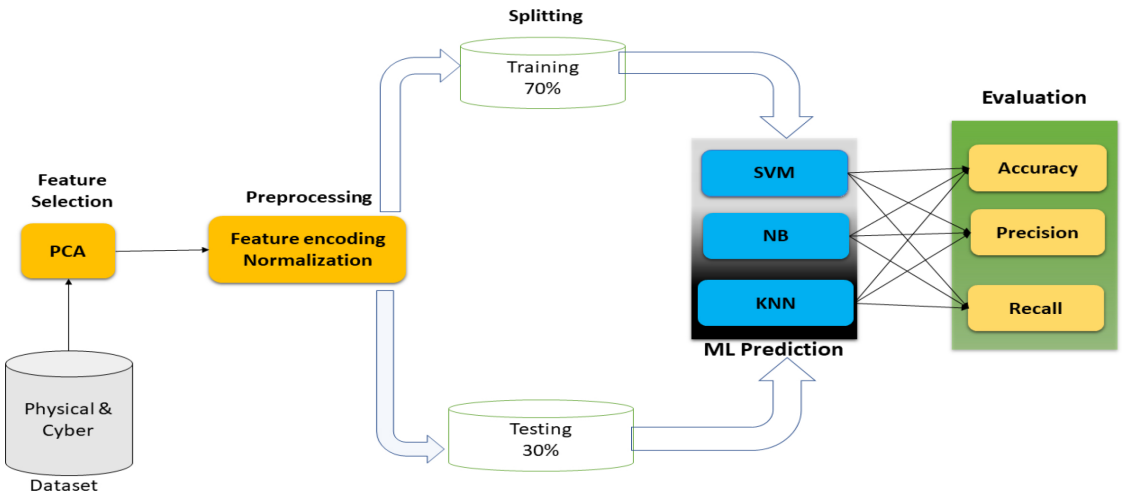

Fig. 1. Proposed ML detection security approach.

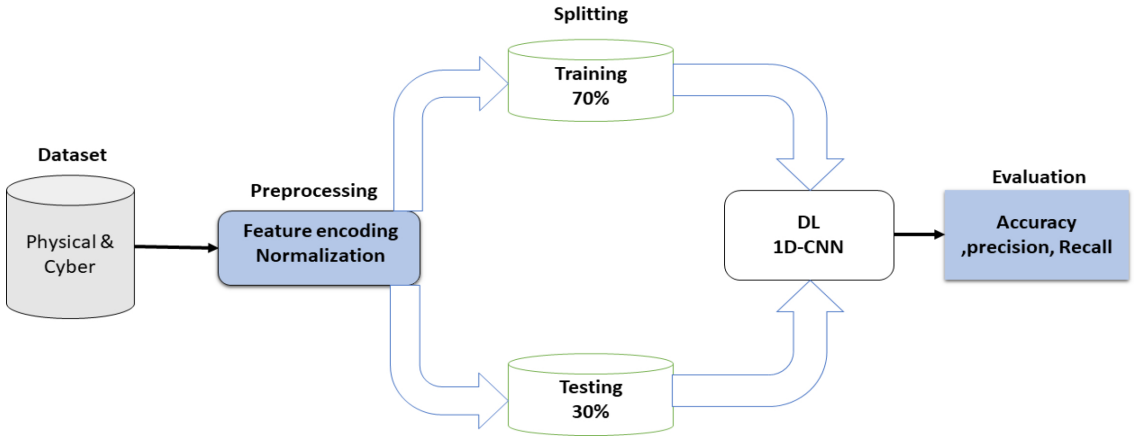

Fig. 2. Proposed 1D-CNN detection security approach.

Dataset description

The proposed approach utilized the IEEEData-Port 'CYBER-PHYSICAL DATASET FOR UAVS UNDER NORMAL OPERATIONS AND CYBER-ATTACKS' it is a new dataset collected on 2023 by.[32] This dataset is generated by using the following equipment: Two DJI Tello EDU drones, ALFA AWUS036ACH network adapter, Sagemcom SAC2V2s WiFi access point, and two computers. Several flight missions of inconsistent sophistication were instructed to accumulate the physical and cyber datasets. The data involved 20 attacked flights and 20 where UAV1 was benign, totaling 40 flights. The dataset contained physical and cyber attributes for different missions under cyberattacks and normal activities. The total attributes are 40 cyber and 20 physicals.

These flights include square missions, back-and-forth missions, search missions, rectangle missions, and spiral missions.

Feature selection

The goal of Feature Selection (FS) procedures in ML is to discover the most useful subset of features that permits one to produce optimized models. The goal of FS procedures in ML is to discover the most useful subset of features that permits one to produce optimized models. This proposed employed Principal Component Analysis (PCA) as FS. PCA is a dimensionality reduction that determines meaningful associations in our data, changes the existent data according to these associations, and then quantifies the significance of these associations to maintain the considerable necessary associations and drop the others. Thus, the performance of the proposed approach increases. The PCA feature selection is employed in ML techniques only.

Splitting dataset

After the feature selection process, the dataset is divided into two parts, the first for training and the second for testing. The split ratio is 70% for training and 30% for testing.

Preprocessing

Data preprocessing converts the data into a more efficient format in ML tasks. The methods are typically utilized at the before phases of the ML product channel to confirm accurate developments. This research employed two preprocessing operations: Normalization and Feature encoding. Normalization is an essential operation due high variant in the utilized UAV dataset. This operation allows a change of the data in a pattern, making it more manageable for algorithms to tease a meaningful association between variables. It can calculate by using the following formula in Eq. (1)[33]

$$X_{\text{Normalization}} = \frac{x - \text{mean}(x)}{\text{Standard deviation}} \quad (1)$$

Feature encoding is the other operation that is employed in the UAV dataset. This operation is essential because ML techniques can only function with numerical values. For this cause, it is required to change the appropriate features' categorical features into numerical ones. This proposed employed "LabelEncoder" Python instruction to classes (DoS, Replay, and benign) to (0, 1, and 2) respectively.

