Journal of Theoretical and Applied Information Technology
15th May 2026. Vol.104. No.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

QUASI OPPOSITIONAL LEARNING BASED AFRICAN BUFFALO OPTIMIZATION FOR ROBUST FEATURE SELECTION IN NETWORK INTRUSION DETECTION SYSTEM

PRASANNA KUMAR KRISHANAMOORTHY[1], SUBRAMANIYAN RADHAKRISHNAN[2]

[1]Department of Computer Science and Engineering, Takshashila University, Tindivanam, India

[2]Department of Electronics and Communication Engineering, Takshashila University, Tindivanam, India

E-mail: [1]Prasannakumar.k@takshashilauniv.ac.in, [2]Subramaniyan.r@takshashilauniv.ac.in

ABSTRACT

Detecting the anomaly network behavior is complex to establish the secure communication in network or system. The anomaly activities in networks seriously threaten the privacy of data, functions and the whole network infrastructure. The redundant, irrelevant and high-dimension features cause the overfitting issue in the learning process, resulting in high False Positive Rate (FPR) and less classification performance. To eliminate the redundant and high-dimension features, this article developed the Quasi Oppositional Based Learning (QOBL) strategy – African Buffalo Optimization (ABO) algorithm. The QOBL strategy is included in conventional ABO algorithm which improves the search ability and convergence rate for enhancing performance of feature selection process. In the classification phase, Recurrent Neural Network – Long Short-Term Memory (RNN-LSTM) technique is utilized to find intrusions in networks with high accuracy and less FPR. QOBL-ABO and RNN-LSTM based classifier obtained 99.99% accuracy on NSL-KDD and 99.94% on UNSW-NB15 dataset when compared to previous algorithms like Deep Neural Network (DNN).

Keywords: *African Buffalo Optimization, Long Short-Term Memory, Network Intrusion Detection System, Quasi Oppositional Based Learning and Recurrent Neural Network.*

1. INTRODUCTION

Widespread utilization of the internet has greatly enhanced convenience in daily life, but it has made cybersecurity threats more complex and challenging to address [1]. Network Intrusion Detection Systems (NIDS) are utilized for detecting security attacks in information systems [2]. Several IDSs rely on signature-based detection techniques, analyzing file patterns or typical data entries [3-5]. Because of a high number of components and devices, there has been a developing demand for intrusion detection systems that are strong and able to detect irregularities [6]. As the count of equipment increases, there is a high demand for effective IDS able to identify subtle anomalies [7]. The NIDS tasks have become much difficult recently as new network attacks continue emerging and network data traffic grows [8]. Machine Learning (ML)-based algorithms have been majorly utilised on IDS due to their capability for learning and identifying patterns from difficult data by statistical and advanced techniques. Intrusion detection techniques based on ML algorithms are distributed into two classes: supervised and unsupervised learning [9].

Deep Learning (DL)-based algorithm is the main branch of ML, which is dependent on neural networks with at least two hidden layers [10]. DL algorithms are much appropriate in automatic learning and extracting the features from huge data and have effective performance [11]. Instead of these benefits, feature engineering plays a significant part in DL-based algorithms while facing high dimension structured information [12]. The redundant, irrelevant and high-dimension features cause the overfitting issue in the learning process and result in a high False Positive Rate (FPR) in real environments [13]. There has been wide range of research employing diverse feature selection approaches to analyzing IDS to enhance performance and minimize FPR [14]. The one feature selection technique is dependent on the assumption of significance indicators for removing unnecessary features [15]. In this research, the feature selection technique and classifier to IDS on different datasets. The main contributions of this work are as follows:

- The QOBL- African Buffalo Optimization (QOBL-ABO) algorithm is proposed to improve feature selection by maximizing convergence speed and search capability.
- The RNN-LSTM classifier is used to capture temporal dependencies and minimize false positive rates in intrusion detection.
- The combined optimization-DL approach is introduced to address high-dimensionality and overfitting issues in IDS.

This research manuscript is organized below: Section 2 analyses previous research and summarizes literature review. Section 3 provides explanation of developed algorithm. Section 4 gives results and discussion of developed algorithm, and Section 5 concludes manuscript.

2. LITERATURE REVIEW

The existing algorithms used for NIDS are analyzed and summarized in this section with its advantages and disadvantages.

Joao Figueiredo et al. [16] developed new Deep Neural Network (DNN) based IDS method to classifying network traffic. The network with multi layers among input and output layer that has difficult non-linear relationships. The developed method learned to recognise the attacks through analyzing the huge enough group of labeled samples; next, the method was utilized for identifying the new DDoS attack samples. The developed method has much reliability of model, but the method doesn't use feature selection stage, that minimizes classification performance.

