Original scientific paper
https://doi.org/10.33180/InfMIDEM2023.304

Informacije MIDEM
Journal of Microelectronics, Electronic Components and Materials
Vol. 53, No. 3(2023), 167 – 176

Detection of Burst Header Packet Flooding Attacks via Optimization based Deep Learning Framework in Optical Burst Switching Network

Ramkumar Vahalingam[1], Bhavani Rajagopal[2], Sathishkumar Arumugam[3] and Muneeswari Ganesa Pandian[4]

[1]Assistant Professor, Department of Computer science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
[2]Department of Electronics and Communication Engineering, K. Ramakrishnan college of Technology Samayapuram, Tamil Nadu, India
[3]Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai
[4]Department School of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh, India

Abstract: Optical Burst Switching (OBS) technique has the greatest potential for securing future Internet connections. In real-time applications, OBS adoption is motivated by the lack of Quality of Service (QoS) in OBS networks. The accuracy of existing methods for detecting the misbehaving nodes that cause Burst Heading Packet (BHP) flooding attacks is typically poor. To overcome these issues, a novel Elephant Herd Algorithm-based Deep Learning (EHA-DL) network has been proposed for detecting BHP flooding attacks. The proposed approach is divided into three phases: pre-processing, feature selection, and classification. The Elephant Herd Algorithm (EHA) is used to select the most crucial features after pre-processing the raw data to increase the effectiveness of the model. To decrease overfitting and increase detection accuracy, a MobileNet is used to construct the model for the classification phase using the select features of BHPs. The performance of the experimental outcomes was assessed using evaluation metrics like accuracy, specificity, recall, and f-measure. The EHA-DL approach method yielded a 99.27% accuracy rate, which was comparatively high when compared to other approaches. In optical burst switching networks, the method effectively and highly efficiently detects flooding assaults and maintains network stability.

Keywords: Optical Bust Switching; Quality of Service; Burst Header Packet (BHP) flooding attack; Deep learning

Detekcija napadov s hitrimi naslovnimi paketi s pomočjo optimizacije na osnovi globokega učenja v omrežju optičnega hitrega prekapljanja

Izvleček: Tehnika optičnega hitrega preklapljanja (Optical Burst Switching - OBS) ima največji potencial za zavarovanje prihodnjih internetnih povezav. Pri aplikacijah v realnem času je razlog za uvedbo OBS pomanjkanje kakovosti storitev (QoS) v omrežjih OBS. Natančnost obstoječih metod za odkrivanje nepravilno delujočih vozlišč, ki povzročajo poplavne napade s paketi BHP (Burst Heading Packet), je običajno slaba. Za odpravo teh težav je bilo predlagano novo omrežje EHA-DL (Elephant Herd Algorithm-based Deep Learning) za odkrivanje poplavnih napadov BHP. Predlagani pristop je razdeljen na tri faze: predobdelava, izbira značilnosti in klasifikacija. Algoritem Elephant Herd Algorithm (EHA) se uporablja za izbiro najpomembnejših značilnosti po predhodni obdelavi neobdelanih podatkov, da se poveča učinkovitost modela. Za zmanjšanje pretiranega prilagajanja in povečanje natančnosti zaznavanja se za izdelavo modela za fazo razvrščanja z izbranimi značilnostmi BHP uporablja mobilna mreža. Uspešnost eksperimentalnih rezultatov je bila ocenjena z ocenjevalnimi metrikami, kot so natančnost, specifičnost, priklic in f-merilo. Metoda pristopa EHA-DL je dala 99,27-odstotno stopnjo natančnosti, ki je bila v primerjavi z drugimi pristopi razmeroma visoka. V optičnih omrežjih s preklapljanjem s prekinitvami metoda uspešno in zelo učinkovito odkriva napade s poplavljanjem in ohranja stabilnost omrežja.

Ključne besede: Optično hitro preklapljanje; kakovost storitev; napad s poplavljanjem paketov BHP (Burst Header Packet); globoko učenje

* *Corresponding Author's e-mail: rv6094542@gmail.com*

How to cite:
R. Vahalingam et al., "Detection of Burst Header Packet Flooding Attacks via Optimization based Deep Learning Framework in Optical Burst Switching Network", Inf. Midem-J. Microelectron. Electron. Compon. Mater., Vol. 53, No. 3(2023), pp. 167–176

1Introduction

Optical fiber communication outperformed conventional communication systems and revolutionized communication technology [1]. Over the last few decades, optical networks have expanded quickly in tandem with rising bandwidth demands [2]. Consequently, optical burst switching networks are commonly used as both a backbone and an access network today [3]. The development of Internet backbone infrastructures has been made possible by OBS, which has grown in importance as a method for switching subwavelengths in networks [4]. Three different node categories, referred to as core nodes, ingress nodes, and egress nodes, make up the primary component of the OBS network. Optical data bursts are processed through control data packets with information by intermediate nodes called core nodes, which avoid buffering [5].

In OBS, the client packet is merged into a burst header packet (BHP) and a Data Burst (DB) at the edge nodes (ingress nodes) [6]. OBS networks still face several QoS and security issues as a consequence of BHP flooding attacks, despite all of their network benefits, including resilience, bandwidth/resource efficiency, and overall financial benefits [7]. Preparing the channel for incoming DB is done using OBS's BHP feature. An attacker can use this function to transmit fake BHPs without being acknowledged by the DB. It is important to understand that Denial-of-Service (DoS) attacks are one of the most significant security risks to networks, which can lower network efficiency through reduced bandwidth utilization and increased data loss [8,9].

