Enhancing Malicious User Recognition Using Coot Optimization Algorithm with Bayesian Belief Network for Cognitive Radio Networks

Rania Aboalela[1,*]

[1]Department of Information Systems, Faculty of Computing and Information Technology at Rabigh, King Abdulaziz University, Jeddah, Saudi Arabia

Email: raboalela@kau.edu.sa

Abstract

As a dynamic paradigm, Cognitive radio networks (CRNs) in wireless transmission enable devices to intelligently adapt their communication parameter based on real-world spectrum availability. Spectrum sensing lies at the core of CRNs, where nodes continue to monitor the spectrum for underutilized or unused band detection. However, the presence of malicious users (MUs) has a significant impact reliability and performance of the network. MUs detection is indispensable to prevent interference or unauthorized access and ensure network integrity. Advanced techniques combining game theory, machine learning, and signal processing are used for effectively identifying and mitigating malicious activities. CRNs can ensure efficient spectrum utilization and enhance security in heterogeneous and dynamic environments by incorporating robust MU detection systems into spectrum sensing protocols. This article presents a Malicious User Recognition using the Coot Optimization Algorithm with Bayesian Belief Network (MUR-COABBN) technique for CRN. The MUR-COABBN technique exploits metaheuristics with a Bayesian machine-learning method for the classification of the MUs in the CRN. In the MUR-COABBN technique, the COA is initially used to choose better feature subsets. Moreover, the detection of MUs can be performed by the use of BBN. Finally, the parameter tuning of the BBN model is carried out using an improved seeker optimization algorithm (ISOA). The experimental evaluation of the MUR-COABBN technique takes place with respect to distinct aspects. The experimentation outcomes implied the improved performance of the MUR-COABBN methodology with other methods under distinct measures. Therefore, the MUR-COABBN model can effectually and accurately improve security in the CRN.

Keywords: Cognitive Radio Network; Metaheuristics; Malicious User Recognition; Coot Optimization Algorithm; Machine Learning; Parameter Tuning

1. Introduction

The dynamic and open nature of cognitive radio networks (CRN) affects CR methods to be vulnerable to many assaults of malicious [1]. The foremost goal of attackers is to poorer the performance in availability, access confidentiality, and control. CRN permits secondary users (SU) or unlicensed consumers to utilize a Primary user (PU) or licensed consumer spectrum resourcefully if it is in the idle position. Therefore, when equated to another kind of system, every sort of attack arises in CRN. Whereas in other systems, the safety for contact was delivered by utilizing decryption and encryption models. In CRN, SU and PU were divided without a signalling switch [2]. Thus, there is a massive necessity for safety methods to defend a system from an attack. The accuracy of spectrum detection was enlarged by utilizing the idea of cooperative spectrum identifying in CRN, while the local detecting outcomes of SU joint created a choice regarding accessible range. The attackers of occurrence mainly create a wrong verdict regarding the band and the complete performance of the system is ruined [3].

In the CRN, discovering an idle spectrum is executed utilizing the spectrum detecting procedure that employs nodes recognized as SU without legal licenses to intellect and examine the work of an elective spectrum employed

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

by PU with legal licenses [4]. To attain the highest performances of spectrum sensing, central and distributed cooperative systems are developed as appropriate performances. Whereas in the 1st method, SU unites and splits its detecting data with a fusion centre (FC) that primarily gathers every SU sensing note to attain an optimal choice on PU. In the 2nd network, SUs work together to divide the sensing data among them and generate the last choice about the PU spectrum occupancy distinctly without any communication with FC [5]. Even with the major benefits of cooperative methods, they are vulnerable to possible assaults by malicious consumers affecting unwanted interventions amid SU and PU, and therefore it decreases the accuracy of the spectrum sensing method [6].

Numerous current researchers assume that SUs always tell the truth. But, is known that wireless systems united lower the chance of malicious events [7]. Malicious consumers report fake radio spectrum sensing outcomes to FC and then the local radio spectrum detecting outcome has been defined [8]. The fake radio spectrum sensing outcomes possibly disturb the performance of CSS in CRN. A CRN consumer might be malicious owing to the device's error. A MU might have hardware faults, report continually the occurrence of PU for its personal use, and account for the lack of PUs to avoid interfering with the PUs. In selfish motives, malicious CR-IoT consumers may account continuously that a PU exists [9]. In the present scenario, the usage of machine learning (ML) methods has been inspired by numerous researchers owing to their precision and learning abilities such as neural networks (NNs), SVM, and RF. ML is a subdivision of AI that is utilized for numerous uses such as data mining, speech, and image processing [10].

This article presents a Malicious User Recognition using the Coot Optimization Algorithm with Bayesian Belief Network (MUR-COABBN) technique for CRN. The MUR-COABBN technique exploits metaheuristics with the Bayesian ML approach for the classification of the MUs in the CRN. In the MUR-COABBN technique, the COA is initially used to choose better feature subsets. Moreover, the detection of MUs can be performed by the use of BBN. Finally, the parameter tuning of the BBN model is carried out using an improved seeker optimization algorithm (ISOA). The experimental analysis of the MUR-COABBN system takes place with respect to distinct aspects. The experimentation outcomes stated the better performance of the MUR-COABBN methodology with other algorithms in terms of distinct measures.

2. Literature Review

Almuqren et al. [11] proposed an Optimum DL Empowered Malicious User Detection for Spectrum Sensing (ODL-MUDSS) model. The offered technique mainly uses the DBN technique for automatic and precise recognition of MU. Furthermore, the detection performance of the DBN method is improved by the usage of the sand cat swarm optimizer (SCSO) system and increases the recognition outcomes. In [12], a novel method dependent upon dual ML solutions is projected. For the initial solution, an innovative stacking model-based MU recognition was developed utilizing dual advanced methods, with chaotic compressive sensing model-based verification for feature extractor with a least of extents and an ensemble ML model for consumers' identification. For 2nd solution, a new DL model has been projected utilizing scalogram imageries as input for the PU spectrum's identification. In [13], a DL-based solution called GitSec is presented. Initially, GitSec presents dual consumer action sequences and uses a similar NN design with an attention mechanism. Next, GitSec builds dual graphs to signify the connections among consumers as per their repository processes. Then, GitSec employs the descriptive feature to improve the performance of recognition. The final result is prepared by decision-making employed by a supervised ML-based classification algorithm.

Maray et al. [14] developed an Intelligent Pattern Recognition utilizing an EO with a DL (IPR-EODL) model. After pre-processing, the IPR-EODL method uses the channel attention LSTM (CA-LSTM) technique for the detection of Android malware. Maniriho et al. [15] project API-MalDetect, a novel DL-based automatic structure for noticing malware attacks. The projected structure employs an NLP-based encoding for API calls and a hybrid automated feature extraction dependent upon CNN and Bi-GRU models to remove features from raw and longer series of API calls. In [16], a DL (DL) based Bi-GRU-CNN system is planned to identify the malware of IoT and categorize the relations using Executable and Linkable Format (ELF) by dual file byte series as an input feature. Moreover, RNN technique-based DL method combinations are measured.

Liu et al. [17] study a malicious traffic recognition model dependent upon the DL technique. This method was presented to enhance the variety of data by making a combative system so that it can understand the strength and growth of data features, while it increases the precision of data investigation outcomes. The FlowGAN technique was utilized to identify malicious system data and manifold convolution encoding. Deconvolution encoding is employed to classify malicious traffic. Aurangzeb and Aleem [18] suggest a technique. The recognition and identification scheme utilizes both dynamic and static study employing an ensemble device. Furthermore, this research establishes that a minor subset of features execute reliably well when they result from simple malware. For this reason, the method also offered a quick, accessible, and precise mechanism for obfuscated Android malware recognition reliant on the DL system utilizing real and emulator-based platforms.