Arun Kumar Silivery et al. [17] introduced the RNN, LSTM-RNN and DNN for NIDS. The normalized information was given as input to the developed hybrid method. The DL-based methods self-learned features and classified information as multiple attack classification. The introduced method effectively extracts the features and minimizes the feature dimensionality. But the introduced method has high False Positive Rate (FPR) because of low representation of normal and abnormal data.

Ruqaya Abdulhasan Abed et al. [18] implemented feature selection techniques like the Pearson Correlation Analysis (PCA) technique and the Singular Value Decomposition (SVD) technique. Additionally, the data utilizing techniques like Stochastic Gradient Descent (SGD), Ridge Regression (RR) and Convolutional Neural Network (CNN) on converted feature areas. The implemented method reduces feature area dimensionality and extracts significant features for classification. However, implemented model doesn't address the issue of vanishing gradients in training phase, which minimizes the detection performance.

Yakubu Imrana et al. [19] presented the two-layer feature extraction and fusion method that used the focal loss function for handling class imbalance issues in IDS. The presented method has a two-phase feature extraction NIDS technique that efficiently leads to benefits of RNN and CNN by feature fusion. This presented method enabled the effective identification of network intrusions through including temporal and spatial feature learning from neural networks. Imbalanced class problem through using modified focal loss function, that improved accuracy of presented technique. But the presented method has a high false positive rate because of insufficient of sequential data in classification.

Shamshair Ali et al. [20] suggested the hybrid DL-based method, which synergizes the LSTM Auto Encoders and Multilayer Perceptron to detect the intrusions. The integration of these techniques facilitated the analysis of sequential information and pattern recognition, enabling the method for detecting anomaly activities in IoT networks. Suggested model improved robustness of method against zero-day attacks through learning unusual patterns without past knowledge. The suggested method extracted the significant features and performed the accurate classification. Though the suggested method has used the whole feature subset for the classification phase that includes irrelevant features, it minimized the classification performance.

In the above analysis, these existing algorithms have some limitations: they don't use the feature selection phase, do not address the issue of vanishing gradient and have high FPR. These limitations minimize the detection performance of NIDS. To overcome these limitations, here feature selection process is performed by developed QOBL-ABO algorithm, which incorporates the QOBL strategy to enhance the search ability and convergence rate for effective feature selection. Then, the classification phase is performed by using a developed RNN-LSTM network, which classifies the network traffic with high classification performance by minimizing the FPR and mitigating the vanishing gradient issue.

Many existing models have explored feature selection and DL algorithms for NIDS including metaheuristic-based optimization approaches like PSO, GWO and WOA and hybrid model like CNN,

RNN and LSTM. These models have limitations includes slow convergence, ineffective elimination of inappropriate features and high false positive rates. While certain model incorporates feature selection or DL-based approaches, some other works integrate improved optimization strategy with sequential DL-based approach. The proposed algorithm develops previous optimization and DL-based approaches, provides hybrid model which address the drawbacks. The incorporation of QOBL within ABO improves exploration and exploitation balance, ensures better feature subset selection when comparing to traditional metaheuristics approaches. Additionally, RNN-LSTM classifier efficiently extracts temporal dependencies in network traffic, provides enhanced detection accuracy and minimized false positive rates.

Despite the advancements in ML and DL-based NIDS, several challenges remain unresolved. Existing models suffer from high-dimensional feature spaces leads to overfitting and increased computational complexity. Moreover, many existing models lacks efficient feature selection mechanisms or fail to optimize selection process, resulted in redundant and inappropriate features that degrades classification performance. Additionally, higher False Positive Rates (FPR) and inadequate handling of sequential dependencies in network traffic limits reliability of intrusion detection systems. This manuscript focuses on enhancing feature selection and classification performance in NIDS using optimization and DL approaches. The scope is limited to software-based IDS using benchmark datasets, without considering real-time deployment or hardware-level intrusion detection mechanisms.

Research Questions

Based on above issues, this manuscript aims to address the following research questions

- RQ1 – How can feature selection be enhanced to efficiently remove redundant and high-dimensional features in NIDS?
- RQ2 – Can the integration of Quasi-Oppositional Based Learning improve the performance of metaheuristic optimization approaches for feature selection?
- RQ3 – How can DL approaches be developed to extract sequential patterns in network traffic while minimizing false positive rates?

RQ4 – Does the integration of optimized features selection with a classifier significantly enhance intrusion detection performance when comparing with existing models?

3. PROPOSED METHOD

The effective DL-based NIDS is developed by using pre-processing and a feature selection process. NSL-KDD and UNSW-NB15 datasets are utilized here, which includes traffic data, and these are pre-processed by using label encoding and robust scalar to enhance the data quality. Next, the feature selection phase is processed by using the developed QOBL-ABO algorithm and at last, the features are classified by using the RNN-LSTM network. Figure 1 describes the process of NIDS.