BHP flooding is a type of assault where a lot of BHPs are sent into a network to control the switches [10]. Malicious nodes flood the network with BHPs during a BHP flooding assault, which reduces network bandwidth usage. Since it takes over the core switch and fills the wavelength division multiplexing channel, regular BHP is unable to transmit [11]. Flood attacks result in serious data loss, network performance degradation, and bandwidth waste when edge nodes send BHP at high speeds to reserve bandwidth for future bursts of data. Another major danger to network security is denial-of-service (DoS) attacks [12,27].

Numerous strategies have been developed in the literature for defending against BHP flooding attacks and DoS against OBS networks, with positive results. However, because OBS core switches have limited capabilities, it is still difficult for developers and researchers to come up with an effective technique that achieves high accuracy with a minimal number of features. This study's main goal is to reduce those risks by analyzing edge node behavior in OBS networks during BHP flood attacks. In this research, a novel Elephant herd algorithm-based Deep learning (EHA-DL) has been proposed for detecting BHP flooding attacks [28]. The major contribution of the proposed technique is;
The primary goal is to develop a novel Elephant herd algorithm-based Deep learning (EHA-DL).
The Elephant Herd Algorithm (EHA) is utilized to select the most crucial features after pre-processing the raw data to increase the effectiveness of the model.
To decrease overfitting and increase detection accuracy, a MobileNet is used to construct the model for the classification phase using the select features of BHP.
Evaluation measures like accuracy, precision, recall, specificity, and f-measure were used to evaluate the performance of the experimental results.

The following examples illustrate the remaining section of this study: the literature survey is explained in Section 2. The proposed approach and its corresponding algorithm are described in Section 3. The findings of the performance analysis are described in Section 4. Section 5 encloses a conclusion and future work.

2 Literature survey

In 2018, Uzel, V.N., and Eşsiz, E.S., et al [13] presented machine learning methods for categorizing BHP Flooding Attacks into four class labels. The following techniques are employed in classification: Multilayer Perceptron (MLP), Logistic, Decision Tree (J48), Reduce Error Pruning (REP) Tree, Naive Bayes (NB), and Random Tree (RT). As a consequence, it has been discovered that J48 and RT produce the best outcomes with greater accuracy.

An approach to lower the likelihood of BHP flooding assaults in OBS networks was proposed by Rajab, A., et al. [14] in 2018. Based on the principles derived by the proposed learning algorithm, the results show that 93% of BHP flooding attacks will be accurately classified into either the Behaving (B) or Mis-behaving (M) classes. Based on comparisons with experts or human network managers, the results of the proposed decision tree model are overwhelmingly positive.

In 2018, Hasan, M.Z., et al [15] introduced a Deep Convolution Neural Network (DCNN) model for autonomously identifying edge nodes. The demonstration demonstrated that the suggested model performs as expected for datasets with a specific collection of features. The results show that the suggested deep model performs better than any other conventional model (SVM, KNN, and Naive Bayes).

Haque, M.M., and Hossain, M.K. [16] proposed the use of K-means in 2019 to detect malicious nodes in an OBS network. In experiments, the model could categorize all nodes as behaving or non-behaving with 90% accuracy after only 20% of the data was used for training. Based on various performance metrics, the proposed model outperforms existing methods.

In 2019, Rajab, A., [17] suggested using machine learning (ML) to detect and block misbehaving ingress nodes at an early stage. More than two ingress nodes, more than 530 runs, and simulation data were used to test a range of machine-learning techniques. The runtime results, expressed in milliseconds, show that decision tree classifiers outperform the other algorithms in terms of efficiency and prediction.

In 2020, Kamrul Hossain and Mokammel Haque [18] suggested using a Gaussian mixture model (GMM) predictor to forecast how traffic will behave in an OBS network. Only 1% of the test data were labelled, and they discovered the highest accuracy of 69.7% using the tied covariance type of the constructed GMM.

in 2020, Almaslukh, B., [19] suggested an effective and efficient ML-based security method for identifying BHP flooding attacks. A phase of feature selection and a phase of categorization make up the suggested methodology. Comparing the efficacy as well as efficiency of the suggested method with related research, it is found to be appropriate for OBS security of networks.

A method for identifying BHP flooding attacks using particle swarm optimization and support vector machines (PSO-SVM) was presented by Liu, S., et al. [20] in 2021. The outcomes of the experiments demonstrate that the PSO-SVM model's detection efficiency is 95.0%. In identifying assaults in OBS networks and preserving the security and stability of the network, the suggested method is efficient and highly effective.

In 2021, EFEOLU, E. and Gürkan, T.U.N.A. [21] introduced K* algorithms and Sequential Minimal Optimization (SMO) for categorizing BHP attacks. Based on standard performance metrics, the suggested SMO and K* algorithms' performances are contrasted. The findings demonstrate that the K* algorithm is more effective at forecasting BHP Flooding attacks than the SMO algorithm.

