IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 15 March 2024, accepted 4 April 2024, date of publication 9 April 2024, date of current version 23 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3386570

RESEARCH ARTICLE

Modified Marine Predators Algorithm With Deep Learning-Driven Security Solution for IoT-Assisted UAV Networks

S. ANANTHA BABU[1], ABADHAN RANGANATH[2], MANISH M. GOSWAMI[3], T. GNANAPRAKASAM[4], AND MOHAMAD KHAIRI ISHAK[5]

[1]School of Computer Science and Engineering, Presidency University, Bengaluru 560064, India
[2]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, Telangana 500075, India
[3]S. B. Jain Institute of Technology, Management and Research, Nagpur 441501, India
[4]Department of CSE, Alliance University, Bengaluru 560076, India
[5]Department of Electrical and Computer Engineering, Ajman University, Ajman, United Arab Emirates

Corresponding author: Mohamad Khairi Ishak (m.ishak@ajman.ac.ae)

This work was supported in part by the Ajman University, United Arab Emirates.

ABSTRACT Unmanned Aerial Vehicles (UAVs) are advanced technologies that are initially utilized for military apps like border monitoring and reconnaissance in opposed territories. Internet of Things (IoTs) assisted UAV networks suggest the combination of IoT technology with UAVs to generate a networked system that improves the abilities and utility of UAVs for several apps. UAVs' inherent features namely quick deployment, high dynamicity, low deployment and operational costs, and line of sight communication motivated researchers in the IoT field to assume UAV's combination into IoT systems near the concept of UAV-assisted IoT systems. However, security concerns with UAVs are evolving as UAV nodes are suitable attractive targets for cyber threats because of extremely developing volumes and poor and weak inbuilt security. Therefore, this paper presents a Modified Marine Predators Algorithm with a Deep Learning-Driven intrusion detection (MMPADL-ID) approach for IoT Assisted UAV Networks. The presented MMPADL-ID technique proposes to identify and classify the presence of intrusions in accomplishing security in IoT-assisted UAV networks. In the MMPADL-ID technique, the feature selection process is performed by the design of MMPA. In addition, the MMPADL-ID technique incorporates the Elman neural network (ENN) model for the recognition and classification of the intrusions. Furthermore, the honey badger algorithm (HBA) can be applied for the hyperparameter tuning of the ENN model and results in improved performance. The simulation value of the MMPADL-ID technique can be tested on benchmark datasets. An extensive comparative outcome reported the better solution of the MMPADL-ID algorithm with existing approaches for various aspects.

INDEX TERMS Intrusion detection system, unmanned aerial vehicles, Internet of Things, security, deep learning.

I. INTRODUCTION

As UAVs become most popular in smart cities, safety and privacy issues are increased accordingly [1]. The IoTs are employed by drones to offer inter-location services for navigation. IoT-based UAV networks are different and comprised of environmental monitoring, precision agriculture, infrastructure assessment, search and rescue, disaster response, etc. These networks can have the ability to revolutionize industries by offering real-time data and insights, which were earlier challenging or expensive to attain [2]. The application of UAVs increases the problems of unauthorized access and safety breaches for sensitive data. As UAVs collect and transfer an enormous quantity of data, privacy issues, and intrusion detection and avoidance must be important [3]. An extensive incorporation of UAVs in smart cities could

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

be presented as a new measurement of public safety and urban management. These multipurpose aircraft provide real-time data-gathering capacity through different fields in traffic monitoring to disaster response [4]. However, this development raises a major problem: ensuring the security and confidentiality of gathered and transferred information [5].

The major problem is the vulnerability of UAV networks to intrusions that have serious effects on data integrity and public security [6]. Since, UAVs become essential for core applications, protecting their functions against possible attacks has become preeminent. Moreover, the sensitive type of data control requires robust privacy-maintaining processes. A UAV-based intrusion detection system (UAV-IDS) is established for identifying anomalous behavior or illegitimate actions in a network by automatically evaluating the activities or behaviors depending on certain strategies and hypotheses that have been directed by the security guidelines of the specified network [7]. The UAV-IDS monitors the network transmission, data files, and system configuration for analyzing if occur the attacks. Current security protection is often reduced to overcome the particular difficulties caused by UAV utilization in smart cities [8]. This space in present solutions highlights the requirement for a specific architecture precisely developed for this condition. In addition, the existing landscape of UAV privacy and security measures shortages a tailored and wide-ranging algorithm for smart cities [9]. Numerous present techniques consider conventional network security methods, managing the complexities of UAV functions. Also, privacy-maintaining approaches are not commonly considered for the dynamic type of UAV networks, resulting in suboptimum security [10].

This study presents a Modified Marine Predators Algorithm with a Deep Learning-Driven intrusion detection (MMPADL-ID) approach for IoT Assisted UAV Networks. In the MMPADL-ID technique, the feature selection (FS) process is performed by the design of MMPA. In addition, the MMPADL-ID technique incorporates the Elman neural network (ENN) model for the recognition and classification of the intrusions. Furthermore, the honey badger algorithm (HBA) can be applied for the hyperparameter tuning of the ENN model and results in improved performance. The simulation value of the MMPADL-ID technique can be tested on benchmark datasets.

