An Intelligent Network Intrusion Detection Framework for Reliable UAV-Based Communication

Sujit Bebortta and Sumanta Kumar Singh

1 Introduction

Unmanned aerial vehicles (UAVs) have recently gained popularity, which has paved the way for their deployment in a variety of industries, including applications for border security, crowd surveillance, and vegetation index study. These UAVs have been extensively integrated with the Internet and IoT devices as a result of advancements in the Internet of Things (IoT), making remote data collection and dissemination possible [1, 2]. The IoT-enabled UAVs have served a variety of purposes during the COVID-19 outbreak, ranging from the delivery of medications in remote locations to the monitoring of COVID-19 impacted regions. Due to the sensitivity of the information carried by UAVs, it is crucial to communicate this information securely inside the UAV network [2].

Data from Ground Control Stations (GCSs) or the sensors installed inside the UAVs are mostly used by them to operate. Such data are sent or received wirelessly, which increases the risk of data compromise by hackers during transmission and increases the risk to the entire network. As UAV intrusions increase in frequency, defensive measures against attacks on such systems are urgently required. Intrusion detection systems (IDS) [3–6] may include the solution to the current problem. The threat landscape for UAVs is continually shifting as a result of technological advancements, therefore traditional signature-based IDS detection will be unable to adequately protect the UAV. Depending on the objective, many UAV platforms can be

S. Bebortta (✉)
School of Information and Computer Sciences, Department of Computer Science, Ravenshaw University, Odisha 753003, India
e-mail: sujitbebortta1@gmail.com

S. K. Singh
Department of Computer Science and Engineering, Gandhi Institute of Education and Technology, Baniatangi 752060, Odisha, India
e-mail: sksingh@giet.edu.in

B. K. Roy et al. (eds.), *Cryptology and Network Security with Machine Learning*,
Algorithms for Intelligent Systems, https://doi.org/10.1007/978-981-99-2229-1_16

used. Various properties, including payloads, essential sensors, and control systems, to mention a few, could change as a result [7].

Network intrusion has been viewed as a significant security risk that could adversely affect many IoT-based UAV applications in light of the aforementioned problems. Due to the integration of the several heterogeneous technologies, these UAV-based systems are now being extensively exposed to many types of cyberattacks [7]. IoT devices physically connected to the system could be harmed by any system vulnerability given the significance and complexity of establishing IDS. These damages may cause either long- or short-term failures, depending on the size and form of the cyberattack. In order to safeguard user privacy and guarantee that UAVs function as intended, this paper discusses a few security issues relating to UAV networks. An intelligent intrusion detection framework for UAV-based communication networks has been proposed to secure the UAV network against threats. To achieve improved prediction performance, the proposed framework integrates an ensemble of Random Forest (RF) and Artificial Neural Network (ANN) models. A real-world UAV dataset was analysed, which provides fresh research directions for understanding the efficacy of the proposed intelligent architecture [9]. The key performance parameters of the proposed framework, such as attack prediction accuracy, precision, recall, and CPU time, are contrasted with those of other popular frameworks. The study also offers a comprehensive analysis of a few articles of qualitative literature, enabling the development of some future specifications for the current UAV network. Next, the findings from the current study are provided, along with a few prospective directions for future investigation into privacy-preserving UAV networks.

The remaining portions of the article are structured as follows: The related studies reviewed in this research are covered in Sect. 2, the framework for constructing IDS for UAV networks is covered in Sect. 3, and the experimental results and comparison with other cutting-edge studies are covered in Sect. 4. The concluding remarks and potential paths for extending the work are offered in Sect. 5.

2 Related Studies

UAVs have grown in popularity recently in organisational planning to broaden inclusion and achieve execution goals. Utilising IDS frameworks has become essential in modern firms to ensure framework dependability for the intended presentation of such organisations. The authors in [10] create their suggested Intrusion Detection and Prevention System (IDPS) module using the Deep Q-learning Network (DQN) model so that UAVs can intuitively recognise suspicious movement and take immediate steps as necessary to maintain network security. Additionally, the reward function for their model was modified to make it easier to train on the dataset they investigated and to correctly capture the minor classes. An ultra-dense remote UAV network based on Femto Access Points (FAPs) was researched in [11]. It was proposed that the Convolution Neural Network may be recommended by a multi-objective optimization problem (CNN). Additionally, a Q-network was specifically created to allow clients in the connected UAV-based femtocaching network to deal with requests being intercepted.

