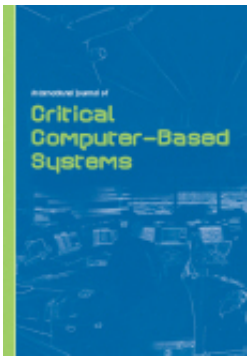
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Critical Computer-Based Systems

ISSN online: 1757-8787 - ISSN print: 1757-8779
https://www.inderscience.com/ijccbs

Tuna swarm optimisation-based feature selection and deep multimodal-sequential-hierarchical progressive network for network intrusion detection approach

G. Gowthami, S. Silvia Priscila

DOI: 10.1504/IJCCBS.2023.10061716

Article History:

Received:	16 June 2023
Last revised:	19 September 2023
Accepted:	06 November 2023
Published online:	30 January 2024

Tuna swarm optimisation-based feature selection and deep multimodal-sequential-hierarchical progressive network for network intrusion detection approach

G. Gowthami* and S. Silvia Priscila

Department of Computer Science,
Bharath Institute of Higher Education and Research,
Chennai, Tamil Nadu, India
Email: gowthami.ramya@gmail.com
Email: silviaprisila.cbcs.cs@bharathuniv.ac.in
*Corresponding author

Abstract: Network intrusion detection system (NIDS) is important for securing network information. Neural network (NN) has recently been used for NIDS, which gained prominence results. Conventional neural network (CNN) has been introduced in network traffic data because of its single structure. The classification of assaults will no longer be useful due to redundant or inefficient features. Tuna swarm optimisation (TSO) has been introduced for feature selection (FS). First, pre-processing and feature extraction stages enable more efficient processing of features if handled independently. In order to examine the exploration space accuracy and position the best features, the second feature selection step of the TSO methodology involved selecting a subset of features by reducing the number of features. Lastly, multimodal deep auto encoder (MDAE) and gated recurrent unit (GRU) allow deep multimodal-sequential-hierarchical progressive network (DMS-HPN) intrusion detection method. Its DMS-HPN technique would routinely learn the temporal features among neighbouring network connections, simultaneously integrating diverse feature information inside a network. Datasets like UNSW-NB15 and CICIDS 2017 assess the effectiveness of the proposed DMS-HPN approach. Classification algorithms are evaluated via precision, recall, F-measure, and accuracy. Compared to conventional classifiers, the presented DMS-HPN classifier achieves the greatest accuracy.

Keywords: network intrusion detection systems; NIDS; feature selection; FS; multimodal deep auto encoder; MDAE; conventional neural network; CNN; gated recurrent unit; GRU; tuna swarm optimisation; TSO.

Reference to this paper should be made as follows: Gowthami, G. and Priscila, S.S. (2023) 'Tuna swarm optimisation-based feature selection and deep multimodal-sequential-hierarchical progressive network for network intrusion detection approach', *Int. J. Critical Computer-Based Systems*, Vol. 10, No. 4, pp.355–374.

Biographical notes: G. Gowthami was pursuing her PhD in 2022 at Vehicular Ad Hoc Network in the Department of Computer Science at Bharath Institute of Higher Education and Research, Chennai. She is working as an Associate Professor in the Department of Computer Science at Swami Vivekananda Rural First Grade College, Bangalore, Karnataka, India. She published the research article 'Efficient intrusion detection and classification using enhanced MLP deep learning model' in Springer and completed NPTEL courses. Her research interests include mobile networks, wireless sensor networks, satellite and

wireless communication, embedded systems, antennas and wave propagation with network simulator, electromagnetic and transmission lines, IoT, machine learning and deep learning.

S. Silvia Priscila has been working as an Associate Professor in the Department of Computer Science, Bharath Institute of Higher Education and Research at Tamil Nadu in India. She has been awarded a PhD from the Bharathiar University. She has 15 years of teaching experience. A few articles were published in various research fields and indexed in Scopus WoS. Data mining and machine learning are her specialisations.

1 Introduction

The internet has given network users a great deal of ease through the quick growth of information and communication technology (ICT). Because of the rise in distributed denial of service (DDoS), probing, and cross-site scripting, the issue of information security is, nevertheless, getting more and more important (Vinayakumar et al., 2019). Network intrusion detection system (NIDS) is a crucial security mechanism in cybersecurity defences to locate and stop hostile incursion (Li et al., 2018; Ali et al., 2018). When creating IDS, two strategies should be considered: misuse-based and anomaly-based (Almansor and Gan, 2018). The IDS tries to match the patterns of previously recognised network assaults when using the misuse-based method (Abdullahi et al., 2023). It regularly updates its database by storing the patterns of recognised network attacks (Ahmad et al., 2023). On the other hand, the anomaly-based IDS try to identify unknown network threats by contrasting them with the typical connection patterns (Othman et al., 2011; Almansor and Gan, 2018).

An efficient IDS model requires much information to train and test. The data quality is extremely important for the IDS model results (Ojha et al., 2017; Rajest et al., 2023a). After gathering the statistical qualities from the data observable attributes and constituent parts, the low-quality and unnecessary information can be removed (Sahu et al., 2014). The data may, however, be excessive, unbalanced, high-dimensional, or incomplete (Ojha et al., 2017). Thus, IDS research needs to analyse the given datasets thoroughly (Anand et al., 2023). In reality, network intrusion detection falls under the description of a typical problem because it is responsible for monitoring network activity every minute and deciding when to alert the network system administrators (Angeline et al., 2023). To ensure network systems operate steadily and effectively, intrusion detection devices must specifically quickly and automatically detect attacks or potential threats masked in network traffic (Devi and Rajasekaran, 2023). Two algorithms artificial fish swarm (AFS) and artificial bee colony (ABC) by Hajisalem and Babaie (2018) have been experimented with using UNSW-NB15 and NSL-KDD datasets.

Feature selection (FS) is commonly used. To put it simply, it is used in IDS. This work targeted at utilising a wrapper technique to lower the amount of features to increase NIDS performance and detection rate. Particle swarm optimisation (PSO), firefly algorithm (FFA), genetic algorithm (GA), and grey wolf optimiser (GWO) are all examples of bio-inspired metaheuristic algorithms that this research aimed to use to create a model for NIDS. The latter model is evaluated with the help of classifiers. Unfortunately, most current studies only pay minimal attention to traffic statistics. Given

that they think the goal of the characterising network connections has complicated linkages, current work has proposed auto-encoder neural network (NN)-based unsupervised learning towards deriving middle representations of features (Javaid et al., 2016; Shone et al., 2018). Additionally, some researches aim to use recurrent neural networks (RNN) to investigate temporal data by contemplating the context of neighbouring network connections (Yin et al., 2017; Kim et al., 2016; Sivapriya et al., 2023). With the use of multimodal deep auto encoder (MDAE) and LSTM, He et al. (2019) proposed a multimodal-sequential with deep hierarchical progressive network (MS-DHPN). The proposed revision to this paradigm adds a FS to it. In the field of artificial intelligence, deep learning has emerged as one of the most significant developments of the recent decade (Fraihat et al., 2023). The multimodal structure of these approaches and the challenge of improving NIDS accuracy plague all of them (Sohlot et al., 2023). Classification for detection takes longer as a result of an excessive number of features that are largely meaningless (Cirillo et al., 2023).

In this study, the researcher aimed to provide a FS model for NIDS. Based on the tuna swarm optimisation (TSO), this model seeks to enhance the functionality of NIDS (Xie et al., 2021). The major contribution of the work employs wrapper-based techniques with the TSO for FS (Jeba et al., 2023; Saxena and Chaudhary, 2023). TSO aims at improving the performance of NIDS (Kanyimama, 2023). The wrapper-based method is performed based on TSO and has been used to choose a smaller set of input features to find the perfect ones (Rajasekaran et al., 2023; Regin et al., 2023a). Then, access sub-feature vectors by creating an MDAE, and a probability graph model is introduced to study the division of every level feature (Rajest et al., 2023b). Sequence modelling using the gated recurrent unit (GRU) technology also supports an intelligent approach. Attack detection across current networks has been used to assess the results of the proposed DMS-HPN technique. The proposed system gives better results in accuracy and stability among binary and multiclass classification using two benchmark datasets from 2015 to 2017. The overall organisation of the paper is described as follows. In Section 1, an overview of the introduction is discussed. In Section 2, a review of literature with their issues and merits has been discussed. Section 3, an overview of the proposed methodology with its issues, has been discussed in detail. The results achieved by the proposed system and existing methods have been shown in Section 4. Finally, the overall research is concluded with their issues in Section 5.