Panda (2019) introduced the Flower Pollination method (FPA) and subsequently employed a Decision Forest method that penalizes attribute classifiers to detect flooding threats. The efficacy of the suggested approach is evaluated using several performance criteria, such as recall, informedness, specificity, sensitivity, precision, and accuracy.

According to a literature review, BHP flood attacks typically have low detection accuracy for the misbehaving nodes that contribute to BHP attacks, but they can achieve high detection accuracy with a small number of features. To overcome these challenges, a novel Elephant herd algorithm-based Deep learning has been proposed.

3 Proposed methodology

In this research, a novel Elephant herd algorithm-based Deep learning (EHA-DL) has been proposed for detecting BHP flooding attacks. The proposed method is categorized into three phases: pre-processing, feature selection, and classification. The EHA is used to select the most crucial features after pre-processing the raw data to increase the effectiveness of the model. To decrease overfitting and increase detection accuracy, a MobileNet is used to construct the model for the classification phase using the selected features of BHP. The overall block of the proposed method is depicted in Fig 1.

3.1 Pre-processing

It is essential for improving the data's suitability for model analysis and learning. Initial data is typically incomplete in the actual world, also known as "dirty data." Direct learning from these data could result in some mistakes. Data preparation is the process of transforming "dirty data" into a format that machine language can "learn" easily. This phase involves data cleaning, data transformation, and data noise removal.

Data Cleaning: In this process, only a small number of missing values are removed from the data, so it does not affect the analysis. It also removed the Packet Size Byte (D11), which is a constant value and does not provide any useful information.

Data transformation: This procedure involves the not behaving, NB Block, Block, Block, node status behaving, NB, probably not behaving, and No Block Wait are transformed into one-hot encoding, which improves the processing efficiency of the classifier. One-hot encodings, for instance, of the "Node Status," such as " B, NB, PNB," are {0, 1, 0}, {1, 0, 0}, and {0, 0, 1} correspondingly.After transformation, all the data are transformed into numeric values. The features should be normalized to make the various indicators comparable to remove the dimensional impact between data features. Afterward, min-max normalization is used to standardize data, removing the influence of various samples' attributes with varying orders of magnitude as well as improving classification accuracy by searching for the best gradient descent solution.

$$Normal_p = \frac{P - P_{min}}{P_{max} - P_{min}} \quad (1)$$

Where, $Normal_p$ represents the normal value, P_{max} and P_{min} represents the minimum and maximum data before normalization. By using this technique, the data is compressed to a number that is proportionally equal to the original value and falls within the [0, 1] range.

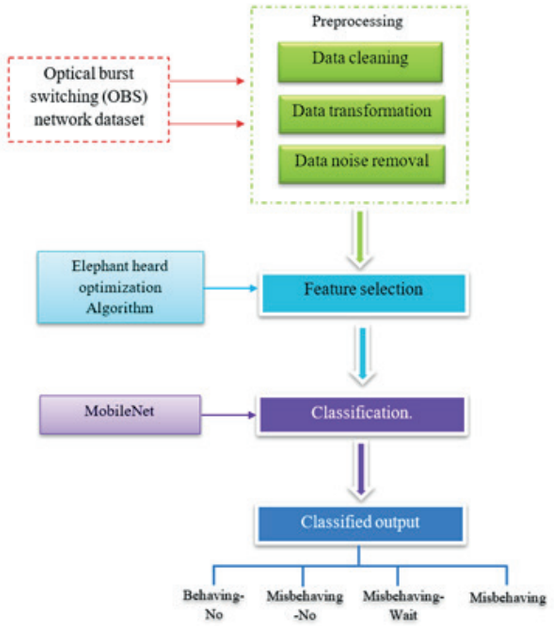

Figure 1: The overall block of the EHA-DL model

Data noise removal: The Gaussian distribution is used to introduce noise into the data to make the variables statistically more significant and to level the values of the variables. Additionally, it serves to avoid overfitting during developing models. A mathematical formula for Normal distribution is given in equation (2)

$$\varphi(q) = \frac{1}{\sqrt{2\pi\tau}} \exp\{-(-(q-\omega)^2 / 2\tau^2 \quad (2)$$

Where, π, τ denotes the variance and expectation of Gaussian distribution.

3.2 Feature selection via elephant herd algorithm (EHA)

Following preprocessing, the feature selection stage removes as much of the pre-processed data as feasible to enhance model training performance. EHA is used to select relevant features [23, 24, 25]. It is based on how elephants behave and live. Elephant intelligence (EHA) is a heuristic intelligence system that draws inspiration from elephants' nomadic lifestyle. Elephants are social animals with a sophisticated structure that consists of a female and young. The EHA selects the most pertinent features from the extracted features. After the matriarch dies, the best female elephant in the clan is designated as the most relevant feature of the data; the irrelevant features represent the male elephants with the lowest fitness value. The number of elephants in this algorithm indicates the features that were extracted from the input layer.