Investigated models for IDSs

This study applied several ML and DL models for each cyber and physical attribute individually to

produce an efficacious IDS. The ML techniques are SVM, NB, and KNN, where the DL is the CNN model. These techniques are summarized next.

Support vector machine

Support vector machine (SVM) is a supervised classifier. It is widely employed in the classification area, and its mathematical reason is severe and has a stable theoretical basis.[34] It cannot exclusively deal with linear classification issues but even deals with nonlinear classification issues. The SVM can bypass the drawbacks of under-learning, over-learning, and emotional optimization that quickly appear in other intelligent techniques.[35] Since IDS is a nonlinear multi-classification issue, this article assumes SVM based on kernel function to convert the nonlinear issue into a linear classification issue.

Naïve bayes

Naive Bayes (NB) technique is the easy Statistical Bayesian technique. "It is called Naive" as it considers that all variables contribute towards category and are mutually correlated. This deduction is anointed class-dependent independence.[36] It can predict class membership possibilities, such as the likelihood that a provided data item belongs to a unique class label.[37] The NB technique is based on Bayes Theorem, and is utilized when the dimensionality of the data is high.

K-nearest neighbor

The K-Nearest Neighbor (KNN) technique is the easiest of all ML techniques.[38] It is based on the regulation that similar samples typically lie in the nearest environs. KNN is an instance-based learning approach. Instance-based methods are even called lazy learners as they keep all of the training models and only construct a classifier once a unique, unlabeled sampling is required to be classified. KNN technique needs less analysis period during the training step than other ML techniques but more analysis period during the classification operation.[39] The primary motivations to use KNN are comfortable to implement and understand, Training is high-speed, it is robust to clangorous training data, and It serves agreeably on applications in which a representative can have multiple class labels.[40]

One-dimensional convolutional neural network

1D-CNN is a trendy construction of Artificial Neural Networks (ANN). It has been established to conduct distinguished time-domain signal analysis and computer vision. Similarly, to other ANN, 1D-CNN has input, hidden, and output layers.[41,42] The individual layer consists of neurons linked from one layer to the other with biases and weights matrices. However, the distinction is that 1D-CNN neurons are organized convolutionally by kernels and filters in their layers. The kernels construct a pile of convolutional layers by transmitting the output of one layer to the subsequent layer.[43]

As shown in Fig. 3 the proposed 1D-CNN for physical and cyber detection.

The proposed 1DCNN model comprises nine convolution layers, seven max-pooling layers, and five

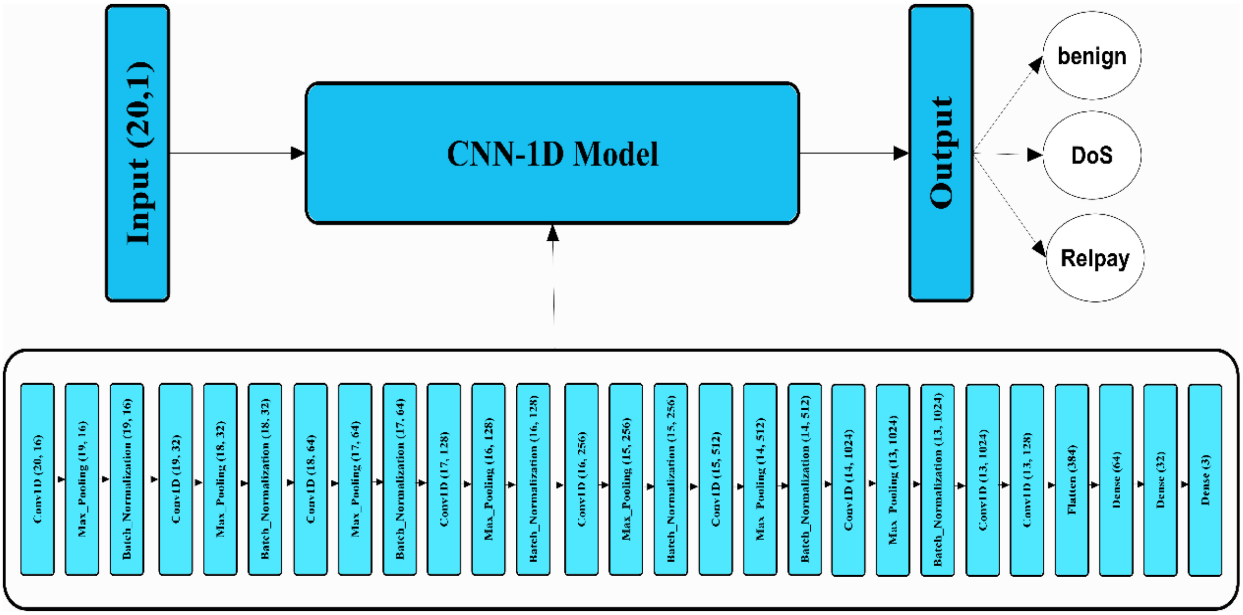

Fig. 3. Proposed 1D-CNN architecture.

batch normalization layers. In addition to dropout, flatten and dense layers. Each layer can summarize follow:

Convolutional layer (CL) is named the feature extraction layer. Representations of features extracted from the earlier layer from regional perspective fields are transmitted to the following CL. Thus, the local perspective fields specify the input data size and the spatial consideration of features extracted in the CL. The proposed approach employed Kernel-size = 2, strides-size = 1, padding = 'Valid', and activation function = 'ReLu'.

