IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 October 2023, accepted 21 December 2023, date of publication 3 January 2024,
date of current version 11 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3349469

RESEARCH ARTICLE

A Novel Intrusion Detection System Based on Artificial Neural Network and Genetic Algorithm With a New Dimensionality Reduction Technique for UAV Communication

KORHAN CENGIZ[1,2], (Senior Member, IEEE), SWATI LIPSA[3], RANJAN KUMAR DASH[3], (Senior Member, IEEE), NIKOLA IVKOVIĆ[4], (Senior Member, IEEE), AND MARIO KONECKI[4]
[1]College of Information Technology, University of Fujairah, Fujairah, United Arab Emirates
[2]Department of Electrical and Electronics Engineering, Istinye University, 34010 Istanbul, Turkey
[3]Department of Information Technology, Odisha University of Technology and Research, Bhubaneswar 751003, India
[4]Faculty of Organization and Informatics, University of Zagreb, 42000 Varaždin, Croatia

Corresponding author: Swati Lipsa (slipsait@outr.ac.in)

ABSTRACT Unmanned aerial vehicles (UAVs) are increasingly being deployed in crucial missions for the armed forces, law enforcement, industrial control monitoring, and other sectors. However, these hostile operating circumstances, along with the UAVs' dependence on wireless protocols, pose substantial security threats, limiting their mainstream application. With network security being such a major issue for UAV networks, the machine learning-based intrusion detection system (IDS) has been determined to be an effective strategy for protecting them. Additionally, though the existing methods offer effective strategies for detecting and categorizing abnormalities in the system, they are limited by their inability to adjust to various attack patterns. The dataset used as well as the memory and computational requirement of existing models, poses new challenges. One of the main concerns pertains to the reduced computational and memory demands of these models. So, the work carried out in this paper addresses this challenge. A new dimensional reduction technique based on correlation coefficient, information gain, and principal component analysis (PCA) is introduced to reduce the dimensionality of the UAV Attack Dataset. A novel intrusion detection system based on an artificial neural network (ANN) and genetic algorithm (GA) is then proposed. The genetic algorithm is used to generate the optimal weights of the artificial neural network. A comparison is made between the proposed model and the backpropagation network and its variant in terms of its convergence and prediction accuracy. Furthermore, the performance of the proposed model is compared with that of other classifiers. This comparison reveals that the proposed model is time efficient with an increased prediction accuracy of at least 6% more than other classifiers.

INDEX TERMS Artificial neural network, backpropagation, genetic algorithm, information gain, intrusion detection system, Pearson correlation coefficient, principal component analysis, sparsity, unmanned aerial vehicles.

I. INTRODUCTION

This Unmanned Aerial Vehicles (UAVs), sometimes known as "drones", are a relatively new type of aircraft that is controlled by an autonomous computer-based pilot rather than a human pilot on board [3]. UAVs were initially utilized by the military to train soldiers or destroy the enemy while protecting the lives of human pilots. Since their inception, unmanned aerial vehicles (UAVs) have advancesemendous with by made enormous advancements in technology and capability, opening up a plethora of intriguing applications for drones beyond the military. Many exciting potential

The associate editor coordinating the review of this manuscript and approving it for publication was Ganesh Naik.

applications for unmanned aerial vehicles have been driven by the fact that modern UAVs can be operated remotely by humans or through a sophisticated computer-based autopilot system. These applications across several sectors [4] include agriculture, forestry, environmental protection, and security, where they are employed for crucial tasks like rescue, surveillance, and transportation. Further, these kinds of applications introduced a large number of new requirements and concepts for employing UAV.

The pervasiveness of this technology, as well as the intrusive implementation of UAVs in numerous crucial domains, has raised security issues [5], including public safety, aviation security, and national defense systems. As a result, UAVs demand better administration, data storage, communication, and instantaneous intelligent decision-making. These demands become even more important when it is desired for a group of UAVs [6] to operate in coordination with one another and make decisions in a distributed decentralized way. Most unmanned aerial vehicle (UAV) systems rely on a central server or cloud-based framework to handle data using intricate Machine Learning (ML) techniques. In reality, many typical cyberattacks [7] are also pertinent to unmanned aerial vehicles (UAVs), but their effects would be more severe because UAVs are so reliant on intelligent systems that largely depend on artificial intelligence and machine learning to make decisions when humans are not present.

Conventional network security approaches are largely based on passive defense mechanisms [8], rendering it difficult to withstand network attacks with dynamic technology. The limitations of conventional security methods are addressed by intrusion detection technology, which takes a proactive and defensive approach towards securing a network. Despite the widespread interest in intrusion detection systems (IDSs) among users, there are still certain issues that need to be resolved before they can be fully implemented [9]. Specifically, with today's high-bandwidth, high-traffic computer networks, traditional IDS struggle to deliver adequate performance and efficiency. Moreover, with the increase in sophistication, automation, and dispersed nature of attacks, traditional IDSs somehow fail to guarantee proficient security requirements. Therefore, to enhance the detection efficacy and reduce the false alarm rates of IDS, numerous researchers are incorporating machine learning techniques [10] to handle the intrusion detection issue.

Machine learning [11] has significant potential as a way to address many of the issues mentioned above raised by the massive amounts of network traffic induced in UAV networks. Artificial intelligence (AI) approaches using ML allow for the smart processing of huge amounts of complicated datasets, train AI models to detect patterns with the least human involvement, and adapt to the ever-changing conditions and inconsistent behavior of UAVs, all of which are crucial for the functioning of UAVs. Additionally, the availability of real-time data pertaining to different attacks to train the ML-based IDS is an important challenge. However, datasets like the UAV attack dataset can be used effectively to meet this challenge. The data set contains real-time data on malicious and normal types of UAVs. The main types of attacks considered in this dataset are GPS spoofing and jamming, which are common attacks for UAVs. Moreover, the huge number of features as well as the features with zero values in many instances make it computationally difficult to train the ML models. Hence, it is of utmost importance to reduce the dimensionality of such datasets and to extract the important features. Though, the artificial neural network has the advantage of extracting important features intrinsically during its training even for large datasets, its slow convergence due to the gradient descent learning algorithm puts a stringent constraint on its use.

The work carried out in this paper proposes a dimensionality reduction technique based on the correlation coefficient, information gain, and principal component analysis to reduce the number of features to some acceptable number that requires less computational time and memory. A hybrid model of artificial neural networks and genetic algorithms is then proposed in which GA is used to generate the optimal weights of ANN to accelerate its convergence to optimal solutions.

The rest of the paper is organized as follows: Section II delves into recent work on IDS in UAVs. Section III presents the design and implementation of our proposed model, while the details of the dataset are discussed in Section IV. Section V provides the results and highlights the performance of the proposed model with respect to its effectiveness for intrusion detection, and finally, Section VI concludes the paper.

II. RELATED WORKS

UAV networks are frequently used in crucial scenarios for the exchange of sensitive data. However, due to their computational and communication constraints, UAV infrastructures are vulnerable to anomalies and attacks. Generally, UAV-IDS are designed to identify a broad spectrum of anomalies and threats, including path and message forgeries, malware and viruses, UAV capture and spoofing, routing attacks, and GPS spoofing. To detect intrusions, the authors in [12] suggest using a Deep Belief Network (DBN) that has been improved with particle swarm optimization (PSO). Firstly, a DBN-based classification model is built, and then the PSO algorithm is applied to optimize the DBN's hidden layer node count to yield the most effective DBN architecture. The study [13] introduces an autonomous intrusion detection system to identify advanced and complex cyberattacks that take advantage of drone networks. Machine learning algorithms like naive Bayes, decision trees, support vector machines, k-nearest neighbors, and deep learning multi-layer perceptrons were evaluated by launching malicious activities against a drone network set up as a testbed.

The work carried out in [14] develops a 5G network security framework for UAVs and satellites that utilizes machine learning to efficiently determine vulnerabilities and malicious attacks. The approach consists of two parts: part one, which involves developing a model for intrusion detection using a suite of machine learning (ML) algorithms, and part two, which involves integrating that model into either a ground-based or space-based gateway. The authors in [15] suggest a lightweight intrusion detection and prevention system (IDPS) module for UAVs. Additionally, to make it feasible for UAVs to independently identify suspicious behavior and initiate appropriate measures to maintain network security, the IDPS module is trained with Deep Reinforcement Learning (DRL) and, more particularly, Deep Q-learning (DQN). The article [16] provides an overview of the security risks and mitigation strategies associated with UAV communications. They summarized their work by discussing possible attacks on UAV communications while analyzing their security needs, which are motivated by the broad use of UAVs and their potential applications in numerous fields.