2 Literature review

Kasongo and Sun (2020) adopted on using machine learning (ML) techniques like support vector machine (SVM), k-nearest neighbour (kNN), logistic regression (LR), artificial neural network (ANN), and decision tree (DT) for IDS. Network attack detection by IDS based on ML techniques is reliable and accurate. In order to train and evaluate these models, the University of New South Wales (UNSW Sydney) examined the UNSW-NB15 intrusion detection dataset. Moreover, the XGBoost algorithm is used in a filter-based feature reduction strategy. Aleesa et al. (2021) developed to test models just once rather than testing them separately for each file, its UNSW-NB15 dataset in various isolated files and labelled it based on binary classification. It looked at how well deep learning performed using the improved dataset and two categorisation categories. It

compared the outcomes of the suggested deep learning model with related works. The effectiveness of deep learning and ML models in the enlarged dataset has been assessed using accuracy and error rates.

Using the UNSW-NB15 dataset benchmark, Moualla et al. (2021) developed a unique network IDS that helps maintain network security and defend against cyberattacks. To address problems with skewed datasets, it employs the synthetic minority oversampling technique (SMOTE). Then, a Gini impurity-based extremely randomised trees classifier is presented to select the most important features for each pre-existing class in the dataset. The results show that compared to other works, its system is more accurate, has a lower false alarm rate, and a better receiver operating characteristics (ROC). Four separate algorithms for the categorisation of cyber-attacks were developed by Hammad et al. (2020): naive Bayes (NB), random forest (RF), J48, and zeroR. In addition, the UNSW-NB15 dataset is partitioned into two clusters using K-Means and expectation maximisation (EM) clustering techniques, with each cluster reflecting either attacks on the network or normal network activity. Following the aforementioned classification and clustering methods, the optimal collection of features is chosen using correlation-based feature selection (CFS).

Hemanth (2021) developed a cybersecurity system known as the IDS, which monitors and identifies any security risks to the network software and hardware. Many academics have focused on creating IDS using ML techniques to address the issues mentioned earlier. Convolutional neural network (CNN) is a deep learning technique created to address the issue of spotting network intrusion. It trained the CNN algorithm using the UNSW NB15 public dataset data. Husain et al. (2019) implemented the contrast to the earlier standard KDD99; UNSW-NB15 represents contemporary network threats and network traffic. Extreme gradient boosting (XGBoost) was applied as a ML technique that offers a very effective and accurate data-predicting model. In order to aid in identifying between different forms of network attacks, it can choose a subset of 23 out of 39 accessible attributes. The bivariate analysis allowed us to determine the proportion of records corresponding to a specific value range and a given assault type.

Almomani (2021) proposed to identify the generic assault, a hybrid model for network IDS based on algorithms like PSO, GWO, multiverse optimisation (MVO), moth-flame optimisation (MFO), whale optimisation algorithm (WOA), FA, and bat algorithm. It is used to identify the general attack using ML classifiers like RF, C4.5 (J48), and SVM. Zeeshan et al. (2021) proposed a based deep intrusion detection (PB-DID) architecture. This has been implemented for UNSW-NB15 and Bot-IoT datasets depending on transmission control protocol (TCP). It is used to build a dataset of packets from internet of things (IoT) traffic.

Recursive feature elimination (RFE) with information gain and RF were proposed by Yin et al. (2023) as a multilayer perceptron (MLP) network-based hybrid FS methodology for multiclass network anomalies (IGRF). Alsaleh and Binsaeedan (2021) constructed a range of ML classifiers, such as the extreme gradient boosting (XGBoost) and NB algorithms, to investigate the impact of the SSA on increasing ML-based network anomaly detection. The UNSW-NB15 and NSL-KDD datasets were used for categorisation since they are tailored to network intrusion attempts. For IDS, Alazzam et al. (2020) used a pigeon-inspired wrapper FS method. The algorithms were evaluated using datasets from the knowledge discovery community, including KDDCUP99, NSL-KDD, and UNSW-NB15. Also, compared to the sigmoid approach, its cosine similarity method for binarising the algorithm converges more fast.

He et al. (2019) developed a multimodal-sequential intrusion detection method by LSTM and MDAE with a unique hierarchical progressive network topology. It examined the performance of detecting attacks within contemporary networks using NSL-KDD, UNSW-NB15, and CICIDS 2017. Tama et al. (2019) implemented a basis of hybrid FS and two-level classifier ensembles, an enhanced IDS. To minimise the feature size of the training datasets, a hybrid FS methodology that combines three methods – PSO, ant colony algorithm (ACO), and GA is implemented in NSL-KDD and UNSW-NB15. When choosing features, a reduced error pruning tree (REPT) classifier classification performance is considered. A two-step statistical significance test is then performed to confirm the findings. Sumaiya Thaseen et al. (2021) proposed a CFS combined with the NN. Datasets like NSL-KDD and UNSW-NB have been introduced for experimentation (Lodha et al., 2023). Performance can be increased by achieving a secure, error-free integrated network management. Saheed (2022) adopted the most important safeguard – electronic medical records and patient data privacy that combines the benefits of artificial intelligence and cyber security. Health-related data within healthcare systems is governed by stringent laws, such as the EU General Data Protection Regulation (GDPR), which carries severe penalties and fines for non-compliance.

3 Proposed methodology

Pre-processing, feature extraction, FS, classification, and outcome evaluation are the phases of the proposed study. Firstly, a pre-processing and feature extraction module has been introduced to separate the complicated features from traffic data. Secondly, the TSO algorithm is presented to pick a subset of input variables by decreasing features (Gaayathri et al., 2023). Thirdly, DMS-HPN, known as the deep multimodal-sequential, employs a hierarchical progressive network to detect current attacks. DMS-HPN is composed of three layers (Sajini et al., 2023). To incorporate the compound features in every traffic flow at the low level, a multimodal fusion algorithm depending on MDAE is offered in the top layer. GRU is proposed as sequential learning in the second layer to extract the temporal data involving high-level traffic flows. Finally, results are evaluated using the evaluation metrics. The proposed framework for the DMS-HPN method detection process is shown in Figure 1.

3.1 Pre-processing and feature extraction

The pre-processing and feature extraction is to extract various degrees of features from traffic data. The record, which is represented as $F = (f_1, f_2, \ldots, f_n)$ where f is the number of features in the feature set and n is the total number of features in each record (TCP packet) travelling from source to destination via the network.

Multiple feature groups for each record are accessible, as shown in Figure 2 and as $F_{groups} = \{F_1, F_2, \ldots, F_m\}$ where m is the amount of feature groups and also this work divides 1, 2, 3, and 4 groups for experimentation.

Figure 1 Flow diagram of proposed DMS-HPN system (see online version for colours)