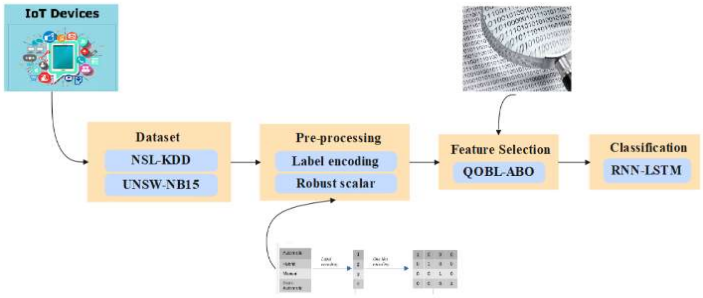

Figure 1: Process of NIDS

3.1 Dataset

NSL-KDD [21] and UNSW-NB15 [22] datasets are utilized in this article, which includes traffic data, and the description of these datasets is explained.

3.1.1 NSL-KDD dataset

This is increased form of KDD Cup'99 dataset. The dataset includes a total of 125,973 traffic files in training and 22,544 files in testing set. Dataset is classified to five various classes: Normal, Remote-to-Local (R2L), Denial of Service (DoS), Probe and User-to-Root (U2R). The dataset includes diverse traffic files with null duplicates. Table 1 describes per-class samples in NSL-KDD dataset.

Table 1: PER-Class SAMPLES in NSL-KDD Dataset.

Classes	Training set	Testing set
U2R	52	200
R2L	995	2754
Probe	11,656	2421
DoS	45,927	7458
Normal	67,343	9711
Total	125,973	22,544

3.1.2 UNSW-NB15 dataset

Dataset includes 100 GB of gathered raw traffic with 9 attack kinds like worms, fuzzers, generic, analysis, exploits, backdoor, shellcode, DoS and reconnaissance. The dataset has 175,341 files on training and 82,332 files on testing set. Every instance has 49 attributes, includes 2 class label attributes. Table 2 describes per-class samples of UNSW-NB15 dataset.

Table 2: per-Class SAMPLES of UNSW-NB15 dataset.

Classes	Training set	Testing set
Worms	130	44
Fuzzers	18,184	6062
Generic	40,000	18,871
Analysis	2000	677
Exploits	33,393	11,132
Backdoor	1746	583
Shellcode	1133	378
DoS	12,264	4089
Reconnaissance	10,491	3496
Total	175,341	82,332

3.2 Pre-processing

Data are fed as input to pre-processing stage to enhance quality of data. Here, label encoding and robust scalar are used for pre-processing, which is explained in detail.

Label encoding – While categorical features are utilized in the format of one-hot vectors, the neural network's dimension gets high and introduces complexities in training. For exploiting categorical features, it is required to represent the categorical features in efficient way. Include the embedding layer for converting one-hot vector to input of neural networks. For every categorical feature, embedding vector's dimension is represented as (e_{dim}) and its mathematical formula is given as Equation (1)

$$e_{dim} = round(\#(category)^{\alpha}) \quad (1)$$

In the above Equation (1), $\#(category)$ represents amount of categories for every categorical feature, α represents parameter and the $round(.)$ represents rounding function.

Robust scaler – The robust scaler is a data transformation technique, the same as min-max normalization through that transfers the information. The median and quartile ranges are utilized to scale the data for a good understanding of outliers. Mathematical equation for robust scalar is given as Equation (2),

$$x_{robust} = \frac{x_i - x_{median}}{Q_3(x) - Q_1(x)} \quad (2)$$

In above Equation (2), x_{median} defines data median, $Q_1(x)$ and $Q_3(x)$ represents first and third quartile of data.

3.3 Feature Selection

Pre-processed information is fed as input to feature selection, here, QOBL-ABO algorithm is utilized to chose relevant features from whole feature subset.

3.3.1 African Buffalo Optimization (ABO) algorithm

It is a recent meta-heuristic algorithm that offers an efficient communication and management architecture for the migration lifestyle process. It mimics voting behavior in decision-making, with movements managed through majority decisions. In its movement, it utilizes two sounds such as "maaa" and "waaa" for the exploration and exploitation phases. The sound "maaa" directs buffalos to stay in and exploit the current position that has enough pasture and is safe the sound "waaa" is utilized for exploring various positions due to the present position lacking in enough pasture. By utilizing these sounds, buffalos have the capability for optimizing their search to obtain optimal areas of food and its mathematical formula is given as Equation (3),