An elephant herd consists of multiple clans, each headed by a matriarch who may be responsible for caring for calves or other related females. The algorithm suggests the following guidelines: Elephants live in clans, with a certain number of elephants belonging to each tribe. In addition, every tribe has a matriarch who serves as the leader (the most physically fit elephant in the clan). Every generation, a predetermined number of elephants (the worst candidates) must leave the clan, and the matriarch is in charge of the entire clan of elephants. The Elephant Herding Optimization algorithm consists of two stages: separation operators and clan update operators. The entire population of elephants is initially split up into 'y' clans. Each elephant m_x a new position is influenced by the matriarch m_x. The clan m_x elephant 'y' can be determined using

At first, all elephants in the population are divided into "y" clans. The matriarch m_x has an impact on every elephant m_x that moves into a new position. It is possible to identify the clan m_x elephant 'y' using

$$P_{n,m_{x,y}} = P_{m_{x,y}} + \alpha \times \left(P_{best,m_x} - \lambda_{m_{x,j}} \right) \times L \quad (3)$$

where $P_{n,m_{x,y}}$ represents the old and new places of elephant "y" in clan x, P_{best,m_x} represents the position with the highest fitness values inside clan "x," and [0,1] is a scaling factor. L is a random number with an average distribution and a value in the interval [0, 1]. The best elephants in each clan are chosen using

$$P_{n,m_{x,y}} = \beta \times P_{ct,m_x} \quad (4)$$

In the following iteration, the position of the clan leader $P_{n,m_{x,y}}$ will vary based on the influence of the clan center P_{ct,m_x}, with $\beta \in [0.1]$ representing the scaling factor. The value of a clan center is calculated using Eq. (5):

$$P_{ct,m_x,k} = \frac{1}{N_{m_x}} \times \sum_{y=1}^{N_{m_x}} P_{ct,m_x,k} \quad where 1 \le k \le K \quad (5)$$

The total number of elephants in the clan, N_{m_x}, is represented by the k[th] dimension of each elephant. The information of every clan member is connected to the updating of the matriarch position in Equation (4).

During the separation process, the worst solution individuals are swapped out for randomly initialized individuals. Elephant populations grow as a result, and their ability to explore is enhanced. Each tribe's least valuable elephants are moved to the location shown by

$$P_{w,m_x} = P_{Min} + \left(P_{Max} - \lambda_{Min} + 1\right) \times L \tag{6}$$

The positions of the elephant with the lowest and highest fitness values in clan "x" are denoted by P_{w,m_x} and; L is a random number with a normal distribution falling between [0, 1].

Selecting a random number slows down convergence by introducing problems like random replacement of the smallest person and lack of exploitation. To address this problem, the LF mode and the EHO are combined. The model for the LF is,

$$LF\left(L\right) = \begin{cases} 1 & L < 1 \\ (L)^{-F} & L \geq 1 \end{cases} \tag{7}$$

The progress of EHA with LF is obtained by combining equations 5 and 6.

$$P_{w,m_x} = P_{Min} + \left(P_{Max} - \lambda_{Min} + 1\right) \times LeF\left(L\right) \tag{8}$$

As a result, the EHA provides the most pertinent features, which are as follows:

$$RF_x = \left\{rf_1, rf_2, rf_3, \ldots\ldots, rf_n\right\} \tag{9}$$

Following the inputs' multiplication by the feature vectors, the features that were randomly selected are then added together. The input layer can be expressed numerically as

$$I_x = \sum_{x=1}^{n} RF_x w_x + B_x \tag{10}$$

In this instance, RF_x represents the input features, w_x indicates the weight values, B_x indicates the bias value, and I_x displays the IL.

3.3 Classification via MobileNet

The selected features are classified by utilizing MobileNet. The convolution used in conventional networks is regular, however in this network, depth-wise separable convolution (DSConv). Requiring fewer modulo parameters than a standard convolution network, a MobileNet [26] network built on DSConv can carry out the same feature extraction function. Hardware resource constraints related to networks can thus be loosened. Pairwise convolution (PWConv) and depth-wise convolution (DWConv) are combined to create a depth-wise separable convolution. Figure 2 illustrates the structure.

DWConv does not support multidimensional convolution kernels; instead, each convolution kernel is limited to handling a single channel. After DWConv, the number of channels cannot be raised. Furthermore, using feature data from several channels at the same spatial position is not feasible due to the sequential nature of each convolution operation between each channel. PWConv must be paired with the feature maps produced by DWConv to produce new feature maps. PWConv is distinct from regular convolution due to its convolution kernel size of 1x1. A combination of sev-