II. RELATED WORKS

Ntizikira et al. [11] presented the Security and Privacy-Preserving Intrusion Detection and Prevention for UAVS (SP-IoUAV) method. Significant to this method was the incorporation of DNNs such as the CNN-LSTM network. Additionally, multi-factor authentication (MFA) improves access security. In [12], this study deployed a novel functional encryption (FE) algorithm. Securing the data transmission amongst FE, UE, MBS, and UAV methods is performed in the network in 2-stages: the primary stage is among MBS and UE whereas the secondary stage is among UE and MBS using UAV. In the execution, the Dolev-Yao attack framework has been examined that intruders are capable of intercepting or varying the UE data. He et al. [13] developed a conditional GAN (CGAN)-based collective IDS with blockchain (BC)-authorized distributed federated learning. This analysis presented LSTM in the CGAN training. The aggregated data with CGAN is employed as augmented data. This technique permits combined training of the CGAN model. Wang et al. [14] designed an ID attack-defense game for IoT systems. This consideration makes an analytical structure. In [15], a Federated Continuous Learning model with a Stacked Broad Learning System (FCL-SBLS) relying on a Digital Twin Network (DTN) was developed. An asynchronous federated learning model has been utilized and a Deep Deterministic Policy Gradient (DDPG)-based UAV chosen technique helped by DTN was developed.

Fotohi et al. [16] implemented a technique named SID-UAV. The SID-UAV approach employs a self-matching model, which comprises different stages namely the path detection and analysis, destructive UAV response, decision-making, and registration of the information database. Cheema et al. [17] employed a BC-assisted registration and authentication technique. This method considered several communication-related features namely the large count of connections a drone can support, backhaul limitations, and available bandwidth. In [18], a fog computing-based smart agricultural model was introduced. This technique accepts the notion of a charging token then, accomplishing a trip, UAVs obtain tokens from the fog node. IDS was utilized at the fog nodes, which could be implemented in ML techniques for classifying UAV behavior as normal or malicious. Gao et al. [19] developed an enhanced multi-objective genetic technique, which integrates a natural chromosome encoding format and specially constructed genetic operators. An effectual unlocking approach is also built. In [20], a combined mathematical model implementing a novel bi-level iteration optimization technique is introduced, addressing the deployment coordination, sortie, and maintenance for carrier-based aircraft in maritime distributed operations.

III. THE PROPOSED MODEL

In this study, we have developed and designed an automated intrusion detection, named MMPADL-ID technique on the IoT-assisted UAV networks. The presented MMPADL-ID technique's purpose is to identify and classify the presence of intrusions in accomplishing security in IoT-assisted UAV networks. In the MMPADL-ID system, the 3 main procedures are contained such as MMPA-based FS, ENN-based classification, and HBA-based hyperparameter tuning. Fig. 1 represents the entire flow of the MMPADL-ID approach.

A. FEATURE SELECTION USING MMPA

In this work, the MMPA is applied to choose the features from the network data. MPA is a metaheuristic algorithm and is further modified with an entropy algorithm named Reyni

Entropy [21]. MPA is stimulated by the behaviors of marine predators while foraging the prey where the predator uses Levy's and Brownian strategies as their optimum foraging mechanism. The velocity ratio v of prey towards the predator creates a trade-off between Brownian and Levy's movements. If v is smaller or equivalent to 0.1, the optimum approach for the predator to move in the L'evy step (exploration stage) irrespective of once the prey moves in Levy's or Brownian strategy. But if v is equivalent to 1 after the optimum technique for the predator moves in Brownian step once the prey moves in Levy's step. Lastly, if $> 10v$, the predator does not move, irrespective of whether the prey moves in Levy's or Brownian because it comes in itself (exploitation stage). The MPA algorithm can be mathematically modeled as follows:

Initialization: the primary outcome can distribute uniformly with the searching region utilizing the subsequent equation, whereas $A\in$ Fusion (k).

$$\vec{x} = A_{\min} + \vec{i} \otimes (A_{\max} - A_{\min}) \tag{1}$$

In Eq. (1), $A_{\min}$ and $A_{\max}$ signify the vectors with low and up boundaries. $i\rightarrow$ represents a random vector and the component-wise multiplication is $\otimes$.

Elite and *Prey* matrix construction: According to the survival of fitness model, the top predator is optimum at hunting. Therefore, the topmost predator constructs a matrix named Elite.

$$Elite = \begin{pmatrix} A^1_{1,1} & A^1_{1,2} & \cdots & \cdots & A^1_{1,d} \\ A^1_{2,1} & A^1_{2,1} & \cdots & \cdots & A^1_{2,d} \\ A^1_{N,1} & A^1_{N,2} & \cdots & \cdots & A^1_{N,d} \end{pmatrix} \tag{2}$$

In Eq. (2), the top predator vector is $A^1\rightarrow$and simulated N times to build up the *elite* matrix and the number of dimensions is d. N is the number of individuals. If the top predator is updated, this matrix is updated at the iteration end. Another matrix, p, is *Prey* and has a similar dimension as Elite and is used by the predator for updating the position:

$$\vec{P} \begin{pmatrix} A^1_{1,1} & A^1_{1,2} & \cdots & \cdots & A^1_{1,d} \\ A^1_{2,1} & A^1_{2,1} & \cdots & \cdots & A^1_{2,d} \\ A^1_{N,1} & A^1_{N,2} & \cdots & \cdots & A^1_{N,d} \end{pmatrix} \tag{3}$$

In Eq. (3), the *nth* dimensional of d Prey is $A_{N,d}$. The optimization technique comprises three stages, low-velocity ratio, high-velocity ratio, and unit-velocity ratio. The prey quickly finds the food during the high-velocity ratio, and it is defined mathematically:

$$if\ t < \frac{1}{3} t_{\max} \tag{4}$$

$$\vec{V}_i = \vec{R}_x \otimes \left(E\vec{l}ite_i - \vec{R}_x \otimes \vec{P}_i \right) \tag{5}$$

$$\vec{P}_i = \vec{P}_i + F.\vec{N} \otimes \vec{V}_i \tag{6}$$

Here, the numerical vector is represented by $\vec{R}_x$, the component-wise multiplication is indicated as $\otimes$, the set numerical value that is 0.4 denotes F, the numerically generated random vector is $\vec{N}$, t and $t_{\max}$ are current and maximum iterations, correspondingly. Next, the unit velocity ratio-based transition stage is given as follows:

