DESIGN AND IMPLEMENTATION OF AN ENHANCED MODEL OF SUPPORT VECTOR MACHINE WITH RADIAL BASIS FUNCTION AND PARTICLE SWARM OPTIMIZATION FOR DETECTION OF DDoS ATTACKS

Anthony Obogo Otiko[1], Emmanuel A. Edim[2], Emmanuel U. Oyo-Ita[3]

[1'3]Department of Computer Science, University of Cross River State, Calabar.
[2]Department of Computer Science, University of Calabar

---***---

Abstract:

The increasing reliance on networked systems in the Information and Communication Technology (ICT) landscape has made them crucial for managing Critical Infrastructure (CI) and information access. However, this dependence has also made these systems vulnerable to Distributed Denial-of-Service (DDOS) attacks, which disrupt services by flooding target hosts with traffic. Traditional security measures often fall short against these attacks due to their dynamic nature and evolving tactics. To address this challenge, various researchers have explored the potential of Machine Learning (ML). This study proposes a hybrid solution that combines a Support Vector Machine (SVM) with a Radial Basis Function (RBF) kernel and Particle Swarm Optimization (PSO) for feature selection to enhance DDOS attack detection accuracy. Using the KDD-99 dataset, the SVM-PSO model is trained and evaluated, achieving a superior performance of 99.99% compared to SVM-RBF alone with 99.72%. The findings demonstrate the efficacy of the proposed approach in detecting DDOS attacks, showcasing its potential for bolstering cyber defences. Additionally, comparative analysis with state-of-the-art algorithms highlights the superior accuracy of the SVM-RBF-PSO model, underscoring its effectiveness in mitigating DDOS threats. This study contributes valuable insights into enhancing network security through innovative machine learning techniques, addressing the persistent challenges posed by DDOS attacks.

Keywords: Algorithm, artificial intelligence, Denial of Service, Distributed Denial of Service, Kernel PCA, Support Vector Machine, Malicious Traffic.

1.0 Introduction

In the rapidly evolving landscape of Information and Communication Technology (ICT), the reliance on networked systems for information access and communication has become paramount (Agboola, 2023). With the expansion of services facilitated by ICT, including the management of Critical Infrastructure (CI), society's dependency on these systems has grown substantially. Any disruption to these systems, even for short durations, can have far-reaching consequences across various facets of modern life.

Distributed Denial-of-Service (DDOS) attacks, in particular, have emerged as a significant threat in the digital realm (Kaur et al., 2019). These attacks leverage distributed computing power to inundate target hosts with traffic, leading to service disruptions. The proliferation of DDOS attacks, coupled with the limitations of traditional security measures, has made them a persistent challenge for network defenders.

Despite efforts to mitigate DDOS attacks, their dynamic nature and evolving tactics pose ongoing challenges for detection and prevention. Traditional security measures often prove insufficient against the scale and sophistication of modern DDOS attacks, necessitating innovative approaches to bolster cyber defenses (Shukla et al., 2022).

Hence, diverse researchers have applied the viabilities of Machine Learning (ML), knowledge-based approaches, and statistical analysis to tackle the problem of DDOS attacks. However, each method presents its unique set of limitations and challenges. For instance, statistical methods often struggle to precisely determine the normal distribution of network packets (Sharafaldin et al., 2019). While ML techniques offer promising results, however, the optimal selection of best features remains a primary concern considering the prodigious size of datasets.

While traditional Feature Selection (FS) methods have demonstrated viability, their efficacy remains subject to scrutiny (Khaire and Dhanalakshmi, 2022). Notably, recent trends underscore the increasing adoption of Meta-heuristic approaches, particularly as wrapper methods for feature selection, showcasing substantial effectiveness in mitigating the impact of overwhelming dataset sizes within the context of DDOS attack detection. Considering Meta-heuristic approaches for FA, (Paniri et al., 2020) applied Ant Colony (AC), (Awadallah et al., 2022) applied Binary Horse herd optimization algorithm, (Rostami and Kaveh, 2021) utilized the biogeography-based optimization (BBO) and artificial bee colony (ABC), (Rostami et al., 2020) integrated Particle Swarm Optimization (PSO) on medical dataset for FS. All the methods have shown the viability of AI approaches in machine learning.