The work proposed in [17] enhances UAV functionality by employing a blockchain-based, decentralized machine learning technique. Their suggested approach, when applied to a fleet of UAVs, has the ability to vastly improve data integrity and storage to make intelligent decisions. The paper [18] concentrates on the research done on ML strategies for IDSs in VANETs and UAV-enhanced networks. Furthermore, they emphasize the main unresolved research issues in the literature and offer suggestions for enhancing the security of intelligent transportation systems. The intrusion detection approach developed [19], called Attention-based Spatio-Temporal Graph Convolutional Network (ATGCN), integrates a graph convolutional network and a gated recursive unit to form a spatio-temporal graph convolutional network to address the temporal and spatial dynamic properties of UAV networks. The work carried out in [20] aims to identify suspicious behavior in UAV groups and classify the attack accordingly. To achieve this goal, the authors built an experimental setup by imitating traffic transmission among a fleet of UAVs and focused on analyzing how the transmission of traffic changes both when it is operating normally and when it encounters an attack.

For UAV networks, the study [21] introduces a DRL method that is optimized using the Black Widow Optimisation (DRL-BWO) algorithm. Additionally, the DRL relies on a DBN trained with improved reinforcement learning for tracking potential threats. The method developed in [22] employs one-class classifiers and principal component analysis (PCA) to identify attacks. This enables the use of flight records as a source of training data and is incorporated into a fully functional IDS (MAVIDS), resulting in a flexible and ubiquitous method. The authors in [23] propose a deep convolutional neural network-based autonomous intrusion detection system (UAV-IDS-ConvNet) to detect hostile threats targeting UAVs. The suggested method takes into account encrypted Wi-Fi traffic data logs from three popular UAV types: Parrot Bebop UAVs, DJI Spark UAVs, and DBPower UDI UAVs. The study in [24] presents a technique called SID-UAV, which can prevent communications between UAVs from being hampered by malicious UAVs. The SID-UAV system automatically finds the route between UAVs that poses the least risk. The paper [25] introduces a conditional generative adversarial net (CGAN) based on collaborative IDS with blockchain-enabled distributed federated learning. When training convolutional generative adversarial networks (CGANs), this research incorporates long-short-term memory (LSTM) to improve the performance of the generative network to identify intrusion. The data normalization method designed in [26] enables us to recognize early indicators of a cyber attack. They outline a novel database format to facilitate the detection of UAV intrusions and specify sets of parameters that could potentially signal an attack. To accomplish these targets, they conducted an experimental analysis of the effect of threats on UAV parameters, built a software component for gathering information from UAVs, and figured out how to normalize and exhibit the data in a way that would make it easy to identify attacks.

The study in [27] designs a method for detecting intrusions in an Internet of Drones (IoD) network using crystal structure optimization with deep autoencoders based intrusion detection (CSODAE-ID). The proposed CSODAE-ID model employs a novel Modified Deer Hunting Optimization-based Feature Selection (MDHO-FS) method to choose the feature subsets and the Autoencoder (AE) approach to classify attacks in the IoD environment. In order to detect and classify intrusions in the IoD environment, the research [28] proposes a Sea Turtle Foraging Algorithm with Hybrid Deep Learning-based Intrusion Detection (STFA-HDLID). Here the features were selected using the STFA method, and classification was performed by a DBN trained with the Sparrow Search Optimization (SSO) algorithm. The authors in [29] suggest modeling typical drone swarm behavior with a timed probabilistic automata (TPA)-based IDS and then looking for any variations that could indicate an attack. When it comes to protecting against drone swarm threats, this IDS solution is effective and versatile.

Since this domain of study is still in its early stages, it highlights the importance of developing an IDS based on machine learning approaches so that even the most inexperienced UAV developer can benefit from increased security. This IDS may also act as a model to facilitate the adoption of similar technologies in the commercial sector.

Drones can be compromised in several ways due to their heavy reliance on wireless connectivity. Such attacks may result in devastating consequences, consisting of both commercial and noncommercial damages. In this scenario, there is a dearth of knowledge on how hackers take control of a UAV and intercept or even crash it. As drones can be exploited for malicious attacks, it is essential to identify such attacks and restrict them before they can cause any damage.

III. PROPOSED INTRUSION DETECTION SYSTEM FOR UAV COMMUNICATION

Let's assume X is a dataset with $m \times n$ dimension where m is the number of instances while n represents the number of features. Dimensionality reduction techniques such as principal component analysis (PCA), linear discriminant analysis, linear regression, random forest, truncated singular value decomposition (SVD), and Uniform Manifold Approximation and Projection (UMAP), etc. cannot be directly applied to the dataset with a very large number of features due to resource constraints such as CPU and RAM. This necessitates the use of statistical techniques like Pearson correlation coefficient or goodness of fit to decide the degree of correlation or the degree of casuality between each feature and the target class variable. Additionally, if the dataset is sparse, this statistical technique alone may not be used while removing any feature. Thus, the results of any two independent statistics must be crosschecked and common features that are of least importance may be discarded.

The motivation to use ANN and GA is discussed in the following lines. There are many different types of neural networks and it is not possible to a priori know which type and configuration would be optimal for some specific application. Therefore researchers rely on prior knowledge and previously published research while choosing one when making this decision. Convolutional neural networks (CNNs) are inspired by the visual systems of mammals, have an architecture with convolution kernels, and are invariant to some image transformation. As a result, their usage in image and video recognition and classification has been highly effective. In light of increased success in that area, CNNs are increasingly used in research. However, since our research is not focused on image or video recognition, we have chosen the basic ANN approach for this study.

There are many nature-inspired algorithms that can be used for hyperparameter optimization, for example, there are more than 500 listed in [32]. Some of them are well-researched classical nature-inspired algorithms such as genetic algorithms or ant colony optimization, while many newer algorithms have been studied in recent years such as Harris Hawk Optimization [33], Grey Wolf Optimization, and FireFly Optimization. Since hyperparameter optimization is a type of continuous variable problem we have chosen a genetic algorithm that has confirmed its excellent properties for constrained and unconstrained continuous variable problems. For many years now, at the well-known IEEE CEC conference, there has been competition for the best algorithm on sets of problem instances within agreed conditions and metrics. In recent years, from CEC 2010 until now, almost all the winners are variants of genetic algorithms, evolutionary strategies, or differential evolution [34], [35]. A recent assessment published by top researchers in this area [36] confirms once again that the aforementioned classical nature-inspired algorithms show better performance on the continuous variable problem than many new algorithms.

A. OUTLIER DETECTION

The outliers are detected by using the 2-sigma rule i.e. a value x_k is detected as an outlier if it deviates the mean($\bar{x}$) by at least twice the standard deviation(σ_i).

B. PROPOSED DIMENSIONALITY REDUCTION TECHNIQUE

Pearson's correlation coefficient and information gain are the statistical techniques that are used to find the correlation between two variables and to measure the reduction of impurity in the dataset respectively. The dimensional reduction techniques such as linear regression use the former one while the latter one is used in random forest. However, the reason behind not choosing any stand-alone techniques for reducing the dimensionality of the dataset is discussed earlier. Hence, the proposed dimensionality reduction technique is a cascading of Pearson's correlation coefficient, information gain, and principal component analysis.

$$r(x_i) = \frac{\sum_{i=1}^{m}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{m}(x_i - \bar{x})^2(y_i - \bar{y})^2}} \tag{1}$$

$$G(X, x_i) = E(X) - \sum_{c_j \epsilon C} \frac{|S_{c_j}|}{|S|} E(S_{c_j}) \tag{2}$$

$$Sparsity = 1 - \frac{count\_nonzero(X)}{size(X)} \tag{3}$$

Pearson's correlation coefficient lists all the features that are very little correlated with the target value. However, when the data is very sensitive, discarding any feature may affect the system's performance significantly. So, information gain is computed for each feature concerning the target value. The two lists are crosschecked and the features with their respective values of Pearson correlation coefficient and information gain below the predefined threshold values are discarded.

Principal component analysis can be applied to the dataset to further reduce its dimensionality. PCA is also very effective when the dataset is sparse in nature. The steps taken to reduce the dimensionality of the dataset are listed in Algorithm 1.

C. SYSTEM MODEL

The following two scenarios involving UAV systems demonstrate the presence and absence of an IDS in these systems.