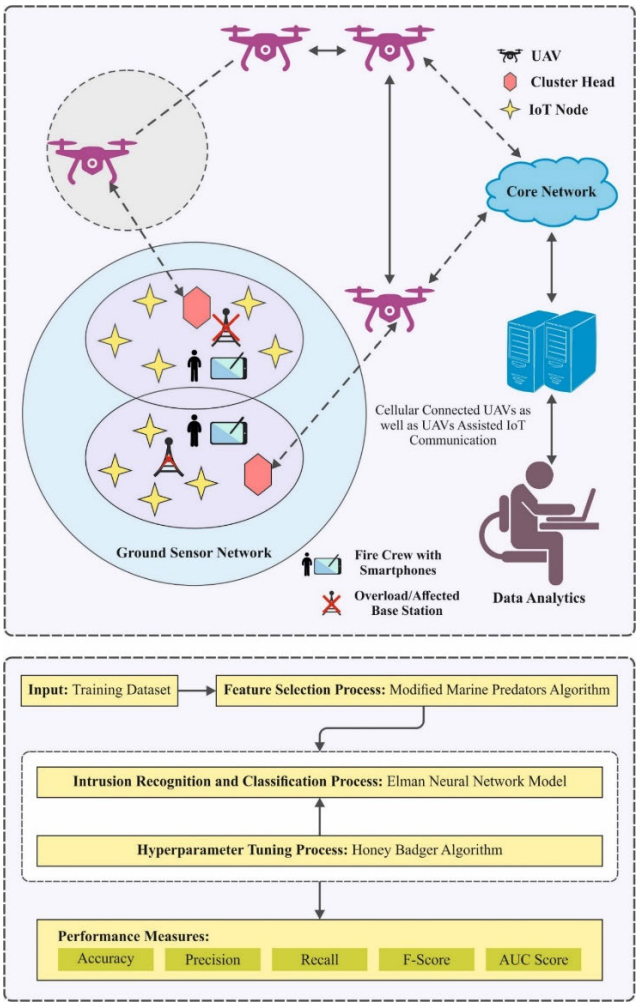

FIGURE 1. The overall flow of the MMPADL-ID approach.

$$if\ \frac{1}{3} t_{\max} < t < \frac{2}{3} t_{\max} \tag{7}$$

Initially, the population is evaluated by Eq. (8):

$$\vec{V}_i = \vec{R}_x \otimes \left(E\vec{l}ite_i - \vec{R}_L \otimes \vec{P}_i \right) \tag{8}$$

$$\vec{P}_i = \vec{P}_i + F.\vec{N} \otimes \vec{V}_i \tag{9}$$

Next, the population is estimated using the following equations:

$$\vec{V}_i = \vec{R}_B \otimes \left(\vec{R}_B \otimes E\vec{l}te_i - \vec{P}_i \right) \tag{10}$$

$$\vec{P}_i = \vec{P}_i + F.AP \otimes \vec{V}_i \tag{11}$$

where adaptive parameter AP can be utilized for the calculation of step size:

$$AP = \left(1 - \frac{t}{t_{\max}} \right)^{\left(2\frac{t}{t_{\max}}\right)} \tag{12}$$

At last, a low-velocity ratio is determined. FAD is calculated for the last selection of prey:

$$\vec{P}_i = \begin{cases} \vec{P}_i + AP\left[x_{\min} + \vec{R} \otimes (x_{\max} - x_{min})\right] \otimes \vec{B} \\ if\ r < 0.4 \\ \vec{P}_i + [0.4(1-r) + r](\vec{P}_{r1} - \vec{P}_{r1}) \\ if\ r \geq 0.4 \end{cases} \quad (13)$$

In Eq. (13), the binary vector of value one or zero is $\vec{B}$. The Reyni entropy has been calculated to eliminate the ambiguity between $\vec{P}_i$ elected prey and calculate the fitness. *Prey* satisfies the entropy function and can pass for the fitness assessment.

$$Ent\left(\vec{P}_i\right) = \frac{1}{1-\alpha}\log\sum_{i=1}^{n}\vec{P}_i^{\,\alpha}, \alpha > 1\ and\ \neq 1 \quad (14)$$

In Eq. (14), the entropy value of all the rows of chosen i^{th} prey is *Ent*. For the final selection, we use these values as follows:

$$Fnc = \begin{cases} \vec{Sel}(k)\ for\ \vec{P}_i \geq Ent \\ ignore,\ Elsewhere \end{cases} \quad (15)$$

Finally, the elected vector $\vec{Sel}(k)$ can exploited for the fitness computation. This procedure is repeated till the maximum iterations are reached.

During this MMPA algorithm, the purposes are combined as a single objective equation such that an existing weight classifies all the objective significance [22]. During this case, it can be executed a FF that incorporates both purposes of FS as expressed in Eq. (16).

$$Fitness\,(X) = \alpha \cdot E\,(X) + \beta * \left(1 - \frac{|R|}{|N|}\right) \quad (16)$$

whereas, $Fitness(X)$ signifies the fitness value of subdivision X, $E(X)$ denotes the classifier rate of errors by deploying the selected features from the X subset, $|R|$ and $|N|$ signify the elected feature counts, and the count of novel features from the database, α and β are the weighted of classifier errors and decrease ratio, $\alpha \in [0, 1]$ and $\beta = (1-\alpha)$.