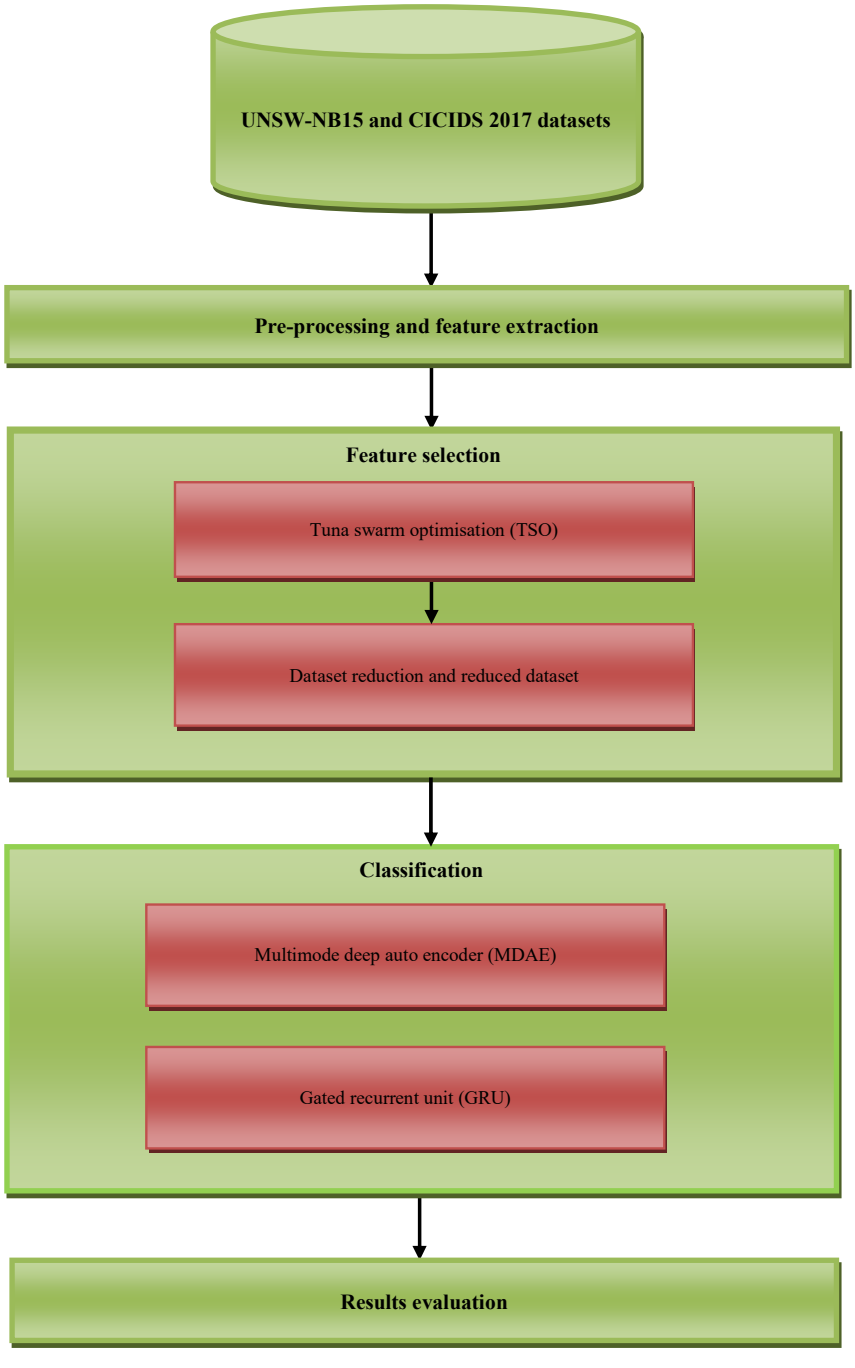
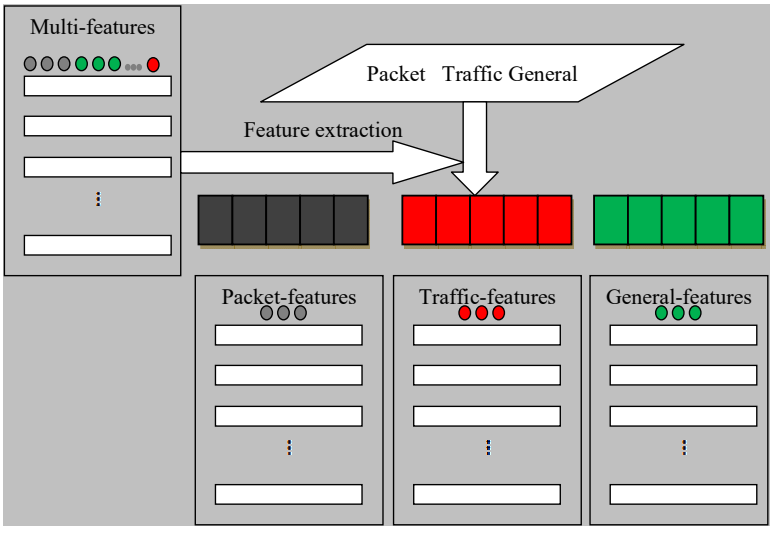


Figure 2 Multi-features extraction (see online version for colours)



3.2 TSO-based feature selection (FS)

Finding the most significant inputs, also known as FS minimises the number of inputs for processing and analysis. In order to assess the search space accuracy and identify the best answer, FS approaches are used to pick out key features. The method of feature selection using the TSO algorithm is detailed below (Xie et al., 2021). The proposed algorithm mathematical model is thoroughly explained in this section.

- *Initialisation:* equation (1) discusses how TSO begins the optimisation process by creating beginning populations uniformly at random in the search space,

$$X_i^{\text{int}} = rand.*(ub - lb) + lb, i = 1, 2, ..., NP \tag{1}$$

  where NP is the number of tuna populations, X_i^{int} is the i^{th} initial individual, ub and lb are the upper and lower search space limits, and $rand$ is a uniformly distributed random vector from 0 to 1.

- *Spiral foraging:* schools of tuna communicate with one another as well as whirling after their prey. The following equations (2)–(6) provide the mathematical formula for the spiral foraging strategy based on the assumptions as mentioned earlier,

$$X_i^{t+1} = \begin{cases} \alpha_1.\left(X_{best}^t + \beta.\left|X_{best}^t - X_i^t\right|\right) + \alpha_2.X_i^t, i = 1, \\ \alpha_1.\left(X_{best}^t + \beta.\left|X_{best}^t - X_i^t\right|\right) + \alpha_2.X_i^t, i = 2, 3, .. NP \end{cases} \tag{2}$$

$$\alpha_1 = a + (1-a).\frac{t}{t_{\max}}, \tag{3}$$

$$\alpha_2 = (1-a) - (1-a).\frac{t}{t_{\max}}, \tag{4}$$

$$\beta = e^{bl}.\cos(2\pi b) \tag{5}$$

$$l = e^{\left(3\cos\left(\left(\left(t_{\max}+\frac{1}{t}\right)^{-1}\right)^{\pi}\right)\right)}, \tag{6}$$

where X_i^{t+1} is the i^{th} individual of the t + 1 iteration, X_{best}^t is the current optimal individual (food), α_1 and α_2 are weight coefficients, an is a constant to determine which the tuna finds the best individual in the initial phase, t denotes the iterations, $t_{\max}$ denotes the maximum number of iterations. A b is randomly generated for spiral search reference point. The equation (7) is used to explain the mathematical model,

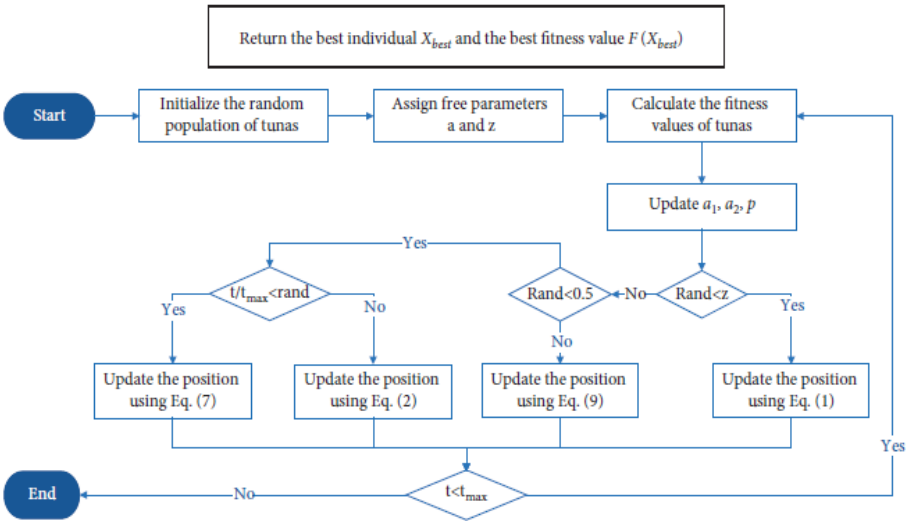
$$X_i^{t+1} = \begin{cases} \alpha_1.\left(X_{rand}^t + \beta.\left|X_{rand}^t - X_i^t\right|\right) + \alpha_2.X_i^t, i = 1, \\ \alpha_1.\left(X_{rand}^t + \beta.\left|X_{rand}^t - X_i^t\right|\right) + \alpha_2.X_i^t, i = 2, 3, .. NP \end{cases} \tag{7}$$

where X_{rand}^t is a search space reference point that was chosen at random in the context of t. For instance, metaheuristic algorithms typically begin with broad, global investigation and then narrow in on a specific target. As a result, TSO changes the spiral foraging reference points from random humans to ideal people as the iteration count increases.

$$X_i^{t+1} = \begin{cases} \alpha_1.\left(X_{rand}^t + \beta.\left|X_{rand}^t - X_i^t\right|\right) + \alpha_2.X_i^t, i = 1, \text{if } rand < \dfrac{t}{t_{\max}} \\ \alpha_1.\left(X_{rand}^t + \beta.\left|X_{rand}^t - X_i^t\right|\right) + \alpha_2.X_i^t, i = 2, 3, .. NP \\ \alpha_1.\left(X_{rand}^t + \beta.\left|X_{rand}^t - X_i^t\right|\right) + \alpha_2.X_{i-1}^t, i = 1, \text{if } rand \geq \dfrac{t}{t_{\max}} \\ \alpha_1.\left(X_{rand}^t + \beta.\left|X_{rand}^t - X_i^t\right|\right) + \alpha_2.X_{i-1}^t, i = 2, 3, .. NP \end{cases} \tag{8}$$

where TF is a random number generated between the range (1, –1).