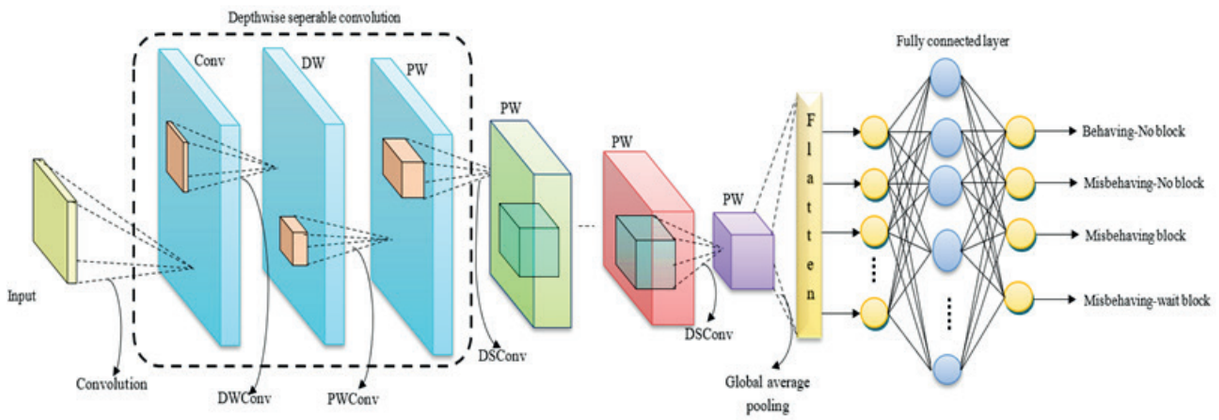

Figure 2: Architecture of proposed MobileNet

eral convolutions with rectified linear units (ReLUs) makes up the fundamental model's degrees of abstraction. employing the resolution multiplier variable ω to reduce the dimensionality and internal depiction of each layer in the input using the same variable. The kernel has dimensions of $k_s * k_s$, while the feature vector map has dimensions of $f_m * f_m$. The variable that is input is called x, while the variable that is output is denoted by y. To assess the total computing efforts C_{eff} for the network's central abstract layers, utilize equation (9) as follows.

$$C_{eff} = k_s * k_s * \omega * \alpha f_m + \omega * \rho * \alpha f_m * \alpha f_m \quad (11)$$

The multiplier value is clear for context, and the range from 1 to n is taken into account for the weed classification breakdown that results. The value of the variable resolution multiplier is expected to be 1, and it is recognized as ω. The variable $cost_{eff}$ is used to identify the computational efforts, and Equation (12) is used to assess it.

$$cost_{eff} = k_s * k_s * \omega * \rho * f_m * f_m \quad (12)$$

The DWConv and MobileNet are integrated, and PW-Conv is restricted in the reduction variable identified by the variable D, which resembles Equation (13),

$$D = \frac{f_s * f_s * \omega * \alpha f_m + \omega * \rho * \alpha f_m * \alpha f_m}{f_s * f_s * \omega * \rho * f_m * f_m} \quad (13)$$

The resolution multiplier and width multiplier both contribute to adjusting the window area for precise prediction in various circumstances.

4 Results and discussion

In this section, the performance analysis and comparative are discussed in detail. The proposed EHA-DL experiments are performed in Anaconda using an Intel Core i7 processor running at 3.40 GHz and 8 GB of RAM. This subsection has been divided into the following: dataset preparation, evaluation metrics, and analyses.

4.1 OBS network dataset description

Numerous BHP DDoS assaults on OBS networks are documented in the OBS Network Dataset [19]. The goal class label has 21 attributes, and there are 1,075 instances.

Table 1: Number of instances for each class in the OBS network dataset.

Class Label	MB-No block	MB-wait block	B Block	M B block	Total
Number of instances	500	300	120	155	1075

Is target label has four different class kinds, including Behaving block (B block), misbehaving no block (MB-No block), Mis behaving block (MB block), and Misbehaving-wait block (MB-wait block). Every feature in the dataset has a numeric value aside from the node state feature. The test dataset makes up 25% of the total data, while the training dataset makes up 75%. Table 1 shows the number of instances for each class in the dataset.

4.2 Evaluation metrics

The effectiveness of the suggested technique was evaluated using various parameters, including specificity, recall, F1 score, accuracy, and precision based on the datasets gathered.

Accuracy is the proportion of the test set that was accurately predicted. The specificity, also known as the true negative rate, is a measure of how many negatives are accurately predicted. A recall also known as true positive rate or sensitivity gauges the percentage of positives that are accurately anticipated. How many of the precision measures that an algorithm predicted to be positive truly. F-measure calculates a suggested method's performance by allowing for both recall and precision.

$$Accuracy(A) = \frac{TP + TN}{all\ samples} \quad (14)$$

$$Specificity(S) = \frac{TN}{TN + FP} \quad (15)$$

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

$$Recall(R) = \frac{TP}{TP + FN} \quad (17)$$

$$F\ measure = \frac{P \times R}{P + R} \quad (18)$$

Where, false positives and negatives of the sample data are denoted by FP and FN instead of true positives and negatives (TP and

TN), respectively. Table 2 and Fig. 3 both provide visual representations of the effectiveness of the suggested approach for categorizing various BHP flooding attack types.

Table 2: Performance analysis of the proposed EHA-DL

Parameters	MB-No block	MB-wait block	B Block	MB block
Accuracy	98	98.32	99.54	99.15
Specificity	97.25	96.25	99.15	98.45
Recall	98.21	98.25	99.47	97.54
Precision	97.42	97.64	98.25	96.18
F measure	98.75	97.56	99.05	97.25

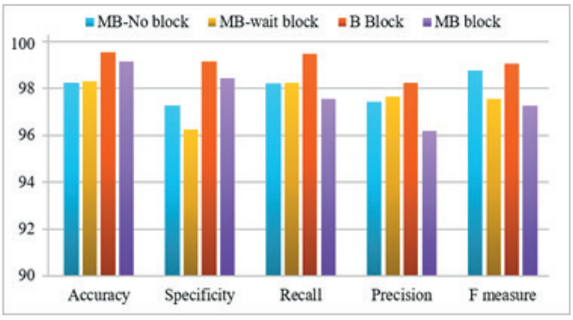

Figure 3: Graphical representation of different BHP flooding attack

Table 1 shows the performance of the proposed EHA-DL for categorizing the various kinds of BHP flooding attacks, including MB-wait block, NB-No block, B block, and MB block. The precision, specificity, recall, accuracy, and f1 score serve as the success metrics. For the OBS dataset, the suggested approach achieves an overall accuracy of 99.24%. The overall performance of the EHA-DL is depicted in fig 3.