B. INTRUSION DETECTION USING THE ENN MODEL

At this stage, the ENN model can be used for the classification and recognition of the intrusions. ENN is a multiple-layer dynamic NN [23]. Due to its dynamic recursive design, it takes an optimum approximation capability to a non-linear function. ENN has been separated into 4 layers namely input, context, output, and hidden layer (HL). The linking of input, HL, and output layers is the same as that of FFNNs. But the alteration is that the context layer has along with storing the resultant value of neurons of the HL at the earlier moment. The spatial formula of a layer of ENN at k moment is:

$$\begin{cases} z\,(k) = g(\omega_{j,q} \cdot h\,(k)) \\ h\,(k) = f\,\left(\omega_{j,m} \cdot c\,(k) + \omega_{i,j} \cdot u\,(k-1)\right) \\ c\,(k) = h\,(k-1) \end{cases} \quad (17)$$

whereas, $u(k-1)$ implies the input layer vector at the moment $k-1$; $h(k)$,$g(\cdot)$ and f denotes the transfer purposes of output and HLs correspondingly; $c(k)$, and $z(k)$ signifies the resultant vectors of the HL, context, and output layers at the moment k; $\omega_{i,j}$, $\omega_{j,m}$, and $\omega_{j,q}$ stands for connection weighted among input and HLs, context and HLs, HL and output layers correspondingly. Fig. 2 represents the infrastructure of ENN.

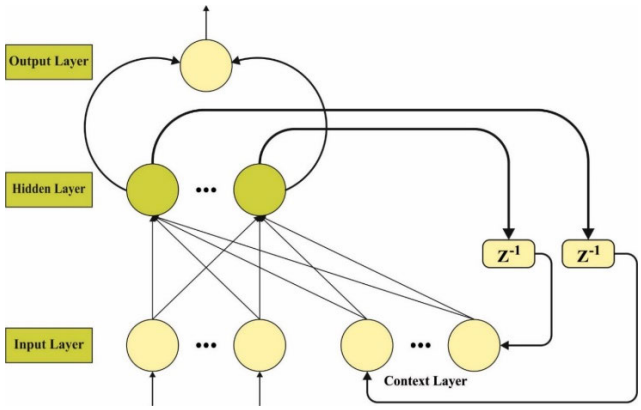

FIGURE 2. Structure of ENN.

The weight of the Elman network can be changed by reducing MSE, the minimal MSE is executed for adjusting the weights of the Elman network.

$$MSE = \frac{1}{N}\sum_{k=1}^{N}[z\,(k) - z_t\,(k)]^2 \quad (18)$$

In which, $z(k)$ denotes the actual value at time k, $z_t(k)$ represents the predictive value at time k.

C. HYPERPARAMETER SELECTION USING HBA

Finally, the HBA adjusts the parameters related to the ENN model. HBA stimulates the feeding behavior of honey badgers [24]. Honey Badger has two different ways to get their food while foraging. First, they use smell concentration to approach and find the honey. This phenomenon is named "digging mode". The next phenomenon is named "honey mode," where they find honey by emulating honeyguide birds. The mathematical modeling of HBA simulates the hunting behaviors of honey badgers. While the HBA takes exploitation and exploration stages, it can be considered a global optimizer approach. Consider that the HBA approach optimizer N D-dimensional solutions defined by the population of solution candidates:

$$N = \begin{bmatrix} x_{11} & x_{12} & x_{13} & \cdots & x_{1D} \\ x_{21} & x_{22} & x_{23} & \cdots & x_{2D} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{n1} & x_{n2} & x_{n3} & \cdots & x_{nD} \end{bmatrix} \quad (19)$$

In Eq. (19), the count of agents is n, and the location of i^{th} agents are $x_i = [x_i^1, x_i^2, \ldots, x_i^D]$, and ub_i and lb_i are the up and low boundaries, correspondingly.

The initial position of the agent is expressed by Eq. (20):

$$x_i = lb_i + r \times (ub_i - lb_i) \tag{20}$$

Now r is a randomly generated value within [0, 1].

Parameter I. The intensity I_i defines i^{th} prey's degree of concentration and the separation between them and the honey badgers:

$$I_i = r_1 \times \frac{S}{4\pi d_i^2} \tag{21}$$

In Eq. (21), the random integer within [0 1] is r_1. The source strength is expressed as S:

$$S{=}(x_i - x_{i-1})^2 \tag{22}$$

The distance between i^{th} honey badgers and prey is d_i:

$$d_i = x_{prey} - x_i \tag{23}$$

In Eq. (23), the location of prey recognized as the optimum solution is x_{prey}.

Define the α variable. To enable the progressive shift from exploration to exploitation, α is a parameter with iteration and is represented by:

$$\alpha = C \times e^{\frac{-t}{t_{\max}}} \tag{24}$$

In Eq. (24), C is a constant and the maximum iteration count is t_{max}.

Once the honey badger upgrades its location, there exist 2 methods. Through iteration in the digging process, (25) defines the new position of a honey badger.

$$x_{new} = x_{prey} + F \times \beta \times I \times x_{prey} + F \times r_2 \times \alpha \times d_i \times |\cos(2\pi r_3) \times [1 - \cos(2\pi r_4)]| \tag{25}$$

In Eq. (25), F is a flag which alters the search direction:

$$F = \begin{cases} 1 & if\ r_5 \leq 0.5 \\ -1 & else \end{cases} \tag{26}$$

In Eq. (26), r_2, r_3, r_4, and r_5 are randomly generated values within [1, 0], correspondingly. β is a constant that represents the capability of honey badger to attain food. During the digging model, the behavioral pattern of honey badgers is similar to the structure of the cardioid shape.

During the honey method, a novel location of a honey badger by iteration can be defined by:

$$x_{new} = x_{prey} + F \times r_6 \times \alpha \times d_i \tag{27}$$

In Eq. (27), the random number between 0 and 1 is r_6. Flag F allows an agent to alter the searching direction to increase the probability of escaping from the local optimum and explore the search range. The fitness optimum is a vital aspect of the HBA methodology. An encoded performance has been deployed to establish the better efficiency of candidate performances. Presently, the accuracy value is a major condition deployed to design an FF.

$$Fitness = \max(P) \tag{28}$$

$$P = \frac{TP}{TP + FP} \tag{29}$$

Here, FP and TP denote the false and true positive values.