In the absence of IDS in the UAV system - A UAV launches off from its starting point and follows its planned flight route until it reaches its destination. Sometime afterward, a spoofer starts to use GPS spoofing to move this UAV from its current actual position to its current fake position. With persistent attacks, the ground station displays

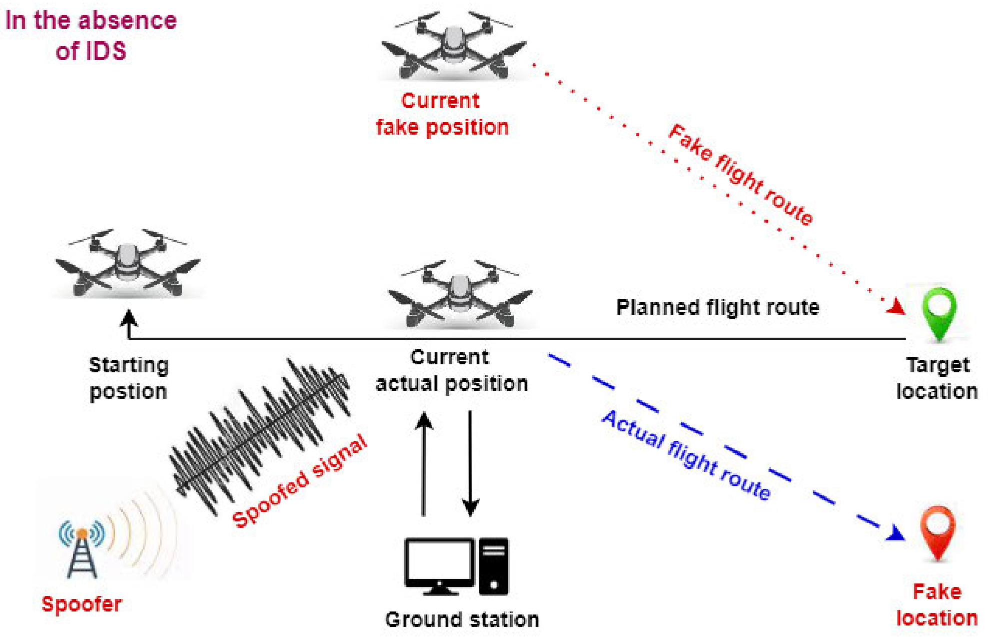


FIGURE 1. UAV system in the absence of IDS.

Algorithm 1 Dimensionality_Reduction(X)

```
cor_list=[]
IG_list=[]
for each $x_i \epsilon X$ do
    Calculate $r(x_i)$ using equation(1)
    if $r(x_i) < r_{min}$ then
        cor_list.append($x_i$)
    end if
    Calculate $G(X, x_i)$ using equation(2)
    if $r(x_i) < IG_{min}$ then
        IG_list.append($x_i$)
    end if
end for
discard_feat=$cor\_list \cap IG\_list$, where ∩ represents intersection
for each f ϵ discard_feat do
    X=X.remove(f)
end for
n_components=number of columns of X
Compute Sparsity of X using equation(3)
while Sparsity ¬0 do
    Reduced_X=principal_component_Analysis(n_components)
    Compute Sparsity of Reduced_X using equation(3)
    if Sparsity == 0 then
        break
    else
        n_components=n_components-1
    end if
end while
```

that this UAV is traveling along the fake flight route toward the target location. But in reality, the UAV is navigating via the real actual fake flight route to land at a fake location. This is presented in Fig.1.

In the presence of IDS in the UAV system - As mentioned above, the UAV launches off from its starting point to reach its destination via a planned flight route. Then sometime during the travel, a spoofer carries out GPS spoofing to move the UAV from its current position. However, in the presence of an IDS-enabled ground station, the spoofing attack gets detected and blocked. As a result, the UAV continues to follow its planned flight path to its target location. The system is shown in Fig.2.

D. PROPOSED HYBRID MODEL OF ANN AND GA

The backpropagation network uses a gradient descent technique with backward error propagation. At each step, the error is computed using the following equation:

$$E(\vec{W}) = \frac{1}{2}\sum_{d\epsilon X}(y_d - o_d)^2 \tag{4}$$

where, y_d is the target output while o_d is the computed output. The backpropagation algorithm searches this error surface in a gradient descent manner to find the optimal weights. However, the slow convergence and the problem of getting stuck to a local minima are the basic flaws of this type of learning technique.

The above-mentioned problem of the backpropagation network can be minimized by combining it with a genetic algorithm which is responsible for finding the optimal weights in an acceptably quick manner. Let's assume the ANN has i input neurons, h hidden neurons, and o output neurons. The total number of trainable weights is $(i+o)h+2$. If each weight($W_{i,j}$) has length d, each gene represents one weight ($W_{i,j} \epsilon P$) and the length of each gene is d.

The chromosome which is a combination of genes can be encoded by a string of length $L = (i+o)hd + 2d$ and each chromosome represents $(i+o)h+2$ weights. If P is the size

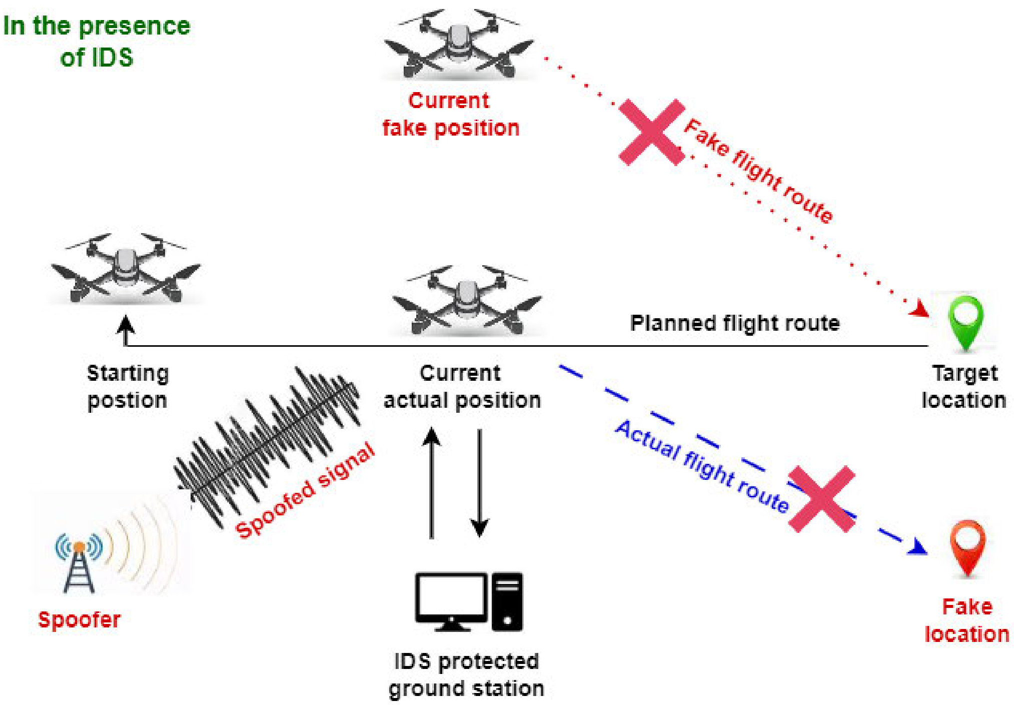


FIGURE 2. UAV system in the presence of IDS.

of the population, the initial population of p chromosomes is randomly generated.