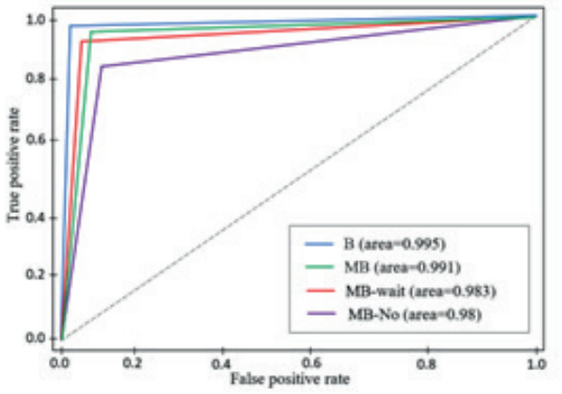

Figure 4: ROC curve of the proposed EHA-DL

Using the collected dataset that yields a higher AUC, the ROC computed for the various classes of HE is shown in Figure 4. AUC values of 0.995 for B, 0.991 for MB, 0.983 for MB-wait, and 0.98 for MB-no blocks were obtained by the proposed EHA-DL network, which can be evaluated using TPR and FPR parameters.

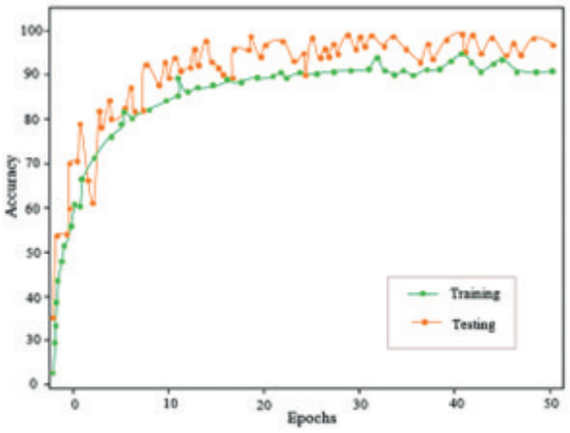

Figure.5: Accuracy curve of the proposed EHA-DL

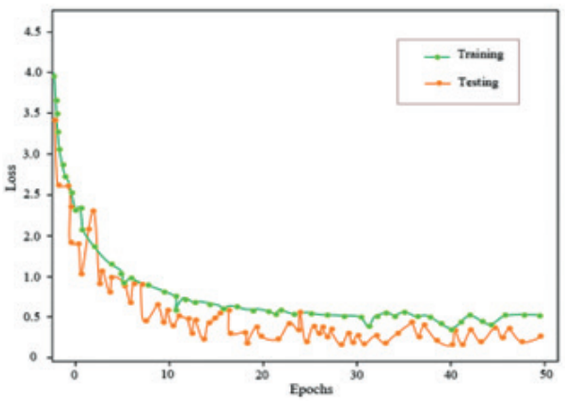

Figure 6: Loss curve of the proposed EHA-DL

The accuracy range is plotted on the vertical axis and the number of epochs on the horizontal axis to depict the accuracy curve in Figure 5. The accuracy of EHA-DL grows with the number of epochs. When the number of epochs is increased, the loss of the EHA-DL is shown in Figure 6. For identifying the various classes of BHP flooding attacks using the dataset, the proposed EHA-DL gets a high accuracy range. To achieve the highest possible testing precision, this study first calculated the number of training epochs required. As a result of achieving a testing accuracy of 99.15% with a small error rate, the findings show that the classification accuracy of EHA-DL was attained after 50 training epochs.

4.3 Comparative analysis

The effectiveness of the proposed EHA-DL achieves high accuracy in its findings. The suggested EHA-DL

was evaluated in comparison to other methods, including the Gaussian Mixture Model (GMM) [18], DCNN [15], K-mean algorithm [16], and PSO-SVM [20].

Table 3: Comparison of the proposed technique with existing techniques

Techniques	Accuracy (%)	Specificity (%)	Recall (%)	Precision (%)	F measure (%)
GMM	83.45	80.32	79.05	85.66	77.58
DCNN	88.25	86.44	90.15	82.42	85.38
K-mean	90.21	92.1	88.54	89.71	86.22
PSO-SVM	95.02	93.42	94.85	92.15	96.69
Proposed EHA-DL	99.27	97.75	98.35	97.37	98.15

The suggested EHA-DL's accuracy of 99.5%, which is better than the existing technique, was evaluated using a variety of metrics, including specificity, precision, recall, F measure, and accuracy of each existing technique. Table 3 shows the comparative analysis of the proposed with state-of-the-art method.

Figure 7 shows the comparative analysis of the proposed novel Elephant herd algorithm based Deep learning network approach (EHA-DL) and Existing methods GMM [18], DCNN [15], K-mean algorithm [16], and PSO-SVM [20] methods. The comparative analysis indicates that the proposed EHA-DL outperforms the current methodologies. While the accuracy of current models such as GMM has 83.45%, DCNN has 87.25%, K-mean is 90.21%, and PSO-SVM is 95.02%, the suggested EHA-DL has a maximum accuracy of 99.27%. It illustrates that the suggested method is efficient and produces a very precise result.