IV. RESULTS AND DISCUSSION

In this study, the attack detection analysis of the MMPADL-ID technique can be tested employing the benchmark database, comprising 125973 samples with 5 classes as represented in Table 1. The MMPADL-ID technique has chosen 26 features from the available 42 features.

The suggested technique is simulated by using the Python 3.6.5 tool on PC i5-8600k, 250GB SSD, GeForce 1050Ti 4GB, 16GB RAM, and 1TB HDD. The parameter settings are given as learning rate: 0.01, activation: ReLU, epoch count: 50, dropout: 0.5, and size of batch: 5.

TABLE 1. Details on database.

Classes	No. of Instances
Dos	45927
R2l	995
Probe	11656
U2r	52
Normal	67343
Total No. of Instances	125973

Fig. 3 shows the confusion matrices achieved by the MMPADL-ID approach under 80:20 and 70:30 of the TR phase/TS phase. The simulated values indicate the effective recognition with all five classes.

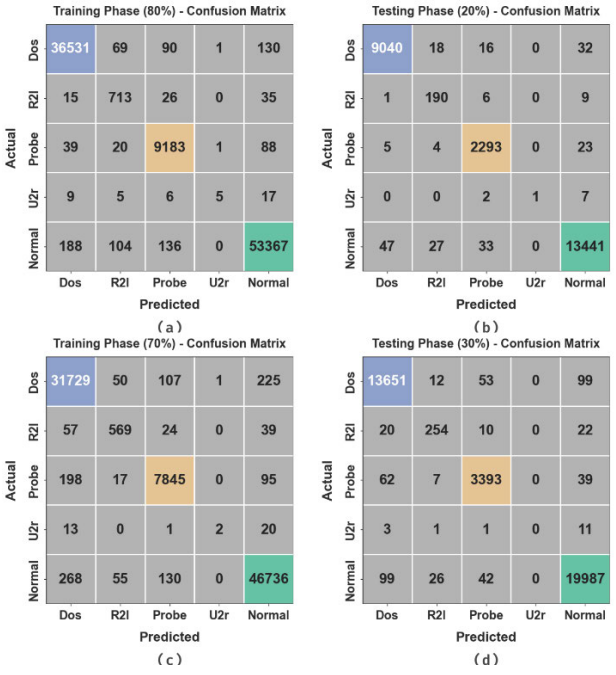

FIGURE 3. Confusion matrices of (a-c) TR phase of 80% and 70% and (b-d) TS phase of 20% and 30%.

The recognition results of the MMPADL-ID technique with 80:20 of TR Phase/TS Phase are exposed in Table 2 and Fig. 4. The outcome depicted that the MMPADL-ID method reaches successful recognition on each 5 class. With 80% of the TR Phase, the MMPADL-ID system provides an average $accu_y$ of 99.61%, $prec_n$ of 89.16%, $reca_l$ of 79.82%, F_{score} of 80.15%, and AUC_{score} of 89.77%. Additionally, based on 20% of the TS Phase, the MMPADL-ID model gives an average $accu_y$ of 99.63%, $prec_n$ of 95.19%, $reca_l$ of 79.87%, F_{score} of 80.07%, and AUC_{score} of 89.80% respectively.

TABLE 2. Recognition outcome of MMPADL-ID technique with 80:20 of TR Phase/TS Phase.

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
80% of TR Phase					
Dos	99.46	99.32	99.21	99.26	99.41
R2l	99.73	78.27	90.37	83.88	95.08
Probe	99.60	97.27	98.41	97.84	99.07
U2r	99.96	71.43	11.90	20.41	55.95
Normal	99.31	99.50	99.20	99.35	99.31
Average	99.61	89.16	79.82	80.15	89.77
20% of TS Phase					
Dos	99.53	99.42	99.28	99.35	99.47
R2l	99.74	79.50	92.23	85.39	96.02
Probe	99.65	97.57	98.62	98.10	99.19
U2r	99.96	100.00	10.00	18.18	55.00
Normal	99.29	99.47	99.21	99.34	99.30
Average	99.63	95.19	79.87	80.07	89.80

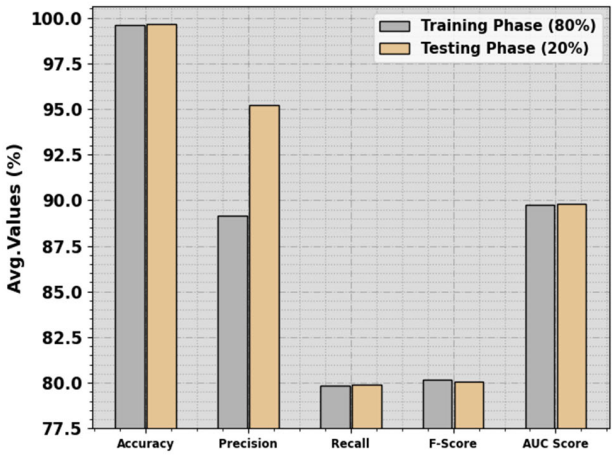

FIGURE 4. Average of MMPADL-ID technique with 80:20 of TR Phase/TS Phase.

The recognition analysis of the MMPADL-ID method with 70:30 of TR Phase/TS Phase is described in Table 3 and Fig. 5. The simulated values pointed out that the MMPADL-ID system attains efficacious recognition on each five classes. According to 70% of the TR Phase, the MMPADL-ID technique offers an average $accu_y$ of 99.41%, $prec_n$ of 88.66%, $reca_l$ of 76.44%, F_{score} of 77.38%, and AUC_{score} of 87.98%. Also, with 30% of the TS Phase, the MMPADL-ID model gives an average $accu_y$ of 99.46%, $prec_n$ of 75.89%, $reca_l$ of 75.58%, F_{score} of 75.73%, and AUC_{score} of 87.57% correspondingly.