1) WEIGHT EXTRACTION FROM THE CHROMOSOME

Let $c_1, c_2, \ldots c_L$ represent a chromosome and let c_{kd+1}, $c_{kd+2} \ldots c_{(k+!)d}$ represents k^{th} gene of this chromosome. The weight w_k can be expressed as:

$$x_k = \begin{cases} \dfrac{c_{kd+1} \times 10^{d-2} + c_{kd+2} \times 10^{d-3} + \cdots + c_{(k+1)d}}{10^{d-2}} \\ \text{for} \\ d \leq c_{kd+1} \leq 9 \\ -\dfrac{c_{kd+1} \times 10^{d-2} + c_{kd+2} \times 10^{d-3} + \cdots + c_{(k+1)d}}{10^{d-2}} \\ \text{for} \\ 0 \leq c_{kd+1} \leq d \end{cases} \tag{5}$$

2) FITNESS FUNCTION

The weights are extracted from each chromosome using the equation (5). The input is passed through the ANN. The output is produced by using these weights and biases. However, the output generated by ANN is not categorical, which is in contrast to class-specific targets. Hence, the following equation is used to convert the non-categorical output of ANN to categorical outputs:

$$p_{c,c\epsilon C} = \frac{o_c}{\sum_{c\epsilon C}\{o_c\}} \tag{6}$$

The predicted output i.e. $\hat{y}_j$ can be estimated by using the following equation:

$$\hat{y}_j = c \text{ for } \max_{c\epsilon C} p_i \tag{7}$$

The root mean square error (RMSE) for each chromosome can be calculated by using the equation:

$$RMSE(C_i) = \sqrt{\frac{\sum_{j=1}^{m}(y_j - \hat{y}_j)^2}{m}} \tag{8}$$

The fitness function (F_i) of i^{th} chromosome can be generated by taking the reciprocal of $RMSE(C_i)$ i.e.

$$F_i = \frac{1}{RMSE} \tag{9}$$

The steps to generate the fitness function of each chromosome are presented in Algorithm 2.

Algorithm 2 Fitness_function()

```
for each chromosome $C_i \epsilon$ population do
    Extract weight $w_k$, where $k = 0, 1 \ldots (l+m)n+2$ using equation(5)
    Use the weights $w_k$ to train the ANN over dataset $Reduced_X$
    Compute the error $E_j$ using equation(4).
    Compute the root mean square error $RMSE = \sqrt{\frac{\sum_{j=1}^{m}(y_j - \hat{y}_j)^2}{m}}$
    The fitness function $F_i = \frac{1}{RMSE}$
end for
```

3) CROSSOVER

The fitness function is estimated for each chromosome belonging to the population. The chromosomes are sorted with respect to their calculated fitness function in decreasing order of these values. The chromosomes with the lowest fitness values are replaced by the chromosomes with the highest fitness values. Two chromosomes with the best fitness values are selected to generate the offspring. The cross-over operation is employed for this purpose. During the generation of offspring, a two-point cross-over operation is performed.

Algorithm 3 Crossover()

```
    Sort chromosomes $C_i \epsilon P$ with respect to their increasing values of fitness function $F_i$
    Replace $C_j, F_j^{min}$ with $C_i, F_i^{max}$
    Select two chromosomes $C_i$ and $C_j$ with best fitness function as two parents $P_i$ and $P_j$
    $d1 = randint(0, L)$ and $d2 = randint(0, L)$
    $Off_i = P_i$ and $Off_j = P_j$
    $Off_i[d1 : d2] = P_j[d1 : d2]$
    $Off_j[d1 : d2] = P_i[d1 : d2]$
    append($Off_i$ and $Off_j$) to population P
    Fitness_function($Off_i$)
    Fitness_function($Off_j$)
```

4) PROPOSED ALGORITHM TO TRAIN ANN BY UPDATING ITS WEIGHTS THROUGH GA

Initially, the population P_0 is generated randomly, where each chromosome has the length $L = (i + o)hd + 2d$. The fitness function of each chromosome is computed using Algorithm 2, i.e., Fitness_function(). The RMSE of the chromosome is calculated using Eq.(8). If its value is less than 0.0001 for all chromosomes, the respective weights for the ANN are extracted using Eq.(5). Otherwise, Algorithm 3, i.e., Crossover(), is executed to produce the offspring, and the initial population P_0 becomes P_1 i.e., the next generation population. The above-mentioned process is repeated till the Algorithm 4 converges to the optimal weights.

IV. DATASET

The dataset [30] has three directories: Each directory contains 60 CSV files. The files contain similar data with respect to their relative ordering of appearance in the respective directories, i.e., the first CSV file. The data are not labeled. The different classes are extracted while reading the directories. The data extraction from these directories is depicted in Fig.3.

The extracted dataset(X) contains 293769 number of instances, each with 829 number of features. The number of non-zero data in the dataset is 2697289, while its size is 243534501. Thus, the sparsity is calculated using Equation (3) = 0.988.

During the concatenation and merging operations, the features are filled up with NA. The replacement of NA with the mean value of features reduces the sparsity to 0.73. Outliers are detected and also filled with the mean value of features. Subsequently, the proposed dimensionality reduction algorithm, i.e., Dimensionality_Reduction is applied to X to reduce the number of features to 10, and the new dataset Reduced_X has 293769 instances and 10 features.

Algorithm 4 Proposed Algorithm to Train ANN by Updating Its Weights Through GA()

```
i=0
Randomly generate $P_i$ number of chromosomes of length $L = (i + o)hd + 2d$.
**while** !True **do**
    Calculate fitness function for each $C_j \epsilon P_i$ using Algorithm fitness_function()
    **if** $RMSE(C_j) \leq 0.0001$ for all $C_j \epsilon P_i$ **then**
        Extract the weights using equation(5).
        break
    **else**
        i=i+1
        call Algorithm Crossover() to produce the offsprings
        Crossover() updates the population to $P_{i+1}$
    **end if**
**end while**
```

V. RESULTS

The simulation is carried out in the Google Colab environment using Python programming. The architecture of the proposed model is depicted in Fig.4. The different parameters used for simulation are presented in Table 1. The proposed model is trained and validated over Reduced_X by using a 5-fold cross-validation technique.

TABLE 1. Parameters for simulation.

Parameters	Value
Number of input neurons	10
Number of hidden neurons	5
Number of output neurons	3
Total number of weights	65
Total number of bias	2
Gene(weight length)	2
Chromosome length	134
Population size	100

A. CONVERGENCE OF THE PROPOSED MODEL

The proposed model is trained and validated on the Reduced_X dataset with a 5-fold cross-validation technique. During each iteration, the dataset is randomly divided into five disjoint parts, of which four parts are used to train the model, while the rest one part is used to validate the model. The root means square error generated during each iteration is stored separately for training and validation. As the computed output and the target output class are specific, the denominator of the expression supersedes largely the numerator. Thus, a very low value, such as 0.001, is set

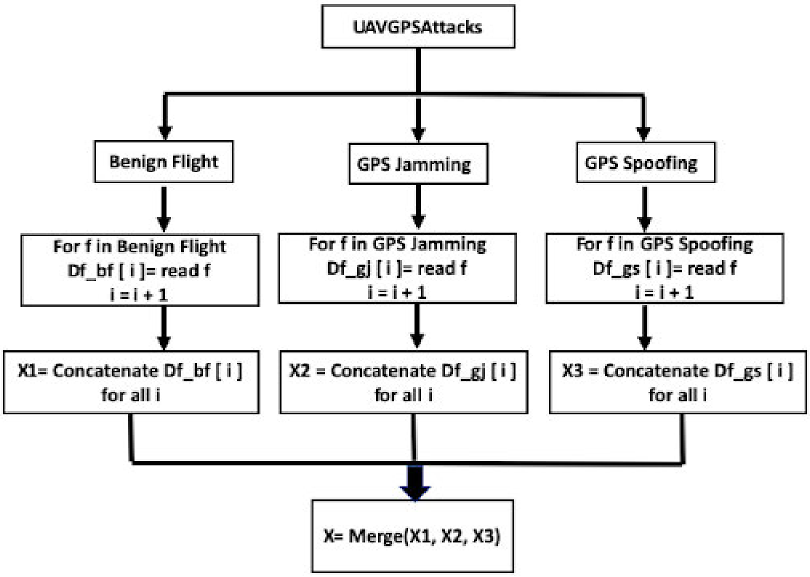


FIGURE 3. Extraction and merging of data from the dataset.

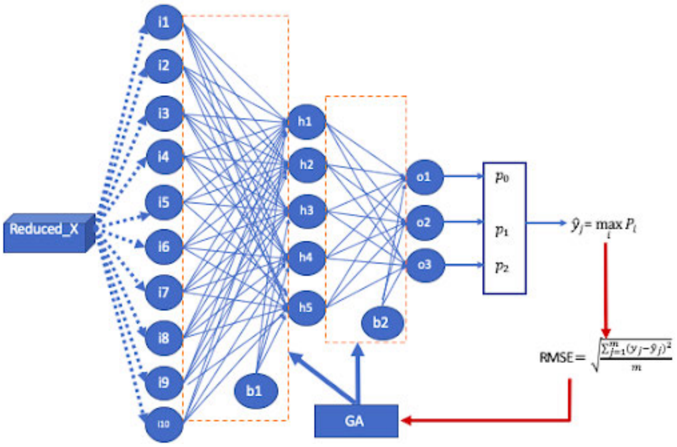


FIGURE 4. Proposed hybrid model of ANN and GA.

as the stopping criterion for the algorithm for both training and validation purposes. The convergence of the proposed algorithm towards optimal weights of the ANN is shown separately for training and validation in Fig.5. From this figure, it can be observed that the proposed model converged to optimal weights during 10,000 iterations during training with for training, while for validation, it converged during 45,000 iterations.