Figure 3 Flowchart of TSO (see online version for colours)



The TSO process is shown in great detail in Figure 3. When hunting together, tuna use two distinct foraging strategies to narrow down on their prey. At each iteration, individuals choose between two foraging strategies at random, with probability z, or they renew their position in the search space. Until the halt condition is met, every TSO is updated and calculated for the entirety of the optimisation procedure. At this point, the perfect individual and the associated fitness value are revisited (Regin et al., 2023b).

3.3 Deep multimodal-sequential with hierarchical progressive network (DMS-HPN) classification

Intrusion detection works by classifying a given subset of features and feature groups. Targets/labels or categories are other names for classes. Classification is supervised learning in which the targets are also given access to the input data (selected features). The DMS-HPN intrusion detection approach has been introduced for NIDS.

- *Multimodal fusion model:* group of features in NIDS, the multimodal fusion model (MDAE) based on multimodal learning technology is used (He et al., 2019; Wang et al., 2020). Based on the realisation that a traffic flow feature correlation is heterogeneous and complementary, MDAE was developed. Figure 4 depicts the architecture of the MDAE network. A joint network is the top layer, fusing the multimodal data from these GRBM interpreters to provide a combined feature representation. Hence, the objective is to study the final consensus representation $F' = \{F_{joint}\}$ when provided traffic flow data using m feature groups, $F_{groups} = \{F_1, F_2, \ldots, F_m\}$.

  Forward encoding and back decoding are the two main components of the MDAE model training techniques, as shown in Figure 4. The higher RBM is fed with the hidden layers of that Gaussian Restricted Boltzmann Machines (GRBM) after the intermediate layer Gaussian RBM interpreters have been built, and the resulting joint network is then constructed. To be more precise, the joint distribution $P(v, h)$is computed via an energy function by visible unit v and binary hidden unit h. Gaussian RBM is represented in equations (9)–(10).

$$P(v, h) = \frac{\exp(-E(v, h))}{Z} \tag{9}$$

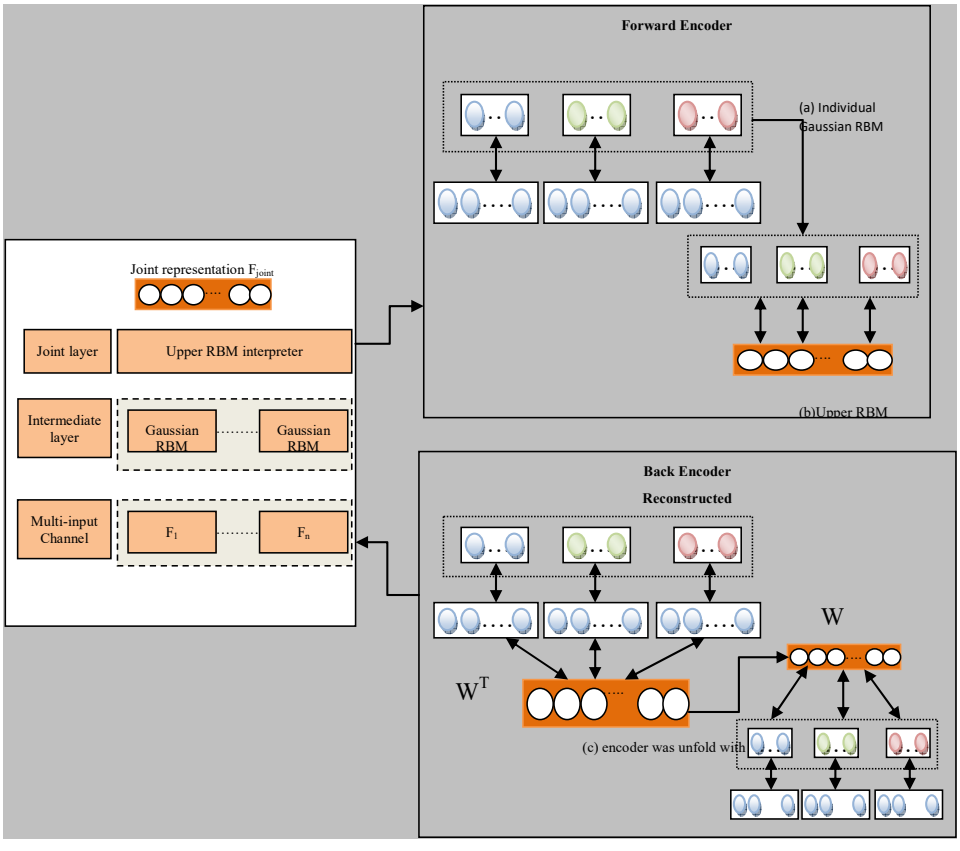
$$E(v, h) = \frac{1}{2\sigma^2} v^T v - \frac{1}{\sigma^2}\left(c^T v + b^T h + h^T W v\right) \tag{10}$$

  where W is denoted as the weight matrices with the visible layer and hidden layer, c and b is denoted as the biases of visible layer and hidden layer, Z is a normalisation constant, $E(v, h)$ is denoted as the energy function, and h is a hyper-parameter. The conditional probability distributions of the Gaussian RBM have been computed using the following equations (11)–(12) when $\sigma = 1$,

$$P\left(h_i = 1 \mid v\right) = sigmoid(Wv + b) \tag{11}$$

$$P\left(v_i \mid h\right) = \mathcal{N}(Wv + b) \tag{12}$$

Figure 4 Architecture of MDAE with construction process (see online version for colours)



RBM parameters $\theta(W, b, c)$and contrastive divergence algorithm for training Gaussian RBM can be acquired. The following equation (13) is the learning rule,

$$\Delta W = E_{data}(vh) - E_{model}(vh) \tag{13}$$

where E_{model} denotes the expectation is computed by the RBM model and E_{data} is the expectation found by training data. After being transformed into a deep auto-encoder with multiple inputs and outputs during the forward encoding phase, the stacked RBM are reverse decoded during the subsequent phase. Each component's parameters are defined by the weight matrices used in the appropriate decoder and encoder.

- *Sequential learning model:* GRU is a sequential learning model (Cho et al., 2014). The update gate, reset gate, activation, and candidate activation are each represented by the letters $(z, r, H, \bar{H})$ in Figure 5. Equations (14)–(17) cover the specific formulas. The amount of old information will decrease if a lot of new information is retained, and vice versa.

$$z_t = sigmoid\left(W_{xz}x_t + W_{hz}h_{t-1} + b_z\right) \tag{14}$$

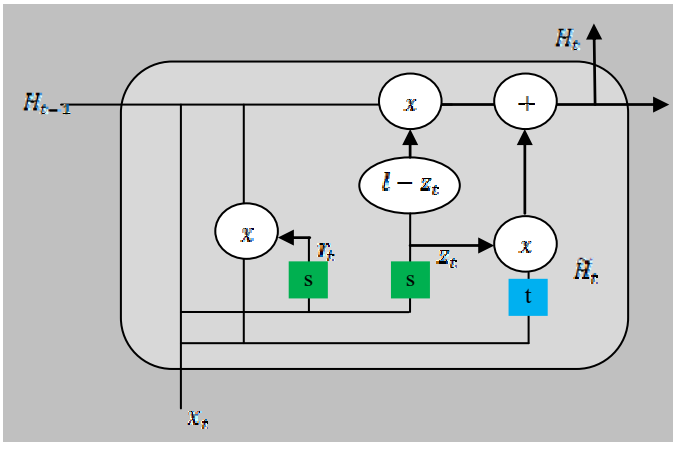
$$r_t = sigmoid\left(W_{xr}x_t + W_{hr}h_{t-1} + b_r\right) \tag{15}$$

$$\tilde{H}_t = \tanh\left(W_{x\tilde{H}}x_t + W_{H\tilde{H}}r_t \odot H_{t-1} + b_{\tilde{H}}\right) \tag{16}$$

$$H_t = z_t \odot H_{t-1} + (1 - z_t) \odot \tilde{H}_t \tag{17}$$

The input gate, forget gate, and update gate are made simpler by GRU, and the cell states and hidden states are combined. By lowering the model parameters, the GRU unit substantially shortens the model training process while maintaining the benefits of LSTM (Chung et al., 2014).