TABLE 3. Recognition outcome of MMPADL-ID technique with 70:30 of TR Phase/TS Phase.

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
70% of the TR Phase					
Dos	98.96	98.34	98.81	98.57	98.93
R2l	99.73	82.34	82.58	82.46	91.22
Probe	99.35	96.77	96.20	96.48	97.94
U2r	99.96	66.67	05.56	10.26	52.78
Normal	99.06	99.20	99.04	99.12	99.06
Average	99.41	88.66	76.44	77.38	87.98
30% of TS Phase					
Dos	99.08	98.67	98.81	98.74	99.02
R2l	99.74	84.67	83.01	83.83	91.44
Probe	99.43	96.97	96.92	96.94	98.30
U2r	99.96	00.00	00.00	00.00	50.00
Normal	99.11	99.15	99.17	99.16	99.10
Average	99.46	75.89	75.58	75.73	87.57

Fig. 6 illustrates the classifier analysis of the MMPADL-ID technique in various aspects. Figs. 6a-6c shows the $accu_y$ analysis of the MMPADL-ID method with 80:20 and 70:30. The figure indicates that the MMPADL-ID system achieves rising values over improving epochs. Additionally, the improving validation with training reveals that the MMPADL-ID approach gains effectively on the test dataset. Lastly, Figs. 6b-6d represents the loss analysis of the MMPADL-ID methodology at 80:20 and 70:30. The simulated values show that the MMPADL-ID algorithm gets nearer outcomes of training and validation loss. It is noticed that the MMPADL-ID model attains proficiency on the test database.

Fig. 7 shows the classifier performance of the MMPADL-ID system at 80:20 and 70:30. Figs. 7a-7c exhibits the PR analysis of the MMPADL-ID technique with 80:20 and 70:30. The simulated outcomes reported that the MMPADL-ID model led to raised values of PR. Furthermore, the MMPADL-ID algorithm can attain greater PR values on all 5 classes. Then, Figs. 7b-7d denotes the ROC analysis of the MMPADL-ID methodology at 80:20 and 70:30. The figure exhibited that the MMPADL-ID method resulted in enhanced ROC values. Also, the MMPADL-ID system has attained higher ROC values on all five classes.

In Table 4, a comprehensive result of the MMPADL-ID technique is provided [25]. Fig. 8 examines a comparative $accu_y$ and $prec_n$ results of the MMPADL-ID system. The outcome points out that the MMPADL-ID method gains effectual performance. Based on $accu_y$, the MMPADL-ID methodology gains an increased $accu_y$ of 99.63% but the DRL-BWO,

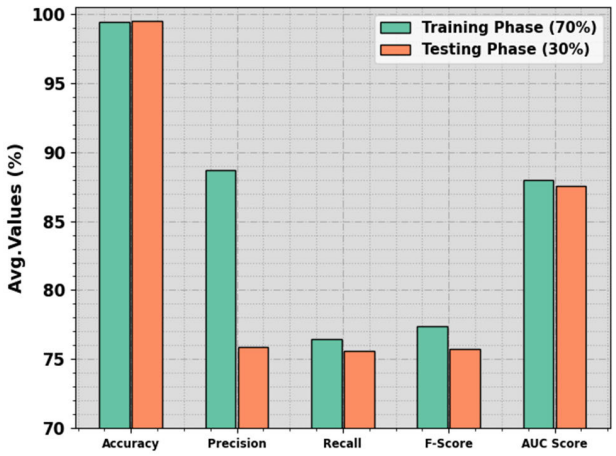

FIGURE 5. Average of MMPADL-ID technique with 70:30 of TR Phase/TS Phase.

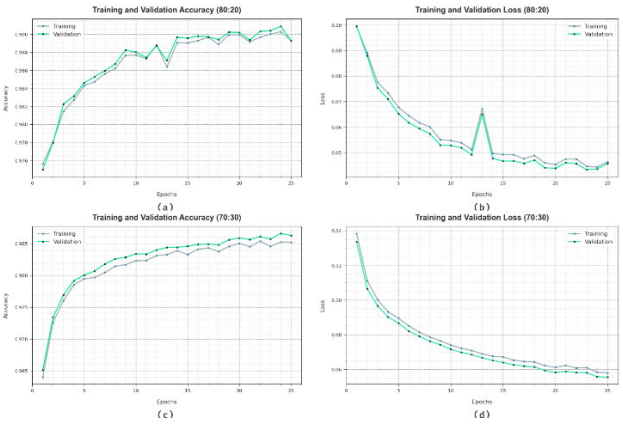

FIGURE 6. $Accu_y$ curve of (a-c) 80:20 and 70:30 (b-d) Loss curve of 80:20 and 70:30.

TABLE 4. Comparative outcome of MMPADL-ID algorithm with other methods.

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
MMPADL-ID	99.63	95.19	79.87	80.07
DRL-BWO Model	98.70	94.95	75.00	74.20
IDBN Model	95.32	91.06	74.03	72.11
T-SID Model	94.38	94.22	79.50	72.89
DL Model	91.80	93.83	75.47	73.56
DPC-DBN Model	94.39	94.70	78.12	73.59
AK-NN Model	91.78	92.64	79.77	74.25

IDBN, T-SID, DL, DPC-DBN, and AK-NN approach gains decreased $accu_y$ values of 98.70%, 95.32%, 94.38%, 91.80%, 94.39%, and 91.78%, individually. Additionally, with $prec_n$, the MMPADL-ID approach obtains improved $prec_n$ of 95.19% but, the DRL-BWO, IDBN, T-SID, DL, DPC-DBN, and AK-NN methods acquire reduced $accu_y$ values