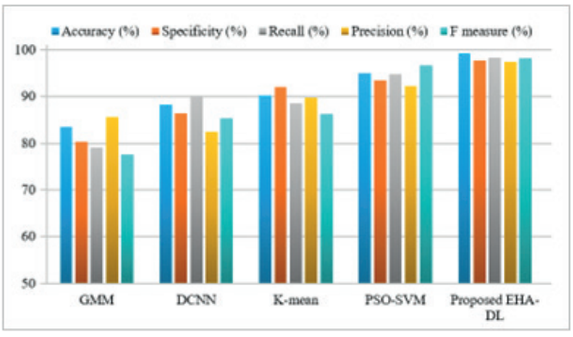

Figure 7: Comparative analysis of the proposed with the existing method

The current GMM, DCNN, K-mean algorithm, and PSO-SVM approaches have raised the precision of the proposed EHA-DL by 10.4%, 8.8%, 6.2%, and 3.6%. The application of extensive classification from a sizable database is what accounts for the improved precision. The suggested EHA-DL has a recall that is 11.4%, 9.6%, 7.2%, and 2.7% higher than the current techniques. When compared to the current approaches, the highest specificity value of 97.75% for the suggested EHA-DL is comparatively high.

5 Conclusion

In this research, a novel Elephant herd algorithm-based Deep learning network has been proposed for detecting BHP flooding attacks. The proposed method is categorized into three phases: pre-processing, feature selection, and classification. The EHA is used to select the most crucial features after pre-processing the raw data to increase the effectiveness of the model. To decrease overfitting and increase detection accuracy, a MobileNet is used to construct the model for the classification phase using the select features of BHPs. Evaluation measures like precision, accuracy, specificity, recall, and f-measure were utilized to calculate the effectiveness of the proposed method. The proposed EHA-DL approach technique acquired a 99.27% accuracy which is relatively high compared to the existing method. In optical burst switching networks, the method effectively and highly efficiently detects flooding assaults and maintains network stability. The suggested framework is being extended, and the thorough design and assessment will be covered in future projects.

6 Acknowledgments

The authors would like to thank the reviewers for all of their careful, constructive and insightful comments in relation to this work.

7 Conflict of Interest Statement

The authors declare that they have no conflict of interest.

8 References

1. M. Vidmar, Optical-fiber communications: components and systems. *Informacije Midem-Ljubljana-*, vol. 4, pp.246-251, 2001. http://dx.doi.org/10.33180/infmidem2019.102
2. B. Batagelj, V. Janyani and S. Tomažič, 2014. Research challenges in optical communications towards and beyond. *Informacije Midem*, vol. *44*, no. 3, pp.177-184, 2020. http://dx.doi.org/10.33180/infmidem2019.407