In response to the escalating threat posed by DDOS attacks, this study proposes a machine learning-based solution that hybridizes the Support Vector Machine (SVM) with the Radial Basis Function (RBF) kernel. Furthermore, the selection of features is optimized using the Particle Swarm Optimization (PSO) algorithm. By integrating SVM with PSO, the aim is to enhance the accuracy and reliability of DDOS attack detection.

The proposed model is applied to the KDD-99 dataset obtained from the UCI Machine Learning Repository, which contains instances of both normal and malicious network activities. Leveraging this dataset, the study seeks to train and evaluate the effectiveness of the SVM-PSO model in discerning patterns indicative of DDOS attacks within network traffic.

The primary contribution of this study lies in the application of PSO as a feature selection mechanism on the SVM RBF kernel for classifying network attacks.

2.0 Related Works

Malik and Aslam (2013) devised a hybrid approach that combines multi-objective particle swarm optimization with the random forest algorithm. The authors suggest employing this method to effectively identify Probe attacks to enhance the detection rate and reduce the rate of false alarm discovery while identifying Probe attacks. Particle Swarm Optimization (PSO) removes superfluous features, whereas Random Forest (RF) identifies Probe assaults. The author's proposed approach has a detection rate of 90.7%.

Li et al., (2018) constructed a model that incorporates the Gini index. This model comprises the gradient boosting decision tree (GBDT) and particle swarm optimization (PSO). The Gini index was used to select the best feature subset. The network assault was detected using the gradient lifting decision tree algorithm. The GBDT parameters were optimized using the Particle Swarm Optimization (PSO) technique. The model was evaluated based on its detection rate, accuracy, F1-score, precision, and false alarm rate. An evaluation was carried out using the NSL-KDD Dataset. According to the findings, the model demonstrated high accuracy and effective intrusion detection capabilities. The model achieved a detection rate of 78.48%, a precision rate of 96.44%, an F1-score of 86.54%, and a false acceptance rate of 3.83%.

Ren et al. (2019) proposed an IDS integrating data sampling, feature selection, and a unified hybrid data optimization procedure. The model achieved optimal training dataset selection and feature identification using Genetic Algorithm (GA) and Random Forest (RF).

Nazir and Khan (2021) introduced Tabu Search–Random Forest (TS–RF) for feature selection, demonstrating an accuracy rate of 83.12% and a false positive rate (FPR) of 3.7% on the UNSW-NB15 dataset. Despite positive results, they acknowledged not addressing the class imbalance issue in the dataset. Overall, these studies contribute valuable insights into the application of advanced techniques for intrusion detection, showcasing strengths and areas for further enhancement.

3.0 Research Methodology

The proposed research methodology comprises three key phases: data preprocessing, feature selection, and classification with performance evaluation. Firstly, in the data preprocessing phase, the objective is to refine and clean the raw data to prepare it for analysis. This involves tasks such as handling missing values, normalizing data, and eliminating noise or outliers to ensure the data is in a suitable format for subsequent analysis. Secondly, in the feature selection phase, the focus is on identifying and extracting essential attributes from the preprocessed data. The aim is to retain only those features that significantly contribute to detecting network intrusions, thereby reducing dimensionality, enhancing model performance, and improving result interpretability. To achieve this, a meta-heuristic approach utilizing the PSO algorithm for feature selection is proposed. Lastly, the classification and performance evaluation phase involves using the features selected by the PSO algorithm to train a machine learning classification model, specifically the SVM algorithm. SVM categorizes network activities as normal or intrusive based on learned patterns. Following training, the model's performance is assessed using metrics such as accuracy, precision, recall, and F1-score to ensure its reliability and effectiveness in identifying network intrusions. The proposed methodology approach can be visualized in Figure 3.1.