B. PERFORMANCE OF THE PROPOSED MODEL

The prediction accuracy of the proposed model is shown in Fig.6. The class-wise performance of the proposed model in terms of precision, recall, f1-score, and accuracy is presented in Table 2. Furthermore, the confusion matrix generated by the proposed model is depicted in Fig.7.

C. COMPARISON OF THE PROPOSED MODEL WITH BPN

The backpropagation neural network with a gradient descent algorithm is simulated over training and validation datasets using a five-fold cross-validation technique. Additionally, one more hidden layer is added to this BPN to increase

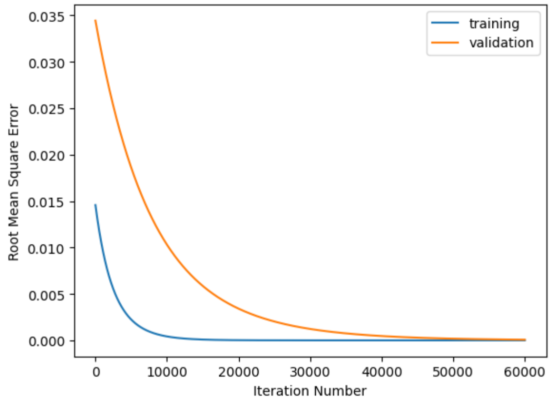


FIGURE 5. Computed root mean square error for training and validation of the proposed model.

TABLE 2. Performance of the proposed model.

Attack type	Code	precision	recall	f1-score	Accuracy
Benign	0	1.00	1.00	1.00	0.99
GPS jamming	1	1.00	0.99	0.99	
GPS spoofing	2	0.97	1.00	0.99	

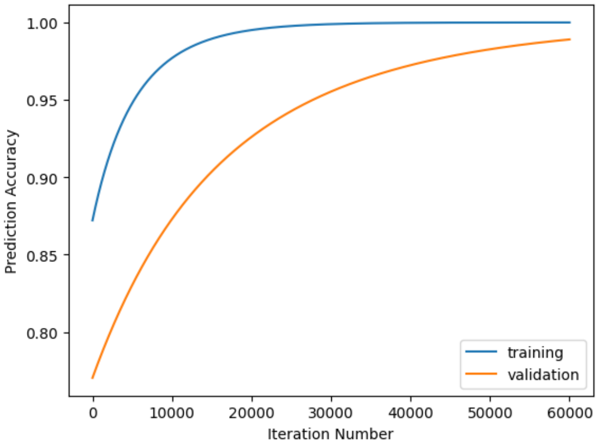


FIGURE 6. Prediction accuracy of the proposed model during training and validation.

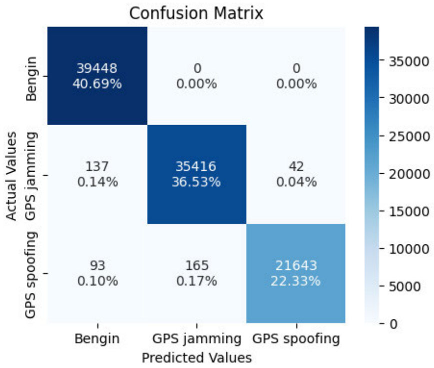


FIGURE 7. Confusion matrix.

prediction accuracy, since the hidden layer intrinsically extracts features during training and validation. The Fig.8 depicts the convergence of these methods during their training. The proposed model converges to optimal weights at around 30000 iterations as opposed to no convergence by BPN and BPN + 1 HL even after 80000 iterations. Further, the prediction accuracy of BPN i.e. 0.895 as compared to the proposed model is not that much appreciable. The addition of one hidden layer to BPN significantly increases its prediction accuracy to 0.9324 which is 6% less than that of the proposed model. The comparison of the prediction accuracy of the proposed model, BPN, and BPN with one extra hidden layer is shown in Fig.9 and Table 3.

D. COMPARISON OF THE PROPOSED MODEL AGAINST OTHER CLASSIFIERS

The performance of the proposed model is compared with other classifiers such as Naive Byes, Random forest, Support vector machine, k-nearest classifier, BPN, and BPN with one extra hidden layer (Table 3). The performance metrics considered for this comparison are precision, recall, f1-score, and accuracy. Additionally, this table also shows the macro average precision, macro average recall, and macro average f1 score for a better way to compare the performance of different classifiers.

This table reveals that the proposed model outperforms the other classifiers in terms of the different metrics. Furthermore, the accuracy of the proposed model is at least 6% more than these classifiers.

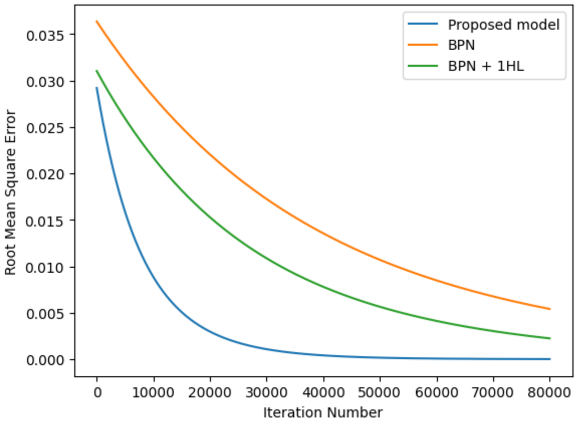


FIGURE 8. Comparison of convergence of proposed model, BPN and BPN with one extra hidden layer.

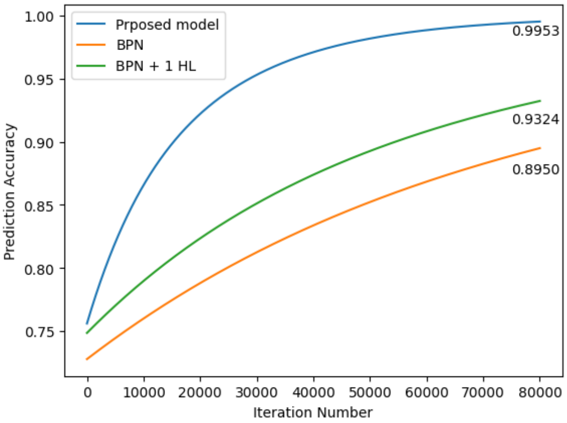


FIGURE 9. Comparison of prediction accuracy of proposed model, BPN and BPN with one extra hidden layer.

E. COMPARISON OF THE PROPOSED MODEL AGAINST OTHER CLASSIFIERS IN TERMS OF COMPUTATIONAL TIME

The computational time required by the different classifiers and the proposed model is shown in Fig.10. This figure reveals the fact that the computational time required by the proposed method is much less than that required by other classifiers. The reason for such a shorter time requirement for the proposed method is due to the embedding of GA into this model to find the optimal weights. In contrast to this, the BPN uses a backpropagation algorithm which converges very slowly. Additionally, the other classifiers require more and/or

TABLE 3. Comparison of performance of the proposed model and other classifiers.