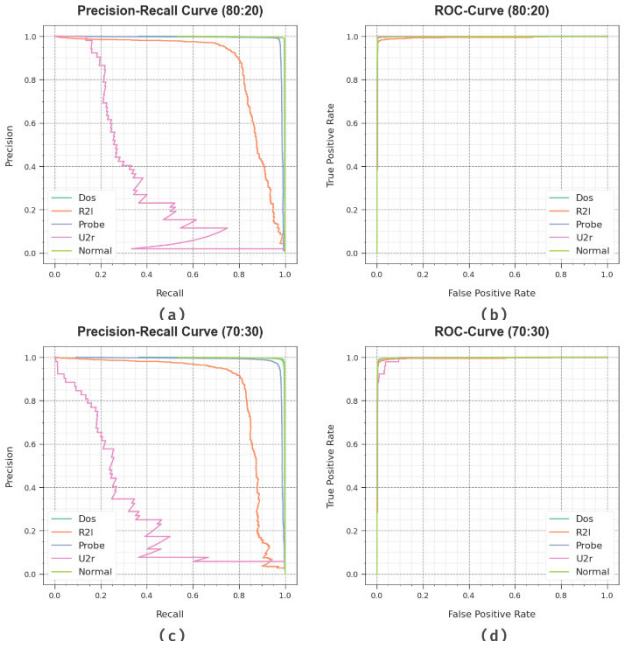

FIGURE 7. PR curve of (a-c) 80:20 and 70:30 (b-d) ROC curve of 80:20 and 70:30.

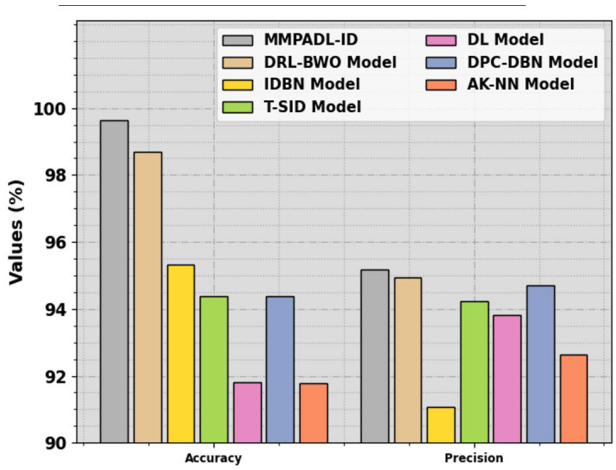

FIGURE 8. $Accu_y$ and $prec_n$ outcome of MMPADL-ID algorithm with other methods.

of 94.95%, 91.06%, 94.22%, 93.83%, 94.70%, and 92.64%, respectively.

Fig. 9 shows a comparative $reca_l$ and F_{score} outcomes of the MMPADL-ID model. The simulated values pointed out that the MMPADL-ID system achieves excellent performance. Moreover, based on $reca_l$, the MMPADL-ID algorithm gets raised $reca_l$ of 79.87% whereas the DRL-BWO, IDBN, T-SID, DL, DPC-DBN, and AK-NN algorithms get diminished $reca_l$ values of 75.00%, 74.03%, 79.50%, 75.47%, 78.12%, and 79.77%, correspondingly. Besides, on F_{score}, the MMPADL-ID model gets raised F_{score} of 80.07% whereas the DRL-BWO, IDBN, T-SID, DL, DPC-DBN, and AK-NN methodologies get lower $reca_l$ values of 74.20%, 72.11%, 72.89%, 73.56%, 73.59%, and 74.25%,

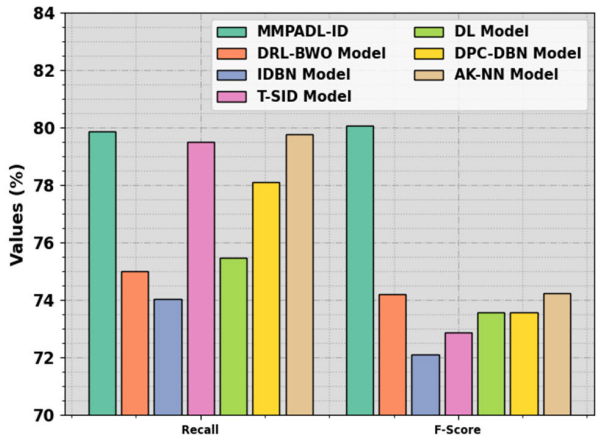

FIGURE 9. $Reca_l$ and F_{score} outcome of MMPADL-ID algorithm with other methods.

respectively. These performances highlighted the better outcome of the MMPADL-ID technique.

V. CONCLUSION

In this study, an automated intrusion detection, called MMPADL-ID system is designed and developed on the IoT-assisted UAV networks. The presented MMPADL-ID technique proposes to detect and classify intrusions in accomplishing security in IoT-assisted UAV networks. In the MMPADL-ID system, the 3 main utilized processes are MMPA-based FS, ENN-based classification, and HBA-based hyperparameter tuning. In this work, the FS process is performed by the design of MMPA, and the HBA is employed for the hyperparameter tuning of the ENN approach resulting in improved performance. The simulation value of the MMPADL-ID technique can be tested on benchmark datasets. An extensive comparative outcome exhibited the improved performance of the MMPADL-ID methodology with existing approaches for various measures. Thus, the MMPADL-ID methodology is executed for automated and accurate intrusion detection in the IoT-assisted UAV network.

REFERENCES

[1] U. I. Vivian, I. N. Cosmas, D.-S. Kim, and J.-M. Lee, "DATA-FedAVG: Delay-aware truncated accuracy-based federated averaging for intrusion detection in UAV network," *J. Korean Inst. Commun. Inf. Sci.*, vol. 48, no. 6, pp. 648–668, Jun. 2023.

[2] R. Hamadi, "Artificial intelligence applications in intrusion detection systems for unmanned aerial vehicles," Ph.D. dissertation, Dept. Comput., Elect., Math. Sci. Eng. (CEMSE), King Abdullah Univ. Sci. Technol., Thuwal, Saudi Arabia, 2023.