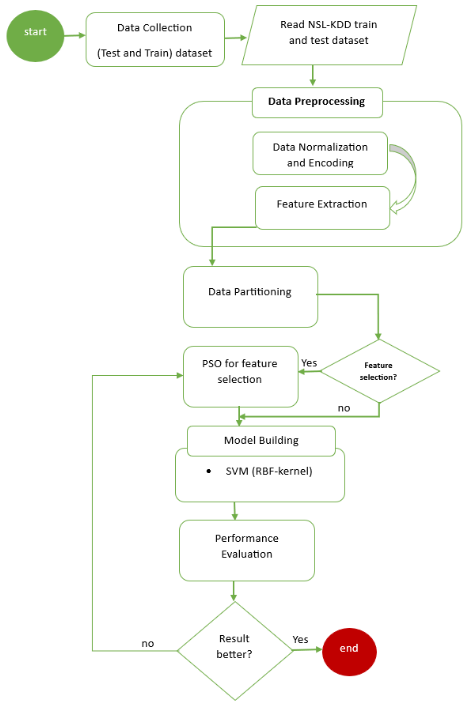


Figure 3.1: Research Design

3.1 Dataset Description

The KDD dataset has 41 attributes and one class label with more than 4 million instances (Ibor et al., 2015; Aggarwal and Sharma, 2015). The dataset has several versions from which 10% of the training data with 494, 021 instances is used in this empirical study. The test set contains 311, 079 instances, which are used to evaluate the performance of the model for accuracy, FPR and other metrics. The dataset also has a class label that indicates the type of attack for each instance. Different configurations of this dataset are available with variation in the number of instances but the number of attributes in each case is 42. The attribute labeled 42 in the data set is the class attribute which indicates whether a given instance is a normal connection instance or an attack.

3.2 Data Preprocessing

The data preprocessing phase is essential to address the disparate range of values exhibited by each characteristic in the intrusion detection data. This phase involves characterizing the data, which includes converting text features to normal values and standardizing numerical features. Specifically, the numerical characteristics of the intrusion data are standardized using the formula outlined in this paper.

$$\frac{V^{ij} - min^j(V^{ij})}{max^j(V^{ij}) - min^j(V^{ij})} \dots \dots \dots \dots \dots \dots 3.1$$

This objective is accomplished by normalizing each feature variable, denoted as Vij, to the interval (0, 1).

3.3 Feature Selection

Considering the number of features from the KDD dataset and the number of intrusion records, feature selection becomes essential. Hence, the proposed feature selection techniques aim to reduce the dimensionality of a feature set while retaining the most relevant features. In DDoS detection, it enhances efficiency by discarding irrelevant features. Therefore, to achieve a reduced feature selection, the study proposes using the Particle Swarm Optimization (PSO) algorithm. PSO optimizes by mimicking the social behaviour of birds foraging for food. Each particle represents a potential solution and possesses position, velocity, and fitness value. The algorithm iteratively refines binary feature vectors to maximize the accuracy of the Random Forest classifier. Particles traverse the search space, updating positions based on the objective function. The goal is to identify a subset of features that maximizes classifier performance. The global best solution represents the selected features with the highest accuracy on validation sets. The particle's velocity is updated using equation 3.2

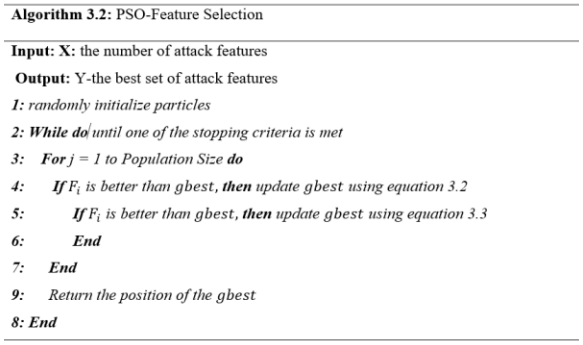
$$v_{id}^{t+1} = w * v_{id}^{t} + c_1 * r_{1i} * (p_{id} - x_{id}^{t}) + c_2 * r_{2i} * (p_{gd} - x_{id}^{t}) \quad 3.2$$