Classifier	Attack type	Micro Average			Macro Average			Accuracy
		Precision	Recall	f1-score	Precision	Recall	f1-score	
Naive Bayes	Benign	0.95	0.93	0.95	0.93	0.91	0.93	0.93
	GPS jamming	0.92	0.91	0.92				
	GPS spoofing	0.93	0.91	0.92				
Random forest	Benign	0.94	0.93	0.94	0.93	0.92	0.93	0.935
	GPS jamming	0.94	0.92	0.94				
	GPS spoofing	0.93	0.91	0.92				
SVM	Benign	0.94	0.93	0.94	0.94	0.92	0.93	0.938
	GPS jamming	0.95	0.93	0.94				
	GPS spoofing	0.94	0.92	0.93				
kNN	Benign	0.93	0.91	0.91	0.92	0.9	0.9	0.915
	GPS jamming	0.91	0.90	0.90				
	GPS spoofing	0.92	0.90	0.91				
BPN	Benign	0.9	0.87	0.89	0.9	0.88	0.89	0.895
	GPS jamming	0.89	0.88	0.89				
	GPS spoofing	0.91	0.89	0.9				
BPN+ 1 HL	Benign	0.94	0.92	0.94	0.93	0.91	0.93	0.932
	GPS jamming	0.93	0.91	0.93				
	GPS spoofing	0.93	0.92	0.93				
Proposed model	Benign	1.00	1.00	1.00	0.99	0.99	0.99	0.995
	GPS jamming	1.00	0.99	0.99				
	GPS spoofing	0.97	1.00	0.99				

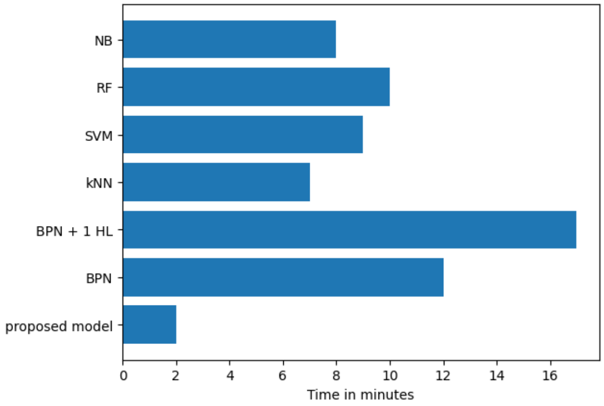


FIGURE 10. Comparison of computational time required by the proposed method and other classifiers.

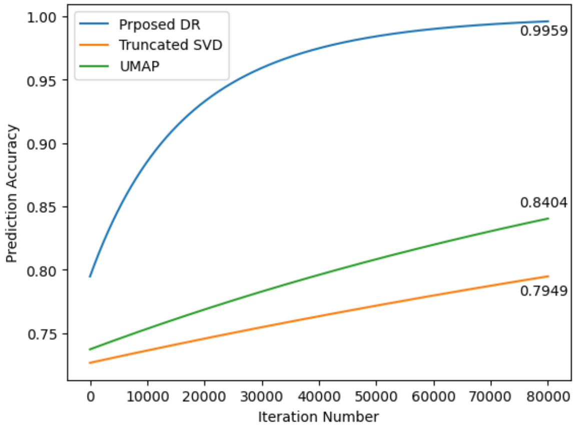


FIGURE 11. Comparison of the proposed dimensionality reduction technique against Truncated SVD and UMAP in terms of accuracy generated by the proposed model.

complex parameters for training and validation. kNN being a lazy learner requires approximately 7 minutes followed by other classifiers. In this list, the BPN+1 HL requires the highest computational time.

F. COMPARISON OF THE PROPOSED DIMENSIONAL TECHNIQUE AGAINST OTHER SIMILAR TECHNIQUES

The proposed dimensional reduction technique is compared against some recent techniques like truncated singular value decomposition (SVD) and Uniform Manifold Approximation and Projection (UMAP). The truncated SVD performs factorization on the data matrix and is well-suited for a sparse matrix. UMAP is a manifold learning and dimension reduction technique that can deal with higher dimensional data efficiently. These techniques, along with the proposed dimensional reduction technique, are applied to the initial dataset (X) separately. The proposed model is trained and validated over these reduced datasets. The prediction accuracy of the proposed model over these datasets is plotted and shown in Fig.11. This figure clearly depicts the beneficial effects of the proposed method over other methods, as it measures the correlation coefficient and information gain of each feature against the target class before discarding the features, thereby reducing some degree of sparsity. In contrast to this, truncated SVD and UMAP work directly on the dataset to reduce the number of features to appropriate numbers. It can be noted here that the zeros are also converted to their counter-values during such a reduction process. Hence, the accuracy of the proposed model sharply decreases to 0.8404 and 0.79 for reduced datasets generated by UMAP and truncated SVD.

G. COMPETENCY OF THE PROPOSED MODEL FOR DIFFERENT DATASETS

In order to evaluate the competency of the proposed model, it is applied to two datasets (KDD99 and UNSW-NB 15 [31]) widely used for intrusion detection systems.

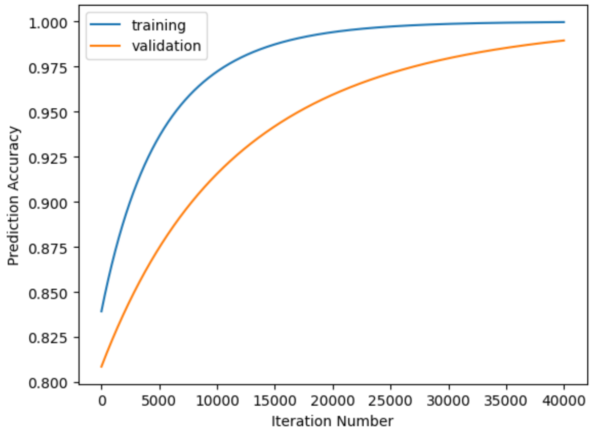


FIGURE 12. Accuracy of the proposed model over KDD99 dataset.

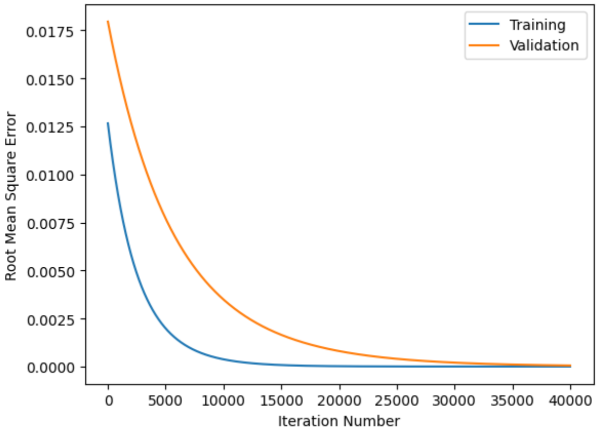


FIGURE 13. Generated RMSE by the proposed model over KDD99 dataset.

After performing an initial read operation, the number of records and features in the KDD99 dataset is 494021 and 43 (excluding categorical features), respectively. The dataset does not contain missing values, and most values are nonzero. The proposed dimensional reduction technique is applied to this data to yield only 13 features. The proposed model is trained and validated over this dataset with a split of 70% to 30%, respectively. The prediction accuracy and root mean square error generated during training and validation are shown in Fig.12 and Fig.13.

The training data of the UNSW-NB 15 dataset are only considered for this study which comprises of 2934817 records and 19 features. The number of zeros present in this dataset is 5684348 (excluding one categorical feature) while the total number of value counts is 52826706. Thus, the calculated sparsity for this dataset is 0.1. The proposed dimensional reduction technique reduces the number of features to 13. The proposed model is trained and validated on the training and validation dataset. The prediction accuracy and root mean square error generated during the training and validation are shown in Fig. 14 and Fig.15 respectively. The proposed model is well-converged to optimal weights of ANN for both cases.

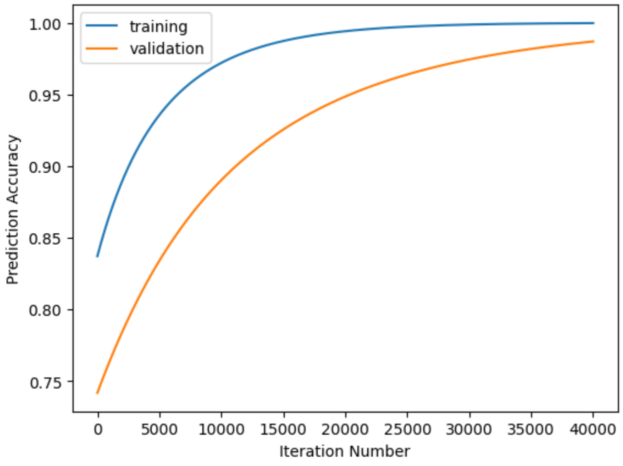


FIGURE 14. Accuracy of the proposed model over UNSW-NB 15 dataset.