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

3. The Proposed Method

In this work, we have introduced a new MUR-COABBN algorithm for CRN. The MUR-COABBN technique exploits metaheuristics with the Bayesian ML approach for the classification of the MUs in the CRN. It contains three major processes such as COA-based feature subset selection, BBN-based MU recognition, and ISOA-based hyperparameter-tune process. Fig. 1 illustrates the complete flow of the presented MUR-COABBN technique.

A. System Model

We reflect a set of N CR with a collocated spectrum sensor in the occurrence of a main transmitter [19]. Every sensor utilizes energy detectors. The sensors direct their detecting information to access points over switch networks that are supposed to be ideal. Depending upon the information gained from the sensor, the access point creates a choice about the absence or presence of the main sign utilizing a recognition scheme and data fusion. Assume that $e_n[k]$ signifies the energy detector output at $the\ n^{th}$ sensor throughout the k^{th} sensing iteration. While hypotheses H_0 and H_1 signify the absence and presence of the main sign, correspondingly.

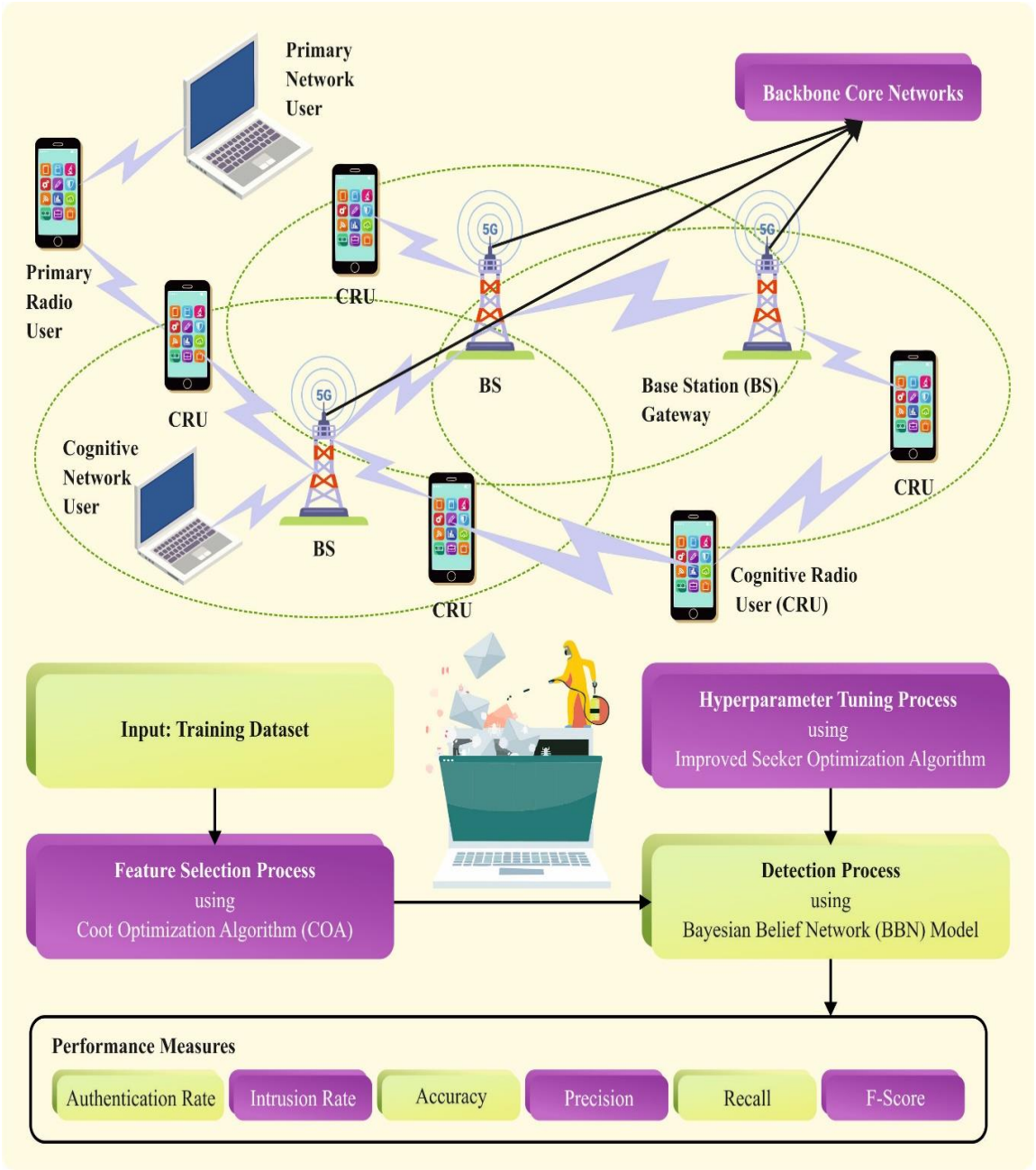

Figure 1. Overall flow of the MUR-COABBN technique

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

The n^{th} consumer's energy sensor output in the baseline was assumed below

$$e_n[k] = \begin{cases} \int_{T_k}^{T_k+T-1} |h_n(t)s(t) + z_n(t)|^2 \, dt; & H_1 \\ \int_{T_k}^{T_k+T-1} |z_n(t)|^2 \, dt; & H_0 \end{cases} \quad (1)$$

Whereas $s(t)$ denotes the main transmitted signal, T represents the distance of the sensing range, $z_n(t)$ refers to the additive white Gaussian noise (AWGN) for n^{th} sensor, $h_n(t)$ embodies the channel among n^{th} spectrum sensor and main transmitter.

B. COA-based Feature Subset Selection

Initially, the MUR-COABBN technique takes place the COA is used to choose better feature subsets. The COA is a noticeable meta-heuristic optimizer model stimulated by the joint performances detected in coot groups and water birds of the Rallidae family [20]. This technique pretends an effective coot population, recurrently altering their locations depending upon pre-defined instructions that imitate the foraging forms of coot groups. The COA includes dual different methods of bird motion over the surface of the water, described by uneven and constant movements at an early and following stage, correspondingly. Thus, 4 different actions of coots on the surface of the water were examined below:

- Motion at random
- Chain motion
- Altering the location of the group leader
- Motion of leaders to guide a cluster to the finest position

The population produced randomly is intended utilizing Eq. (2):

$$X(k) = rand(1, d) \times (ub - lb) \quad (2)$$

$X(k)$ represents the position at time k, through d demonstrating the size of searching space (the number of optimizer parameters). The lower and upper limits are represented by lb and ub, correspondingly. These explanations describe the 4 different motion stages:

The coot must be traveled at random in the searching space utilizing Eq. (3) in order to signify this motion.

$$W = rand(1, d) \times (ub - lb) \quad (3)$$

The coots' motion permits them to examine numerous regions within the searching space, and this procedure would permit the system to escape from every local goal that might turn stuck. Then, the method progressed out of this local opinion; Eq. (4) is employed to discover the novel coot locations.

$$X(k) = X(k) + Z \times R_2 \times \big(W - X(k)\big) \quad (4)$$

Here, $R2$ represents a randomly produced value in the interval of $zero$ to one, and Z is intended to utilize Eq. (5)

$$Z = 1 - L \times \left(\frac{1}{I_{ter}}\right) \quad (5)$$

The highest iteration count was signified by the variable "I_{ter}" whereas L specifies the existing iteration.

Chain motion includes initially computing the distance among the dual coots, where most coots are enthused near the subsequent coot by almost half of the route, as revealed in Eq. (6):

$$X(k) = 0.5 \times \big(X(k-1) + X(k)\big) \quad (6)$$

Whereas $X(k-1)$ denotes the 2nd coot.