Max-Pooling layer is an essential DL concept connecting convolution function. Its primary role is to decrease the dimensionality to progressively decrease the number of parameters. It decreases or downsamples a feature map's vector size without yielding its meaning. In this study used pool_size = 2 and strides = 1.

Batch Normalization During the training phase, the statistical issuance of each layer input modifications as the parameters of the earlier layers differ. It delays the training by instructing lower learning rates, which makes it excessively difficult to train representatives with saturating nonlinearities. Batch normalization (BN) has just been presented to enhance performance, stability, and speed via normalizing the input layer by rescaling.

Full connection layer (FCL) is set up before the hidden features, and the output layer extracted from the actual data via the feature map layer are fully connected as inputs of the classification layer. This layer spatially combines the hidden features to extract practical data from the feature map layers. Multiple FCLs can execute multiple nonlinear transformations theoretically, which contributes to acquiring the tacit expression of input data.

This study investigated four IDS strategies for each cyber and physical dataset individually. Three traditional ML techniques are SVM, NB, and KNN, and 1DCNN as a deep learning model.

Evaluation

The IDS approach working is represented in precision, accuracy, and recall representations. Accuracy represents the percentage of instances that have been organized correctly, which is delivered by Eq. (2)[44]

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{2}$$

where FN is a false negative, FP is false positive, TP is true positive, and TN is true negative.[45,46] In the precision determines the ratio of correctly recognized positive experiments out of the totality of indicated positives, which is presented by Eq. (3)[47]

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{3}$$

Recall displays the ratio of accurately recognized positive instances out of all actual positive instances, which is defined as Eq. (4)[48,49]

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{4}$$

Table 1. The result of Cyber attacks.

Cyber	Model	Accuracy	Precision	Recall
	NB	71.68	71.49	71.68
	SVM	91.66	92.16	91.66
	KNN	97.90	97.90	97.90
	1D-CNN	99.14	99	98.66

Results and discussion

This section displays the results acquired via the ML with classifiers including SVM, NB, and KNN, while 1D-CNN is a deep learning model. The results of classifiers will be shown based on physical and cyber attributes individually.

Table 1 shows the results of the evaluation of cyber results using the proposed ML with classifiers including SVM, NB, and KNN, while 1D-CNN is a deep learning model. The proposed via the 1D-CNN showed superior results of accuracy where it achieved 99.14% compared to the accuracy obtained by the machine learning algorithms where NB, SVM, and KNN achieved 71.68, 91.66 and 97.90 respectively for cyber detection.

Fig. 4 displays a confusion matrix for all cyber results using NB, SVM, KNN and 1D-CNN.

Fig. 5 displays the cyber results curve by the accuracy with validation accuracy and the curve via loss and validation loss for 1D-CNN model.

Table 2 shows the results of the evaluation of physical results using the proposed ML with classifiers including SVM, NB, and KNN, while 1D-CNN is a deep learning model. The proposed via the 1D-CNN showed superior results of accuracy where it achieved 99.79% compared to the accuracy obtained by the machine learning algorithms where NB, SVM, and KNN achieved 83.16%, 93.42%, and 93.16% respectively.

Fig. 6 displays a confusion matrix for all physical results using NB, SVM, KNN, 1D- CNN.

Fig. 7 displays the Physical results curve by the accuracy with validation accuracy and the curve via loss and validation loss.

Testing Set _ NB

TARGET / OUTPUT	Class0	Class1	Class2	SUM
Class0	3033 30.54%	371 3.74%	124 1.25%	3528 85.97% 14.03%
Class1	1420 14.30%	1725 17.37%	424 4.27%	3569 48.33% 51.67%
Class2	1 0.01%	472 4.75%	2361 23.77%	2834 83.31% 16.69%
SUM	4454 68.10% 31.90%	2568 67.17% 32.83%	2909 81.16% 18.84%	7119 / 9931 71.68% 28.32%

Testing Set _ SVM

TARGET / OUTPUT	Class0	Class1	Class2	SUM
Class0	2961 29.82%	547 5.51%	20 0.20%	3528 83.93% 16.07%
Class1	49 0.49%	3320 33.43%	200 2.01%	3569 93.02% 6.98%
Class2	4 0.04%	8 0.08%	2822 28.42%	2834 99.58% 0.42%
SUM	3014 98.24% 1.76%	3875 85.68% 14.32%	3042 92.77% 7.23%	9103 / 9931 91.66% 8.34%

Testing Set _ KNN

TARGET / OUTPUT	Class0	Class1	Class2	SUM
Class0	3464 34.88%	61 0.61%	3 0.03%	3528 98.19% 1.81%
Class1	77 0.78%	3439 34.63%	53 0.53%	3569 96.36% 3.64%
Class2	2 0.02%	13 0.13%	2819 28.39%	2834 99.47% 0.53%
SUM	3543 97.77% 2.23%	3513 97.89% 2.11%	2875 98.05% 1.95%	9722 / 9931 97.90% 2.10%

Testing Set _ 1D-CNN

TARGET / OUTPUT	Class0	Class1	Class2	SUM
Class0	3483 35.07%	45 0.45%	0 0.00%	3528 98.72% 1.28%
Class1	5 0.05%	3538 35.63%	26 0.26%	3569 99.13% 0.87%
Class2	0 0.00%	9 0.09%	2825 28.45%	2834 99.68% 0.32%
SUM	3488 99.86% 0.14%	3592 98.50% 1.50%	2851 99.09% 0.91%	9846 / 9931 99.14% 0.86%

Fig. 4. Confusion matrix of cyber results.

