A New IDS for Detecting DDoS Attacks in Wireless Networks using Spotted Hyena Optimization and Fuzzy Temporal CNN

C. M. Nalayini, Jeevaa Katiravan*

Department of Information Technology, Velammal Engineering College, India
nalayinicm13@gmail.com, jeevaakatir@gmail.com

Abstract

Cyber-attacks are rapidly increasing in the internet era due to the growth of information technology. The distributed denial of service (DDoS) attacks are increasing dramatically due to the distributed services in cloud networks. In this paper, a new Intrusion Detection System (IDS) is proposed to improve the performance of the networks by detecting DDoS attacks effectively in wireless networks. In this work, we propose a new feature selection method called Split Filter Feature Selection and Spotted Hyena Optimization Based Feature Optimization Method (SFSH-FOM) to select the most contributed features that are helpful for enhancing the classification accuracy. In this work, a new deep learning algorithm named Fuzzy Temporal Features incorporated Convolutional Neural Network (FT-CNN) is proposed for performing effective classification. Here, a new cross layer feature fusion technique is also proposed by using FT-CNN and LSTM for enhancing the performance. The experiments have been carried out to evaluate the proposed IDS using the standard datasets, namely the KDD'99 dataset, the NSL-KDD dataset, and the DDoS dataset by considering the evaluation metrics such as detection accuracy, recall, precision, and F1-score, and it has also been proved as better than other IDSs in terms of accuracy and false alarm rate.

Keywords: Fuzzy Decision Tree, Feature selection, CNN, FT-CNN, LSTM

1. Introduction

Recently, the Distributed Denial of Service (DDoS) attacks are treated very serious issue in network communication due to more financial loss to the industries and general bodies in the world [1-2]. The DDoS attacks are increasing day by day due to the usage of various additional devices in Internet. For example, Internet of Things (IoT), Ubiquitous Computing (UC), Fog Computing (FC) and Cloud Computing (CC).

Majority of the scenarios in Internet, the additional devices are capable of interacting with different applications which executes remotely. It leads to interrupt the services or launching the devices as a specific point as a DDoS attack [3] that is aggregate for many reasons including simple and ease of execution, attackers not required much technical skills and a greater number of applications and platforms. The DDoS attack is very serious attack and it is capable of affecting the data communication in network [4]. More number of DDoS attacks are gathered and able to send huge volume of unnecessary data to the destination in the network. Moreover, the intruders are utilizing the recent technologies for attacking the networks and internetworks recently. Generally, the Denial of Service (DoS) and DDoS are capable of affecting the network users easily. The different attacks are having separate goals to affect the data communication service in network. Especially, the DoS/ DDoS attack is disrupting the data communication in an organization, corporate companies and financial corporations. Even though, these attacks are to be handled by a system called Intrusion Detection System (IDS) that is developed by a human with the full of instructions.

An IDS is a software that contains the various rules that are developed by the developer for identifying the behavior of the users and if any patterns are matched with them then declare as attacker and detect them. Generally, the IDSs are categorized into two such as Network IDS (NIDS) and Host based IDS (HIDS). The IDSs are to be developed by applying the feature selection and classification techniques while considering the standard benchmark datasets and network trace dataset as input for the IDS. Another one method is to incorporate the trust mechanism on standard routing protocols to know the genuineness of the nodes in the network. Feature selection and classification are applied frequently for analyzing the network dataset and to identify the intruders and detect them easily. Here, the feature selection is applied for selecting the most important features which are helpful to enhance the classification accuracy by applying the entropy, Information Gain, Chi-Square and statistical formulae. Next, the classification is the process of categorizing the instances according to the given conditions. Moreover, the classification process is classified into two such as two class/ binary classification and multi-class classification. The binary classification is categorized the instances into two such as "Normal" and "Attack". The multi-class classification classifies the instances into many such as "Normal", "DoS Attack", "Probe Attack", "U2R Attack" and "R2L Attack". The classification is done by using many classification algorithms that are available as ML and DL algorithms in the literature.

*Corresponding Author: C. M. Nalayini; E-mail: nalayinicm13@gmail.com

DOI: 10.53106/160792642023012401003

Then, the application of ML and DL algorithms are very useful for predicting the attacks. The different kinds of ML methods such as Naïve Bayes (NB), Random Forest (RF), Decision Tree (DT), Artificial Neural Networks (ANN) and Support Vector Machine (SVM). The ML algorithms are used for performing both training and testing processes. In the training process, the available instances are to verified whether it has any suspicious behaviors or not. If it is identified the suspicious activity then, the feature name and the feature value are to be stored for future reference. In the testing process, the stored feature name and values are to be matched with the stored features and their values. The Deep Learning (DL) techniques are useful for learning the instances multiple times instead of single learning. In addition, it has more than one layers including convolutional layers, max-pooling layers, soft-max layer and fully connected layer for learning the instances deeply. Finally, it identifies the number of patterns for predicting the intruders by monitoring the intrusion activities. The various DL algorithms such as Convolutional Neural Network (CNN), Deep Belief Network (DBN), Long Shortest Time Memory (LSTM), Recurrent neural Network (RNN) are used to perform effective classification on datasets.

This paper proposes a new IDS for detecting the DDoS attacks effectively in wireless networks. The newly proposed IDS uses the newly proposed feature optimization technique to select the optimal features and also apply the new deep learning technique for performing classification. The major contributions of this papers are as below:

1. To develop a new IDS for detecting DDoS attacks in wireless networks effectively.
2. To propose a new Split Filter Feature Selection and Spotted Hyena Optimization based Feature Optimization Method (SFSH-FOM) for choosing the useful features to improve the classification accuracy with less time taken.
3. To develop a new deep learning algorithm called Fuzzy Temporal features incorporated CNN for performing effective classification.
4. To propose a new cross layer feature fusion technique by using FT-CNN and LSTM to improve the performance of the classifier in terms of accuracy.
5. To evaluate the proposed IDS using network datasets namely NSL-KDD dataset, CAIDA dataset and CIC-DDoS2019 by considering the evaluation metrics such as detection accuracy, recall, precision and F-score.

Reminder of this paper is organized as below: The relevant works of IDS, feature optimization, classification and deep learning are described with merits, demerits and contributions in section 2. The section 3 explains the proposed IDS architecture with the explanation of necessary components. The proposed IDS is described with background information about the proposed model is explained in section 4. Section 5 demonstrate the performance of the proposed IDS by considering the necessary evaluation metrics and also explained the standard datasets that are used in this work. The proposed work is concluded with contributions and achievements with future works.

2 Literature Survey

The related works in the direction of DoS attack detection, IDSs, Feature selection and Classification [5-12]. Among them, Botha and Solms [1] developed a fuzzy aware dynamic and proactive method for managing the intrusion detection systems and also manages the intrusion detection process. Shams et al [2] developed a new IDS that combines the SVM and trust mechanism to detect the DoS attacks. In their IDS, it is capable of maintaining the nodes and their malicious behaviors. Hoque et al [12] developed a new greedy feature selection method by using mutual information to find an optimal number of features that are useful for making effective decisions on datasets in the process of prediction and detection.