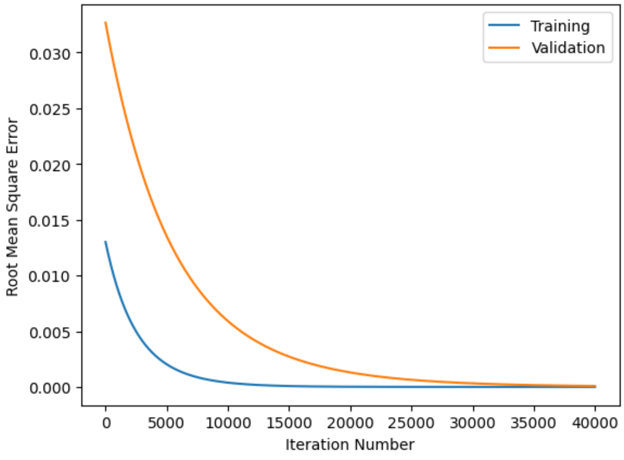


FIGURE 15. Generated RMSE by the proposed model over UNSW-NB 15 dataset.

VI. CONCLUSION

UAVs or drones have seen exponential growth in recent years, ushering in a new era of aviation in which unmanned aerial vehicles are used for both commercial and military purposes. These autonomous vehicles offer numerous benefits owing to their characteristics such as adaptability, user-friendliness, low operating costs, and minimal energy usage. However, due to their widespread application in mission-critical environments, modern UAVs are subject to a wide range of security threats, including spoofing, command injection, jamming, and denial of service, among others. As the severity of these threats becomes more apparent, intelligent intrusion detection systems are gaining importance as a vital security tool against these attacks. In light of the enormously complicated and diversified nature of attacks, an algorithmic approach becomes impractical, and it is essential to adapt machine learning-based decision-making solutions generated through intelligent analysis of massive datasets. Artificial intelligence approaches provide mechanisms to collect, analyze, and use network traffic to further train the AI model and, subsequently, provide efficient network protection with minimal false positives. The work carried out in this paper introduces a new dimensional reduction approach based on correlation coefficient, information gain, and principal component analysis to reduce the dimension of the UAV Attack Dataset. Furthermore, we have designed a novel intrusion detection system that uses a combination of ANN and GA. The ideal weights of the artificial neural network are generated with the application of a genetic algorithm. Both the backpropagation network and its variant are compared to the proposed model in terms of convergence and prediction accuracy. Additionally, competing classifiers are evaluated against the performance of the proposed model. This analysis demonstrates that the proposed model outperforms competing classifiers by at least 6% in terms of prediction accuracy while simultaneously saving a significant amount of time. Lastly, the proposed model, being light in terms of parameters, can be embedded directly into the UAV to prevent and respond to threats.

The proposed IDS can be employed in UAVs to enhance security in critical applications such as military operations by training and validating it over real-time attacks. This will indeed make it a robust system capable of dealing with adversarial attacks. Finally, IDS could be used to detect and prevent data exfiltration from UAVs. This could be achieved by using IDS to monitor the UAV's communication network and detect any data exfiltration attempts.

ACKNOWLEDGMENT

The authors express their gratitude to the esteemed reviewers for their constructive feedback on the improvement of the presented work in this article.

REFERENCES

[1] G. O. Young, "Synthetic structure of industrial plastics," in *Plastics*, vol. 3, 2nd ed., J. Peters, Ed. New York, NY, USA: McGraw-Hill, 1964, pp. 15–64.

[2] W.-K. Chen, *Linear Networks and Systems*. Belmont, CA, USA: Wadsworth, 1993, pp. 123–135.

[3] C. Stöcker, R. Bennett, F. Nex, M. Gerke, and J. Zevenbergen, "Review of the current state of UAV regulations," *Remote Sens.*, vol. 9, no. 5, p. 459, May 2017.

[4] P. S. Ramesh and J. M. L. Jeyan, "Comparative analysis of the impact of operating parameters on military and civil applications of mini unmanned aerial vehicle (UAV)," *AIP Conf.*, vol. 2311, no. 1, Dec. 2020, Art. no. 030034.

[5] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: A survey," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 95–101, Feb. 2020.

[6] D. Kucherov, A. Kozub, and O. Kostyna, "Group behavior of UAVs in obstacles presence," in *Proc. 4th Int. Conf. Methods Syst. Navigat. Motion Control (MSNMC)*, Oct. 2016, pp. 51–54.

[7] C. Gudla, M. S. Rana, and A. H. Sung, "Defense techniques against cyber attacks on unmanned aerial vehicles," in *Proc. Int. Conf. Embedded Syst., Cyber-Phys. Syst., Appl. (ESCS)*, 2018, pp. 110–116.

[8] A. Tabassum, A. Erbad, and M. Guizani, "A survey on recent approaches in intrusion detection system in IoTs," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 1190–1197.

[9] C. A. Pushpam and J. G. Jayanthi, "Methodical survey on IDS with feature selection," in *Proc. 2nd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Jul. 2020, pp. 606–613.

[10] S. Lipsa and R. K. Dash, "A novel intrusion detection system based on deep learning and random forest for digital twin on IoT platform," *Int. J. Scholarly Res. Eng. Technol.*, vol. 2, no. 1, pp. 51–64, Mar. 2023.

[11] S. Lipsa and R. K. Dash, "A novel dimensionality reduction strategy based on linear regression with a fine-pruned decision tree classifier for detecting DDoS attacks in cloud computing environments," in *Proc. 1st Int. Symp. Artif. Intell. (ISAI)*, Haldia, India, Feb. 2022, pp. 15–25.

[12] X. Tan, S. Su, Z. Zuo, X. Guo, and X. Sun, "Intrusion detection of UAVs based on the deep belief network optimized by PSO," *Sensors*, vol. 19, no. 24, p. 5529, Dec. 2019.

[13] N. Moustafa and A. Jolfaei, "Autonomous detection of malicious events using machine learning models in drone networks," in *Proc. 2nd ACM MobiCom Workshop Drone Assist. Wireless Commun. 5G Beyond*, Sep. 2020, pp. 61–66.

[14] R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, "Machine-learning-enabled intrusion detection system for cellular connected UAV networks," *Electronics*, vol. 10, no. 13, p. 1549, Jun. 2021.

[15] O. Bouhamed, O. Bouachir, M. Aloqaily, and I. A. Ridhawi, "Lightweight IDS for UAV networks: A periodic deep reinforcement learning-based approach," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2021, pp. 1032–1037.

[16] L. Wang, Y. Chen, P. Wang, and Z. Yan, "Security threats and countermeasures of unmanned aerial vehicle communications," *IEEE Commun. Standards Mag.*, vol. 5, no. 4, pp. 41–47, Dec. 2021.

[17] A. A. Khan, M. M. Khan, K. M. Khan, J. Arshad, and F. Ahmad, "A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs," *Comput. Netw.*, vol. 196, Sep. 2021, Art. no. 108217.

[18] H. Bangui and B. Buhnova, "Recent advances in machine-learning driven intrusion detection in transportation: Survey," *Proc. Comput. Sci.*, vol. 184, pp. 877–886, Jan. 2021.

[19] Z. Chen, N. Lyu, K. Chen, Y. Zhang, and W. Gao, "UAV network intrusion detection method based on spatio-temporal graph convolutional network," *J. Beijing Univ. Aeronaut. Astronaut.*, vol. 47, no. 5, pp. 1068–1076, 2021.

[20] E. Basan, M. Lapina, N. Mudruk, and E. Abramov, "Intelligent intrusion detection system for a group of UAVs," in *Proc. 12th Int. Conf. Adv. Swarm Intell. (ICSI)*. Qingdao, China: Springer, Jul. 2021, pp. 230–240.

[21] V. Praveena, A. Vijayaraj, P. Chinnasamy, I. Ali, R. Alroobaea, S. Y. Alyahyan, and M. A. Raza, "Optimal deep reinforcement learning for intrusion detection in UAVs," *Comput., Mater. Continua*, vol. 70, no. 2, pp. 2639–2653, 2022.

[22] J. Whelan, A. Almehmadi, and K. El-Khatib, "Artificial intelligence for intrusion detection systems in unmanned aerial vehicles," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107784.

[23] Q. A. Al-Haija and A. Al Badawi, "High-performance intrusion detection system for networked UAVs via deep learning," *Neural Comput. Appl.*, vol. 34, no. 13, pp. 10885–10900, 2022.

[24] R. Fotohi, M. Abdan, and S. Ghasemi, "A self-adaptive intrusion detection system for securing UAV-to-UAV communications based on the human immune system in UAV networks," *J. Grid Comput.*, vol. 20, no. 3, p. 22, Sep. 2022.

[25] X. He, Q. Chen, L. Tang, W. Wang, and T. Liu, "CGAN-based collaborative intrusion detection for UAV networks: A blockchain-empowered distributed federated learning approach," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 120–132, Jan. 2023.