$$m_{k+1} = m_k + lp1(bg_{max} - w_k) + lp2(bg_{max.k} - w_k) \quad (3)$$

In the above Equation (3), the m_k represents maaa sound with particular reference to buffalo $k(k = 1,2,\dots,n)$, bg_{max} represents the position of optimal buffalo in herd, the $bg_{max.k}$ represents optimal position identified through individual buffalo, the $lp1$ and $lp2$ represents learning parameters $\in [0,1]$. By using the above Equation (3), the m_{k+1} represents indication for repositioning of buffalo from present position m_k to new position which reflected the excess memory ability in migration lifestyle. Mathematical expression for actual adjustment of herd movement is given as Equation (4),

$$w_{k+1} = \frac{(w_k + m_k)}{\lambda} \quad (4)$$

In above Equation (4), the w_{k+1} is movement for new position, the w_k represents present exploration values which shows "waaa" sound when m_k represents present exploitation values and the λ

represents parameter which determines unit of time interval across movement of buffalo generally set to 1. The algorithm described the ABO algorithm through initially positioning random kth buffalos in solution area. The last optimal solution acquired depended on adjusting buffalos' movement in iteration process. In every iteration, fitness value of every buffalo acquired and good between whole is employed to bg_{max}, while the optimal value for every individual is employed to $bg_{max.k}$. Every buffalo updates their position and movement depending on optimal neighboring buffalo following the above Equations (3) and (4). Employing this updation enables the buffalo's movement toward the optimal solution and tracks it.

3.3.2 Quasi-Oppositional Based Learning (QOBL)

Several swarm intelligence-based approaches adopt random processes for searching in iteration process, that causes slow convergence. Hence, opposition learning is introduced for generating related feasible solutions, analysing related solutions and choosing good candidate solutions for enhancing the search ability of conventional algorithms to solve non-linear optimization issues. Mathematical formula for oppositional learning is given in Equation (5),

$$P^o = lb + ub - P \quad (5)$$

In above Equation (5), $P = (p_1, p_2, \dots, p_n)$ represents a point in n-dimensional space. The new oppositional learning technique is introduced, known as "quasi-opposition-based learning" that gives solutions effective than oppositional learning. Mathematical formula for quasi-oppositional learning is given in Equation (6),

$$P^{qo} = rand\left(\frac{lb+}{2}, P^o\right) \quad (6)$$

In the above Equation (6), the $lb + ub/2$ is centre of $[lb, ub]$ interval and the $rand(lb + ub/2), P^o$ is random number.

3.4 Classification

RNN is a very popular technique for training the sequential data. The standard RNN have difficulty when it is utilized for training with a large step size. The below sections have described the process of RNN and LSTM networks.

3.4.1. RNN

RNN is extended version of standard feed-forward neural network, has a cyclic connection that allows for modeling sequences. Here, employs that input, hidden vector and result vector sequences are described through X, H and Y. Input is determined as $X = (x_1, x_2, \dots, x_T)$. Mathematical formula for RNN is given as Equations (7) and (8),

$$h_t = \sigma(W_x x_t + W_h h_{t-1} + b_h) \quad (7)$$

$$y_t = W_y h_t + b_y \quad (8)$$

In the above Equations (7) and (8), σ represents non-linearity function, W defines weight matrix and b defines bias term.

3.4.2. Long Short-Term Memory (LSTM)

LSTM captures sequential information with long-term dependencies. Structure of LSTM utilizes connections of feed-forward and connections of looping feedback. This is beneficial to retain data from a long time. The mathematical equations for executing values of three gates and cell state are given as Equations (9) to (13),

$$i_t = \sigma(W_i x_t + W_i h_{t-1} + W_i c_{t-1} + b_i) \quad (9)$$

$$f_t = \sigma\left(W_f x_t + W_f h_{t-1} + W_f c_{t-1} + b_f\right) \quad (10)$$

$$c_t = f_t c_{t-1} + i_c \tanh(W_c x_t + W_c h_{t-1} + b_c) \quad (11)$$

$$o_t = \sigma(W_o x_t + W_o h_{t-1} + W_o c_t + b_o) \quad (12)$$

$$h_t = o_t \tanh(c_t) \quad (13)$$

In the above equations, σ represents sigmoid function and $i, f, o\ and\ c$ represents input, forget, output and cell state, W_{ci}, W_{cf} and W_{co} represents weight matrices. The three gates in the LSTM control data flow. Input gate determines proportion of input. While measuring cell state, this proportion has an impact. The forget gate passes past memory h_{t-1}. By utilizing LSTM resolves the exploding and vanishing gradients issues because of three gates. In the RNN-LSTM structure, the recurrent hidden layer is replaced through the LSTM cell. Input is get and next sequentially moved by 4 layers. Activation function is utilized as Rectified Linear Unit (ReLU), which passes input directly to positive scores and results in zero. This is feasible for implementation and supports to protect against overfitting. Mean Squared Error (MSE) is used as loss function which processes mean squared variance among actual and predicted values. At last, one sigmoid layer gives the result from the cell state, which identifies the deviations from the abnormal behavior. Unlike traditional metaheuristic approaches like GWO and WOA, the proposed QOBL-ABO model introduced improved search mechanism by combining quasi-oppositional learning with behavior-based optimization. In GWO and WOA, search process relies majorly on mathematically predefined position updated and random initialization, that leads to premature convergence and limited exploration of search space. ABO uses adaptive exploration and exploitation by "waaa" and "maaa" signals, enables dynamic decision-making depending on environmental feedback. Moreover, incorporation of