With the emergence of the IoT, UAV technology has found extensive use in a variety of industries, including defence, crowd monitoring, vegetation monitoring, and wildlife protection. Concerns about the security of the data being communicated have been highlighted by the coordination of UAV with 5G technology. The authors of [12] examined the security design concerns of UAVs using the CSE-CIC IDS-2018 dataset in light of 5G network and satellite innovation. The intrusion detection module also used a number of machine learning models to evaluate harmful packets in the UAV network. Finally, the effectiveness of their model was shown in terms of F1-score, precision, recall, and prediction accuracy. A blockchain-based decentralised system was suggested for securing data in UAV networks in order to facilitate a continuous self-configurable system [13]. To evaluate the effectiveness of the suggested blockchain-based machine learning approach, the case study of cooperative intrusion detection in UAVs was taken into consideration.

In [14], the quantitative properties of UAVs, such as signal-to-noise ratio (SNR) and energy threshold, were employed to create a feature-based classification model by utilising traditional machine learning algorithms. Furthermore, the gathered spectrogram images were run through the CNN model. Quantitative analysis was used to assess the prediction effectiveness of both methodologies for determining false alarm rates and achieving high classification accuracy for jamming. A multi-agent driven deep learning technique was suggested by the authors in [15] in order to obtain good predictive performance in a UAV context. Their suggested strategy used a deep reinforcement learning model that was approximated across a deep neural network in order to reduce the operational cost of energy delivery to UAV networks.

The development of IDS for UAV network security has, however, had a huge gap that hasn't received much attention. Therefore, the current study suggests an ensemble of RF and ANN models for facilitating on-time detection of attacks in the network in order to accurately identify the cyberattacks imposed over UAVs. To conduct the experimental investigation, the model uses data on actual network traffic that is produced by a UAV network. The results show that the suggested method converges quickly and performs better than other algorithms in terms of accuracy, precision, recall, f-measure, and CPU time.

3 Proposed Framework

This section deals with the proposed framework with an emphasis on the machine learning models using in this study for developing the IDS for UAVs. In Fig. 1, an overview of the proposed intelligent intrusion detection framework is presented. Here, the environment comprises the UAV network operating over some GCS and embedded with several sensor devices for capturing data. The data from the UAV network is first captured by the RF-ANN algorithm to build the training phase for the proposed model. Further, the attacks identified in the UAV network are classified

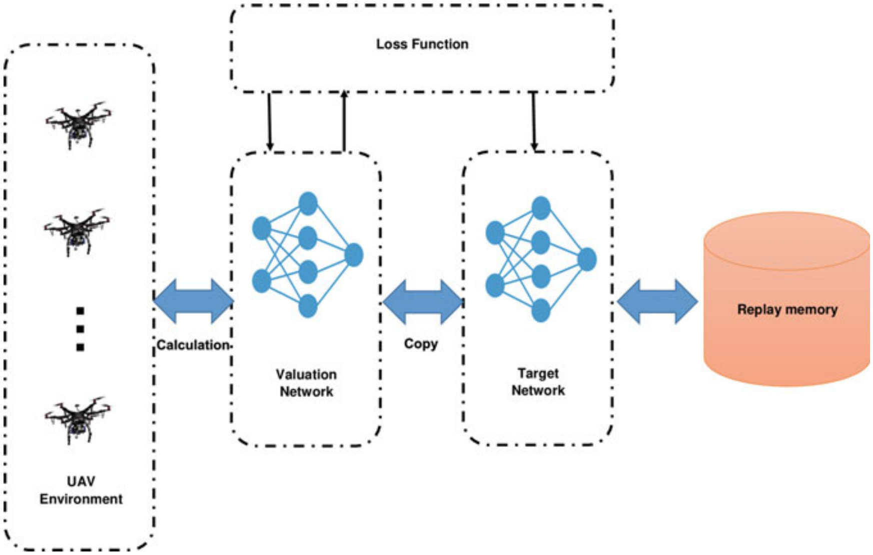

Fig. 1 Proposed framework for UAV-based IDS System

accordingly. The replay memory module acts as an intermediate storage unit for storing the transition sample to train the RF-ANN model.

3.1 Machine Learning Models

In this section, we present the machine learning models, viz., RF and ANN, which we used to construct the proposed framework for identifying the attacks in the UAV network. The models are further tested against different performance metrics to illustrate the efficacy of the proposed model.