In this motion, the coot adapts its position by the leader of the cluster. The coot tactics the leader, and there are numerous approaches to select the leader in dissimilar circumstances. Meanwhile, the coot's position was upgraded utilizing the normal place of the leader. Simultaneously, Eq. (7) is employed for selecting the leader.

$$M = 1 + (kMODNL) \quad (7)$$

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

Here, M denotes the index integer of the leader where the coot will select dependent upon the assumed tool. The existing coot is signified by variable k', whereas the leader counts can specified by $NL = 1$. MOD, Modulus function, certifying M rests from the effective range. So, $X(k)$ should move itself to support the leader known as 'M'. $X(k)$ denotes the task of upgrading its location by leader 'M'. Eq. (8) is applied to define the location of the subsequent coot and is intended dependent upon the leader number M.

$$X(k) = G(M) + 2 \times R_1 \times cos(2R\pi) \times \big(G(M) - X(k)\big) \tag{8}$$

$X(k)$ represents the coot's existing position, $G(M)$ specifies the leader place that has been selected, R_1 refers to the randomly generated value among $zero$ and one, π has the constant value of 3.14, and R specifies the randomly produced number among $(-1\ and\ 1)$.

Movement of leaders to guide a cluster to the finest position

Where the leaders were situated, the coots traveled nearer to them. However, the leader moves their locations in search of the finest places for the coot groups to track them. Overall, the optimal position for the leader was defined by utilizing Eq. (9).

$$G(k) = \begin{Bmatrix} B \times R_3 \times \cos(2R\pi) \times \big(g_{Best} - G(k)\big) + g_{Best}\ R4 < 0.5 \\ B \times R_3 \times \cos(2R\pi) \times \big(g_{Best} - G(k)\big) - g_{Best}\ R4 > 0.5 \end{Bmatrix} \tag{9}$$

Eq. (10) describes the variables. R within the array of [-1, 1], R_3, and R_4 are the randomly produced numbers within $[0\ and\ 1]$, and B is stated as follows:

$$B = 2 - L \times \left(\frac{1}{I_{ter}}\right) \tag{10}$$

Whereas I_{Ter} signifies the highest iteration, and L denotes the existing iteration.

Feature selection (FS) is a data pre-processing method in pattern recognition and machine learning that could dramatically enhance the solution of learning algorithms and decrease the cost of trained model [21]. The FS problem includes selecting d features from the datasets with D-dimensional features and $Minstances(d < D)$. The major purpose of the COA is to enhance the performance metric $f(X)$. x_m takes the value 0 (not chosen) 1 or (the m^{th} features are chosen).

$$\begin{gathered} \min f(x) \\ s.t.X = (x_1, x_2, x_D) \\ x_m \in \{0,1\}, m \in \{1,2,D\} \end{gathered} \tag{11}$$

C. MU Detection using BBN Model

At this stage, the detection of MUs can be performed by the use of BBN. As a probabilistic graphical method, BBN presents information about the uncertain area and shows higher performance in handling uncertainty [22]. BBN is a powerful technique to represent conditional and causality probabilities amongst different factors. When the factor is probabilistic, then this technique is suitable. Any model represented by this technique can be more easily understood by the practitioner than any other approach as the relationships and the factors amongst them are represented by the edges and nodes. Bayesian Network is used for predicting environmental performance. The state of performance measure is conditionally reliant on and the performance indicators used are probabilistic. Fig. 2 defines the infrastructure of BBN.

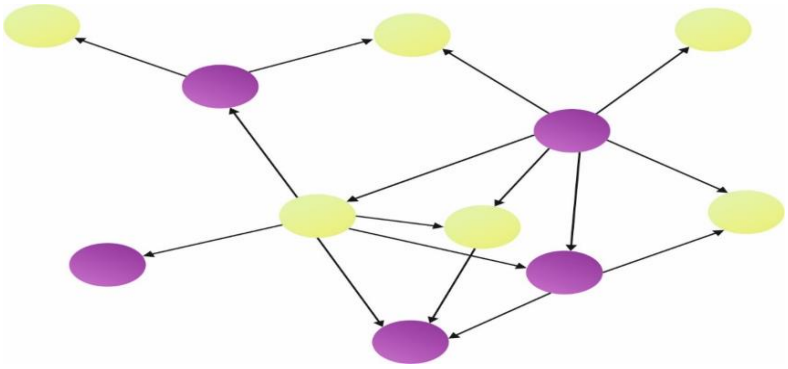

Figure 2. Architecture of BBN

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

BBN includes two parts $= (G, \theta)$. The initial part, "G" represents the directed acyclic graph (DAG) that consists of arcs and nodes. The variable of the dataset $X_1, \ldots \ldots, X_n$ represents the node, and arcs indicate dependences. The next part is the conditional dependence of θ in which $\theta_{xi|\pi xi} = P_B(x_i|\pi_{xi})$ indicates the direct parent variable of x_i in G.

$$P_B(X_{1,\ldots,}X_n) = \prod_{i=1}^{n} P_B(X_i|\pi_{Xi}) = \prod_{i=1}^{n} X_i|\pi_{Xi} \tag{12}$$

In the BBN, a stochastic variable is characterized as the node, and probabilistically dependence amongst the stochastic variables is signified as an edge among the nodes. The BBN computes the posterior distribution probability of unobserved random variables. "Backward" probability propagation finds the possible scenario representing the set of evidence.

In BBN, Inference is applied to the possibility update for the theory as evidence. "A" and "B" denote the parent nodes, "C" represents the child node. Diagnostic and predictive support are the two types of inference support or the node X_i. Diagnostic support for X_i node is a bottom-up method that reflects an evidence cation node associated with X_i via the child node. In contrast, prognostic assistance for X_i node is a top-down method that reflects the evidence node associated with X_i via the parent node.

D. Hyperparameter Tuning Process

Eventually, the parameter tuning of the BBN algorithm is carried out using ISOA. Recently, the SOA is a type of heuristic stochastic search method presented [23]. The SOA examines the stochastic exploration of human behaviours and studies human behaviours as high-level agents, primarily leveraging the latest research findings from agent systems, brain science, AI, and cognitive science in human study. Different current optimizer methods, the SOA mimics human intellectual searching performance, but all the individuals can assume that optimum individual, but they have better communication, learning, and cognitive capabilities, collaboration. So the exploration can be utilized as population and the searcher's location was deployed as the candidate performance in the SOA that simulates human intellectual searching performance. By mimicking the human examination for "knowledge gradients" and unknown logic, a better performance of the problem can achieved. However, the SOA takes restrictions as small exploration accuracy and an inclined to develop locked from the local optimal. An ISOA depends on the degree of adaptical membership that has been generated to resolve these problems. As it evades skipping valley regions by reducing searching step dimensions from the central and late phases of this method, it can be appropriate for a multi-objective optimizer. The population places were primarily established arbitrarily. Next, adaptive searching step and searching direction processes can executed on the upgraded locations of all the seekers:

$$\alpha_{ij} = \omega abs(x_{\min} - x_{\max})\sqrt{-\ln(u_{ij})} \tag{13}$$

whereas α_{ij} implies the search step, μ_{ij} denotes the degree of membership (DoM), the inertia weighted was represented by ω, and $x_{\min}$ and $x_{\max}$ relate to the minimal and maximal main function values.

$$u_{ij} = rand(u_i, 1), j = 1, \ldots D \tag{14}$$

$$u_i = u_{\min} + (u_{\max} - u_{\min}) * (\frac{t}{T})^{(1-\frac{t}{T})} \tag{15}$$

During the ISOA, the DoM can altered solely by iteration counts t. In addition, an adaptive power was established depending on linear DoM, as illustrated in Eqs. (14) and (15), whereas T depicts the maximal iteration counts. This variation causes the value of change from the DoM to reduce with enhancements in iterations. Therefore, this method takes place a comparatively smaller search step under the central and late stages, efficiently resolving the problem of the model becoming inclined to suitable stuck from the local optimal. Furthermore, the search direction is formulated as:

$$d_{ij}(t) = sign(\omega d_{i,pro} + \phi_1 d_{i,ego} + \phi_2 d_{i,alt}) \tag{16}$$

In which, ϕ_1 and ϕ_2 signify the random real numbers from the range of 0 and 1;$d_{i,pro}$, $d_{i,ego}$, and $d_{i,alt}$ denotes the pre-action direction, self-interest direction, and altruism direction, correspondingly. Eventually, by employing the above-mentioned process for updating the seeker position, new populations can be generated. Afterward, these populations are measured, till the end situation is met, and the global optimal can modified again. Algorithm 1 offers a complete explanation of the ISOA pseudocode.