QOBL improved population diversity by evaluating candidate and -opposite solutions, by accelerating convergence and enhancing global search ability. This mechanism efficiently avoids local optimal stagnation and ensures robust feature subset selection. As a result, QOBL-ABO provides stable and scalable optimization algorithm for high-dimensional intrusion detection issues while comparing with traditional metaheuristic algorithms.

4. EXPERIMENTAL ANALYSIS

Performance of implemented approach is simulated by Python environment and configurations are 8GB RAM, i5 processor and Windows 11 (64 bit). Evaluation measures taken to analyse performance of implemented algorithm are given below.

Accuracy - The ratio of accurately classified samples to whole samples and is measured by using Equation (14),

$$Accuracy = \frac{TN+TP}{TN+TP+FN+FP} \quad (14)$$

Recall – It is defined as True Positive Rate (TPR), defines ratio of correctly identified positive samples among total samples and is measured by using Equation (15),

$$Recall\ (TPR) = \frac{TP}{FN+TP} \quad (15)$$

Precision – It is determined as ratio of accurately detected positive samples among all predicted positive instances and is calculated by using Equation (16),

$$Precision = \frac{TP}{TP+FP} \quad (16)$$

F1-score – This is average of precision and recall and is measured by using Equation (17),

$$F1-score = \frac{2\times Precision\times Recall}{Precision+Recall} \quad (17)$$

In above equations, the TP is True Positive determined as correct identification of positive instances. The FN is a False Negative determined as the misidentification of positive instances. The FP is False Positive determined as misidentification of negative instances, and the TN is True Negative determined as correct identification of negative instances.

In Table 3, performance of optimization-based feature selection approach is analyzed. Particle Swarm Optimization (PSO), Grey Wolf Optimization (GWO) and Whale Optimization Algorithm (WOA) are conventional feature selection techniques considered to validate performance of developed QOBL-ABO technique. The QOBL-ABO based feature selection algorithm obtained 99.99% accuracy on NSL-KDD and 99.94% in UNSW-NB15 dataset.

Table 3: Performance QOBL-ABO for Feature Selection Algorithm.

Algorithms	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
NSL-KDD dataset				
PSO	94.53	94.23	93.94	94.07
GWO	96.11	95.85	95.53	95.68
WOA	97.76	97.52	97.23	97.36
QOBL-ABO	99.99	99.99	99.99	99.99
UNSW-NB15 dataset				
PSO	94.16	93.82	93.57	93.66
GWO	96.23	95.89	95.66	95.77
WOA	97.38	97.01	96.79	96.91
QOBL-ABO	99.94	99.79	99.79	99.79

In Table 4, performance of classifier is analyzed by NSL-KDD and UNSW-NB15 datasets. CNN LSTM and RNN are conventional classifiers considered to validate performance of RNN-LSTM classifier. RNN-LSTM based classifier obtained 99.99% accuracy on NSL-KDD and 99.94% accuracy on UNSW-NB15 dataset.

Table 4: Performance of RNN-LSTM Classifier using NSL-KDD and UNSW-NB15 DATASET.

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
NSL-KDD dataset				
CNN	92.82	92.51	92.21	92.37
LSTM	94.92	94.61	94.32	94.49
RNN	96.17	95.81	95.51	95.66
RNN-LSTM	99.99	99.99	99.99	99.99
UNSW-NB15 dataset				

CNN	93.28	92.47	92.18	92.36
LSTM	95.12	94.83	94.67	94.74
RNN	96.34	95.89	95.71	95.81
RNN-LSTM	99.94	99.79	99.79	99.79

4.1 Analysis of NSL-KDD

Figure 2 is accuracy vs epochs graph, Figure 3 defines loss vs epochs graph, Figure 4 represents the ROC curve, Figure 5 defines confusion matrix for NSL-KDD dataset.