3.1.1 Random Forest (RF) Algorithm

The RF algorithm is popularly used as a supervised ensemble learning algorithm to achieve higher predictive performance. The RF algorithms work by combining many decision trees which are generated randomly across the input vector and assist in handling complex datasets by simplifying classification. By utilising the majority voting technique, the forecast outcome from the decision trees is taken into consideration. By choosing the most popular class, the underlying decision trees are capable of anticipating future events. As a result, these features increase the RF classifier's resilience to resolving real-world issues and also highlight its effectiveness for multi-class datasets. The Gini Index, which measures the impurity of classes for the provided dataset, is the foundation upon which the RF algorithm creates the prediction model. As a result, the Gini Index for a certain dataset DS when choosing random features in class X can be defined as

$$G = \sum_{i=1}^{n} \frac{f\left(X_i, DS\right)}{|DS|} \times \sum_{j=1}^{m} \frac{f\left(X_j, DS\right)}{|DS|} \tag{1}$$

where $f\left(X_i, DS\right)$ represents that the attributes selected belong to class X_i.

3.1.2 Artificial Neural Network (ANN) Algorithm

To handle the non-linear UAV network intrusion data considered in this study, we use the artificial neural network (ANN) model. The ANN is a popular method for dealing with complicated non-linear data with a high degree of effectiveness [20, 22]. Several publications have also noted that a time series analysis using this model's effectiveness [22, 23]. This model takes into account three layers: the input layer, the output layer, and the hidden layer. Consequently, if we take O_t we can model it as follows to reflect the output for the ANN,

$$O_t = \sum_{j=1}^{l} \left(p\left(\ln(j)\right) \times \omega_{jk}\right) + \rho_k \tag{2}$$

From the Eq. (2) if the bias for the output layer is represented by rho k, assuming that $j = 1, 2, \ldots, l$ and $k = 1, 2, \ldots, s$ represent the nodes in the hidden and output layers, respectively, then ω_{jk} signifies the weight between the nodes of the hidden layer and output layer. In this instance, the activation function is represented by $p\left(\ln(j)\right)$ and can be represented as

$$\ln(j) = \sum_{p=1}^{s} \left(\theta_p \omega_{pj}\right) + \rho_j \tag{3}$$

where θ_p stands for the number that corresponds to the $p^t h$ node in the input layer, with the values $p = 1, 2, \ldots, 4, s$. As a result, we use the sigmoid function as the activation function to process the result of Eq. (3), which is denoted by the following representation:

$$P\left(D|X_i\right) = \prod_{j=1}^{n} P\left(d_j|X_i\right) \tag{4}$$

Substituting the values of Eqs. (3) and (4) in Eq. (2), we obtain,

$$O_t = \sum_{j=1}^{l} \left(p \left(\sum_{p=1}^{s} \left(\theta_p \omega_{pj} \right) + \rho_j \right) \times \omega_{jk} \right) + \rho_k \tag{5}$$

4 Results and Discussions

This section presents the experimental outcomes obtained over the UAV data by exploiting the proposed framework. The data comprises cyberattacks over UAVs induced using simulations over PX4 autopilot and Gazebo simulator [9]. The data comprises logged sensor data values captured pervasively across autopilots. The dataset comprises attacks deployed over various UAV platforms; however, this study exploits the Plane UAV platform having a standard plane model constituting of 23198 benign and 1055 malicious sensor values with the simulation type as software-in-the-loop to facilitate interoperability of the proposed framework over different UAVs.

Figure 2 presents the comparative study of different machine learning models like RF and ANN in comparison with the proposed RF-ANN framework. It is observed that the proposed model outperforms the RF and ANN model in terms of recall and F-measure; however, the RF model outperforms all other models in terms of precision. In Fig. 3, the accuracy for different models is compared. It is observed that the proposed framework provides the highest prediction accuracy of 99.372%. Finally, the CPU time for the proposed model is observed to be 76.117 seconds which is faster in comparison to the CPU time for RF and ANN models. Table 1 gives a detailed comparative overview of the different performance metrics considered in this study for the proposed framework and baseline algorithms (Fig. 4).