Figure 5 Structure of gated RNN (see online version for colours)



3.4 Multimodal real-time model

DMS-HPN, a multimodal real-time model, was created to fully utilise the data in low and high traffic levels. A flexible MDAE was built to create DMS-HPN while considering input diversity in various selected feature views. Cross-entropy loss function has been used to measure the error of the actual labels x_t and the prediction labels $\hat{x}_t$. It is represented by the equation (18),

$$L = -\sum_{t=1}^{T} x_t \log\left(\hat{x}_t\right) + (1 - x_t)\log\left(1 - \hat{x}_t\right) \tag{18}$$

Entropy has been used as loss function for multi-classification. It is represented by the equation (19)

$$L = -\sum_{t=1}^{T} x_t \log\left(\hat{x}_t\right) \tag{19}$$

4 Results and discussion

In this section experimentation evaluation is performed on attack detection methods. The evaluation has been experimented with using UNSW-NB15 and CICIDS2017 datasets. On the subject of detecting assaults within contemporary networks, DMS-HPN suggested a method. The Australian Centre for Cyber Security (ACCScyber) security research team developed the UNSW-NB15 datasets to assess IDS (Moustafa and Slay, 2016). The Canadian Centre for Cybersecurity (CIC) released the CICIDS 2017 dataset in the latter part of 2017 (Sharafaldin et al., 2018). The key details for the two datasets are presented in Table 1.

Table 1 Two datasets information

Dataset	*Features*	*Labels*	*Training samples*	*Testing samples*	*Years*
UNSW-NB15	42	10	175,341	82,332	2015
CICIDS 2017	83	8	93,500	28,481	2017

4.1 Evaluation metrics

The proposed approach's performance is measured using precision, recall, F-measure, and accuracy. These metrics have been computed based on the confusion matrix (Table 2), having two rows and two columns with the intention of relating to the amount of false positive (Fp), false negative (Fn), true positive (Tp) and true negative (Tn).

Table 2 Confusion matrix

		Predicted	
		Positive	*Negative*
Actual	Positive	Tp	Fp
	Negative	Fn	Tn

- *Precision:* the proportion of all identified attack recordings that were accurately classified as records of attacks. It is represented by equation (20).

$$\text{Precision} = \frac{Tp}{Tp + Fp} \tag{20}$$

- *Recall:* the proportion of all assault recordings that were accurately detected. Its alternative name is true positive rate (TPR). It is represented by equation (21).

$$\text{Recall} = \frac{Tp}{Tp + Fn} \tag{21}$$

- *F-measure:* it is the harmonic mean of precision and recall. It is represented by equation (22).

$$\text{F-measure} = \frac{2(\text{Recall} \times \text{Precision})}{\text{Recall} + \text{Precision}} \tag{22}$$

- *Accuracy:* the proportion of records that were successfully categorised out of all records. It is represented by equation (23).

$$\text{Accuracy} = \frac{Tp + Tn}{Tp + Tn + Fp + Fn} \tag{23}$$

4.2 Results comparison

Table 3 shows the overall results of comparing classification methods with two different datasets. The results achieved by the proposed classifier (DMS-HPN) and existing classifiers like MDAE, LSTM, GRU, and MS-DHPN are measured via precision, recall, F-measure, and accuracy. The results show that the proposed system has higher precision, recall, F-measure, and accuracy results of 86.50%, 87.10%, 87.50%, and 92.60% for the UNSW-NB15 dataset.

4.3 Discussion and findings

The results show that the proposed system has higher precision, recall, F-measure, and accuracy results of 86.50%, 87.10%, 87.50%, and 92.60% for the UNSW-NB15 dataset. The results of the proposed system for the CICIDS 2017 dataset are 98.30%, 98.70%, 99.10%, and 99.50% via metrics like precision, recall, F-measure, and accuracy.

Table 3 Evaluation results of attack detection methods vs. datasets

Datasets	*Methods*	*Metrics*			
		Precision (%)	*Recall (%)*	*F-measure (%)*	*Accuracy (%)*
UNSW-NB15	MDAE	79.90	80.10	80.00	81.20
	LSTM	80.20	81.00	80.60	81.50
	GRU	80.40	81.20	81.60	82.50
	MS-DHPN	84.90	86.50	85.90	87.20
	DMS-HPN	86.50	87.10	87.50	92.60
CICIDS 2017	MDAE	90.50	90.90	91.40	91.80
	LSTM	96.80	97.10	97.50	97.90
	GRU	97.80	98.10	98.45	98.80
	MS-DHPN	98.10	98.40	98.90	99.10
	DMS-HPN	98.30	98.70	99.10	99.50

Precision results produced by MDAE, LSTM, GRU, and MS-DHPN methods are 6.60%, 6.30%, 6.10%, and 1.60% lower when compared to the proposed system for the UNSW-NB15 dataset. Similarly, the proposed classifier has 7.80%, 1.50%, 0.50%, and 0.20% highest precision when compared to MDAE, LSTM, GRU, and MS-DHPN methods in the CICIDS 2017 dataset compared to MDAE, LSTM, GRU, and MS-DHPN methods in the CICIDS 2017 dataset.

Existing classifiers like MDAE, LSTM, GRU, and MS-DHPN have produced 7.00%, 6.10%, 5.90%, and 0.60% lower recall results compared to the proposed system for the UNSW-NB15 dataset. In the CICIDS 2017 dataset, the proposed classifier has 7.80%,

1.60%, 0.60%, and 0.30% highest recall compared to MDAE, LSTM, GRU, and MS-DHPN methods in the CICIDS 2017 dataset.

Figure 6 Precision comparison of attack detection methods (see online version for colours)

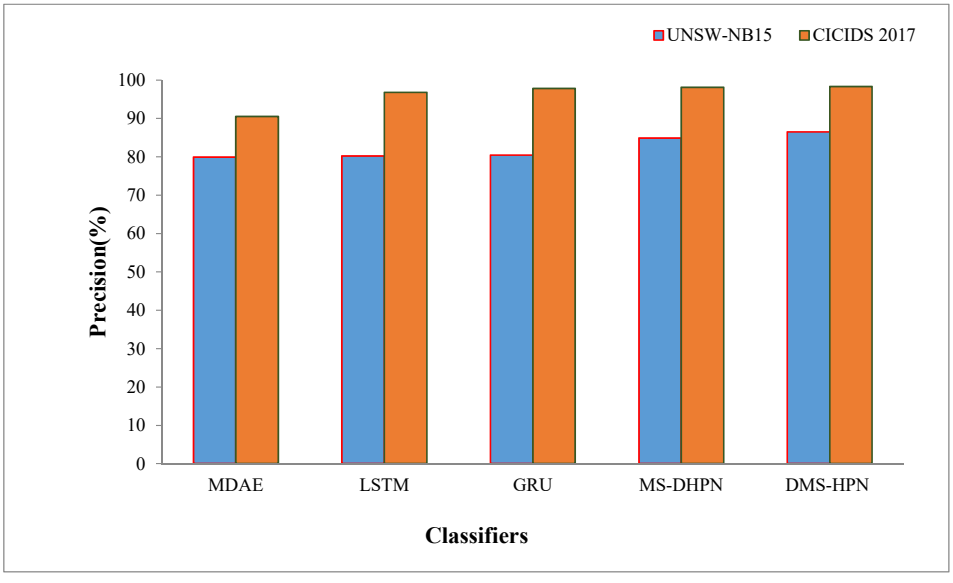
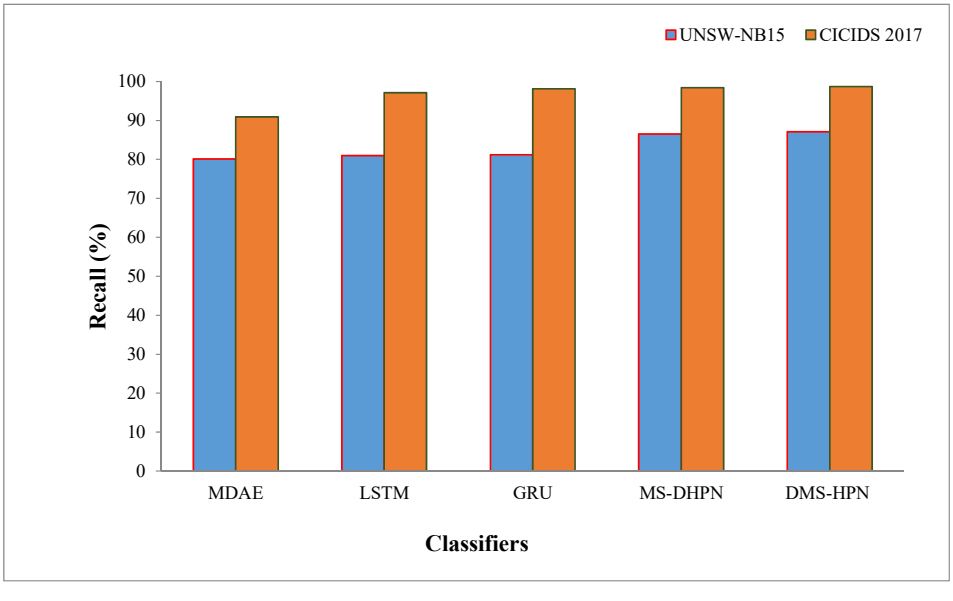