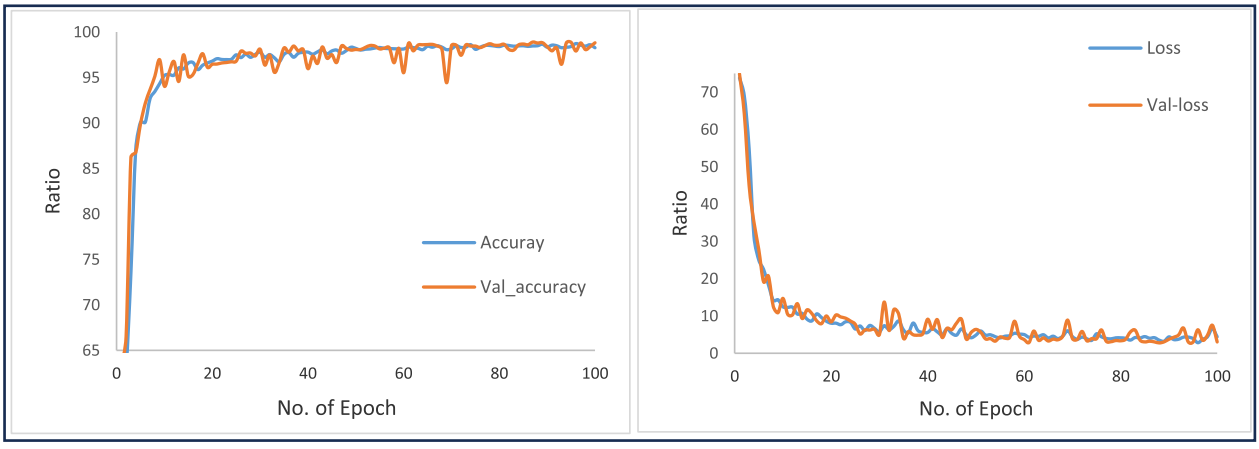

Fig. 5. Curve of accuracy with validation accuracy and loss and validation loss for 1D-CNN cyber results.

Table 2. The result of physical attacks.

Physical	Model	Accuracy	Precision	Recall
	NB	83.16	79.35	83.16
	SVM	93.42	93.65	91.93
	KNN	93.16	93.16	93.16
	1D-CNN	99.79	99.79	99.79

Testing Set _ NB

TARGET / OUTPUT	Class0	Class1	Class2	SUM
Class0	263 14.06%	13 0.69%	7 0.37%	283 92.93% 7.07%
Class1	37 1.98%	51 2.73%	195 10.42%	283 18.02% 81.98%
Class2	5 0.27%	58 3.10%	1242 66.38%	1305 95.17% 4.83%
SUM	305 86.23% 13.77%	122 41.80% 58.20%	1444 86.01% 13.99%	1556 / 1871 83.16% 16.84%

Testing Set _ SVM

TARGET / OUTPUT	Class0	Class1	Class2	SUM
Class0	273 14.61%	3 0.16%	7 0.37%	283 96.47% 3.53%
Class1	25 1.34%	175 9.36%	83 4.44%	283 61.84% 38.16%
Class2	2 0.11%	3 0.16%	1298 69.45%	1303 99.62% 0.38%
SUM	300 91.00% 9.00%	181 96.69% 3.31%	1388 93.52% 6.48%	1746 / 1869 93.42% 6.58%

Testing Set _ KNN

TARGET / OUTPUT	Class0	Class1	Class2	SUM
Class0	253 13.52%	10 0.53%	20 1.07%	283 89.40% 10.60%
Class1	24 1.28%	215 11.49%	44 2.35%	283 75.97% 24.03%
Class2	16 0.86%	14 0.75%	1275 68.15%	1305 97.70% 2.30%
SUM	293 86.35% 13.65%	239 89.96% 10.04%	1339 95.22% 4.78%	1743 / 1871 93.16% 6.84%

Testing Set 1D-CNN

TARGET / OUTPUT	Class0	Class1	Class2	SUM
Class0	281 15.02%	2 0.11%	0 0.00%	283 99.29% 0.71%
Class1	1 0.05%	281 15.02%	1 0.05%	283 99.29% 0.71%
Class2	0 0.00%	0 0.00%	1305 69.75%	1305 100.00% 0.00%
SUM	282 99.65% 0.35%	283 99.29% 0.71%	1306 99.92% 0.08%	1867 / 1871 99.79% 0.21%

Fig. 6. Confusion matrix of physical results.

The exceptional performance of the 1D-CNN model suggests its superiority over traditional machine learning algorithms in this evaluation. Several reasons can explain why 1D-CNN is considered the best choice in this proposed. The deep learning architecture of 1D-CNNs allows for automatic feature extraction. Traditional machine learning algorithms often require manual feature engineering, where domain knowledge and expertise are needed to select and engineer relevant features. In contrast, 1D-CNNs can automatically learn and extract relevant features from the raw input data, alleviating the burden of manual feature engineering and potentially uncovering more intricate patterns that may be difficult for human experts to identify.

The superior accuracy achieved by the 1D-CNN model in this evaluation demonstrates its capability to effectively learn and generalize from the given dataset. The high accuracy indicates that the 1D-CNN model was able to discern and classify patterns within the physical and cyber data with great precision, outperforming the other machine learning algorithms in terms of prediction. Fig. 8 displays a comparison that will take place between cyber and physical results with proposed classifiers. The comparison is based on accuracy. The performance of accuracy using physical with 1D-CNN got (99.79%) The highest value is within physical and cyber results.