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

Algorithm 1: Pseudocode of ISOA

Initialization:

Dimensional D, generation T, inertia weight ω, Population N, DoM $u_{\min}$, $u_{\max}$

Randomly initialize the position of seeker x, ϕ_1 and ϕ_2, P_i and P_g of the searcher

Cycle

For $i = 1: N$

For $j = 1: D$

$d_{ij}(t) = sign(\omega d_{i,pro} + \phi_1 d_{i,ego} + \phi_2 d_{i,alt})$

$u_i = u_{\min} + (u_{\max} - u_{\min}) * (\frac{t}{T})^{\left(1-\frac{t}{T}\right)}$

$u_{ij} = rand(u_{j,}1)$

$\alpha_{ij} = \omega abs(x_{\min} - x_{\max})\sqrt{-\ln(u_{ij})}$

$\Delta x_{i,j}, (t+1) = \alpha_{ij}(t) d_{ij}(t)$

$x_{ij}(t+1) = x_{ij}(t) + \Delta x_{ij}(t+1)$

IF func(x_{ij}) >func(p_{ij}) then $p_{ij} = x_{ij}$

End IF

IF func(χ_{ij}) >func(p_{gj}) then $p_{gj} = \chi_{ij}$

End IF

End

End

The ISOA deploys an objective function (OF) through a controlled purpose to accomplish multi-objective optimizer and acquire lower reflectivity and higher phase sensitivity:

$$OF = \begin{cases} S, R_{\min} < 0.01 \\ 0, others \end{cases} \quad (17)$$

The OF can be planned to recognize the maximal value of S from the searching region, to indirectly minimize the rate of $R_{\min}$ that signifies minimal reflectivity. $R_{\min}$ above 0.01 will solve neglect of the performance.

The fitness function (FF) represents an important reason prompting the performance of the ISOA. The hyperparameter limit procedure comprises the solution encoding approach for assessing the efficiency of the candidate's performance. In this work, the ISOA reflects the precision of leading standards to project the FF, which can be expressed below.

$$Fitness = \max(P) \quad (18)$$

$$P = \frac{TP}{TP + FP} \quad (19)$$

Whereas, TP signifies the true positive and FP denotes the false positive rates.

4. Performance Validation

The experimental assessment of the MUR-COABBN model was tested database, which contains 4000 samples under 2 class labels as depicted in Table 1.

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

Table 1: Details on database

Classes	No. of Instances
Normal	2000
Malicious Users	2000
Total Instances	4000

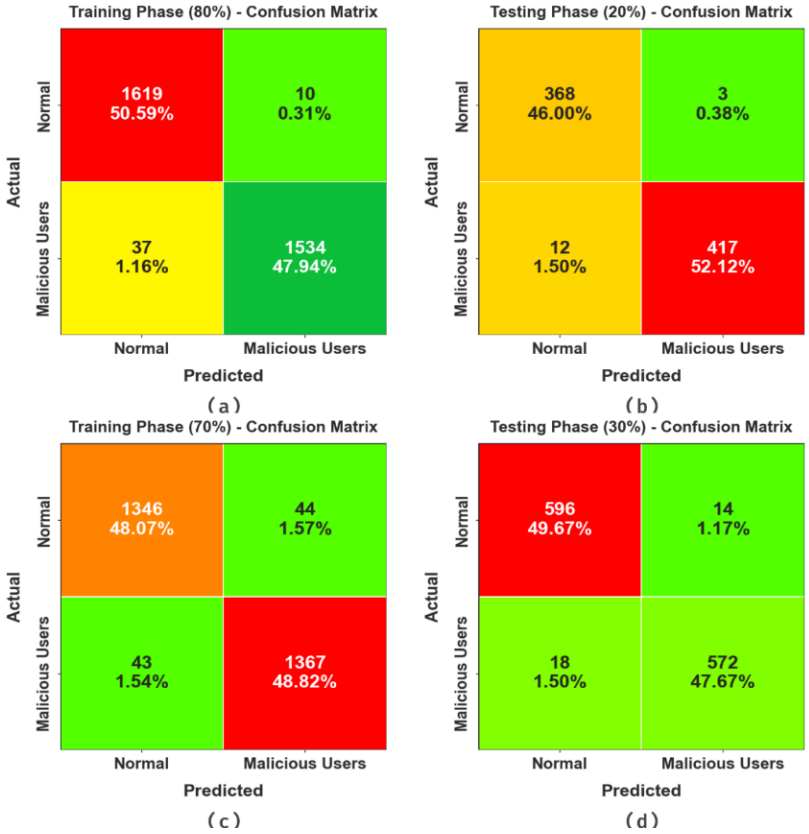

Figure 3. Confusion matrices of MUR-COABBN (a-b) 80%TRAS/20%TESS and (c-d) 70%TRAS/30%TESS

Fig. 3 exhibits the confusion matrices attained by the MUR-COABBN technique at 80:20 and 70:30 TRAS/TESS. This outcome pointed out that the MUR-COABBN model has effective detection with normal and malicious classes correctly.

Table 2 and Fig. 4 inspect the malicious user recognition study of the MUR-COABBN technique at 80%TRAS and 20%TESS. This outcome highlighted that the MUR-COABBN system properly identified the existence of normal and malicious user instances. With 80%TRAS, the MUR-COABBN approach provides an average $accu_y$ of 98.52%, $prec_n$ of 98.56%, $reca_l$ of 98.52%, and F_{score} of 98.53%. Similarly, depending on 20%TESS, the MUR-COABBN algorithm reaches an average $accu_y$ of 98.20%, $prec_n$ of 98.06%, $reca_l$ of 98.20%, and F_{score} of 98.12%.

Table 2: Malicious user recognition outcomes of the MUR-COABBN system under 80%TRAS and 20%TESS

Classes	$\boldsymbol{Accu_y}$	$\boldsymbol{Prec_n}$	$\boldsymbol{Reca_l}$	$\boldsymbol{F_{score}}$
TRAS (80%)				
Normal	99.39	97.77	99.39	98.57
Malicious Users	97.64	99.35	97.64	98.49
Average	98.52	98.56	98.52	98.53
TESS (20%)				
Normal	99.19	96.84	99.19	98.00
Malicious Users	97.20	99.29	97.20	98.23
Average	98.20	98.06	98.20	98.12