Figure 7 Recall comparison of attack detection methods (see online version for colours)



F-measure results attained by the existing classifiers like MDAE, LSTM, GRU, and MS-DHPN are 7.50%, 6.90%, 5.90%, and 1.60% lesser f-measure when compared to the proposed classifier in UNSW-NB15 dataset. The proposed classifier has 7.70%, 1.60%,

0.65%, and 0.20% highest f-measure when compared to MDAE, LSTM, GRU, and MS-DHPN methods in the CICIDS 2017 dataset.

Figure 8 F-measure comparison of attack detection methods (see online version for colours)

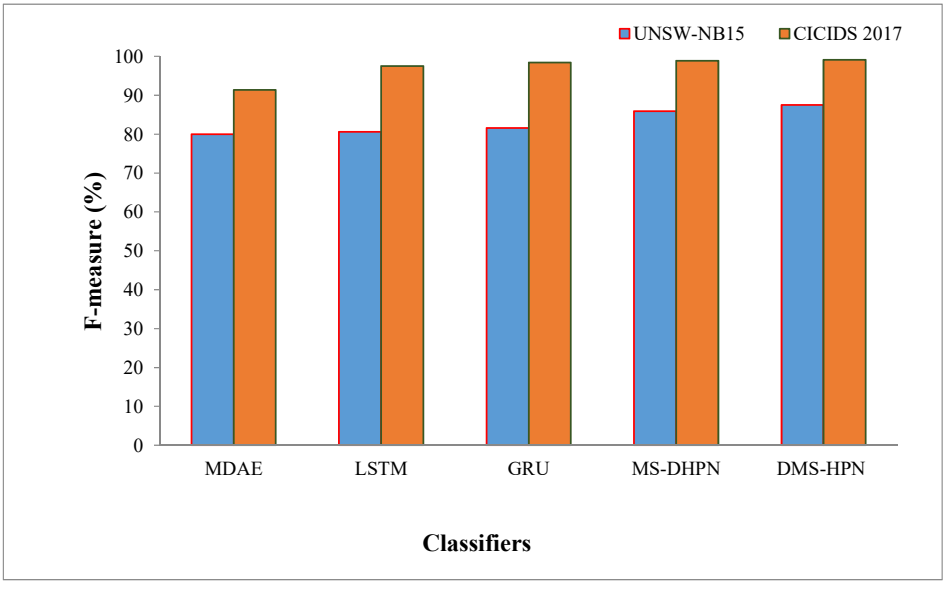
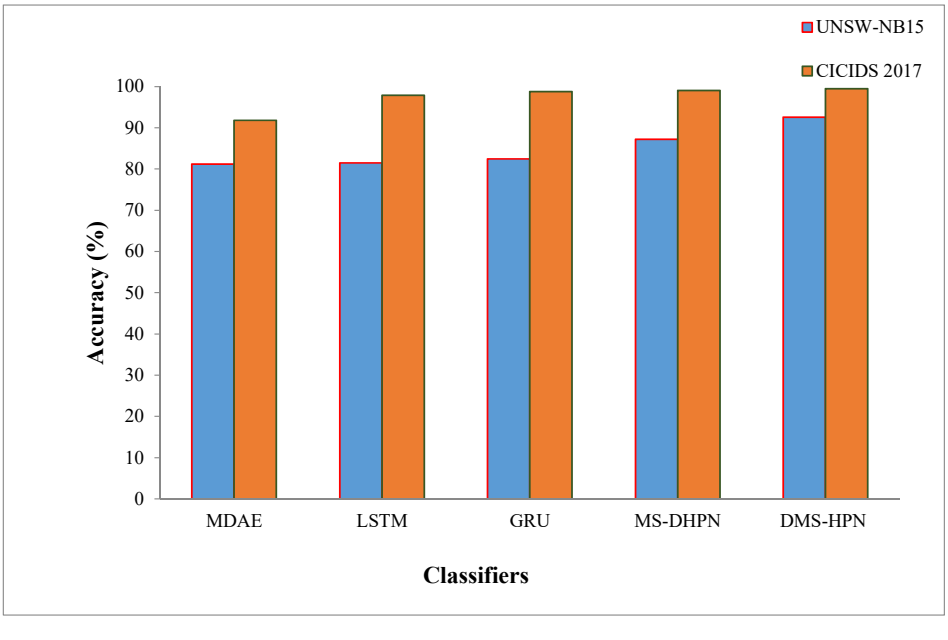


Figure 9 Accuracy comparison of attack detection methods (see online version for colours)



Accuracy results achieved by other classifiers MDAE, LSTM, GRU, and MS-DHPN are 11.40%, 11.10%, 10.10%, and 5.40% highest accuracy compared to the proposed system in the UNSW-NB15 dataset. The proposed classifier has the 7.70%, 1.60%, 0.70%, and 0.40% highest accuracy compared to MDAE, LSTM, GRU, and MS-DHPN methods in the CICIDS 2017 dataset.

Attack detection methods like MDAE, LSTM, GRU, MS-DHPN, and the proposed system for precision results are shown in Figure 6. The results show that the proposed system has higher results of 86.50% and 98.30% for UNSW-NB15 and CICIDS 2017 datasets. MDAE, LSTM, GRU and MS-DHPN has precision results of 79.90%, 80.20%, 80.40% and 84.90% for UNSW-NB15 and 90.50%, 96.80%, 97.80% and 98.10% for CICIDS 2017 which is lower when compared to the proposed method.

The recall comparison in attack detection methods like MDAE, LSTM, GRU, MS-DHPN, and the proposed system is shown in Figure 7. UNSW-NB15 and CICIDS 2017 datasets, the proposed system gives higher recall results of 87.10% and 98.70%. MDAE, LSTM, GRU and MS-DHPN has given recall results of 80.10%, 81.00%, 81.20% and 86.50% for UNSW-NB15 and 90.90%, 97.10%, 98.10% and 98.40% for CICIDS 2017 which is lower when compared to proposed method.

F-measure comparison of methods like MDAE, LSTM, GRU, MS-DHPN, and the proposed system for UNSW-NB15 and CICIDS 2017 datasets are illustrated in Figure 8. MDAE, LSTM, GRU and MS-DHPN give F-measure of 80.00%, 80.60%, 81.60% and 85.90% for UNSW-NB15 and 91.40%, 97.50%, 98.45% and 98.90% for CICIDS 2017 which is lower when compared to the proposed method.

Figure 9 shows the accuracy comparison of methods like MDAE, LSTM, GRU, MS-DHPN, and the proposed system. The proposed system has higher accuracy rates of 92.60% and 99.50% for UNSW-NB15 and CICIDS 2017 datasets. Existing methods like MDAE, LSTM, GRU and MS-DHPN gives accuracy results of 81.20%, 81.50%, 82.50% and 87.20% for UNSW-NB15 and 91.80%, 97.90%, 98.80% and 99.10% for CICIDS 2017 which is lower when compared to the proposed method.