Siris and Papagalou [13] investigated the different methodologies that are useful for detecting the SYN flooding attacks. They have considered two methods such as adaptive threshold method and cumulative sum of a particular application. The performance of their model is investigated according to the detection rate, time taken for detection and false positive rate. Zhang et al [14] developed a new framework by using RF for detecting the attacks in wireless network environment. They have identified the various patterns using RFs and outlier detection method. The proposed hybrid method enhances the detection accuracy by considering the anomaly and misuse detection processes. Finally, they have evaluated their framework with KDD'99 dataset and achieved better performance in terms of accuracy and false alarm rate.

Zargar et al [15] discussed about the DDoS attack issues and categorized the DDoS attacks. They have categorized DDoS attacks according to the place of prevention and time of prevention. In addition, they have highlighted the need for the comprehensive method. They have proved that their method is effective and efficient in DDoS detection.

Zhang et al [16] conducted an extensive investigation about the DoS attacks for degrading the system performance. They have considered different kinds of networking topologies where the nodes transmit their data to a remote estimator through wireless devices. Moreover, they have developed a new schedule for enhancing the average estimation error. They also provided an optimal schedule for managing attacks through IDS. Ambusaidi et al [17] developed a mutual information aware feature selection method which identifies the useful features which are helpful for enhancing the detection accuracy of the classifier. Their feature selection method is handled the linearly and nonlinearly features. They have developed a new IDS named LSSVM-IDS with the feature selection method. They have evaluated their model and achieved better accuracy with less computational time. Kim and Lee [18] developed a DDoS attack detection system by using SVM. Their system achieved better detection accuracy and less false positive.

Naik et al [19] developed a dynamic fuzzy rule interpolation method for enhancing the overall system's capability and also detects the attacks effectively. Hosseini and Azizi [20] developed a new hybrid model propose a novel hybrid method to detect the DDoS attacks by applying a incremental learning process. They have applied a new technique that used to segregate load between the client side and the proxy sides. Here, the client side has three stages for performing data collection, feature selection and testing processes. They have used NB, DT, MLP and k-NN on proxy for achieving better detection accuracy. Deka et al [21] proposed a new ranking method for ranking the features to perform effective classification on network datasets such as CAIDA, MIT-DARPA and TU-DDoS. Their method achieved above 92% as detection accuracy and also discussed the need for active learning to identify and select the more relevant features. Filho et al [22] developed a novel DoS attack detection system that incorporates the ML algorithms effectively. Moreover, their system has been tested with benchmark datasets and achieved 96% as detection accuracy with less false positive rate as 20%.

Zhong et al [23] proposed a new hierarchical DL technique based on the big data for detecting the DoS attacks. Elsayed et al [24] proposed a DDoSNet as an IDS for detecting the DDoS attacks in software defined networks. Their method works according to the RNN along with an autoencoder. They have evaluated their model by using the CICDDoS 2019 attack that addresses the gaps between the various existing and current DDoS attacks. Saini et al [25] applied ML algorithms for categorizing the instances of the network traffic datasets. Their method is evaluated by using new datasets and categorized the records as normal and attack. The J48 achieved better performance than RF and NB.

Aamir et al [26] proposed a new DL aware IDS to detect the DDoS attacks effectively. Their model applied three DL algorithms such as CNN, DNN and RNN for performing binary and multiclass classification by using live network traffic datasets and proved as an effective and efficient than other methods. Varghese and Muniyal [27] developed a new framework for addressing the challenges in performance measurement of IDSs and also incorporated the intelligence techniques. Their new framework called D3 (DPDK aware DDoS Detection) for providing fast packet processing and monitoring the data transmission. Their framework is capable of achieving effective and efficient performance on CIC-DoS attack datasets and also detect the anomalies effectively.

3 System Architecture

The proposed IDS is explained through an architecture that is shown in Figure 1 that contains seven components namely Network Traffic Datasets, User interface module, decision manager, fuzzy manager, temporal manager, rule manager, rule base and intrusion detection module. Here, the user interface module collects the necessary data from datasets that are stored in network traffic dataset and forward it to decision manager for further processing. The decision manager uses the intrusion detection module that has feature selection and classification phases. These phases apply Spotted Hyena Optimization, Split Filter Feature Selection and Spotted Hyena Optimization Aware Feature Optimization Method (SFSHO-FOM) for performing effective feature selection process and FT-CNN for performing effective classification in this work.

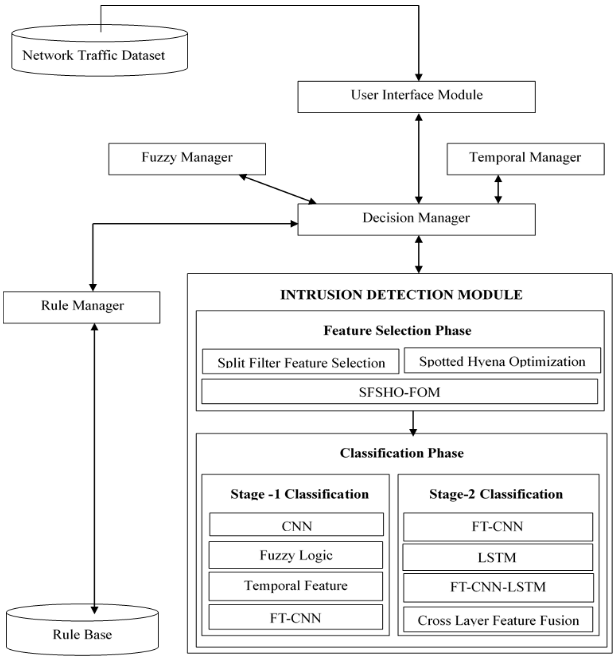

Figure 1. System architecture

4 Proposed Work

This section describes in detail about the proposed IDS to detect the DDoS attack in wireless networks. In this work, a new Split Filter Feature Selection and Spotted Hyena Optimization Aware Feature Optimization Method (SFSHO-FOM) to select the most useful features which are helpful to enhance the classification accuracy. Here, a new DL method called Fuzzy Temporal Features incorporated Convolutional Neural Network (FT-CNN) is developed for performing the classification effectively. In addition, a new cross layer feature fusion technique by using FT-CNN and LSTM is also introduced to improve the classification accuracy.

4.1 Background

This subsection explains the background details such as split filter feature selection, spotted hyena optimization and fuzzy temporal rules that are helpful for understanding the proposed model easily.

A. Filter Feature Selection

The split filter aware feature selection process is a process of dividing the feature sets according to the values such as Information Gain Ratio, Mutual Information, Chi-Square, correlation co-efficient and by applying the conditional probability in the form of Conditional Random Field (CRF). The features of the network traffic data are ranked based on the IGR, CS, CRC and MI values of features. Here, the one third of the feature set is to be identified as best features from the full feature set. Moreover, the CRF is applied to finalize the features from the ranked feature sets. Finally, the best feature set is to be selected and considered as input for the classifier.