It is important to compare the proposed approach with state-of-the-art models as displayed in Table 3.

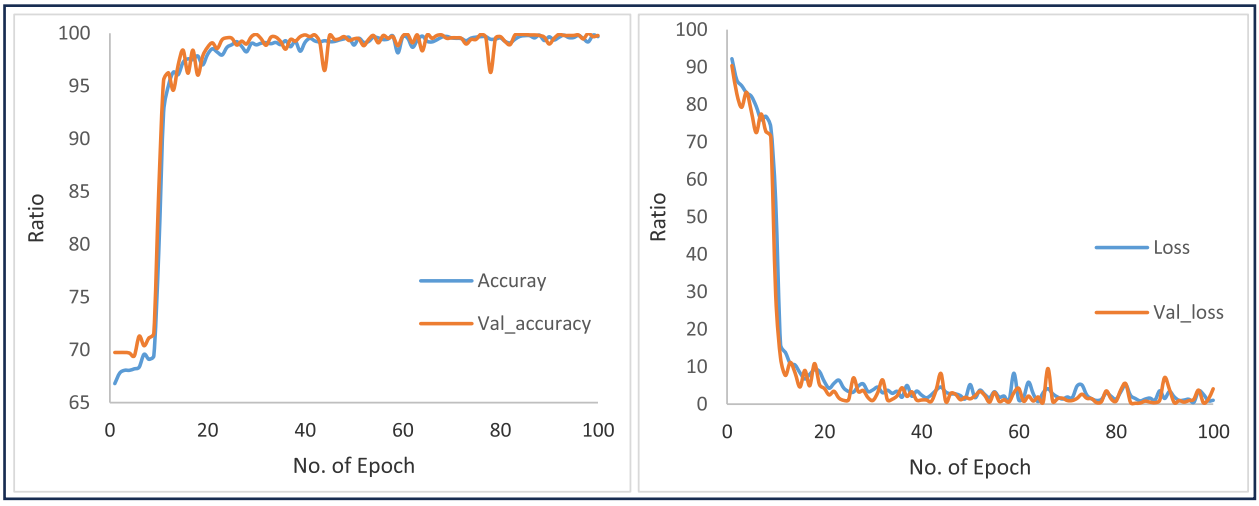

Fig. 7. Curve of accuracy with validation accuracy and loss and validation loss for 1D-CNN physical results.

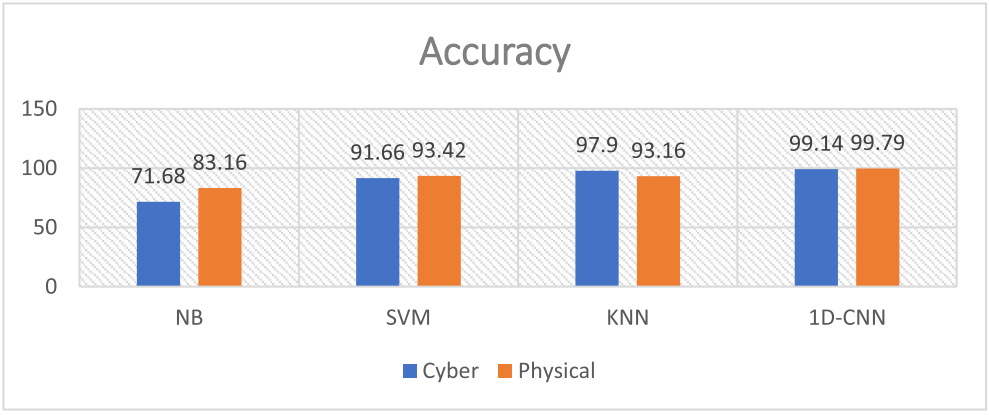

Fig. 8. A comparison between cyber and physical results.

Table 3. A comparison of results with related studies.

Author's	Accuracy
Hassler et al.[12]	94.53
Alsulami et al.[50]	99
Hickling et al.[20]	91
Aldaej et al.[51]	98.58
Shafique et al.[52]	0.99
Proposed model	99.79

Hassler et al.[12] proposed SVM, FNN, LSTM-RNN, and 1D-CNN has obtained a high accuracy of 94.53%. Alsulami et al.[50] proposed artificial immune systems (AIS) and NARX got an accuracy of 99%. Hickling et al.[20] proposed CNN-AD and LSTM with an achieved accuracy of 91%. In their study, Aldaej et al.[51] proposed a hybrid machine learning model utilizing RF with LR with achieved an accuracy of 98.58%. Shafique et al.[52] proposed SVM with different K-fold and achieved an accuracy of 0.99%. This study proposed machine learning algorithms such as SVM, K-NN, and NB with deep learning algorithms (1D-CNN) to detect cyber and physical attacks with a high accuracy of 99.79%. The proposed model utilizing 1D-CNN got good in the domain, dependent on differences in reported precisions between related works.

Conclusion

This study utilized an IDS approach for detecting cyber-attacks on UAVs using ML and DL models. The evaluation results shown the efficiency of the proposed approach, with the 1D-CNN model achieving a higher accuracy of 99.79% compared to other tested ML algorithms. This higher performance of the 1D-CNN model in successfully detection cyber-attacks on UAVs. While the 1D-CNN model shows high accuracy in this work, its scalability to larger datasets or more complex environments is still an issue of

this proposed. Future work needs to address dataset Augmentation and Variety to enhance the robustness and generalizability of the proposed model. Future work should focus on augmenting the dataset with a wider variation of cyber-attacks and physical conditions. This can include generating synthetic data or collecting additional real-world data to ensure a more comprehensive representation of possibility scenarios.