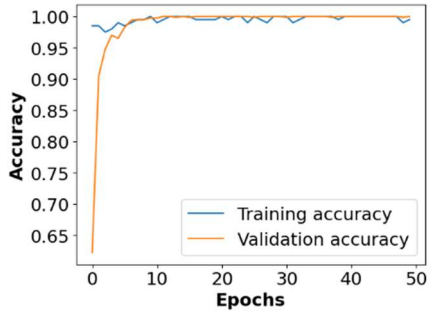

Figure 2: Accuracy vs Epochs for NSL-KDD dataset

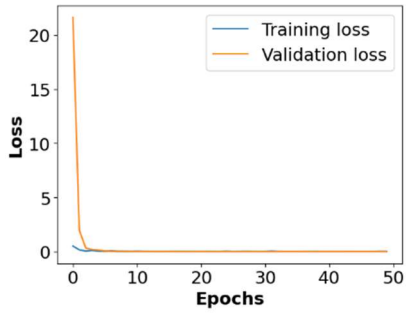

Figure 3: Loss vs Epochs for NSL-KDD dataset

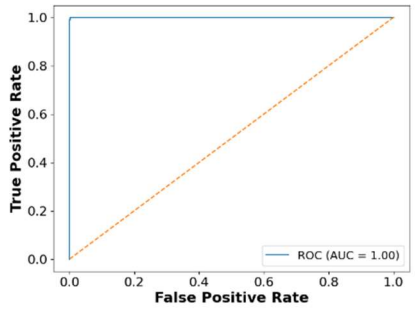

Figure 4. ROC curve for NSL-KDD dataset

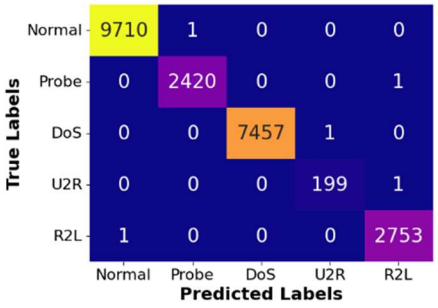

Figure 5: Confusion matrix for NSL-KDD dataset

4.2 Analysis of UNSW-NB15 dataset

Figure 6 defines accuracy vs epochs, Figure 7 defines loss vs epochs graph, Figure 8 represents the ROC, Figure 9 represents confusion matrix on UNSW-NB15 dataset.

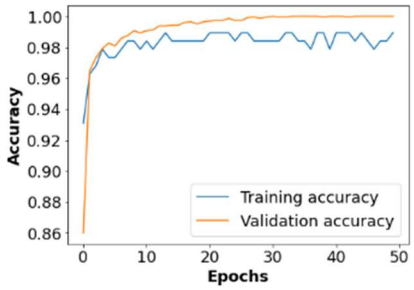

Figure 6: Accuracy vs Epochs for UNSW-NB15 dataset

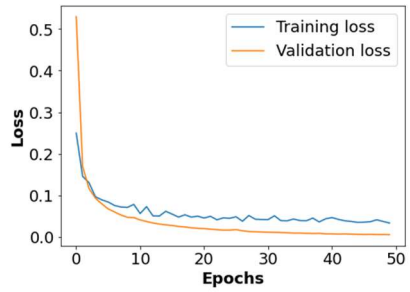

Figure 7: Loss vs Epochs for UNSW-NB15 dataset

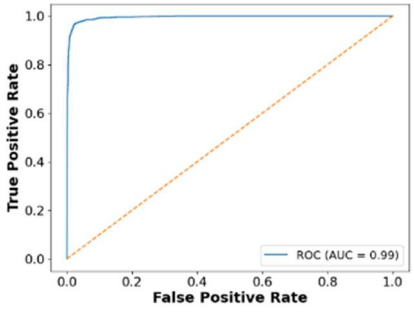

Figure 8: ROC curve for UNSW-NB15 dataset

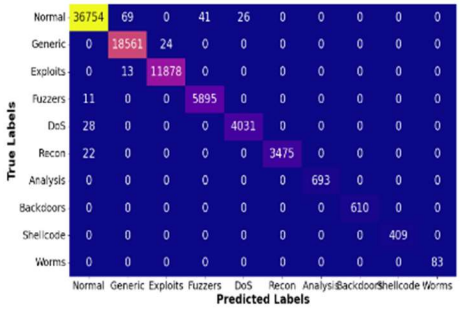

Figure 9: Confusion matrix for UNSW-NB15 dataset

Figure 9: Confusion matrix for UNSW-NB15 dataset

4.3 Comparative Analysis

The efficiency of developed technique is compared to existing approaches like DNN [16], DNN [17], CNN+PCA10 [18], CNN-GRU-FF [19] and LAE-MLP [20] by NSL-KDD and UNSW-NB15 datasets. Table 5 describes comparative analysis of developed algorithm. In this developed algorithm, the QOBL strategy is included in traditional ABO algorithm for feature selection, to select the relevant and appropriate attributes from whole feature subset. Then, chosen features are given to classification phase to classify network intrusions effectively. In the classification phase, the RNN-LSTM is used, which captures the temporal dependencies in data and mitigates the vanishing gradient issue, which helps for high classification performance.