The particle's position is updated using Equation 3.3

$$x_{id}^{t+1} = x_{id}^{t} + v_{id}^{t+1} \quad 3.3$$

In the equations, t symbolizes the t^{th} iteration of PSO, $d \in D$ indicates search space d^{th} dimension, w signifies the inertia weight, c_1 and c_2 are acceleration factors, r_1 and r_2 are random numbers between [0,1]. And $p\,i\,d$ and p_{id} and p_{gd} are (pbest) and (gbest) respectively. p_{id} (pbest) is the best particle in the t^{th} iteration and p_{gd} (gbest) is the best particle in all iterations until then.

The algorithm for the PSO feature selection techniques is presented in algorithm 3.2.



```
Algorithm 3.2: PSO-Feature Selection
Input: X: the number of attack features
Output: Y-the best set of attack features
randomly initialize particles
While do until one of the stopping criteria is met
    For j = 1 to Population Size do
        If $F_i$ is better than gbest, then update gbest using equation 3.2
            If $F_i$ is better than gbest, then update gbest using equation 3.3
            End
    End
    Return the position of the gbest
End
```

3.4 Classification Algorithm

This study focuses on addressing the challenge of detecting Distributed Denial of Service (DDOS) attacks through a classification approach. Considering the nature of DDOS attacks from the KDD dataset as a classification problem, the research proposes employing the Support Vector Machine (SVM) algorithm. SVM is a well-established machine learning technique renowned for its effectiveness in classification tasks. Rooted in the concept of solving large-dimensional problems' dual forms, SVM aims to construct a classifier based on a minimal set of support vectors, thereby adhering to the principle of structural risk minimization (Gaye et al., 2021). The support vector machine (SVM) stands out as an elegant and powerful supervised machine learning algorithm, widely utilized for regression and classification tasks. Its versatility lies in its ability to predict non-linearly separable patterns by projecting the original feature space into a hyperplane in a higher-dimensional space. SVM is considered a non-parametric algorithm, as it recalls and stores all training dataset instances.

For, the kernel, the Radial Basis Function (RBF) kernel was applied. The RBF kernel was used to map non-linear boundaries of the input space into a higher dimensional feature space considering that the kernel value lies between 0 and 1.

$$K(x_i, x_j) = \left(e^{-\gamma\|x_i - x_j\|^2}\right), \gamma > 0 \ldots\ldots 3.4$$

Here, $\|x_i - x_j\|^2$ is the squared Euclidean distance between the two feature vectors and σ is a free parameter. x_i and x_j, depicted as feature vectors in some input space is given as:

3.3 Performance Evaluation

To evaluate the performance of the SVM-PSO model, the accuracy, precision, recall, and f1-score metrics are proposed. The criterion for each of the metrics is calculated according to four main criteria which are True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) as follows:

i. True Positive (TP): Indicates when an alarm is generated and there is an intrusion.
ii. False Negative (FN): Indicates when an alarm is not generated but there is an intrusion.
iii. False Positive (FP): Indicates when an alarm is generated but there is no intrusion.
iv. True Negative (TN): Indicates when an alarm is not generated and there is no intrusion.