[3] R. Majeed, N. A. Abdullah, M. Faheem Mushtaq, M. Umer, and M. Nappi, "Intelligent cyber-security system for IoT-aided drones using voting classifier," *Electronics*, vol. 10, no. 23, p. 2926, Nov. 2021.

[4] A. Zainudin, R. Akter, D. S. Kim, and J. M. Lee, "FedIoV: A federated learning-assisted intrusion messages detection in Internet of Vehicles," in *Proc. Korean Soc. Commun. Stud. Conf.*, 2022, pp. 305–306.

[5] Y. Chen, D. Pi, B. Wang, A. W. Mohamed, J. Chen, and Y. Wang, "Equilibrium optimizer with generalized opposition-based learning for multiple unmanned aerial vehicle path planning," *Soft Comput.*, vol. 2023, pp. 1–14, Dec. 2023.

[6] R. T. Mehmood, G. Ahmed, and S. Siddiqui, "Simulating ML-based intrusion detection system for unmanned aerial vehicles (UAVs) using COOJA simulator," in *Proc. 16th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Dec. 2022, pp. 1–10.

[7] A. Faramarzi, M. Heidarinejad, B. Stephens, and S. Mirjalili, "Equilibrium optimizer: A novel optimization algorithm," *Knowl.-Based Syst.*, vol. 191, Mar. 2020, Art. no. 105190.

[8] N. Alturki, T. Aljrees, M. Umer, A. Ishaq, S. Alsubai, O. Saidani, S. Djuraev, and I. Ashraf, "An intelligent framework for cyber-physical satellite system and IoT-aided aerial vehicle security threat detection," *Sensors*, vol. 23, no. 16, p. 7154, Aug. 2023.

[9] J. K. Samriya, M. Kumar, and R. Tiwari, "Energy-aware ACO-DNN optimization model for intrusion detection of unmanned aerial vehicle (UAVs)," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 8, pp. 10947–10962, Aug. 2023.

[10] Y. Chen, D. Pi, S. Yang, Y. Xu, J. Chen, and A. W. Mohamed, "HNIO: A hybrid nature-inspired optimization algorithm for energy minimization in UAV-assisted mobile edge computing," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 3, pp. 3264–3275, Sep. 2022.

[11] E. Ntizikira, W. Lei, F. Alblehai, K. Saleem, and M. A. Lodhi, "Secure and privacy-preserving intrusion detection and prevention in the Internet of unmanned aerial vehicles," *Sensors*, vol. 23, no. 19, p. 8077, Sep. 2023.

[12] D. Sharma, S. K. Gupta, A. Rashid, S. Gupta, M. Rashid, and A. Srivastava, "A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 7, p. e4114, Jul. 2021.

[13] 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.

[14] D.-C. Wang, I.-R. Chen, and H. Al-Hamadi, "Reliability of autonomous Internet of Things systems with intrusion detection attack-defense game design," *IEEE Trans. Rel.*, vol. 70, no. 1, pp. 188–199, Mar. 2021.

[15] X. He, Q. Chen, L. Tang, W. Wang, T. Liu, L. Li, Q. Liu, and L. Jia., "Federated continuous learning based on stacked broad learning system assisted by digital twin networks: An incremental learning approach for intrusion detection in UAV networks," *IEEE Internet Things J.*, vol. 10, no. 22, pp. 19825–19838, Jun. 2023.

[16] 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.

[17] M. A. Cheema, M. K. Shehzad, H. K. Qureshi, S. A. Hassan, and H. Jung, "A drone-aided blockchain-based smart vehicular network," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4160–4170, Jul. 2021.

[18] J. Sajid, K. Hayawi, A. W. Malik, Z. Anwar, and Z. Trabelsi, "A fog computing framework for intrusion detection of energy-based attacks on UAV-assisted smart farming," *Appl. Sci.*, vol. 13, no. 6, p. 3857, Mar. 2023.

[19] X. Gao, L. Wang, X. Yu, X. Su, Y. Ding, C. Lu, H. Peng, and X. Wang, "Conditional probability based multi-objective cooperative task assignment for heterogeneous UAVs," *Eng. Appl. Artif. Intell.*, vol. 123, Aug. 2023, Art. no. 106404.

[20] C. Li, X. Su, Y. Zhang, W. Han, F. Guo, X. Li, and X. Wang, "Integrated scheduling method for fleet wave sorties and maintenance of naval distributed platforms," *Adv. Eng. Informat.*, vol. 59, Jan. 2024, Art. no. 102340.

[21] S. Bibi, M. A. Khan, J. H. Shah, R. Damaševič ius, A. Alasiry, M. Marzougui, M. Alhaisoni, and A. Masood, "MSRNet: Multiclass skin lesion recognition using additional residual block based fine-tuned deep models information fusion and best feature selection," *Diagnostics*, vol. 13, no. 19, p. 3063, Sep. 2023.

[22] M. Mafarja, T. Thaher, M. A. Al-Betar, J. Too, M. A. Awadallah, I. A. Doush, and H. Turabieh, "Classification framework for faulty-software using enhanced exploratory whale optimizer-based feature selection scheme and random forest ensemble learning," *Int. J. Speech Technol.*, vol. 53, no. 15, pp. 18715–18757, Aug. 2023.

[23] B. Liu, Y. Zhao, W. Wang, and B. Liu, "Compaction density evaluation model of sand-gravel dam based on Elman neural network with modified particle swarm optimization," *Frontiers Phys.*, vol. 9, p. 818, Jan. 2022.

[24] M. A. Elseify, S. Kamel, H. Abdel-Mawgoud, and E. E. Elattar, "A novel approach based on honey badger algorithm for optimal allocation of multiple DG and capacitor in radial distribution networks considering power loss sensitivity," *Mathematics*, vol. 10, no. 12, p. 2081, Jun. 2022.

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