Authors' declaration

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore, any Figures and images, that are not ours, have been included with the necessary permission for republication, which is attached to the manuscript.
- No animal studies are present in the manuscript.
- No human studies are present in the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee at University of Anbar.

Authors' contribution statement

K.M.A advised the writing and investigation of this paper. M.M, M.A assisted in the realization of the ideas and writing of this manuscript. A.K.K, A.A.N, MMA carried out the investigation into techniques and they employed the proposed and achieved the experimentations.

References

1. UL-Hassan M, Al-Awady AA, Ali A, Sifatullah, Akram M, Iqbal MM, *et al.* ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV. Sensors. 2024;24(3):818. https://doi.org/10.3390/s24030818.
2. Wasmi MH, Aliesawi SA, Jasim WM. Distributed semi-clustering protocol for large-scale wireless sensor networks. Int J Eng Technol. 2018;7(4):3119–25. https://doi.org/10.14419/ijet.v7i4.21550.
3. Samriya JK, Kumar S, Kumar M, Xu M, Wu H, Gill SS. Blockchain and Reinforcement Neural Network for Trusted Cloud-Enabled IoT Network. IEEE Trans Consum Electron. 2023;70(1):2311–2322. https://doi.org/10.1109/TCE.2023.3347690.
4. Gupta BB, Quamara M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurr Comput Pract Exp. 2020;32(21):e4946. https://doi.org/10.1002/cpe.4946.
5. Mohsan SAH, Khan MA, Noor F, Ullah I, Alsharif MH. Towards the unmanned aerial vehicles (UAVs): A comprehensive review. Drones. 2022;6(6):147. https://doi.org/10.3390/drones6060147.
6. Yadav AS, Kumar S, Karetla GR, Cotrina-Aliaga JC, Arias-Gonzáles JL, Kumar V. A Feature Extraction Using Probabilistic Neural Network and BTFSC-Net Model with Deep Learning for Brain Tumor Classification. J Imaging. 2022;9(1):10. https://doi.org/10.3390/jimaging9010010.
7. Qureshi NMF, Siddiqui IF, Unar MA, Uqaili MA, Nam CS, Shin DR, *et al.* An aggregate mapreduce data block placement strategy for wireless IoT edge nodes in smart grid. Wirel Pers Commun. 2019;106:2225–36. https://doi.org/10.1007/s11277-018-5936-6.
8. Arul R, Raja G, Bashir AK, Chaudry J, Ali A. A console GRID leveraged authentication and key agreement mechanism for LTE/SAE. IEEE Trans Ind Informatics. 2018;14(6):2677–89. https://doi.org/10.1109/TII.2018.2817028.
9. Ahuja SP, Wheeler N. Architecture of fog-enabled and cloud-enhanced internet of things applications. Int J Cloud Appl Comput. 2020;10(1):1–10. https://doi.org/10.4018/IJCAC.2020010101.
10. Mohsan SAH, Othman NQH, Li Y, Alsharif MH, Khan MA. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. Intell Serv Robot. 2023;16(1):109–37. https://doi.org/10.1007/s11370-022-00452-4.
11. Alfahad NM, Aliesawi SA, Mubarek FS. Enhancing AODV routing protocol based on direction and velocity for real-time urban scenario. J Theor Appl Inf Technol. 2018;96(18):6220–6231.
12. Hassler SC, Mughal UA, Ismail M. Cyber-Physical Intrusion Detection System for Unmanned Aerial Vehicles. IEEE Trans Intell Transp Syst. 2023;1–12. https://doi.org/10.1109/TITS.2023.3339728.
13. Kumar S, Kumar S, Ranjan N, Tiwari S, Kumar TR, Goyal D, *et al.* Digital watermarking-based cryptosystem for cloud resource provisioning. Int J Cloud Appl Comput. 2022;12(1):1–20. https://doi.org/10.4018/IJCAC.311033.
14. Gope P, Sikdar B. An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. IEEE Trans Veh Technol. 2020;69(11):13621–30. https://doi.org/10.1109/TVT.2020.3018778.
15. Gope P, Millwood O, Saxena N. A provably secure authentication scheme for RFID-enabled UAV applications. Comput Commun. 2021;166:19–25. https://doi.org/10.1016/j.comcom.2020.11.009.
16. Khattab A, Jeddi Z, Amini E, Bayoumi M, Khattab A, Jeddi Z, *et al.* RFID security threats and basic solutions. RFID Security. 2017;27–41. https://doi.org/10.1007/978-3-319-47545-5_2.
17. Bansal G, Chamola V, Sikdar B. SHOTS: Scalable secure authentication-attestation protocol using optimal trajectory in UAV swarms. IEEE Trans Veh Technol. 2022;71(6):5827–36. https://doi.org/10.1109/TVT.2022.3162226.
18. Nayyar A, Nguyen BL, Nguyen NG. The internet of drone things (IoDT): Future envision of smart drones. First International Conference on Sustainable Technologies for Computational Intelligence: Proceedings of ICTSCI 2019. Springer;2020:563–80. https://doi.org/10.1007/978-981-15-0029-9_45.
19. Yin Z, Song Q, Han G, Zhu M. Unmanned optical warning system for drones. Global Intelligence Industry Conference (GIIC 2018). SPIE;2018:154–60. https://doi.org/10.1117/12.2503828.
20. Hickling T, Aouf N, Spencer P. Robust adversarial attacks detection based on explainable deep reinforcement learning for uav guidance and planning. IEEE Trans Intell Veh. 2023;8(10):4381–4394. https://doi.org/10.1109/TIV.2023.3296227.