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

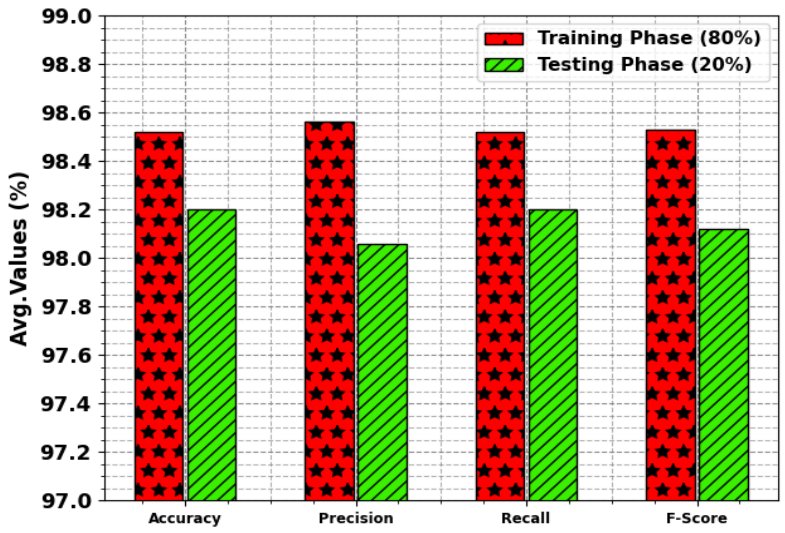

Figure 4. Average of MUR-COABBN method under 80%TRAS and 20%TESS

Figure 5. $Accu_y$ Curve of MUR-COABBN system at 80%TRAS and 20%TESS

The proficiency of the MUR-COABBN method at 80%TRAS and 20%TESS is clearly displayed in Fig. 5 in the procedure of training (TRAA) and validation accuracy (VALA) examination. This figure shows a useful study of the behavior of the MUR-COABBN approach across different numbers of epochs, indicating its learning progression and generalizability proficiencies. Typically, the figure represents a continuous development in the TRAA and VALA with increases in the number of epochs. It guarantees the adaptable features of the MUR-COABBN methodology for the recognition of pattern method at TES and TRA datasets. The higher tendency in VALA describes the ability of the MUR-COABBN method to adjust to the TRA data and additionally to give an accurate classifier on undetected data, displaying abilities of strong generalizability.

Fig. 6 represents an extensive view of the training (TRLA) and validation loss (VALL) consequences of the MUR-COABBN approach on 80%TRAS and 20%TESS above different number of epochs. The gradual reduction in TRLA emphasizes the MUR-COABBN method improving the weights and decreasing the classifier error at both datasets. This figure specifies a greater consideration of the MUR-COABBN method correlated with the TRA data, underlining its efficiency in taking patterns. Considerably, the MUR-COABBN algorithms constantly increase their parameters lessening the differences between the prediction and actual TRA classes.

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

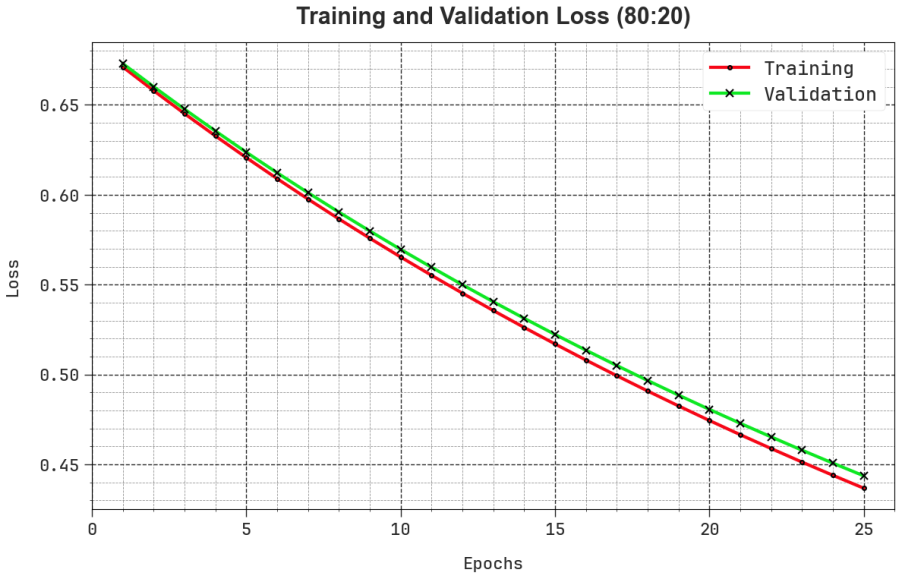

Figure 6. Loss curve of MUR-COABBN technique on 80%TRAS and 20%TESS

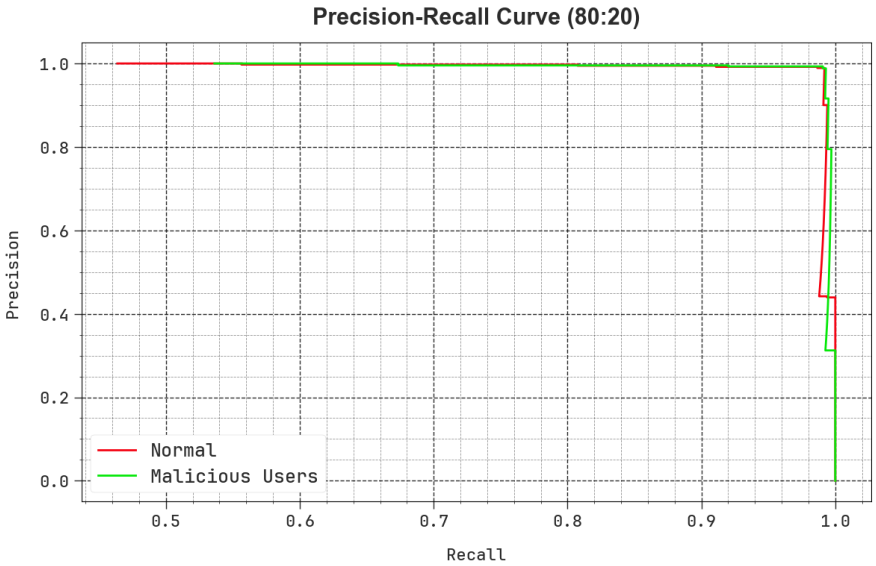

Figure 7. PR curve of MUR-COABBN model at 80%TRAS and 20%TESS

Examining the PR investigation, as portrayed in Fig. 7, the outcomes guaranteed that the MUR-COABBN methodology at 80%TRAS and 20%TESS gradually undertakes enhanced values of PR at each number of classes. It validates the improved capacities of the MUR-COABBN algorithm in the detection of a varied number of classes, demonstrating the ability in the detection class labels.

Similarly, in Fig. 8, the ROC examination acquired by the MUR-COABBN system with 80%TRAS and 20%TESS outperformed the classifier of distinctive labels. It presents a comprehensive consideration of the tradeoff between FRP and TPR across different detection threshold values and epoch counts. This figure underlined the boosted classifier outcomes of the MUR-COABBN technique with every class, showing the efficiency in overwhelming various complexities of classification.

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

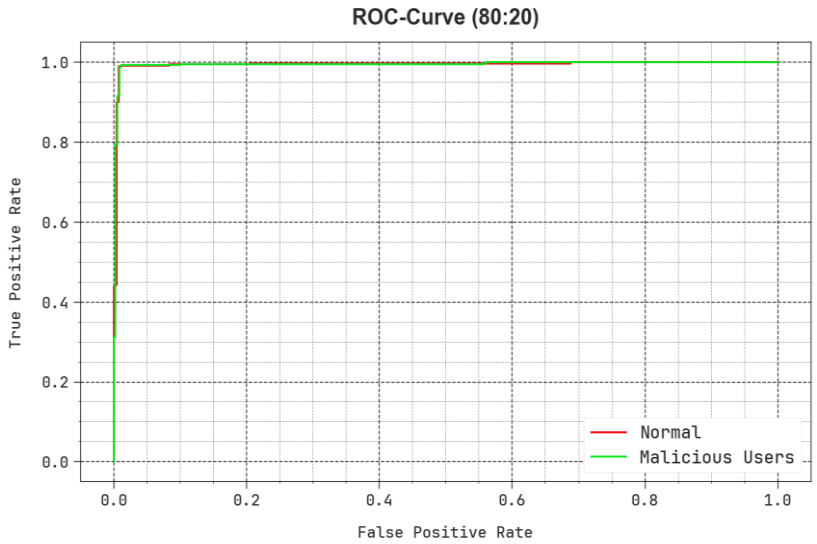

Figure 8. ROC curve of MUR-COABBN technique on 80%TRAS and 20%TESS

Table 3 and Fig. 9 examine the malicious user recognition result of the MUR-COABBN method at 70%TRAS and 30%TESS. This stimulation result pointed out that the MUR-COABBN approach properly recognized the presence of normal and malicious user instances. Based on 70%TRAS, the MUR-COABBN technique gains an average $accu_y$ of 96.89%, $prec_n$ of 96.89%, $reca_l$ of 96.89%, and F_{score} of 96.89%. Moreover, depending on 30%TESS, the MUR-COABBN technique acquires an average $accu_y$ of 97.33%, $prec_n$ of 97.34%, $reca_l$ of 97.33%, and F_{score} of 97.33%.