B. Spotted Hyena Optimization

The spotted hyena optimization is an optimization technique and the big carnivorous canines which live in different kinds of environments such as dry and open. The small and big sizes herbivores including wildebeests, impala and zebras are preyed upon by the swarms of the spotted hyenas [28]. Generally, the spotted hyena is one of the talented social animals that is identified using sense by the individuals and relatives. Moreover, the relatives are also to be ranked and the high-status hold individuals gets high priority according to the trustworthiness [3]. Naturally, the spotted hyenas are the best in the process of group hunting.

Surrounding the Preys: The spotted hyenas are known the prey's places and also surround the prey's located areas. This work considered the best spotted hyena and also identified as a closest to the target hyena because of hunting area is not aware priorly. Once identified the best location by the search agents that are updated the best search location. The mathematical representation of this characteristic of spotted hyena is described below in the equations (1) and (2).

$$\overrightarrow{DIST}_{hyena} = \left|\overrightarrow{CVB}\ .\ \overrightarrow{PosH_p}(IT) - \overrightarrow{PosH}(x)\right|. \quad \textbf{(1)}$$

$$\overrightarrow{PosH}(IT+1) = \overrightarrow{PosH}_{pos}(IT) - \overrightarrow{CVE}.\overrightarrow{DIST}_{hyena}. \quad \textbf{(2)}$$

Where $\overrightarrow{DIST}_{hyena}$ is a distance between the prey and spotted hyena, IT denotes the iteration, the co-efficient values are indicted in the form of vectors in $\overrightarrow{CVB}$ and $\overrightarrow{CVE}$, the position vector prey is represented by the variable $\overrightarrow{PosH}_{pos}$, the position of the hyena is represented by the variable $\overrightarrow{PosH}$.

The CVB and CVE vector values are calculated by using the formulae given in equations (3) to (5).

$$\overrightarrow{CVB} = 2.\overrightarrow{RVd_1}. \quad \textbf{(3)}$$

$$\overrightarrow{CVE} = 2.\overrightarrow{hyena}.\overrightarrow{RVd_2} - \overrightarrow{hyena}. \quad \textbf{(4)}$$

$$\overrightarrow{hyena} = 5 - (ITER * \frac{5}{MAX_{ITER}}). \quad \textbf{(5)}$$

Where, ITER = 1, 2, …... MAX_{ITER}.

$\overrightarrow{hyena}$ decreases linearly between 5 and 0 to balance the exploration and exploitation. It provides more facilities with good development to increases the iterations as maximum (MAX_{ITER}). The random vector values between 0 and 1 interval are represented by using the variables $\overrightarrow{RVd_1}$ and $\overrightarrow{RVd_2}$. Generally, the positions of spotted hyenas to be updated frequently according to the prey's position. This update is done in various dimensions such as 2D, 3D and multi-dimensional.

Hunting Process: Usually, the SH's are hunt in packs and rely over the trusted circle in their network. For defining the behaviour of SH mathematically, it is assumed that as best search and optimal agent to know the prey's location. The location detail is to be updated in another search agent according to the best and optimal search agent. The below equations were applied to explain the hunting process mathematically.

$$\overrightarrow{DIST}_{hyena} = \left|\overrightarrow{CVB}.\overrightarrow{PosH}_{hyena} - \overrightarrow{PosH}_k\right|. \quad \textbf{(6)}$$

$$\overrightarrow{PosH}_k\, \overrightarrow{PosH}_{hyena} - \overrightarrow{CVE}.\overrightarrow{PosH}_{hyena} - \overrightarrow{PosH}_k. \quad \textbf{(7)}$$

$$\overrightarrow{CLUST}_{hyena} = \overrightarrow{PosH_k} + \overrightarrow{PosH_{k+1}} + ... + \overrightarrow{PosH_{k+N\ SH}}. \quad \textbf{(8)}$$

Where, the first SH is represented by using the variable $\overrightarrow{PosH}_{hyena}$, $\overrightarrow{PosH}_k$ represents the positions of other SH's. N_SH indicates the number of SH that is computed by applying the equation (9).

$$\begin{aligned} N_{SH} = CNT_{NS}(&\overrightarrow{PosH_{hyena}}, \overrightarrow{PosH_{hyena+1}}, \overrightarrow{PosH_{hyena+2}}, \\ &..., (\overrightarrow{PosH_{hyena}} + \overrightarrow{MRV})). \end{aligned} \quad \textbf{(9)}$$

Where, $\overrightarrow{MRV}$ indicates the vector value randomly between 0.5 and 1, NS represents the number of solutions and computes the solutions of all SHs. The optimal search location is represented by using the variable $\overrightarrow{MRV}$ and $\overrightarrow{CLUST}_{hyena}$ indicates the group of optimal solutions.

Exploitation Process: The vector value of $SH(\overrightarrow{hyena})$ is reduced to capture the prey. The co-efficient variation for $\overrightarrow{CVE}$ is decreased for updating the SH's vector value that is decreased from 5 to 0 on course iteration processes. The group of SHs catch the preys successfully when satisfy the condition $|\overrightarrow{CVE}| < 1$. Mathematically can be shown below like equation (10).

$$\overrightarrow{PosH}_{(hyena+1)} = \frac{\overrightarrow{CLUST}_{hyena}}{N\_SH}. \quad \textbf{(10)}$$

Where, $\overrightarrow{PosH}_{(hyena+1)}$ updates the other search agents position based on the best search agent position and also save the solution that is identified as best. The Spotted Hyena Optimization technique is used to find the search agent for updating the positions of other search agents and capture the preys.

C. Convolutional Neural Network

The CNN is a widely used model in deep learning technique. The CNN contains two parts such as feature extraction part and the feature mapping part. These two parts are available as two different layers in CNN. In feature extraction layer, every neuron is connected with the block of the previous layer's local area and also extracts the relevant features. In feature mapping layer, every computational layer is composed with various feature mapping processes. Moreover, the feature mapping process contains the constant values and a fitness function is also applied as an activation function for performing feature mapping process in CNN. In addition to that the weight sharing approach is also applied for reducing the parameters in the feature mapping layer of CNN.

Generally, the CNN has two different stages for performing forward transmission and reverse transmission. In the forward transmission, 3X3 convolutional kernel is applied for handling the internal and accidental data in the convolutional layer. Afterwards, a parameter is added for deviating the processes according to the upper feature mapping and also obtained the result through output layer by applying the activation method.

$$h_{w,b}(X) = f(W^T x) = f(\sum_{i=1}^{n} w_i x_i + b). \tag{11}$$

Where, $h_{w,b}(x)$ represents the element position of output matrix, n indicates the number of inputs or dimensions. The variable x_i represents the i^{th} sub kernel of sub-convolutional matric.