5 Conclusions and future work

MDAE and GRU-based classifier, TSO with DMS-HPN has been introduced for the NIDS classification. It has been implemented on UNSW-NB15 and CICIDS 2017 datasets. The proposed framework includes the following steps:

1 pre-processing and feature extraction

2 FS

3 attack detection

4 performance evaluation.

Initially, the pre-processing and feature extraction stage has been introduced to process feature information independently. Secondly, the TSO algorithm has been introduced to select the optimal set of features for increasing the accuracy of the attack detection model. Thirdly, the DMS-DHPN classifier has been introduced by merging the individual classifiers like MDAE and GRU. It can capably combine the diverse level chosen features data by a network connection and can study temporal data among adjacent

network connections at the identical instance. The results of attack detection methods are measured using precision, recall, F-measure, and accuracy metrics. The proposed system gives higher accuracy results of 92.60% and 99.50% in UNSW-NB15 and CICIDS 2017. The major limitation of the present system is that it does not support real-time data. In the future, it will be applied to real-time network data. Some other attacks have also been tested and validated for the same system from a multimodality point of view to enhance the accuracy of NIDS. The present system is extended to an ensemble feature selection model for increasing the results of the IDS system. It may be either a homogenous ensemble model or a heterogeneous ensemble model. For combining the results of the ensemble model, stacking is the best option for classification. Instead of using a single classifier model, classification is also performed by combining the results of various classifiers via the bagging, boosting, and stacking ensemble model. Increasing the number of samples still becomes an unsolvable issue, but it may be solved by introducing parallel processing methods. It can handle the big dataset efficiently and reduce the classifier's running time.

References

Abdullahi, Y., Bhardwaj, A., Rahila, J., Anand, P. and Kandepu, K. (2023) 'Development of automatic change-over with auto-start timer and artificial intelligent generator', *FMDB Transactions on Sustainable Energy Sequence*, Vol. 1, No. 1, pp.11–26.

Ahmad, A.Y.A.B., Kumari, S.S., MahabubBasha Guha, S.K., Gehlot, A. and Pant, B. (2023) 'Blockchain implementation in financial sector and cyber security system', *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, IEEE.

Alazzam, H., Sharieh, A. and Sabri, K.E. (2020) 'A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer', *Expert Systems with Applications*, Vol. 148, No. 6, pp.1–14.

Aleesa, A., Younis, M., Mohammed, A.A. and Sahar, N. (2021) 'Deep-intrusion detection system with enhanced UNSW-NB15 data-set based on deep learning techniques', *Journal of Engineering Science and Technology*, Vol. 16, No. 1, pp.711–727.

Ali, M.H., Al Mohammed, B.A.D., Ismail, A. and Zolkipli, M.F. (2018) 'A new intrusion detection system based on fast learning network and particle swarm optimization', *IEEE Access: Practical Innovations, Open Solutions*, Vol. 6, pp.20255–20261, DOI: 10.1109/access.2018.2820092.

Almansor, M. and Gan, K.B. (2018) 'Intrusion detection systems: principles and perspectives', *Journal of Multidisciplinary Engineering Science Studies*, Vol. 4, No. 11, pp.2458–2925.

Almomani, O. (2021) 'A hybrid model using bio-inspired metaheuristic algorithms for network intrusion detection system', *Computers, Materials & Continua*, Vol. 68, No. 1, pp.409–429.

Alsaleh, A. and Binsaeedan, W. (2021) 'The influence of salp swarm algorithm-based feature selection on network anomaly intrusion detection', *IEEE Access*, Vol. 9, No. 8, pp.112466–112477.

Al-Tashi, Q., Abdul Kadir, S.J., Rais, H.M., Mirjalili, S. and Alhussian, H. (2019) 'Binary optimization using hybrid grey wolf optimization for feature selection', *IEEE Access: Practical Innovations, Open Solutions*, Vol. 7, pp.39496–39508, DOI: 10.1109/access.2019.2906757.

Al-Tashi, Q., Md Rais, H., Abdulkadir, S.J., Mirjalili, S. and Alhussian, H. (2020) 'A review of grey wolf optimizer-based feature selection methods for classification', in *Algorithms for Intelligent Systems*, pp.273–286, Springer: Singapore, Singapore.

Anand, P.P., Sulthan, N., Jayanth, P. and Deepika, A.A. (2023) 'A creating musical compositions through recurrent neural networks: an approach for generating melodic creations', *FMDB Transactions on Sustainable Computing Systems*, Vol. 1, No. 2, pp.54–64.

Angeline, R., Aarthi, S., Regin, R. and Rajest, S.S. (2023) 'Dynamic intelligence-driven engineering flooding attack prediction using ensemble learning', in *Advances in Artificial and Human Intelligence in the Modern Era,* pp.109–124, IGI Global, USA.

Cho, K., Van Merriënboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H. and Bengio, Y. (2014) 'Learning phrase representations using RNN encoder-decoder for statistical machine translation', *Empirical Methods in Natural Language Processing (EMNLP)*, pp.1–15.

Chung, J., Gulcehre, C., Cho, K. and Bengio, Y. (2014) 'Empirical evaluation of gated recurrent neural networks on sequence modeling', *Neural Information Processing Systems (NIPS)*, pp.1–9.

Cirillo, S., Polese, G., Salerno, D., Simone, B. and Solimando, G. (2023) 'Towards flexible voice assistants: evaluating privacy and security needs in IoT-enabled smart homes', *FMDB Transactions on Sustainable Computer Letters*, Vol. 1, No. 1, pp.25–32.

Devi, B.T. and Rajasekaran, R. (2023) 'A comprehensive review on deepfake detection on social media data', *FMDB Transactions on Sustainable Computing Systems*, Vol. 1, No. 1, pp.11–20.

Emary, E., Zawbaa, H.M. and Hassanien, A.E. (2016) 'Binary grey wolf optimization approaches for feature selection', *Neurocomputing*, Vol. 172, pp.371–381, DOI: 10.1016/j.neucom.2015.06.083.

Fraihat, B.A.M., Ahmad, A.Y.B., Alaa, A.A., Alhawamdeh, A.M., Soumadi, M.M., Aln'emi, E.A.S. and Alkhawaldeh, B.Y.S. (2023) 'Evaluating technology improvement in sustainable development goals by analysing financial development and energy consumption in Jordan', *International Journal of Energy Economics and Policy*, Vol. 13, No. 4, p.348.

Gaayathri, R.S., Rajest, S.S., Nomula, V.K. and Regin, R. (2023) 'Bud-D: enabling bidirectional communication with chatgpt by adding listening and speaking capabilities', *FMDB Transactions on Sustainable Computer Letters*, Vol. 1, No. 1, pp.49–63.

Hajisalem, V. and Babaie, S. (2018) 'A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection', *Computer Networks*, Vol. 136, pp.37–50, DOI: 10.1016/j.comnet.2018.02.028

Hammad, M., El-Medany, W. and Ismail, Y. (2020) 'Intrusion detection system using feature selection with clustering and classification machine learning algorithms on the UNSW-NB15 data-set', in *2020 International Conference on Innovation and Intelligence for Informatics, computIng and Technologies (3ICT*), pp.1–6.

He, H., Sun, X., He, H., Zhao, G., He, L. and Ren, J. (2019) 'A novel multimodal-sequential approach based on multi-view features for network intrusion detection', *IEEE Access*, Vol. 7, No. 12, pp.183207–183221.

Hemanth, D.J. (2021) 'Intrusion detection system using convolutional neural network on UNSW NB15 data-set', *Advances in Parallel Computing Technologies and Applications*, Vol. 40, pp.1–8, IOS Press, Netherlands.

Husain, A., Salem, A., Jim, C. and Dimitoglou, G. (2019) 'Development of an efficient network intrusion detection model using extreme gradient boosting (XGBoost) on the UNSW-NB15 data-set', in *2019 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, pp.1–7.

Javaid, A., Niyaz, Q., Sun, W. and Alam, M. (2016) 'A deep learning approach for network intrusion detection system', *Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies (Formerly BIONETICS)*, ACM.

Jeba, J.A., Bose, S.R. and Boina, R. (2023) 'exploring hybrid multi-view multimodal for natural language emotion recognition using multi-source information learning model', *FMDB Transactions on Sustainable Computer Letters*, Vol. 1, No. 1, pp.12–24.

Kanyimama, W. (2023) 'Design of a ground based surveillance network for Modibbo Adama University, Yola', *FMDB Transactions on Sustainable Computing Sy*stems, Vol. 1, No. 1, pp.32–43.