Table 3: Malicious user recognition results of the MUR-COABBN method on 70%TRAS and 30%TESS

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
TRAS (70%)				
Normal	96.83	96.90	96.83	96.87
Malicious Users	96.95	96.88	96.95	96.92
Average	96.89	96.89	96.89	96.89
TESS (30%)				
Normal	97.70	97.07	97.70	97.39
Malicious Users	96.95	97.61	96.95	97.28
Average	97.33	97.34	97.33	97.33

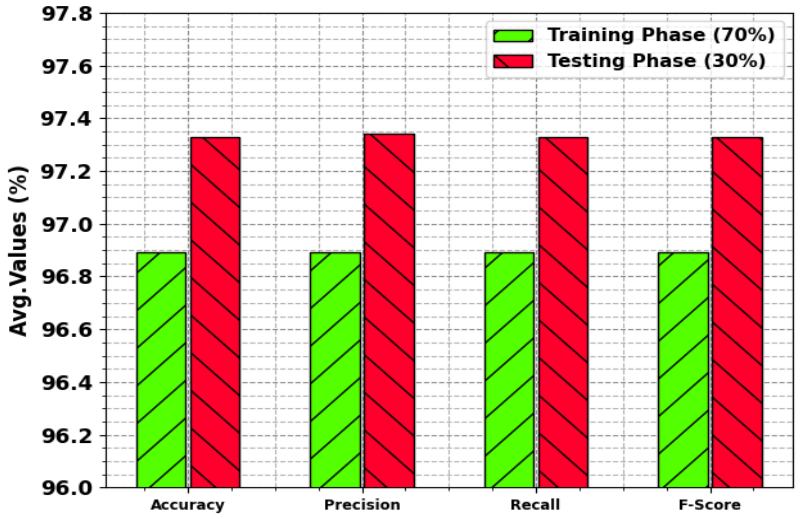

Figure 9. Average of MUR-COABBN model on 70%TRAS and 30%TESS

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

Figure 10. $Accu_y$ Curve of MUR-COABBN method on 70%TRAS and 30%TESS

The effectiveness of the MUR-COABBN technique on 70%TRAS and 30%TESS is graphically demonstrated in Fig. 10 with respective to TRAA and VALA investigations. This figure shows a useful study of the behavior of the MUR-COABBN system across various number of epochs, demonstrating its learning process and generalizability. Significantly, the figure can indicate a continual upgrading in the TRAA and VALA with growth in the number of epochs. It guarantees the adaptable aspect of the MUR-COABBN method in the recognition of pattern method at both datasets. The improved tendency in VALA exhibits the ability of the MUR-COABBN system to adapt to the TRA data and also surpass to present an accurate classifier on unnoticed data, indicating strong generalizability.

Fig. 11 shows a comprehensive illustration of the TRLA and VALL consequences of the MUR-COABBN technique at 70%TRAS and 30%TESS above different numbers of epochs. The advanced decrease in TRLA considers the MUR-COABBN method to improve the weights and diminish the classifier error in both datasets. This figure pointed out a better identification of the MUR-COABBN method associated with the TRA datasets, underscoring its efficiency in taking patterns. In particular, the MUR-COABBN algorithm continually boosted its parameters in reducing the differences between the prediction and actual TRA classes.

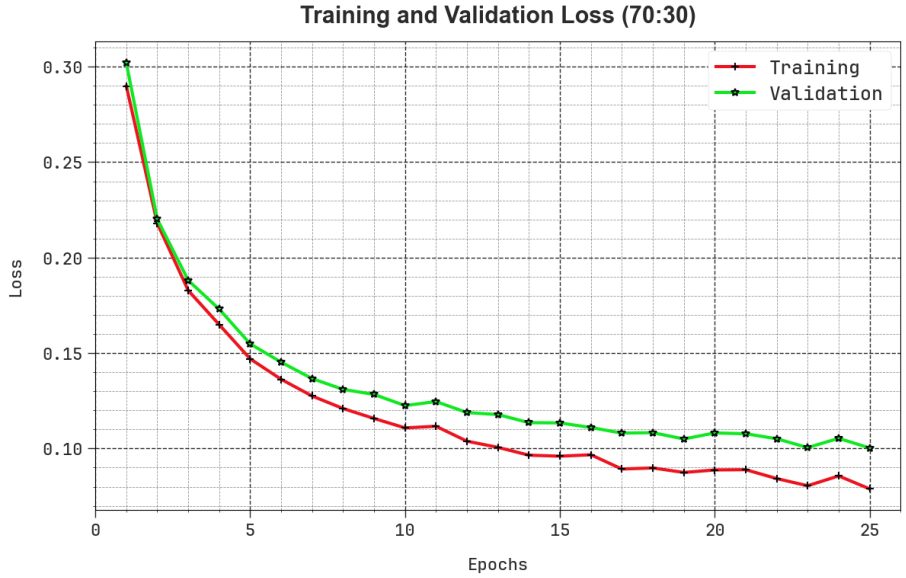

Figure 11. Loss curve of MUR-COABBN algorithm on 70%TRAS and 30%TESS

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

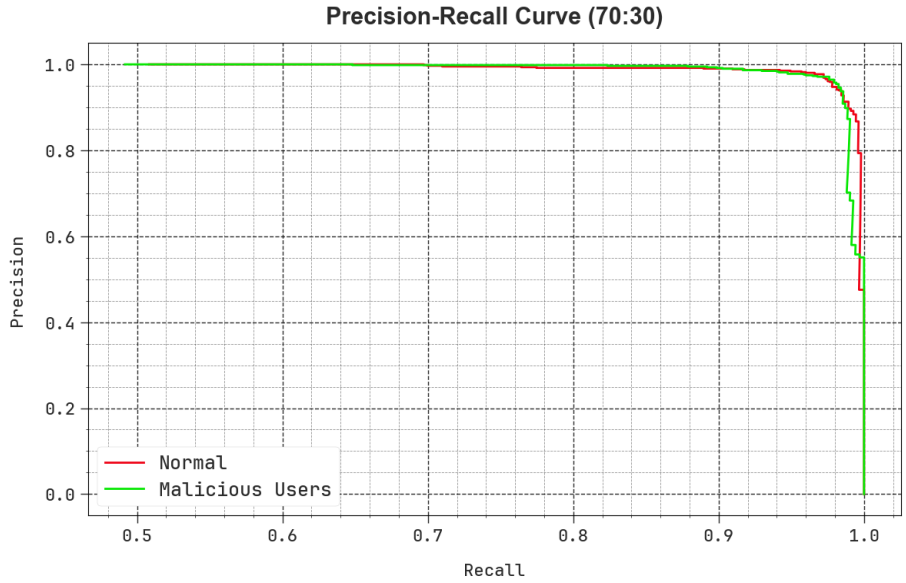

Figure 12. PR curve of MUR-COABBN technique at 70%TRAS and 30%TESS

Reporting the PR examination, as represented in Fig. 12, the outcomes confirmed that the MUR-COABBN technique with 70%TRAS and 30%TESS slowly gains increased values of PR in each class. It authenticates the greater capacities of the MUR-COABBN approach for the recognition of different numbers of classes, demonstrating the ability the recognize class labels.