The weights and the offset values are finetuned by reducing the residual values. The residual values of output layer of CNN are different from the intermediate layer's residual values calculation process. When the middle layers residual values derived from Next layer's weighted sum of the residual values, the error is occurred between the actual value and output value. The formulae given in equations (12) and (13) are used to calculate the residual value of the output layer.

$$\delta_i^{(n_1)} = \frac{\partial}{\partial_{z_i}^{(n_1)}} \frac{1}{2} \left\| y - h_{w,b}(x) \right\|^2 = -(y_i - a_i^{(n_1)}.f'(\partial_{z_i}^{(n_1)})). \tag{12}$$

$$\delta_i^{(n_1)} = \frac{\partial}{\partial_{x_i}^{(n_1)}} \frac{1}{2} \left\| y - h_{w,b}(x) \right\|^2 = -(y_i - a_i^{(n_1)}.f'(\partial_{z_i}^{(n_1)})). \tag{13}$$

Where, y and f indicate that the value of output and the activation method. The variable a represents the h value of every layer and the variable z indicates the forward transmission after applying the activation method.

D. Fuzzy Temporal Rules

Generally, the fuzzy logic is always helpful for making effective and accurate decisions over the datasets. Similarly, the time constraints are also playing major role in the decision-making process on time. In this work, fuzzy logic and time constraints are used for constructing the rules to take decision over the input dataset. The fuzzy temporal rules were incorporated in various machine learning algorithms for obtaining the accurate result. The various standard classifiers including DT, SVM and Neural Network were used fuzzy temporal rules for making decisions on medical datasets and intrusion datasets in the past. Especially, the Neural classifiers applied fuzzy temporal rules instead of activation function for making final decision and achieved better result in the literature. Similarly, the deep learning algorithm is also producing good result on various datasets. This work applies fuzzy temporal rules instead of activation function for enhancing the performance of the CNN.

4.2 Feature Optimization

This subsection describes in detail about the feature optimization technique. This section explains the newly proposed feature optimization method called Split Filter and Spotted Hyena based Feature Selection and Optimization Method (SFSH-FOM) briefly. The proposed SFSH-FSOM consists of two phases. The first phase is performed the feature selection process by applying a newly proposed Split Filter aware Feature Selection algorithm (SFFSA) to select the most useful features from the feature set. The second is optimized the selected features by applying the newly proposed Spotted Hyena Optimization Method (SHOM) that is developed based on Spotted Hyena Optimization technique.

Here, the proposed feature selection and optimization method performs the feature selection process by applying a newly proposed Split Filter Feature Selection Algorithm that applies the various statistical formulae such as IGR, MI, CCV and CRF. Here, the CRF is applied to select the initial level of features and this feature set is to be considered for further selection process by using the values such as IGR value, Mutual Information Gain value, Correlation and Co-efficient value. Then, the features are to be ranked according to the average values of each feature and stored as selected features in a feature set SFS{}.

The selected features are to be given as input for the second phase of this method. That is, feature optimization based on Spotted Hyena Optimization technique. The SHO applies a fitness function for calculating the fitness value. Moreover, the fitness value and Ph values of all the features are considered for finding the optimal feature set according to the distance difference between the hyena and preys. Finally, it returns the optimal features that are helpful for enhancing the effective classification. The proposed SFSH-FOM is explained with necessary steps are as follows:

Algorithm 1. Split filter and spotted hyena aware feature optimization method

Input: Network traffic dataset
Output: Optimal feature set

```
Phase 1: Feature selection
Step 1: Read a feature Fi from feature set Fi = {}
Step 2: Generate the rules for identifying the DDoS attack
        related feature by using CRF.
Step 2: Check whether the feature Fi is related to the DDoS
        attack by applying CRF.
Step 3: If Fi is related to DDoS Attack Then
            SFSi {} = SFSi {} + Fi
          Else
            Move to the next feature
Step 4: Select one third of the features from $SFS_{ij}$
        4.1. Find the IGR value ($SFS_{ij}$) (Sannasi et al 2013).
        4.2. Calculate the MI value for the features
             $SFS_{ij}$ using

        $MI(SFS_i; SFS_j)\int_{SFS_i}\int_{SFS_j} p(x,y)\log\frac{p(x,y)}{p(x)p(y)}dxdy.$   (14)
```

```
    4.3. Compute the Correlation Co-efficient value
         for the feature $SFS_{ij}$ using

         $P(SFS)_{ij} = \frac{Cov(i,j)}{\sigma_i \sigma_j}.$        (15)

    4.4. Find the average value of IGR, MI, CCV for the
         selected features SFSi

         $Mean(SFS_i) = \frac{IGR(SFS_i) + MI(SFS_i) + CCV(SFS_i)}{2}.$        (16)

Step 5: Rank the features according to the average score of
        SFSi
Step 6: Select the first one third of features as selected
        features and update it into SFSi.
```

```
Phase 2: Feature Optimization
Step 1: Read CVB, CVE and N_SH.
Step 2: Find the fitness value for every Search Agent.
Step 3: Let consider the Ph as a best search agent.
Step 4: Let consider the Ch is a group of all the possible
        optimal solutions that are far.
Step 5: While (No. of ITER) do
Step 6: For i=1 to N_SA
        Update the current position of the SA by using the
        formulae given in equation (10).
Step 7: End for
Step 8: Modify the values of hyena, CVB, CVE and N_SH
Step 9: Find the Search Space (SS) for all the SA by using
        the equation (11).
Step 10: If (SS(SAi) > Threshold) Then
         Find the fitness value of SAi
Step 11: Form a group according to the Ph value using all
         the SAs.
Step 12: If the current solution is better than the last optimal
         solution Then
         a. Re-group the SAs based on the Ph values of SAs
         b. Hyena = Hyena +1
Step 13: End While
Step 14: Return the Ph value
Step 15: Find the features that are available in the related
         SAs according to the Ph value.
Step 16: Return the optimal feature set (OFS).
```

4.3 Fuzzy Temporal CNN for Classification

The proposed Fuzzy Temporal CNN (FT-CNN) is explained in detail in this section. Moreover, this section provides sufficient background information about the FT-CNN. This FT-CNN is used for extracting the relevant features from network traffic data. The network traffic flow is a key point in the intrusion detection process. Moreover, the temporal constraints and data uncertainty are also considered in this work for predicting the DDoS attack effectively. Generally, the fuzzy logic is used to resolve the uncertainty issue and also helpful for making effective decision on training process. Recently, to provide information security in the network is a complex task due to the availability of huge data with variety, size and speed as well [13]. The data depth is calculated by conducting the hierarchical data analysis that considers the parameters such as time and space. For handling the large volume of network traffic data, this work divides the area of dataset in the form of grid and also the data location is positioned as (i, j). This FT-CNN is applied an activation method and convolution method that are given in equation (17) (18) and (19).

$$f(a) = max(o,a). \tag{17}$$

$$x_t^{(i)} = f(w_t^{(i)} * x_t^{(i-1)} + c_t^{(i)}). \tag{18}$$

Where, f represents the activation method, a indicates that the input, w and c are representing the learning parameters of the layer i. The variable positioned within the bracket means that the current layer and the i-1 represents the previous layer of the current layer, the variable t means that the time period. This CNN consists of various layers that are in common structure as given in equation (19).

$$x_t^{(i)} = x_t^{(i-1)} + \delta(x_t^{(i-1)}, \theta_t^{(i-1)}). \tag{19}$$

Where, the symbol δ represents the residual function, the variable θ (i−1) represents that the previous layer of the structure with the variables such as ‘w’ and ‘b’. This CNN model can be finetuned by adjusting the parameters for optimizing the residual values.