21. Xiao J, Feroskhan M. Cyber attack detection and isolation for a quadrotor uav with modified sliding innovation sequences. IEEE Trans Veh Technol. 2022;71(7):7202–14. https://doi.org/10.1109/TVT.2022.3170725.
22. Koslowski R, Schulzke M. Drones along borders: Border security UAVs in the United States and the European Union. Int Stud Perspect. 2018;19(4):305–24. https://doi.org/10.1093/isp/eky002.
23. Ozmen MO, Yavuz AA. Dronecrypt-an efficient cryptographic framework for small aerial drones. MILCOM 2018–2018 IEEE Mil. Commun Conf. 2018. p. 1–6. https://doi.org/10.1109/MILCOM.2018.8599784.
24. Lv Z. The security of Internet of drones. Comput Commun. 2019;148:208–14. https://doi.org/10.1016/j.comcom.2019.09.018.
25. Hosseinzadeh M, Sinopoli B. Active attack detection and control in constrained cyber-physical systems under prevented actuation attack. 2021 American Control Conference (ACC). IEEE;2021:3242–7. https://doi.org/10.23919/ACC50511.2021.9483322.
26. Bera B, Saha S, Das AK, Kumar N, Lorenz P, Alazab M. Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment. IEEE Trans Veh Technol. 2020;69(8):9097–111. https://doi.org/10.1109/TVT.2020.3000576.
27. Xiao L, Xie C, Chen T, Dai H, Poor HV. A mobile offloading game against smart attacks. IEEE Access. 2016;4:2281–91. https://doi.org/10.1109/ACCESS.2016.2565198.
28. Vedula V, Lama P, Boppana RV, Trejo LA. On the detection of low-rate denial of service attacks at transport and application layers. Electronics. 2021;10(17):2105. https://doi.org/10.3390/electronics10172105.
29. Whelan J, Sangarapillai T, Minawi O, Almehmadi A, El-Khatib K. Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles. Proceedings of the 16th ACM symposium on QoS and security for wireless and mobile networks. 2020:23–8. https://doi.org/10.1145/3416013.3426446.
30. Muniraj D, Farhood M. A framework for detection of sensor attacks on small unmanned aircraft systems. International Conference on Unmanned Aircraft Systems (ICUAS). IEEE;2017:1189–98. https://doi.org/10.1109/ICUAS.2017.7991465.
31. Kulp P, Mei N. A Framework for Sensing Radio Frequency Spectrum Attacks on Medical Delivery Drones. IEEE Int Conf Syst Man Cybern. 2020;408–413. https://doi.org/10.1109/ICUAS.2017.7991465.
32. Mughal UA, Hassler SC, Ismail M. Machine Learning-Based Intrusion Detection for Swarm of Unmanned Aerial Vehicles. In: 2023 IEEE Conference on Communications and Network Security (CNS). IEEE;2023:1–9. https://doi.org/10.1109/CNS59707.2023.10288962.
33. Wang D, Wang X, Zhang Y, Jin L. Detection of power grid disturbances and cyber-attacks based on machine learning. J Inf Secur Appl. 2019;46:42–52. https://doi.org/10.1016/j.jisa.2019.02.008.
34. Nafea AA, Mishlish M, Muwafaq A, Shaban S, Al-Ani MM, Alheeti KMA, *et al.* Enhancing Student's Performance Classification Using Ensemble Modeling. Iraqi J Comput Sci Math. 2023;4(4):204–14. https://doi.org/10.52866/ijcsm.2023.04.04.016.
35. Nalepa J, Kawulok M. Selecting training sets for support vector machines: A review. Artif Intell Rev. 2019;52(2):857–900. https://doi.org/10.1007/s10462-017-9611-1.
36. Jadhav SD, Channe HP. Comparative study of K-NN, naive Bayes and decision tree classification techniques. Int J Sci Res. 2016;5(1):1842–5. https://doi.org/0.21275/v5i1.nov153131.
37. Sholihin M, Fudzee MFM, Ismail MN. AlexNet-Based Feature Extraction for Cassava Classification: A Machine Learning Approach. Baghdad Sci J. 2023;20(6(Suppl.)):2624. https://doi.org/10.21123/bsj.2023.9120.
38. Alsumaidaie MSI, Alheeti KMA, Alaloosy AK. Intelligent Detection of Distributed Denial of Service Attacks: A Supervised Machine Learning and Ensemble Approach. Iraqi J Comput Sci Math. 2023;4(3):12–24. https://doi.org/10.52866/ijcsm.2023.02.03.002.
39. Sallibi AD, Alheeti KMA. Detection of Autism Spectrum Disorder in Children Using Efficient Pre-Processing and Machine Learning Techniques. International Conference on Decision Aid Sciences and Applications (DASA). IEEE;2023. p. 505–14. https://doi.org/10.1109/DASA59624.2023.10286808.
40. Saha S, Dasgupta S, Anam A, Saha R, Nath S, Dutta S. An Investigation of Suicidal Ideation from Social Media Using Machine Learning Approach. Baghdad Sci J. 2023;20(3(Suppl.)):1164. https://doi.org/10.21123/bsj.2023.8515.
41. Kareem AK, Al-Ani MM, Nafea AA. Detection of Autism Spectrum Disorder Using A 1-Dimensional Convolutional Neural Network. J Comput Sci. 2023;20:1182–93. https://doi.org/10.21123/bsj.2023.8564.
42. Khdier HY, Jasim WM, Aliesawi SA. Deep learning algorithms based voiceprint recognition system in noisy environment. J Phys: Conf Ser. IOP Publishing. 2021;12042. https://doi.org/10.1088/1742-6596/1804/1/012042.
43. Ragab MG, Abdulkadir SJ, Aziz N. Random search one dimensional CNN for human activity recognition. International Conference on Computational Intelligence (ICCI). IEEE;2020:86–91. https://doi.org/10.1109/ICCI51257.2020.9247810.
44. Mukhlif AA, Al-Khateeb B, Mohammed M. Classification of breast cancer images using new transfer learning techniques. Iraqi J Comput Sci Math. 2023;4(1):167–80. https://doi.org/10.52866/ijcsm.2023.01.01.0014.
45. Nafea AA, Omar N, Al-qfail ZM. Artificial Neural Network and Latent Semantic Analysis for Adverse Drug Reaction Detection. Baghdad Sci J. 2024;21(1):0226–0233. https://doi.org/10.21123/bsj.2023.798846.
46. Hmeed AR, Aliesawi SA, Jasim WM. Enhancement of the U-net architecture for MRI brain tumor segmentation. Next Generation of Internet of Things: Proceedings of ICNGIoT 2021. Springer;2021:353–67. https://doi.org/10.1007/978-981-16-0666-3_28.
47. Alsumaidaie MSI, Alheeti KMA, Al-Aloosy AK. Intelligent Detection System for a Distributed Denial-of-Service (DDoS) Attack Based on Time Series. 15th International Conference on Developments in eSystems Engineering (DeSE). IEEE;2023. p. 445–50. https://doi.org/10.1109/DeSE58274.2023.10100180.
48. Tao H, Alawi OA, Kamar HM, Nafea AA, AL-Ani MM, Abba SI, *et al.* Development of integrative data intelligence models for thermo-economic performances prediction of hybrid organic rankine plants. Energy. 2024;130503. https://doi.org/10.1016/j.energy.2024.130503.
49. Mahmood M, Jasem FM, Mukhlif AA, AL-Khateeb B. Classifying cuneiform symbols using machine learning algorithms with unigram features on a balanced dataset. J Intell