Similarly, in Fig. 13, ROC investigation acquired by the MUR-COABBN methodology at 70%TRAS and 30%TESS outperformed the classifier of various numbers of labels. It gives a complete acceptance of the tradeoff between TPR and FRP across diverse detection epoch counts and threshold values. This figure underscored the better classifier values of the MUR-COABBN algorithm with each class, illustrating the efficiency in overwhelming numerous classifier intricacies.

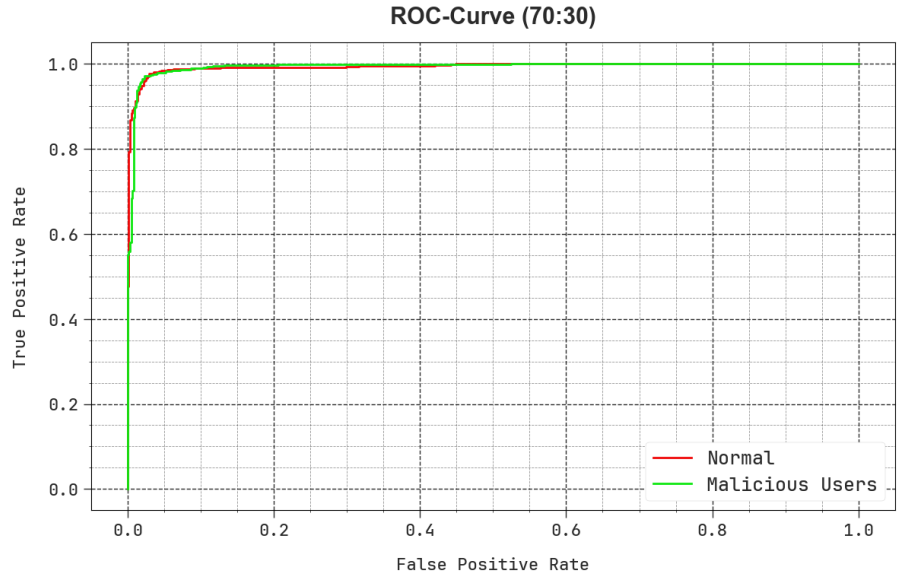

Figure 13. ROC curve of MUR-COABBN method at 70%TRAS and 30%TESS

In Table 4 and Fig. 14, the results of the MUR-COABBN system have undergone comparison with recent approaches in terms of distinct measures [11]. Based on $accu_y$, the MUR-COABBN technique has resulted in boosted $accu_y$ of 98.52% while the SVM, LR, NB, Stacking, and ODL-MUDSS algorithms achieved reduced $accu_y$ of 70.08%, 93.07%, 94.06%, 97.07%, and 97.82%, correspondingly. In addition, based on $prec_n$, the MUR-COABBN method gets a higher $prec_n$ of 98.56% whereas the SVM, LR, NB, Stacking, and ODL-MUDSS

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

techniques have acquired the lowest $prec_n$ of 66.07%, 87.05%, 89.05%, 96.07%, and 97.80%. Moreover, with $reca_l$, the MUR-COABBN technique provides an increased $reca_l$ of 98.52% although the SVM, LR, NB, Stacking, and ODL-MUDSS systems get lessened $reca_l$ of 75.06%, 96.96%, 97.04%, 97.07%, and 97.82%. Finally, based on F_{score}, the MUR-COABBN algorithm obtains an increased F_{score} of 98.53% but, the SVM, LR, NB, Stacking, and ODL-MUDSS methods acquire a decreased F_{score} of 91.49%, 90.81%, 95.67%, 93.59%, and 97.83%.

Table 4: Comparative outcomes of the MUR-COABBN system with other algorithms

Models	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
SVM	70.08	66.07	75.06	91.49
LR	93.07	87.05	96.96	90.81
NB	94.06	89.05	97.04	95.67
Stacking	97.07	96.07	97.07	93.59
ODL-MUDSS	97.82	97.80	97.82	97.83
MUR-COABBN	98.52	98.56	98.52	98.53

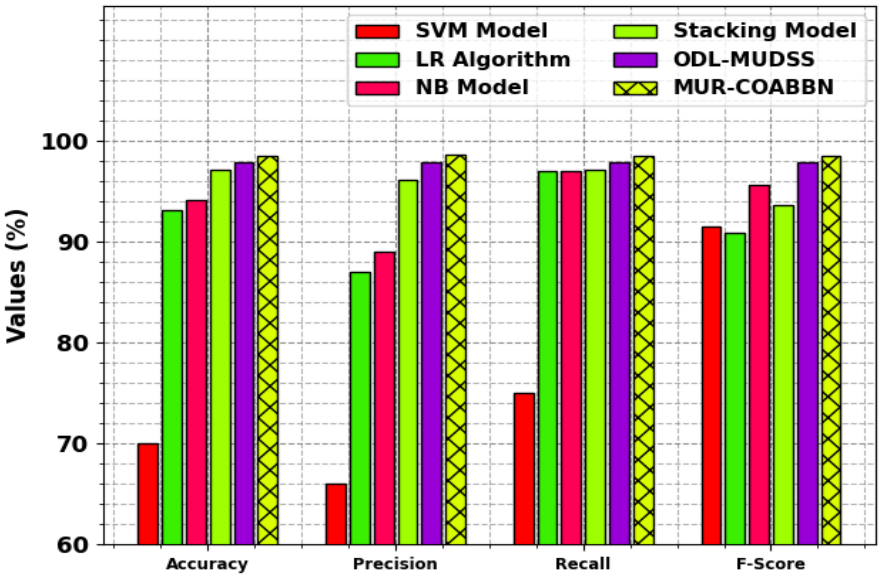

Figure 14. Comparative outcomes of MUR-COABBN models with other systems

In Table 5 and Fig. 15, the computational time (CT) assessment of the MUR-COABBN methodology has been compared with other approaches. According to CT, the MUR-COABBN algorithm gets a lesser CT of 1.70s whereas the SVM, LR, NB, Stacking, and ODL-MUDSS techniques gained a higher CT of 12.16s, 11.39s, 7.71s, 8.83s, and 4.19s, respectively.

Table 5: CT result of the MUR-COABBN method with recent techniques

Models	Computational Time (min)
SVM	12.16
LR	11.39
NB	7.71
Stacking	8.83
ODL-MUDSS	4.19
MUR-COABBN	1.70