Fuzzy Temporal CNN: The FT-CNN removes the missing data from the original dataset. Then, it trains the records as per the selected feature set that are suggested by the proposed feature selection and optimization method in this work. Then, the FT-CNN is applied to perform the training process on the feature selected record set. At the end, the FT-CNN predicts the test data as “Normal” and “DDoS” attack. This model is considered as optimal model that is used to reduce the Mean Square Error (MSE) value and it is represented as L(θ) as shown in the equation (20).

$$L(\theta) = \left\| Y_t - \hat{Y}_t \right\|_2^2. \tag{20}$$

Where, the θ indicates the learning parameters and variables Y_t and $\hat{Y}_t$ representing real and predicted flow matrix.

This work is used the existing architecture of the CNN [29] is shown in Figure 2 which demonstrates the work flow of the CNN with fuzzy temporal rules.

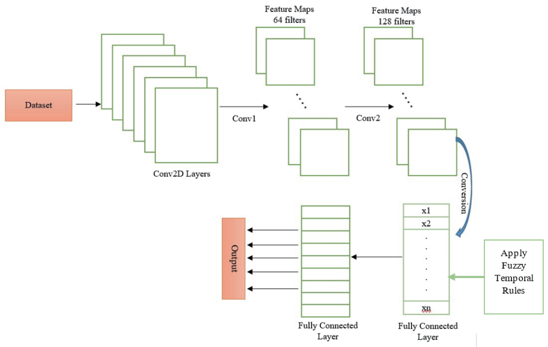

Figure 2. Architecture of CNN with fuzzy temporal rules

Here, the Rectified Linear Unit (ReLU) activation function is used with the consideration of a value with time and fuzzification.

The missing data of $x_t^{(i,j)}$ is calculated by using the formula given in equation (21).

$$X_t^{(i,j)} = \begin{cases} X^{(i,j)}_{t<>48k \quad (k=1,...,7)} \\ X^{(i,j)}_{t<>336p \ (p=1,\ ...,\ 4)} \\ 0 \qquad others \end{cases} . \tag{21}$$

The prediction process of the proposed FT-CNN is explained with necessary steps below:

Algorithm 2. Attack prediction process of Fuzzy Temporal CNN

```
Input: Network Traffic data: $\{x_t^{(i,j)} | t = 0,1,...,n-1\}$;
Output: Record set with result
Step 1: Assign the ∅ value to DS.
Step 2: Find the missing data and perform the missing data
        $x_t^{(i,j)}$ with the equation (21).
Step 3: For $x_t$in all records with temporal constraints do
        a. Build the $x_t$ using the selected records
        b. Place the records ($\{x_t, <t1,t2>, x_t\}$) into the data
           set DS;
        c. Apply fuzzy-temporal rules for identifying the
           suitable record set.
Step 6: End For
Step 7: Assign the learning characteristics θ in FT-CNN;
Step 8: Repeat
Step 9: Selects the subset of $DS_i$ from DS.
Step 10: Handle the FT-CNN by applying the equations
         (17-19) and (11-13).
Step 11: Find the θ value by reducing the dataset $DS_i$.
Step 12: Until reach model and stop the process.
Step 13: Returns the DS with result.
```

The working process of the proposed FT-CNN is categorized into the below steps such as data pre-processing, parameter initialization, forward processing and reverse processing.

Data pre-processing: The missing data is removed from the original dataset. The original data is to be mapped the range between -1 and 1 by using the equation (22).

$$X_i^* = (\frac{X_i - X_{\min}}{X_{\max} - X_{\min}}) * 2 - 1. \tag{22}$$

Where, x_i indicates the original data, the variables $x_{\max}$ and $x_{\min}$ are indicating the maximum and minimum values respectively, and x_i^* is the resultant data.

Initialize the Parameters: The necessary weights are assigned for all the features of the original dataset DS in all layers of FT-CNN randomly and other features holds the value of 0.

Forward processing: The FT-CNN contains various convolutional blocks that are connected based on the weights. A new fitness function is applied as an activation function in this model after processing the convolutional layer. The activation function is shown in equation (23).

$$y_{w,b}^{conv}(x) = f(W^T x) = f(\sum_{i=1}^{n} w_i x_i + b). \tag{23}$$

Where, W^T indicates the weight matrix, x and y $y_{w,b}^{conv}(x)$ are the representing the input and output matrix, the variable b indicates the value of deviation and the variable f represents the activation method.

The gradient dissipation problem is resolved by residual block for reducing the inability of the network weight. The process of reducing the inability is done by using the equation (24).

$$y_{rei}^{(i)} = x^{(i-1)} + \delta(x^{(i-1)}, \theta^{(i-1)}). \tag{24}$$

Where, the variables $x^{(i-1)}$ and $y_{rei}^{(i)}$ are representing the input of currently available residual block and the output of currently available residual block and δ indicates that the residual value of the currently available residual block. Moreover, the residual value of the current residual block is computed by applying the formula given in equation (25).

$$\delta(x,\theta) = W_2\sigma(W_2 x + b_1) + b_2. \tag{25}$$

Where, the variables W_1, W_2, b_1, and b_2 are used for holding the values of weights and deviation at first layer, and the residual block of second layer, σ indicates the ReLU activation method which is non-linear.

Reverse fine-tuning Process: The proposed FT-CNN performs the reverse fine-tuning in this work according to the loss method and the standard Stochastic Gradient Descent (SGD) function for updating the parameters frequently.

The loss function is determined by the MSE value that is calculated above. The SGD value is calculated for every output of the modules. The SGD parameter set (W^1, b^1) from every layer to the next layer that is computed based on the loss method as given in equation (26).

$$g(\theta_{ij}^{(l)}) = \frac{\partial L}{\partial \theta_{ij}^{(l)}} = \frac{\partial L}{\partial y_{ij}^{(l+1)}} \frac{\partial y_{ij}^{(l+1)}}{\partial x_{ij}^{(l+1)}} \frac{\partial x_{ij}^{(l+1)}}{\partial \theta_{ij}^{(l)}}. \quad \textbf{(26)}$$

Where, θ holds the value of the variables w and b, L indicates the loss value with respect to the currently available layer (l) and the next layer (l+1), and the variables x_{ij} and y_{ij} are representing the input value of the respective position and the output value of the respective position.

The parameters are changed frequently in every iteration based on the SGD by using the equation (27).

$$\theta_{ij}^{(l)} = \theta_{ij}^{(l)} - \mu g(\theta_{ij}^{(l)}) = \theta_{ij}^{(l)} - \mu \frac{\partial L}{\partial \theta_{ij}^{(l)}}. \quad \textbf{(27)}$$

Where, the variable μ indicates that the learning rate according to the actual expert experience and also assigned the value 0.0002 as learning rate.