Syst. 2023;32(1):20230087. https://doi.org/10.1515/jisys-2023-0087.

50. Alsulami AA, Zein-Sabatto S. Resilient cyber-security approach for aviation cyber-physical systems protection against sensor spoofing attacks. 11th Annual Computing and Communication Workshop and Conference (CCWC). IEEE;2021. p. 565–71. https://doi.org/10.1109/CCWC51732.2021.9376158.
51. Aldaej A, Ahanger TA, Atiquzzaman M, Ullah I, Yousufudin M. Smart cybersecurity framework for IoT-empowered drones: Machine learning perspective. Sensors. 2022;22(7):2630. https://doi.org/10.3390/s22072630.
52. Shafique A, Mehmood A, Elhadef M. Detecting signal spoofing attack in uavs using machine learning models. IEEE access. 2021;9:93803–15. https://doi.org/10.1109/ACCESS.2021.3089847.

مقارنة بين الكشف عن الهجمات المادية والسيبرانية على الطائرات بدون طيار باستخدام تقنيات التعلم الآلي والتعلم العميق

خطاب معجل علي الهيتي[1]، سارة عباس رافع[2]، مها محمود[3]، أيثم خيري كريم[4]، محمد الجنابي[5]، احمد عادل نافع[3]

[1] *قسم انظمة شبكات الحاسوب، كلية الحاسبات وتكنولوجيا المعلومات، جامعة الانبار، الانبار، العراق.*

[2] *قسم القانون، كلية القانون والعلوم السياسية، جامعة الأنبار، الرمادي، العراق.*

[3] *قسم الذكاء الاصطناعي، كلية علوم الحاسوب وتكنولوجيا المعلومات، جامعة الانبار، الرمادي، العراق.*

[4] *قسم تربية هيت، المديرية العامة لتربية الأنبار، وزارة التربية والتعليم، الأنبار، العراق.*

[5] *جامعة الامام جعفر الصادق، بغداد، العراق.*

المستخلص

يتم استخدام العديد من الطائرات بدون طيار بشكل عام في التطبيقات العسكرية والمدنية. ومع ذلك، فإن هذه الطريقة المادية السيبرانية تتعرض للترهيب من خلال الهجمات السيبرانية. في الآونة الأخيرة، تم تبني أساليب الكشف عن الهجمات القائمة على التعلم الآلي (ML) بشكل فعال للكشف عن الهجمات السيبرانية. قدمت هذه الورقة منهج أمن كشف التسلل (IDS). يبحث النهج المقترح في السمات السيبرانية والمادية للطائرات بدون طيار في ظل العمليات العادية وظروف الهجوم. تم تصنيف نوعين من الهجمات السيبرانية: رفض الخدمة (DoS) وإعادة التشغيل. بعد ذلك، نقوم بتطوير مناهج IDS القائمة على نماذج ML والتعلم العميق (DL)، بما في ذلك آلة ناقل الدعم (SVM)، و(K-Nearest Neighbor (KNN، و(Nive Bayes (NB، والشبكات العصبية التلافيفية أحادية البعد (1DCNN). يتم تدريب النهج المنتج باستخدام السمات المادية والإلكترونية بشكل فردي. تشير النتائج إلى أن نموذج 1D-CNN حقق دقة أعلى (99.79٪) مقارنة بخوارزميات التعلم الآلي. أظهرت النتائج التجريبية كفاءة أداء الطريقة المقترحة.

الكلمات المفتاحية: الهجمات الالكترونية، التعلم العميق، إنترنت الأشياء، أنظمة كشف التسلل، التعلم الآلي، الهجمات المادية، طائرات بدون طيار.