3. P.J. Argibay-Losada, D. Chiaroni, C. Qiao, Optical packet switching and optical burst switching. Springer Handbook of Optical Networks, pp. 665-701, 2020. http://dx.doi.org/10.1007/978-3-030-16250-4_20
4. Y.Coulibaly, A.A.I. Al-Kilany, M.S. Abd Latiff, G. Rouskas, S. Mandala, M.A. Razzaque, Secure burst control packet scheme for Optical Burst Switching networks. In 2015 IEEE International Broadband and Photonics Conference (IBP) IEEE. pp. 86-91, 2015. http://dx.doi.org/ 10.1109/IBP.2015.7230771
5. M. Imran, P. Landais, M. Collier, K. Katrinis, Performance analysis of optical burst switching with fast optical switches for data center networks. In 2015 17th International conference on transparent optical networks (ICTON) IEEE. 1-4, 2015. http://dx.doi.org/10.1109/ICTON.2015.7193596
6. M.K. Dutta, A comparative study among different signaling schemes of Optical Burst Switching (OBS) network for real-time multimedia applications. In Advances in Computational Intelligence: Proceedings of Second International Conference on Computational Intelligence 2018, pp. 107-117, 2020. Springer Singapore. http://dx.doi.org/10.1007/978-981-13-8222-2_9
7. M.K. Dutta, Performance Analysis of Deflection Routing and Segmentation Dropping Scheme in Optical Burst Switching (OBS) Network: A Simulation Study. In Advances in Computational Intelligence: Proceedings of Second International Conference on Computational Intelligence, Springer Singapore. 2018, pp. 119-128, 2020. http://dx.doi.org/10.1007/978-981-13-8222-2_10
8. R. Poorzare, S. Abedidarabad, A brief review on the methods that improve optical burst switching network performance. Journal of Optical Communications. 2019. https://doi.org/10.1515/joc-2019-0092
9. M.K. Hossain, M.M. Haque, M.A.A. Dewan, A Comparative Analysis of Semi-Supervised Learning in Detecting Burst Header Packet Flooding Attack in Optical Burst Switching Network. Computers, vol. 10, no. 8, pp. 95, 2021. https://doi.org/10.3390/computers10080095
10. A.M. Balamurugan, G. Anitha, Secured Header Authentication Design using Time Competent HMAC for Optical Burst Switched Networks. In 2021 6th International Conference on Communication and Electronics Systems (ICCES) IEEE. pp. 311-315, 2021. http://dx.doi.org/10.1109/ICCES51350.2021.9489016
11. S.S. Chawathe, Analysis of burst header packets in optical burst switching networks. In 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA) IEEE. pp. 1-5, 2018, http://dx.doi.org/10.1109/NCA.2018.8548071
12. A.D.A. Rajab, A machine learning approach for enhancing security and quality of service of optical burst switching networks (Doctoral dissertation, University of South Carolina). 2017. https://www.proquest.com/openview/b01c9cdfddbfbf17ca88f1a824606f0f/1?pq-origsite=gscholar&cbl=18750
13. V.N. Uzel, E.S. Eşsiz, Classification BHP flooding attack in OBS network with data mining techniques. In International Conference on Cyber Security and Computer Science (ICONCS 2018), Safranbolu, Turkey, pp. 18-20, 2018. http://indexive.com/uploads/papers/pap_indexive15505834722147483647.pdf
14. A. Rajab, C.T. Huang, M. Al-Shargabi, Decision tree rule learning approach to counter burst header packet flooding attack in optical burst switching network. Optical Switching and Networking, vol. 29, pp. 15-26, 2018. https://doi.org/10.1016/j.osn.2018.03.001
15. M.Z. Hasan, K.Z. Hasan, and A. Sattar, Burst header packet flood detection in optical burst switching network using deep learning model. Procedia computer science, vol. 143, pp. 970-977, 2018. https://doi.org/10.1016/j.procs.2018.10.337
16. M.M. Haque, M.K. Hossain, "A semi-supervised machine learning approach using K-means algorithm to prevent burst header packet flooding attack in optical burst switching network," Baghdad http://dx.doi.org/10.21123/bsj.2019.16.3(Suppl.).0804
17. A. Rajab, "Detecting BHP Flood Attacks in OBS Networks: A Machine Learning Prospective," International Journal, vol. 8, no. 6, 2019. https://doi.org/10.30534/ijsait/2019/26862019
18. M. Kamrul Hossain, M. Mokammel Haque, "A semi-supervised approach to detect malicious nodes in OBS network dataset using gaussian mixture model," In Inventive Communication and Computational Technologies: Proceedings of ICICCT 2019, pp. 707-719, 2020. Springer Singapore.
19. B. Almaslukh, "An efficient and effective approach for flooding attack detection in optical burst switching networks," Security and Communication Networks, 2020,pp. 1-11, 2020. https://doi.org/10.1155/2020/8840058
20. S. Liu, X. Liao, H. Shi, "A PSO-SVM for Burst Header Packet Flooding Attacks Detection in Optical Burst Switching Networks," In Photonics, vol. 8, no. 12, pp. 555, 2021. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/photonics8120555
21. E. Efeoğlu, T.U.N.A. Gürkan, "Performance Evaluation of Sequential Minimal Optimization and K* Algorithms for Predicting Burst Header Packet Flooding Attacks on Optical Burst Switching Net-

works," Balkan Journal of Electrical and Computer Engineering, vol. 9, no. 4, pp. 342-347, 2021. https://doi.org/10.17694/bajece.892150

22. Panda, Mrutyunjaya, Niketa Gandhi, Ajith Abraham. "Decision Forest Classifier with Flower Search Optimization Algorithm for Efficient Detection of BHP Flooding Attacks in Optical Burst Switching Network," In Innovations in Bio-Inspired Computing and Applications: Proceedings of the 10th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2019) held in Gunupur, Odisha, India, 16-18, 2019, 10, 78-87, 2021. https://doi.org/10.1007/978-3-030-49339-4_9
23. J. Li, H. Lei, A.H. Alavi and G.G. Wang. Elephant herding optimization: variants, hybrids, and applications. *Mathematics*, vol. *8*, no. 9, p.1415, 2020. http://dx.doi.org/10.3390/math8091415
24. H. Moayedi, M.A. Mu'azu and L.K. Foong, Novel swarm-based approach for predicting the cooling load of residential buildings based on social behavior of elephant herds. *Energy and Buildings*, vol. 206, p.109579, 2020. http://dx.doi.org/10.1016/j.enbuild.2019.109579
25. A. Vasuki, *Nature-inspired optimization algorithms*. CRC Press, 2020. http://dx.doi.org/10.1201/9780429289071-3
26. P.N. Srinivasu, J.G. SivaSai, M.F. Ijaz, A.K. Bhoi, W. Kim and J.J. Kang, Classification of skin disease using deep learning neural networks with MobileNet V2 and LSTM. *Sensors*, vol. 21, no. 8, p.2852, 2021. http://dx.doi.org/10.3390/s21082852
27. K. Gayathri, K. P. Ajitha Gladis and A. Angel Mary, "Real time masked face recognition using deep learning based yolov4 network," International Journal of Data Science and Artificial Intelligence, vol. 01, no.01, pp. 26-32, 2023. https://kitspress.com/journals/IJDSAI/index.php?info=14&issue=4
28. M. Prabhu, G. Revathy and R. Raja Kumar, "Deep Learning Based Authentication Secure Data Storing in Cloud Computing," International Journal of Computer and Engineering Optimization, Vol. 01, no. 01, pp. 10-14, 2023. https://kitspress.com/journals/IJCEO/index.php?info=14&issue=22

Arrived: 07. 06. 2023
Accepted: 06. 12. 2023