Table 5: Comparative Analysis of developed algorithm.

Datasets	Models	Accuracy (%)	F1-score (%)	DR (%)	FPR
NSL-KDD	DNN [16]	99.63	NA	86.50	0.0011
	DNN [17]	98.95	99.07	99.87	3.49
	CNN-GRU-FF [19]	99.86	NA	99.68	NA
	Proposed QOBL-ABO and RNN-LSTM	99.99	99.99	99.99	0.0008
UNSW-NB15	CNN+PCA10 [18]	97.91	NA	NA	NA
	CNN-GRU-FF [19]	99.54	NA	98.22	NA
	LAE-MLP [20]	99.67	99.70	NA	NA
	Proposed QOBL-ABO and RNN-LSTM	99.94	99.79	99.92	0.0017

The proposed QOBL-ABO and RNN-LSTM model outperformance existing models in terms of accuracy and false positive rate. Unlike existing algorithms, that reply heavily on complete feature sets, proposed model incorporates an optimized feature selection mechanism which minimizes redundancy and enhances generalization. When comparing with existing models, proposed model efficiently extracts temporal dependencies in network traffic. Moreover, integration of QOBL improves convergence speed of optimization process, resulted in enhanced feature subset selection and overall performance.

4.4 Discussion

The performance of developed Q-OBL-ABO and RNN-LSTM network is evaluated with conventional techniques like PSO, GWO, WOA, CNN, LSTM and RNN using NSL-KDD and UNSW-NB15 datasets. Moreover, performance of developed algorithm is comparing to existing models like DNN [16], DNN [17], CNN+PCA10 [18], CNN-GRU-FF [19] and LAE-MLP [20]. These existing algorithms have some limitations, don't using the feature selection phase, and do not address the issue of vanishing gradient and having high FPR. These limitations minimize the detection performance of NIDS. To overcome these limitations, feature selection process is performed by developed QOBL-ABO approach, which incorporates the QOBL strategy to enhance the search ability and convergence rate for effective feature selection. Then, the classification phase is performed by using a developed RNN-LSTM network, which classifies the network traffic with high classification performance by minimizing the FPR and mitigating the vanishing gradient issue.

The optimization-based feature selection with DL-based feature selection with DL-based approach significantly improves intrusion detection performance. The QOBL-ABO approach efficiently minimizes feature dimensionality while preserving relevant feature, that contributes to enhanced classification accuracy. Moreover, the RNN-LSM classifier extracts temporal dependencies in network traffic, ensure more accurate detection of complex attack patterns. When comparing with existing models, the proposed model obtains better balance between accuracy and false positive rate, makes it suitable for cybersecurity systems.

4.4.1 Limitations

Despite obtaining higher performance, proposed model has some challenges. Initially, validation is conducted on benchmark dataset, that not fully represents real-time network environments with evolving attack patterns. The model relies of offline training, and its computational complexity have challenges for real-time deployment in large-scale networks. Moreover, performance of QOBL-ABO approach depends on parameters tuning, that affect generalization across diverse datasets.

5. CONCLUSION

This manuscript developed a NIDS by combining QOBL-ABO algorithm for feature selection, with an

RNN-LSTM-based classifier for intrusion detection. Unlike traditional algorithms, proposed model improves convergence behavior of metaheuristic optimization while handling sequential dependencies in network traffic data. This model addresses challenges of existing models includes high-dimensional feature spaces, redundant feature selection and vanishing gradient problems in DL-based approaches. The proposed approach determines significant practical impact by obtaining high detection accuracy with minimized false positive rates, makes it suitable for real-world cybersecurity applications. By enhancing feature selection efficacy and classification robustness, proposed model assist in fast and more reliable detection of cyber threats, by improving overall network security and minimizing operational overhead for security analysis. The experimental results on NSL-KDD and UNSW-NB15 datasets evaluates the effectiveness of proposed model, obtaining effective performance when comparing with existing approaches. These results represent that proposed model enhances detection accuracy and also ensures reliable and scalable intrusion detection in complex network environments. The QOBL-ABO and RNN-LSTM-based classifier obtained 99.99% accuracy on NSL-KDD and 99.94% in UNSW-NB15 dataset. Future work will focus on extending a proposed model to real-time intrusion detection scenarios and exploring its applicability in distributed and federated learning environments to improve adaptability and scalability.

REFERENCES

[1] Ullah, S. Ullah, G. Srivastava, and J.C. W. Lin, "IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic", *Digital Communications and Networks*, Vol. 10, No. 1, 2024, pp. 190-204.

[2] A. Kiflay, A. Tsokanos, M. Fazlali, and R. Kirner, "Network intrusion detection leveraging multimodal features", *Array*, Vol. 22, 2024, p. 100349.