Then, train the proposed FT-CNN model and to store the necessary parameters of the current optimal model until met the condition of stopping criteria. Finally, test the dataset by applying the proposed and trained FT-CNN for identifying the DDoS attacks and detect them from the data communication service.

4.4 Cross Layer Feature Fusion using FT-CNN and LSTM

This section detailed about the working process of Cross Layer Feature Fusion using FT-CNN and LSTM according to the work [11]. The proposed feature fusion is helpful for fine-tuning the performance of the classifier. The prediction resulted records are considered as input for this cross-layer feature fusion process and also produced the better classification result with better accuracy. The cross-layer feature fusion is demonstrated in Figure 3.

The temporal and global features are extracted from the dataset and also created as a comprehensive feature that are given as input to the neural network. The input features are extracted by input layer and these all processed by hidden layer. Finally, it provides the result through output layer.

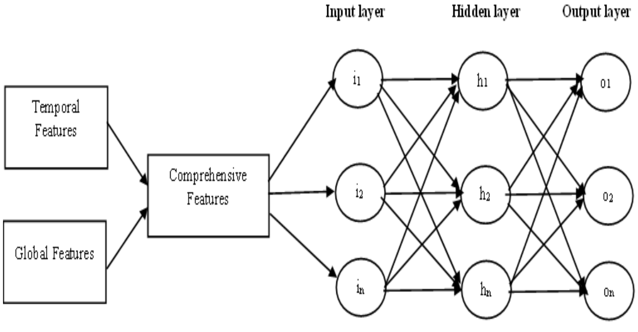

Figure 3. Cross layer feature fusion

Figure 3 shows the cross-layer feature fusion process. The proposed neural network structure contains four different layers such as input layer, feature fusion layer, processing layer and output layer. In this feature fusion layer, it has two layers that are containing the temporal features and global features that are stored in F1 and F2. Moreover, the feature fusion is done and it will produce the final result.

5 Results and Discussion

This section discussed about the various datasets that are applied in this work for evaluating the proposed IDS, evaluation metrics and also demonstrated the performance of the proposed IDS through experimental results. Finally, it demonstrates the comparative analysis for proving the efficiency of the proposed IDS. First, the datasets are explained in detail with necessary detail.

5.1 Data Sets

In this work, three standard datasets such as CIC-DDoS2019 dataset [10], CAIDA dataset [10] and NSL-KDD dataset [10] were used for evaluating the proposed IDS by conducting various experiments. First, this work applies the standard benchmark dataset called CIC-DDoS2019 dataset that has 50,063,112 instances including 50,006,249 rows related to the DDoS attacks and 56,863 records for expressing the value of benign traffic. In this dataset, every record contains 86 features and the statistics for attacks in training process and the testing process.

The training dataset consists of 12 DDoS attacks including Benign with 56,863 flow count, DDoS_Network Time Protocol (NTP) with 1,202,642 flow counts, DDoS_Domain Name System (DNS) with 5,071,011 flow counts, DDoS_Lightweight Directory Access Protocol (LDAP) with 2,179,930 flow counts, DDoS_Microsoft SQL Server (MSSQL) with 4,522,492 flow counts, DDoS_NETwork Basic Input Output System (NetBIOS) with 4,093,279 flow counts, DDoS_Simple Network Management Protocol (SNMP) with 5,159,870 flow counts, DDoS_Simple Service Discovery Protocol (SSDP) with 2,610,611 flow counts, DDoS_User Datagram Protocol (UDP) with 3,134,645 flow counts, DDoS_UDP-Lag with 366,461 flow counts, DDoS_WebDDoS with 439 flow counts, DDoS_SYN with 1,582,289 flow counts and DDoS_TFTP with 20,082,580 flow counts. Second, the CAIDA DDoS dataset that is recorded in the year of 2007.

In this dataset, the data is not guaranteed that as a non-malicious data that is eliminated from dataset. Moreover, this dataset is not able to achieve better result due to the availability of DDoS attacks along with normal attacks. Third, the NSL-KDD dataset is one of the important datasets that is applied world-wide for evaluating the proposed IDSs by various researchers. It has 6 different kinds of DDoS attack that are labelled with attack type along with normal records.

5.2 Performance Metrics

The suitable performance evaluation metrics were applied in this work for measuring the performance of the proposed IDS. These metrics are necessary to know the levels of various classification algorithms and can identify the best for performing detection process. In this work, Intrusion Detection Rate (IDR), False Alarm rate (FA), Precision (PR), Recall (REC), and F1-Score (FS), True Negative Rate (TNR), ROC Curve and Intrusion Detection Accuracy (IDAcc).

$$TNR = \frac{TNR}{TNR + FNR}. \quad \textbf{(28)}$$

$$FA = \frac{FPR}{TNR + FPR}. \quad \textbf{(29)}$$

$$PR = \frac{TRA}{TPA + FPR}. \quad \textbf{(30)}$$

$$REC = \frac{TPA}{TPA + FNA}. \quad \textbf{(31)}$$

$$IDRA = \frac{TPA}{TPA + FNA}. \quad \textbf{(32)}$$

$$FS = 2 * \frac{(PR * REC)}{(PR + REC)}. \quad \textbf{(33)}$$

$$IDA = \frac{TPA + TNR}{PA + FNA + TNR + FPR}. \quad \textbf{(34)}$$

$$O\_IDR = \frac{\sum TP\_Each - Attack\_Type}{\sum TP\_Each - Attack\_Type + \sum FN\_Each - Attack\_Type}. \quad \textbf{(35)}$$

Where, TNR indicates the True Negative Rate, FPR represents the False Positive Rate, FA indicates the False Alarm Rate, PR represents the Precision, REC indicates the Recall, IDRA represents the Intrusion Detection Rate Accuracy, TPA and FNA represent the True Positive Attack and False Negative Attack respectively, the variable FS means that the F-Score, IDA represents the Intrusion Detection Accuracy and O_IDR indicates that the overall intrusion detection rate. The confusion matrix for the evaluation matrix is shown in Table 1.

Table 1. Confusion matrix

	NC	PC
NC	TN	FP
PC	FN	TP

Where, NC indicates the negative class, PC represents the Positive Class.

5.3 Experimental Results

The performance of the proposed IDS is evaluated by using the evaluation metrics such as precision, recall, and F-score. Figure 4 to Figure 6 show the comparative analysis between the proposed IDS and the existing IDSs such as Decision Tree [30], Random Forest [14], MSVM [31], CNN [11], T-CNN [29] and F-CNN [32] in terms of precision, Recall and F-score. Here, five experiments such as E1, E2, E3, E4 and E5 have been done for evaluating the propose model.

According to the Precision, Recall and F-score values of the proposed model is performed well and produce high precision value than the existing IDSs such as Decision Tree [30], Random Forest [14], MSVM [31], CNN [11], T-CNN [29] and F-CNN [32]. The reason for the enhancement is the use of fuzzy temporal features, deep learning, and CRF.