Kasongo, S.M. and Sun, Y. (2020) 'Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 data-set', *Journal of Big Data*, Vol. 7, No. 7, pp.1–20.

Kim, J., Kim, J., Thu, H.L.T. and Kim, H. (2016) 'Long short term memory recurrent neural network classifier for intrusion detection', In *2016 International Conference on Platform Technology and Service (PlatCon*), pp.1–5.

Li, L., Yu, Y., Bai, S., Hou, Y. and Chen, X. (2018) 'An effective two-step intrusion detection approach based on binary classification and k-NN', *IEEE Access: Practical Innovations*, *Open Solutions*, Vol. 6, pp.12060–12073, DOI: 10.1109/access.2017.2787719.

Lodha, S., Malani, H. and Bhardwaj, A.K. (2023) 'Performance evaluation of vision transformers for diagnosis of pneumonia', *FMDB Transactions on Sustainable Computing Systems*, Vol. 1, No. 1, pp.21–31.

Moualla, S., Khorzom, K. and Jafar, A. (2021) 'Improving the performance of machine learning-based network intrusion detection systems on the UNSW-NB15 data-set', *Computational Intelligence and Neuroscience*, Vol. 2021, No. 5557577, pp.1–13.

Moustafa, N. and Slay, J. (2016) 'The evaluation of network anomaly detection systems: statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set', *Information Security Journal: A Global Perspective*, Vol. 25, Nos. 1–3, pp.18–31.

Ojha, V.K., Abraham, A. and Snášel, V. (2017) 'Metaheuristic design of feedforward neural networks: a review of two decades of research', *Engineering Applications of Artificial Intelligence*, Vol. 60, pp.97–116, DOI: 10.1016/j.engappai.2017.01.013.

Othman, Z.A., Adabashi, A.M., Zainudin, S. and Hashmi, S.M. (2011) 'Improvement anomaly intrusion detection using Fuzzy-ART based on K-means based on SNC labeling', *Jurnal Teknologi Maklumat & Multimedia*, Vol. 10, No. 10, pp.1–11.

Rajasekaran, N., Jagatheesan, S.M., Krithika, S. and Albanchez, J.S. (2023) 'Development and testing of incorporated ASM with MVP architecture model for android mobile app development', *FMDB Transactions on Sustainable Computing Systems*, Vol. 1, No. 2, pp.65–76.

Rajest, S.S., Singh, B., Obaid, A.J., Regin, R. and Chinnusamy, K. (2023a) 'Recent developments in machine and human intelligence', *Advances in Computational Intelligence and Robotics*, DOI: 10.4018/978-1-6684-9189-8.

Rajest, S.S., Singh, B., Obaid, A.J., Regin, R. and Chinnusamy, K. (2023b) 'Advances in artificial and human intelligence in the modern era', *Advances in Computational Intelligence and Robotics*, DOI: 10.4018/979-8-3693-1301-5.

Regin, R., Khanna, A.A., Krishnan, V., Gupta, M., Rubin Bose, S. and Rajest, S.S. (2023a) 'Information design and unifying approach for secured data sharing using attribute-based access control mechanisms', in *Recent Developments in Machine and Human Intelligence*, pp.256–276, IGI Global.

Regin, R., Shynu, Rajest, S. S., Bhattacharya, M., Datta, D. and Priscila, S.S. (2023b) 'Development of predictive model of diabetic using supervised machine learning classification algorithm of ensemble voting', *International Journal of Bioinformatics Research and Applications*, Vol. 19, No. 3, DOI: 10.1504/ijbra.2023.10057044.

Saheed, Y.K. (2022) 'A binary firefly algorithm based feature selection method on high dimensional intrusion detection data', in *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, pp.273–288, Springer, Switzerland.

Sahoo, A. and Chandra, S. (2017) 'Multi-objective grey wolf optimizer for improved cervix lesion classification', *Applied Soft Computing*, Vol. 52, pp.64–80, DOI: 10.1016/j.asoc.2016.12.022.

Sahu, S.K., Sarangi, S. and Jena, S.K. (2014) 'A detail analysis on intrusion detection datasets', *2014 IEEE International Advance Computing Conference (IACC)*, IEEE, Gurgaon, India, pp.1348–1353, DOI: 10.1109/IAdCC.2014.6779523.

Sajini, S., Reddi, L.T., Regin, R. and Rajest, S.S. (2023) 'A comparative analysis of routing protocols for efficient data transmission in vehicular ad hoc networks (VANETs)', *FMDB Transactions on Sustainable Computing Systems*, Vol. 1, No. 1, pp.1–10.

Saxena, D. and Chaudhary, S. (2023) 'Predicting brain diseases from FMRI-functional magnetic resonance imaging with machine learning techniques for early diagnosis and treatment', *FMDB Transactions on Sustainable Computer Letters*, Vol. 1, No. 1, pp.33–48.

Sharafaldin, I., Lashkari, A.H. and. Ghorbani, A.A (2018) 'Toward generating a new intrusion detection data-set and intrusion traffic characterization', *ICISSp*, Vol. 1, pp.108–116.

Shone, N., Ngoc, T.N., Phai, V.D. and Shi, Q. (2018) 'A deep learning approach to network intrusion detection', *IEEE Transactions on Emerging Topics in Computational Intelligence*, Vol. 2, No. 1, pp.41–50.

Sivapriya, G.B.V., Ganesh, U.G., Pradeeshwar, V., Dharshini, M. and Al-Amin, M. (2023) 'Crime prediction and analysis using data mining and machine learning: a simple approach that helps predictive policing', *FMDB Transactions on Sustainable Computer Letters*, Vol. 1, No. 2, pp.64–75.

Sohlot, J., Teotia, P., Govinda, K., Rangineni, S. and Paramasivan, P. (2023) 'A hybrid approach on fertilizer resource optimization in agriculture using opposition-based harmony search with manta ray foraging optimization', *FMDB Transactions on Sustainable Computing Systems*, Vol. 1, No. 1, pp.44–53.

Sumaiya Thaseen, I., Saira Banu, J., Lavanya, K., Rukunuddin Ghalib, M. and Abhishek, K. (2021) 'An integrated intrusion detection system using correlation-based attribute selection and artificial neural network', *Transactions on Emerging Telecommunications Technologies*, Vol. 32, No. 2, pp.1–15, DOI: 10.1002/ett.4014.

Tama, B.A., Comuzzi, M. and Rhee, K.H. (2019) 'TSE-IDS: a two-stage classifier ensemble for intelligent anomaly-based intrusion detection system', *IEEE Access*, Vol. 7, No. 7, pp.94497–94507.

Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A. and Venkatraman, S. (2019) 'Deep learning approach for intelligent intrusion detection system', *IEEE Access: Practical Innovations, Open Solutions*, Vol. 7, pp.41525–41550, DOI: 10.1109/access.2019.2895334.

Wang, H., Wang, J., Dong, C., Lian, Y., Liu, D. and Yan, Z. (2020) 'A novel approach for drug-target interactions prediction based on multimodal deep Autoencoder', *Frontiers in Pharmacology*, Vol. 10, No. 10, pp.1–19.

Win, T.Z. and Kham, N.S. (2019) 'Information gain measured feature selection to reduce high dimensional data', in *Proceedings of the 17th International Conference on Computer Applications* Yangon, Myanmar, pp.68–73.

Xie, L., Han, T., Zhou, H., Zhang, Z.R., Han, B. and Tang, A. (2021) 'Tuna swarm optimization: a novel swarm-based metaheuristic algorithm for global optimization', *Computational Intelligence and Neuroscience*, Vol. 2021, No. 9210050, pp.1–22.

Yin, C., Zhu, Y., Fei, J. and He, X. (2017) 'A deep learning approach for intrusion detection using recurrent neural networks', *IEEE Access*, Vol. 5, No. 12, pp.21954–21961.

Yin, Y., Jang-Jaccard, J., Xu, W., Singh, A., Zhu, J., Sabrina, F. and Kwak, J. (2023) 'IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 data-set. *Journal of Big Data*, Vol. 10, No. 1, pp.1–26.

Zeeshan, M., Riaz, Q., Bilal, M.A., Shahzad, M.K., Jabeen, H., Haider, S.A. and Rahim, A. (2021) 'Protocol-based deep intrusion detection for dos and ddos attacks using unsw-nb15 and bot-iot data-sets', *IEEE Access*, Vol. 10, No. 12, pp.2269–2283.