[3] S.M. Kasongo, "A deep learning technique for intrusion detection system using a recurrent neural networks-based framework", *Computer Communications*, Vol. 199, 2023, pp. 11-125.

[4] M. Tahir, A. Abdullah, N.I. Udzir, and K.A. Kasmiran, "A novel approach for handling missing data to enhance network intrusion detection system", *Cyber Security and Applications*, Vol. 3, 2025, p. 100063.

[5] Y. Yin, J. Jang-Jaccard, W. Xu, A. Singh, J. Zhu, F. Sabrina, and J. Kwak, "IGRF-RFE: A hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset", *Journal of Big Data*, Vol. 10, No. 1, 2023, p. 15.

[6] J. Rahman, J. Singh, S. Nayak, B. Jena, L. Mohanty, N. Singh, J. R. Laird, R. Singh, D. Garg, N.N. Khanna, and M.M. Fouda, "A generalized and robust nonlinear approach based on machine learning for intrusion detection", *Applied Artificial Intelligence*, Vol. 38, No. 1, 2024, p. 2376983.

[7] L.A. Maghrabi, "Automated network intrusion detection for Internet of Things security enhancements", *IEEE Access*, Vol. 12, 2024, pp. 30839-30851.

[8] Z. Zoghi and G. Serpen, "Building an intrusion detection system on UNSW-NB15: Reducing the margin of error to deal with data overlap and imbalance", *Concurrency and Computation: Practice and Experience*, Vol. 36, No. 25, 2024, p. e8242.

[9] S.A. Elsaid, E. Shehab, A.M. Mattar, A.T. Azar, and I.A. Hameed, "Hybrid intrusion detection models based on GWO optimized deep learning", *Discover Applied Sciences*, Vol. 6, No. 10, 2024, p. 531.

[10] S.A. Ajagbe, J.B. Awotunde, and H. Florez, "Intrusion detection: A comparison study of machine learning models using unbalanced dataset", *SN Computer Science*, Vol. 5, No. 8, 2024, p. 1028.

[11] S. Walling and S. Lodh, "Enhancing IoT intrusion detection through machine learning with AN-SFS: A novel approach to high-performing adaptive feature selection", *Discover Internet Things*, Vol. 4, No. 1, 2024, p. 16.

[12] Z. Liu, S. Liu, and J. Zhang, "An industrial intrusion detection method based on hybrid convolutional neural networks with improved TCN", *Computers, Materials & Continua*, Vol. 78, No. 1, 2024, pp. 411- 433.

[13] E.U.H. Qazi, M.H. Faheem, and T. Zia, "HDLNIDS: Hybrid deep-learning-based network intrusion detection system", *Applied Sciences*, Vol. 13, No. 8, 2023, p. 4921.

[14] F. Ullah, A. Turab, S. Ullah, D. Cacciagrano, and Y. Zhao, "Enhanced network intrusion detection system for Internet of Things security using multimodal big data representation with transfer learning and game theory", *Sensors*, Vol. 24, No. 13, 2024, p. 4152.

[15] W.T. Valavan and N. Joseph, "Satin bird optimization and sliced Bi-directional gated

recurrent unit based network intrusion detection system", *Computers and Electrical Engineering*, Vol. 128, 2025, p. 110760.

[16] J. Figueiredo, C. Serrão, and A.M. de Almeida, "Deep learning model transposition for network intrusion detection systems", *Electronics*, Vol. 12, No. 2, 2023, p. 293.

[17] A.K. Silivery, R.M.R. Kovvur, R. Solleti, L.S. Kumar, and B. Madhu, "A model for multi-attack classification to improve intrusion detection performance using deep learning approaches", *Measurement: Sensors*, Vol. 30, 2023, p. 100924.

[18] R.A. Abed, E.K. Hamza, and A.J. Humaidi, "A modified CNN-IDS model for enhancing the efficacy of intrusion detection system", *Measurement: Sensors*, vol. 35, 2024, p. 101299.

[19] Y. Imrana, Y. Xiang, L. Ali, A. Noor, K. Sarpong, and M. A. Abdullah, "CNN-GRU-FF: A double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units", *Complex & Intelligent Systems*, Vol. 10, 2024, pp. 3353-3370.

[20] S. Ali, R. Ghazal, N. Qadeer, O. Saidani, F. Alhayan, A. Masood, R. Saleem, M. A. Khan, and D. Gupta, "A novel approach of botnet detection using hybrid deep learning for enhancing security in IoT networks", *Alexandria Engineering Journal*, Vol. 103, 2024, pp. 88-97.

[21] NSLKDDdataset: https://www.kaggle.com/datasets/hassan06/nslkd

[22] UNSW-NB15 dataset: https://research.unsw.edu.au/projects/unsw-nb15-dataset.