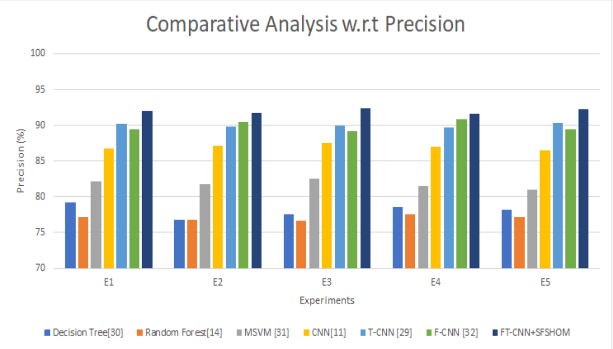

Figure 4. Precision value analysis

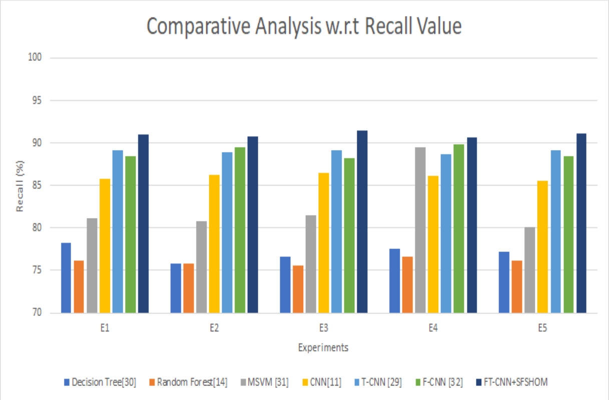

Figure 5. Recall value based comparative analysis

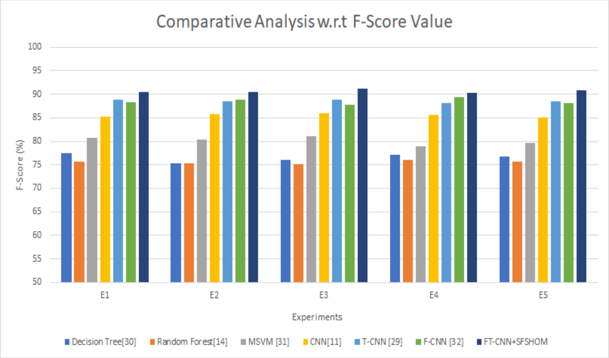

Figure 6. F-Score value based comparative analysis

Table 2 shows the detection accuracy of the proposed IDS on different types of DDoS attacks. Here, we have considered six different types of DDoS attacks such as LDAP, MSSQL, NetBIOS, UDP and SYN. These attacks affected instances are considered as input for conducting experiments to evaluate the effective-ness of the proposed IDS on these attack detection process. Moreover, the relevant works are also considered for showing the efficiency of the pro-posed IDS.

From Table 2, it is observed that the performance of the proposed FT-CNN performs well than the existing deep learning algorithms such as CNN [11], T-CNN [29] and F-CNN [32]. This is due to the fact that the use of fuzzy temporal features on decision making process.

Table 2. Detection accuracy analysis

DDoS attack types	CNN [11]	T-CNN [29]	F-CNN [32]	Proposed FT-CNN
LDAP	97%	97.4	97.7	98.2
MSSQL	95%	95.8	96.1	96.4
NetBIOS	94%	94.8	95.1	95.3
UDP	71%	71.7	72.5	73.2
Syn	100%	100	100	100

The Table 3 demonstrates the effectiveness of the proposed model by comparing with the existing IDSs that are developed by using the deep learning algorithms such as CNN [11], T-CNN [29] and F-CNN [32]. It can be observed that the performance of the proposed model is performed well than the existing models in terms of detection accuracy and false alarm rate. The proposed model is able to detect the DDoS effectively with high detection accuracy and less false alarm rate. The reason for the enhancement is the application of fuzzy logic and temporal constraints along with the activation function in the processes of convolutional operations, feature mapping process and the decision-making process. Finally, the proposed model is able to achieve 97.95% as overall detection accuracy is more than 1% than the accuracy of existing systems.

Table 3. Comparative analysis

Dataset	Model	Accuracy (%)	False alarm rate (%)
NSL-KDD	CNN [11]	99.4	1.65
	T-CNN [29]	99.5	1.57
	F-CNN [32]	99.6	1.55
	Proposed model	99.85	1.48
CAIDA	CNN [11]	97.25	1.53
	T-CNN [29]	97.35	1.47
	F-CNN [32]	97.45	1.41
	Proposed model	98.55	1.36
CIC-DDoS2019	CNN [11]	97.73	1.46
	T-CNN [29]	97.78	1.41
	F-CNN [32]	97.83	1.38
	Proposed model	98.95	1.35

Table 3 provoides the comparative analysis between the proposed IDS and the IDSs developed by using the existing deep learning algorithms such as CNN [30], T-CNN [25] and F-CNN [24]. Here, the detection accuracy of the proposed model is better than the existing algorithms due to the use of effective feature optimization techniques and the classifiers with the incorporation of fuzzy temporal features.

6. Conclusion and Future Work

In this paper, a new IDS has been developed and implemented for detecting DDoS attacks. The proposed IDS uses a newly proposed Feature Optimization Method called SFSH-FOM to select the most contributed features. These features are helpful for enhancing the classifier's accuracy. Here, a new Fuzzy Temporal Features incorporated Convolutional Neural Network (FT-CNN) is also proposed and implemented to perform the effective classification. In addition, a new cross layer feature fusion technique by using FT-CNN and LSTM was also introduced to improve the intrusion detection accuracy. At the end, the proposed IDS achieved an overall detection accuracy of around 98% on different kinds of DDoS attack detection processes with a lower false alarm rate of 1.35%. This work can be enhanced further with the introduction of light-weight feature optimization for achieving better detection accuracy with less time and a lower false alarm rate.

References

[1] M. Botha, R. Solms, Utilising fuzzy logic and trend analysis for effective intrusion detection, *Computers & Security*, Vol. 22, No. 5, pp. 423-434, July, 2003.

[2] E. A. Shams, A. Rizaner, A. H. Ulusoy, Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks, *Computers & Security*, Vol. 78, pp. 245-254, September, 2018.

[3] C. A. Kerrache, N. Lagraa, C. T. Calafate, A. Lakas, TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs, *Vehicular Communications*, Vol. 9, pp. 254-267, July, 2017.

[4] R. Kondaiah, B. Sathyanarayana, Trust based Genetic Neuro-Fuzzy System for Intrusion Detection and Self Adaptive Firefly integrated Particle Swarm Optimization Algorithm for Secure Routing in MANET, *International Journal of Applied Engineering Research*, Vol. 13, No. 8, pp. 5722-5735, January, 2018.