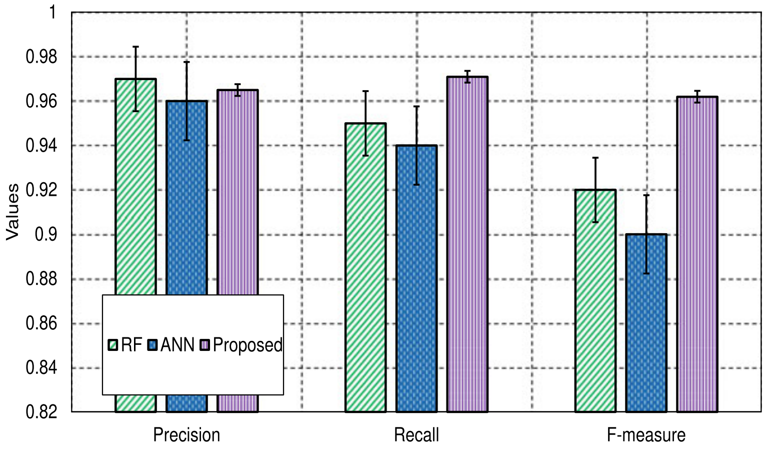

Fig. 2 Comparison of performance for the proposed framework with different machine learning models

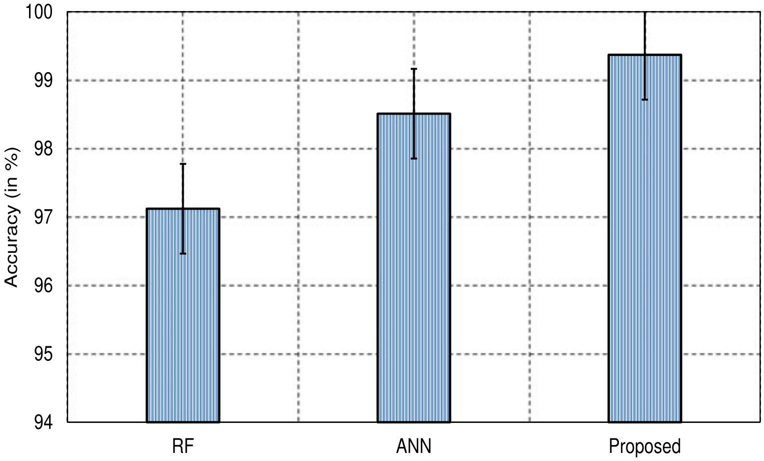

Fig. 3 Comparison of prediction accuracy for the proposed model with different machine learning models

Table 1 Performance metrics for proposed algorithm and baseline algorithms

Models	Precision	Recall	F-measure	Accuracy (in %)	CPU time
RF	**0.970**	0.952	0.922	97.121	86.665
ANN	0.961	0.0.940	0.901	98.511	88.911
Proposed	0.965	**0.971**	**0.962**	**99.372**	**76.115**

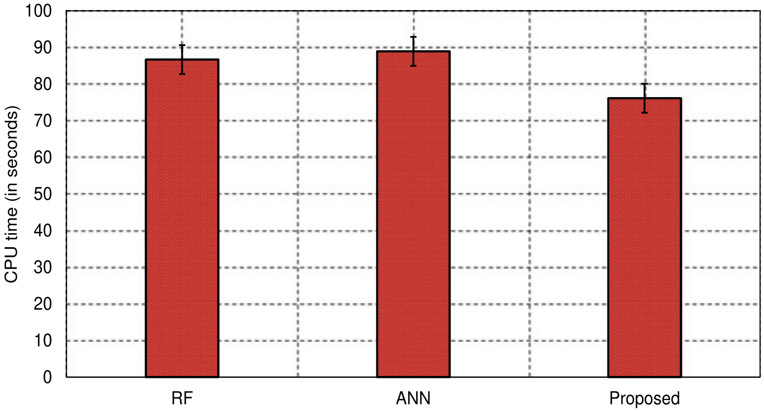

Fig. 4 CPU time for the proposed framework with RF and ANN

5 Conclusions and Future Work

With the growing advancements in UAV technology, the dependence on these technologies has increased drastically in recent times. However, considering the possibility of cyberattacks in heterogeneously connected UAVs, the need for developing IDS to preserve the sensitivity of critical tasks becomes essential for UAVs. This work proposed a machine learning-based hybrid framework by combining RF and ANN algorithms through ensembling technique for achieving higher predictive performance towards the detection of cyberattacks in UAVs. The model was studied in convergence with baseline machine learning algorithms to assess the performance for different parameters like precision, recall, F-measure, accuracy, and CPU time. It was observed that the proposed framework provided the highest predictive performance of 99.372.

In the future, we would like to extend our work by incorporating more precise learning models like the reinforcement learning model over different UAV platforms to achieve higher performance. Further, there are several research gaps that can address other major issues, such as those imposed by attackers which affect the hardware components associated with the compromised UAVs. This paves a new path for future research towards addressing the limitations of IDS for UAV networks.