[26] E. Basan, A. Basan, A. Nekrasov, C. Fidge, E. Abramov, and A. Basyuk, "A data normalization technique for detecting cyber attacks on UAVs," *Drones*, vol. 6, no. 9, p. 245, Sep. 2022.

[27] K. A. Alissa, S. S. Alotaibi, F. S. Alrayes, M. Aljebreen, S. Alazwari, H. Alshahrani, M. A. Elfaki, M. Othman, and A. Motwakel, "Crystal structure optimization with deep-autoencoder-based intrusion detection for secure Internet of Drones environment," *Drones*, vol. 6, no. 10, p. 297, Oct. 2022.

[28] J. Escorcia-Gutierrez, M. Gamarra, E. Leal, N. Madera, C. Soto, R. F. Mansour, M. Alharbi, A. Alkhayyat, and D. Gupta, "Sea turtle foraging algorithm with hybrid deep learning-based intrusion detection for the Internet of Drones environment," *Comput. Electr. Eng.*, vol. 108, May 2023, Art. no. 108704.

[29] V. Subbarayalu and M. A. Vensuslaus, "An intrusion detection system for drone swarming utilizing timed probabilistic automata," *Drones*, vol. 7, no. 4, p. 248, Apr. 2023.

[30] J. Whelan, T. Sangarapillai, O. Minawi, A. Almehmadi, and K. El-Khatib, "UAV attack dataset," IEEE Dataport, 2020, doi: 10.21227/00dg-0d12.

[31] S. Choudhary and N. Kesswani, "Analysis of KDD-cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT," *Proc. Comput. Sci.*, vol. 167, pp. 1561–1573, Jan. 2020.

[32] Z. Ma, G. Wu, P. N. Suganthan, A. Song, and Q. Luo, "Performance assessment and exhaustive listing of 500+ nature-inspired metaheuristic algorithms," *Swarm Evol. Comput.*, vol. 77, Mar. 2023, Art. no. 101248, doi: 10.1016/j.swevo.2023.101248.

[33] A. A. Heidari, S. Mirjalili, H. Faris, I. Aljarah, M. Mafarja, and H. Chen, "Harris hawks optimization: Algorithm and applications," *Future Gener. Comput. Syst.*, vol. 97, pp. 849–872, Aug. 2019, doi: 10.1016/j.future.2019.02.028.

[34] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey wolf optimizer," *Adv. Eng. Softw.*, vol. 69, pp. 46–61, Mar. 2014, doi: 10.1016/j.advengsoft.2013.12.007.

[35] D. Molina, F. Moreno-García, and F. Herrera, "Analysis among winners of different IEEE CEC competitions on real-parameters optimization: Is there always improvement?" in *Proc. IEEE Congr. Evol. Comput. (CEC)*, Donostia, Spain, Jun. 2017, pp. 805–812, doi: 10.1109/CEC.2017.7969392.

[36] A. P. Piotrowski, J. J. Napiorkowski, and A. E. Piotrowska, "Choice of benchmark optimization problems does matter," *Swarm Evol. Comput.*, vol. 83, Dec. 2023, Art. no. 101378, doi: 10.1016/j.swevo.2023.101378.

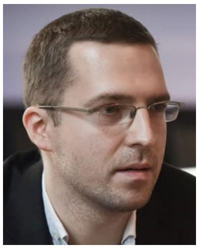
KORHAN CENGIZ (Senior Member, IEEE) was born in Edirne, Turkey, in 1986. He received the B.Sc. degree in electronics and communication engineering from Kocaeli University, in 2008, the B.Sc. degree in electronics and communication engineering from the Faculty of Business Administration, Anadolu University, Turkey, in 2009, the M.Sc. degree in electronics and communication engineering from Namik Kemal University, Turkey, in 2011, and the Ph.D. degree in electronics engineering from Kadir Has University, Turkey, in 2016. Since August 2021, he has been an Assistant Professor with the College of Information Technology, University of Fujairah, United Arab Emirates. Since April 2022, he has been the Chair of the Research Committee of the University of Fujairah. Since September 2022, he has been an Associate Professor with the Department of Computer Engineering, Istinye University, Istanbul, Turkey. He is currently the author of more than 40 SCI/SCI-E articles, including IEEE INTERNET OF THINGS JOURNAL, IEEE ACCESS, *Expert Systems with Applications*, *Knowledge-Based Systems*, and *ACM Transactions on Sensor Networks*; five international patents; more than ten book chapters; and one book in Turkish. He presented more than 40 keynote talks at reputed IEEE and Springer Conferences about WSNs, the IoT, and 5G. His research interests include wireless sensor networks, wireless communications, statistical signal processing, indoor positioning systems, the Internet of Things, power electronics, and 5G. He is a Professional Member of ACM. His awards and honors, including the Tubitak Priority Areas Ph.D. Scholarship, the Kadir Has University Ph.D. Student Scholarship, the Best Presentation Award from ICAT 2016 Conference, and the Best Paper Award from ICAT 2018 Conference. He is an Associate Editor of IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, *IEEE Potentials Magazine*, *IET Electronics Letters*, and *IET Networks*. He is a Handling Editor of *Microprocessors and Microsystems* (Elsevier). He is an editor of more than 20 books. He serves several book editor positions for IEEE, Springer, Elsevier, Wiley, and CRC. He serves several reviewer positions for IEEE INTERNET OF THINGS JOURNAL, IEEE SENSORS JOURNAL, and IEEE ACCESS.

SWATI LIPSA received the B.Tech. and M.Tech. degrees from the Biju Patnaik University of Technology, Rourkela, Odisha, India, in 2008 and 2013, respectively. She is currently an Assistant Professor with the Department of Information Technology, Odisha University of Technology and Research, Bhubaneswar, Odisha, India. She has a good number of publications in different international journals/conferences. Her research interests include wireless sensor networks, cloud computing, network security, machine learning, and software-defined networking.

RANJAN KUMAR DASH (Senior Member, IEEE) received the Ph.D. degree from Sambalpur University, Sambalpur, Odisha, India, in 2008. Currently, he is a Professor and the Head of the Department of Information Technology, Odisha University of Technology and Research, Bhubaneswar, Odisha, India. He has more than 44 publications in different international journals/conferences. His primary research interests include the reliability of distributed systems, wireless sensor networks, soft computing, machine learning, and cloud computing. His current research focus is on enhancing processor performance and energy consumption through the use of machine-learning techniques. He has served on the technical program and organization committees for several conferences.

NIKOLA IVKOVIĆ (Senior Member, IEEE) was born in Zagreb, Croatia, in 1979. He received the M.S. degree in computing and the Ph.D. degree in computer science from the Faculty of Electrical Engineering and Computing, University of Zagreb. His Ph.D. thesis was in the area of swarm and evolutionary computation.

He was the Head of the Department of Computing and Technology, Faculty of Organization and Informatics, University of Zagreb, where he is currently an Assistant Professor. He is a member of two research laboratories—Artificial Intelligence Laboratory and the Laboratory for Generative Programming and Machine Learning, Faculty of Organization and Informatics, University of Zagreb. He teaches computer networks, operating systems, and computer architecture-related courses. He gave several invited talks at international scientific conferences and the guest lectures with different universities in Europe and Asia. His research interests include computational intelligence and optimization, especially swarm intelligence, and also computer networks, security, and formal methods. He was a member of committees for creating new university study programs. He won the Best Presentation Award from the International Conference on Computer Technology and Development (IACT 2015) in Singapore and the International Conference on Frontiers of Intelligent Technology (ICFIT 2018) in Paris and the Excellent Presentation Award from the International Conference on Computer Science and Information Technology (ICCSIT 2016) in Ireland. He joined the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE), in 2008. He serves as a regular reviewer for high-quality scientific journals and takes part in a number of international conference committees.



MARIO KONECKI is currently an Associate Professor with the Faculty of Organization and Informatics, University of Zagreb, Croatia. During his previous work, he as the author or coauthor, published 78 scientific, 20 professional articles, and one faculty textbook. He participated in eight scientific and eight professional projects, and seven of his published scientific articles were awarded awards for the best scientific paper. His main research interests include education, user interface design, web technologies, video game development, artificial intelligence, and assistive technologies. He is a member of the program and organizing committees of a number of scientific and professional conferences. He is a member of the editorial board of several scientific publications. In 2016, he was awarded the award for his contribution to society and volunteering. He has received several awards and recognitions for scientific, teaching, and professional work.