[5] S. Elhag, A. Fernández, A. Bawakid, S. Alshomrani, F. Herrera, On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems, *Expert Systems with Applications*, Vol. 42, No. 1, pp. 193-202, January, 2015.

[6] S. Jamali, G. Shaker, PSO-SFDD: Defense against SYN flooding DoS attacks by employing PSO algorithm, *Computers & Mathematics with Applications*, Vol. 63, No. 1, pp. 214-221, January, 2012.

[7] P. Nancy, S. Muthurajkumar, S. Ganapathy, S. V. N. S. Kumar, M. Selvi, K. Arputharaj, Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks, *IET Communications*, Vol. 14, No. 5, pp. 888-895, March, 2020.

[8] W. Bulajoul, A. James, M. Pannu, Network Intrusion Detection Systems in High-Speed traffic in Computer Networks, *Proceedings IEEE 10th International*

Conference on e-Business Engineering, Coventry, UK, 2013, pp. 168-175.

[9] K. J. Singh, T. De, MLP-GA based algorithm to detect application layer DDoS attack, *Journal of Information Security and Applications*, Vol. 36, pp. 145-153, October, 2017.

[10] M. Ghurab, G. Gaphari, F. Alshami, R. Alshamy, S. Othman, A Detailed Analysis of Benchmark Datasets for Network Intrusion Detection System, *Asian Journal of Research in Computer Science*, Vol. 7, No. 4, pp. 14-33, April, 2021.

[11] R. Yao, N. Wang, Z. Liu, P. Chen, X. Sheng, Intrusion Detection System in the Advanced Metering Infrastructure: A Cross-Layer Feature-Fusion CNN-LSTM-Based Approach, *Sensors*, Vol. 21, No. 2, pp. 1-17, January, 2021.

[12] N. Hoque, D. K. Bhattacharyya, J. K. Kalita, MIFS-ND: A mutual information-based feature selection method, *Expert Systems with Applications*, Vol. 41, No. 14, pp. 6371-6385, October, 2014.

[13] V. A. Siris, F. Papagalou, Application of anomaly detection algorithms for detecting SYN flooding attacks, *Computer Communications*, Vol. 29, No. 9, pp. 1433-1442, May, 2006.

[14] J. Zhang, M. Zulkernine, A. Haque, Random-Forests-Based Network Intrusion Detection Systems, *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, Vol. 38, No. 5, pp. 649-659, September, 2008.

[15] S. T. Zargar, J. Joshi, D. Tipper, A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, *IEEE Communications Surveys & Tutorials*, Vol. 15, No. 4, pp. 2046-2069, Fourth Quarter, 2013.

[16] H. Zhang, P. Cheng, L. Shi, J. Chen, Optimal Denial-of-Service Attack Scheduling with Energy Constraint, *IEEE Transactions on Automatic Control*, Vol. 60, No. 11, pp. 3023-3028, November, 2015.

[17] M. A. Ambusaidi, X. He, P. Nanda, Z. Tan, Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm, *IEEE Transactions on Computers*, Vol. 65, No. 10, pp. 2986-2998, October, 2016.

[18] D. Kim, K. Y. Lee, Detection of DDoS Attack on the Client Side Using Support Vector Machine, *International Journal of Applied Engineering Research*, Vol. 12, No. 20, pp. 9909-9913, 2017.

[19] N. Naik, R. Diao, Q. Shen, Dynamic Fuzzy Rule Interpolation and Its Application to Intrusion Detection, *IEEE Transactions on Fuzzy Systems*, Vol. 26, No. 4, pp. 1878-1892, August, 2018.

[20] S. Hosseini, M. Azizi, The hybrid technique for DDoS detection with supervised learning algorithms, *Computer Networks*, Vol. 158, pp. 35-45, July, 2019.

[21] R. K. Deka, D. K. Bhattacharyya, J. K. Kalita, Active learning to detect DDoS attack using ranked features, *Computer Communications*, Vol. 145, pp. 203-222, September, 2019.

[22] F. S. L. Filho, F. A. F. Silveira, A. M. B. Junior, G. Vargas-Solar, L. F. Silveira, Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning, *Security and Communication Networks*, Vol. 2019, pp. 1-15, October, 2019.

[23] W. Zhong, N. Yu, C. Ai, Applying big data based deep learning system to intrusion detection, *Big Data Mining and Analytics*, Vol. 3, No. 3, pp. 181-195, September, 2020.

[24] M. S. Elsayed, N. A. Le-Khac, S. Dev, A. D. Jurcut, DDoSNet: A Deep-Learning Model for Detecting Network Attacks, *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Cork, Ireland, 2020, pp. 391-396.

[25] P. S. Saini, S. Behal, S. Bhatia, Detection of DDoS Attacks using Machine Learning Algorithms, *2020 7th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 2020, pp. 16-21.

[26] M. Aamir, S. M. A. Zaidi, Clustering based semi-supervised machine learning for DDoS attack classification, *Journal of King Saud University - Computer and Information Sciences*, Vol. 33, No. 4, pp. 436-446, May, 2021.

[27] J. E. Varghese, B. Muniyal, An Efficient IDS Framework for DDoS Attacks in SDN Environment, *IEEE Access*, Vol. 9, pp. 69680-69699, May, 2021.

[28] H. Jia, J. Li, W. Song, X. Peng, C. Lang, Y. Li, Spotted Hyena Optimization Algorithm with Simulated Annealing for Feature Selection, *IEEE Access*, Vol. 7, pp. 71943-71962, May, 2019.

[29] B. Riyaz, S. Ganapathy, A deep learning approach for effective intrusion detection in wireless networks using CNN, *Soft Computing*, Vol. 24, No. 22, pp. 17265-17278, November, 2020.

[30] J. Yang, X. Chen, X. Xiang, J. Wan, HIDS-DT: An Effective Hybrid Intrusion Detection System Based on Decision Tree, *2010 International Conference on Communications and Mobile Computing*, Shenzhen, China, 2010, pp. 70-75.

[31] S. Ganapathy, K. Kulothungan, S. Muthurajkumar, M. Vijayalakshmi, P. Yogesh, A. Kannan, Intelligent feature selection and classification techniques for intrusion detection in networks: a survey, *EURASIP Journal on Wireless Communications and Networking*, Vol. 2013, No. 1, pp. 1-16, November, 2013.

[32] J. An, L. Fu, M. Hu, W. Chen, J. Zhan, A Novel Fuzzy-Based Convolutional Neural Network Method to Traffic Flow Prediction with Uncertain Traffic Accident Information, *IEEE Access*, Vol. 7, pp. 20708-20722, February, 2019.

Biographies

C. M. Nalayini is currently working as an Assistant Professor at Velammal Engineering College. She is pursuing her Ph.D degree in Information and Communication Engineering from Anna University, Chennai, India. Her current research interest includes Network Security, Machine Learning, Deep Learning.

Jeevaa Katiravan received his Ph.D degree from the Department of Information and Communication Engineering at Anna University, Chennai, India. He is currently working as a Professor in the Department of Information Technology at Velammal Engineering College. His research interest includes Network Security, Wireless Networks.