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

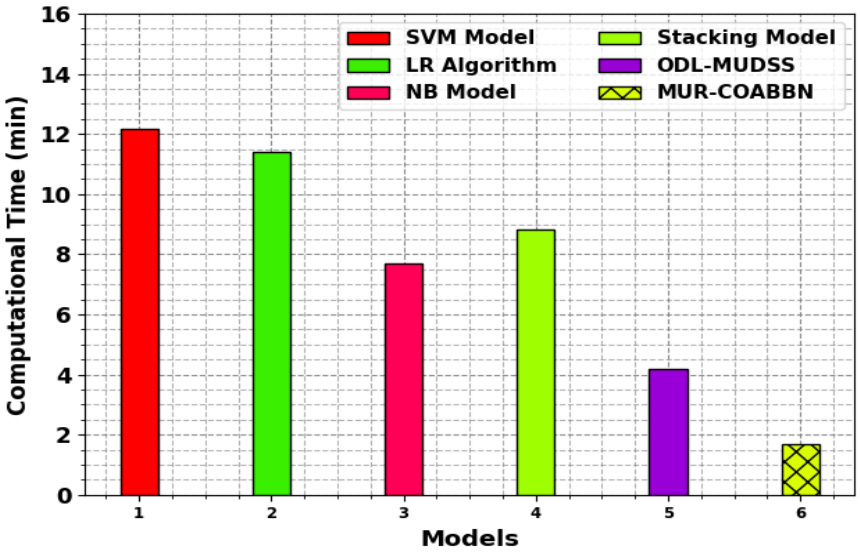

Figure 15. CT analysis of the MUR-COABBN technique with other algorithms

5. Conclusion

In this work, we have presented a new MUR-COABBN method for CRN. The MUR-COABBN technique exploits metaheuristics with the Bayesian ML approach for the classification of the MUs in the CRN. It contains three major processes such as COA-based feature subset selection, BBN-based MU recognition, and ISOA-based parameter-tune procedure. Initially, the MUR-COABBN technique takes place the COA is used to choose better feature subsets. Moreover, the detection of MUs can be performed by the use of BBN. Eventually, the parameter tuning of the BBN system was executed using ISOA. The experimental evaluation of the MUR-COABBN technique takes place in terms of distinct measures. The experimentation outcome stated the better efficiency of the MUR-COABBN algorithm with other methods in terms of distinct measures. Therefore, the MUR-COABBN technique can effectually and accurately improve security in the CRN

Funding: "The author gratefully acknowledges technical support provided by the Department of Information Systems, Faculty of Computing and Information Technology at Rabigh, King Abdulaziz University, Jeddah, Saudi Arabia"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Jain, N. Gupta, and M. Sreenu, ''Blockchain based smart contract for cooperative spectrum sensing in cognitive radio networks for sustainable beyond 5G wireless communication,'' Green Technol. Sustainability, vol. 1, no. 2, May 2023, Art. no. 100019.

[2] M. K. Giri and S. Majumder, ''Extreme learning machine based identification of malicious users for secure cooperative spectrum sensing in cognitive radio networks,'' Wireless Pers. Commun., vol. 130, no. 3, pp. 1993–2012, Jun. 2023.

[3] S. K. Agrawal, A. Samant, and S. K. Yadav, ''Spectrum sensing in cognitive radio networks and metacognition for dynamic spectrum sharing between radar and communication system: A review,'' Phys. Commun., vol. 52, Jun. 2022, Art. no. 101673.

[4] A. Khanna, P. Rani, T. H. Sheikh, D. Gupta, V. Kansal, and J. J. P. C. Rodrigues, ''Blockchain-based security enhancement and spectrum sensing in cognitive radio network,'' Wireless Pers. Commun., vol. 127, no. 3, pp. 1899–1921, Dec. 2022.

[5] A. Upadhye, P. Saravanan, S. S. Chandra, and S. Gurugopinath, ''A survey on machine learning algorithms for applications in cognitive radio networks,'' in Proc. IEEE Int. Conf. Electron., Comput. Commun. Technol. (CONECCT), Jul. 2021, pp. 01–06.

[6] S. K. Ram, ''Energy-efficient adaptive sensing for cognitive radio sensor network in the presence of primary user emulation attack,'' Comput. Electr. Eng., vol. 106, Mar. 2023, Art. no. 108619.

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024

[7] H. Jiang, Z. Yu, and J. Yang, ‘‘Research on key technology of full duplex cognitive radio network,’’ in Proc. J. Phys., Conf., May 2021, vol. 1920, no. 1, Art. no. 012035.

[8] M. Arkwazee, M. Ilyas, and A. Dawood Jasim, ‘‘Automatic spectrum sensing techniques using support vector machine in cognitive radio network,’’ in Proc. 2nd Int. Conf. Adv. Electr., Comput., Commun. Sustain. Technol. (ICAECT), Apr. 2022, pp. 1–6.

[9] A. Shirolkar and S. V. Sankpal, ‘‘Deep learning based performance of cooperative sensing in cognitive radio network,’’ in Proc. 2nd Global Conf. for Advancement Technol. (GCAT), Oct. 2021, pp. 1–4.

[10] K. Arshid, Z. Jianbiao, I. Hussain, G. G. Lema, M. Yaqub, and R. Munir, ‘‘Support vector machine approach of malicious user identification in cognitive radio networks,’’ Wireless Netw., 2022.

[11] Almuqren, L., Maray, M., Alotaibi, F.A., Alzahrani, A., Mahmud, A. and Rizwanullah, M., 2024. Optimal Deep Learning Empowered Malicious User Detection for Spectrum Sensing in Cognitive Radio Networks. IEEE Access.

[12] Benazzouza, S., Ridouani, M., Salahdine, F. and Hayar, A., 2022. A novel prediction model for malicious users detection and spectrum sensing based on stacking and deep learning. Sensors, 22(17), p.6477.

[13] Gong, Q., Liu, Y., Zhang, J., Chen, Y., Li, Q., Xiao, Y., Wang, X. and Hui, P., 2023. Detecting malicious accounts in online developer communities using deep learning. IEEE Transactions on Knowledge and Data Engineering.

[14] Maray, M., Maashi, M., Alshahrani, H.M., Aljameel, S.S., Abdelbagi, S. and Salama, A.S., 2024. Intelligent Pattern Recognition using Equilibrium Optimizer with Deep Learning Model for Android Malware Detection. IEEE Access.

[15] Maniriho, P., Mahmood, A.N. and Chowdhury, M.J.M., 2023. API-MalDetect: Automated malware detection framework for windows based on API calls and deep learning techniques. Journal of Network and Computer Applications, 218, p.103704.

[16] Chaganti, R., Ravi, V. and Pham, T.D., 2022. Deep learning based cross architecture internet of things malware detection and classification. Computers & Security, 120, p.102779.

[17] Liu, H., Han, F. and Zhang, Y., 2024. Malicious traffic detection for cloud-edge-end networks: A deep learning approach. Computer Communications, 215, pp.150-156.

[18] Aurangzeb, S. and Aleem, M., 2023. Evaluation and classification of obfuscated Android malware through deep learning using ensemble voting mechanism. Scientific Reports, 13(1), p.3093.

[19] Kaligineedi, P., Khabbazian, M. and Bhargava, V.K., 2010. Malicious user detection in a cognitive radio cooperative sensing system. IEEE Transactions on Wireless Communications, 9(8), pp.2488-2497.

[20] Naser, A.T., Mohammed, K.K., Ab Aziz, N.F., binti Kamil, K. and Mekhilef, S., 2024. Improved coot optimizer algorithm-based MPPT for PV systems under complex partial shading conditions and load variation. Energy Conversion and Management: X, p.100565.

[21] Yu, Z., Dong, H., Guo, T. and Zhao, B., 2024, February. A Multi-Surrogate Assisted Salp Swarm Feature Selection Algorithm with Multi-Population Adaptive Generation Strategy for Classification. In Asian Conference on Machine Learning (pp. 1590-1605). PMLR.

[22] Rabbi, M., Ali, S.M., Kabir, G., Mahtab, Z. and Paul, S.K., 2020. Green supply chain performance prediction using a Bayesian belief network. Sustainability, 12(3), p.1101.

[23] Yue, C., Zhao, X., Tao, L., Zheng, C., Ding, Y. and Guo, Y., 2024. An Improved Seeker Optimization Algorithm for Phase Sensitivity Enhancement of a Franckeite-and WS2-Based SPR Biosensor for Waterborne Bacteria Detection. Micromachines, 15(3), p.362.

DOI: https://doi.org/10.54216/JCIM.150211
Received: May 09, 2024 Revised: July 14, 2024 Accepted: October 25, 2024