References

1. Alsamhi SH, Afghah F, Sahal R, Hawbani A, Al-qaness MA, Lee B, Guizani M (2021) Green internet of things using UAVs in B5G networks: a review of applications and strategies. Ad Hoc Netw 1(117):102505
2. Sharma R, Arya R (2022) UAV based long range environment monitoring system with Industry 5.0 perspectives for smart city infrastructure. Comput Ind Eng 168:108066
3. Bebortta S, Singh SK (2021) An adaptive machine learning-based threat detection framework for industrial communication networks. In: 2021 10th IEEE international conference on communication systems and network technologies (CSNT). IEEE, pp 527–532
4. Bebortta S, Singh SK (2022) An intelligent framework towards managing big data in internet of healthcare things. In: International conference on computational intelligence in pattern recognition. Springer, Singapore, pp 520–530
5. Bebortta S, Singh SK (2022) An opportunistic ensemble learning framework for network traffic classification in IoT environments. In: Proceedings of the seventh international conference on mathematics and computing 2022. Springer, Singapore, pp 473–484
6. Singh SK, Mishra AK. Rain fall prediction using bigdata analytics. Int J Innov Eng Technol (IJIET) 151. https://doi.org/10.21172/ijiet
7. Sun M, Xu X, Qin X, Zhang P (2021) 10 AoI-energy-aware UAV-assisted data collection for IoT networks: a deep reinforcement learning method. IEEE Internet Things J 8(24):17275–17289
8. Bebortta S, Panda M, Panda S (2020) Classification of pathological disorders in children using random forest algorithm. In: 2020 international conference on emerging trends in information technology and engineering (ic-ETITE) 2020. IEEE, pp 1–6
9. Whelan J, Sangarapillai T, Minawi O, Almehmadi A, El-Khatib K (2020) 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, pp 23–28

10. Bouhamed O, Bouachir O, Aloqaily M, Al Ridhawi I (2020) Lightweight ids for UAV networks: a periodic deep reinforcement learning-based approach. In: 2021 IFIP/IEEE international symposium on integrated network management (IM). IEEE, pp 1032–1037
11. Hajiakhondi-Meybodi Z, Mohammadi A, Abouei J (2021) Deep reinforcement learning for trustworthy and time-varying connection scheduling in a coupled UAV-based femtocaching architecture. IEEE Access 18(9):32263–81
12. Shrestha R, Omidkar A, Roudi SA, Abbas R, Kim S (2021) Machine-learning-enabled intrusion detection system for cellular connected UAV networks. Electronics 10(13):1549
13. Khan AA, Khan MM, Khan KM, Arshad J, Ahmad F (2021) A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. Comput Netw 4(196):108217
14. Li Y, Pawlak J, Price J, Al Shamaileh K, Niyaz Q, Paheding S, Devabhaktuni V (2022) Jamming detection and classification in OFDM-based UAVs via feature-and spectrogram-tailored machine learning. IEEE Access 8(10):16859–70
15. Jung S, Yun WJ, Kim J, Kim JH (2021) Coordinated multi-agent deep reinforcement learning for energy-aware UAV-based big-data platforms. Electronics 10(5):543
16. Cai YD, Feng KY, Lu WC, Chou KC (2006)7 Using LogitBoost classifier to predict protein structural classes. J Theor Biol 238(1):172–6
17. Murphy KP (2006) Naive Bayes classifiers. Univ Br Columbia 18(60):1–8
18. Webb GI, Keogh E, Miikkulainen R (2010) Naïve Bayes. Encyclopedia of machine learning, vol 15, pp 713–714
19. Qi Y (2012) Random forest for bioinformatics. In: Ensemble machine learning. Springer, Boston, MA, pp 307–323
20. Probst P, Wright MN, Boulesteix AL (2019) Hyperparameters and tuning strategies for random forest. Wiley Interdiscip Rev: Data Min Knowl Discov 9(3):e1301
21. CrowdFlower. https://www.crowdflower.com/data-for-everyone/. Accessed 10 Dec 2021
22. Squires M, Tao X, Elangovan S, Gururajan R, Zhou X, Acharya UR (2022) A novel genetic algorithm based system for the scheduling of medical treatments. Expert Syst Appl 14:116464
23. Sarosh P, Parah SA, Bhat GM (2022) An efficient image encryption scheme for healthcare applications. Multimed Tools Appl 25:1–8