Accuracy quantifies the ratio of accurately classified instances, encompassing both true positives and true negatives, relative to the total number of instances, as demonstrated in equation 3.5:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \ldots\ldots\ldots\ldots\ldots\ldots 3.5$$

Precision: the precision metric represents the proportion of accurately classified attack flows (True Positives, TP) relative to all the classified flows (TP + False Positives, FP). Equation 3.6 illustrates the mathematical representation of the precision metric.

$$precision = \frac{TP}{TP + FP} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 3.6$$

Recall: this metric signifies the proportion of correctly classified attack flows (TP) relative to all generated flows (TP + False Negatives, FN). The formula is shown in equation 3.7:

$$Recall = \frac{TP}{TP + FN} \ldots\ldots..3.7$$

F-measure, also known as F-score, measure combines precision and recall into a single metric using their harmonic mean, providing a balanced evaluation of classification performance. Equation 3.8 presents the mathematical expression for calculating the F-score.

$$F - Measure = 2 \times \frac{Precision\ \times Recall}{Precision + Recall} \ldots\ldots\ldots..3.8$$

4.0 Result and Discussion

This section outlines the findings from an empirical study and application that aimed to forecast network anomaly detection using the KDD-99 dataset source from the Kaggle machine learning repositories. The use of machine learning algorithms, specifically the SVM-RBF-PSO algorithm is part of the study technique. The developed models are then thoroughly validated using performance metrics including F1-score, precision, and recall.

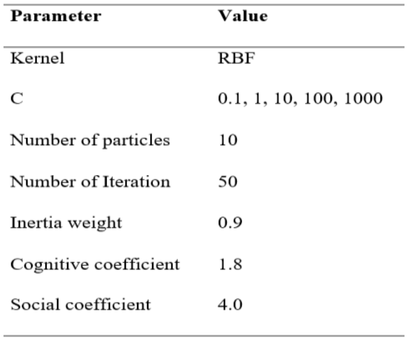
4.1 Environmental Setup

The Anaconda programming environment's computational resilience was utilized in the creation of the network DDOS model. The complexities of the model were executed on a Windows operating system with a dual-core Intel Core i5 processor and 4GB RAM, and they were smoothly integrated into the Python programming language. Implementation was done using SKlearn API, which is designed for complex deep neural network applications. Important Python modules like NumPy, in addition to SKlearn, enabled sophisticated numerical operations, and pandas took care of dataset integration and parsing. A flexible visualization application called Matplotlib was used to show the graphical behaviour of painstakingly constructed machine learning models.

4.2 parameter Settings

Table 4.1 presents the parameter settings for the SVM-PSO model used in feature selection and detection. For the SVM algorithm, for the kernel, the RBF kernel was tested. This kernel transforms input data into higher-dimensional space. The C parameter, ranging from 0.1 to 1000, balances decision boundary smoothness and correct classification. PSO parameters included 10 particles for traversal and 50 iterations for updating positions. The inertia weight (0.9) balances previous velocities, while cognitive (1.8) and social (4.0) coefficients influence particle movement towards historical and neighbour best-known positions, respectively.

Table 4.1: Parameter Settings for SVM-PSO model



Parameter	Value
Kernel	RBF
C	0.1, 1, 10, 100, 1000
Number of particles	10
Number of Iteration	50
Inertia weight	0.9
Cognitive coefficient	1.8
Social coefficient	4.0

4.0 Result Presentation

The results between SVM-RBF and SVM-RBF-PSO models on the KDD-99 dataset are presented in Table 4.2. In terms of precision, SVM-RBF achieved a score of 99.78%, while SVM-RBF-PSO slightly outperformed it with a precision score of 99.91%. Similarly, in the recall, SVM-RBF achieved a score of 99.83%, whereas SVM-RBF-PSO showed a slightly higher recall score of 99.90%. When considering the F1 score, SVM-RBF had a score of 99.80%, while SVM-RBF-PSO maintained a comparable score of 99.81%. Notably, in terms of accuracy, SVM-RBF achieved a high accuracy of 99.72%, whereas SVM-RBF-PSO exhibited a notably higher accuracy of 99.99%.

Table 4.2: SVM-RBF and SVM-RBF-PSO Result Comparison

Metrics	SVM Models	
	SVM-RBF	**SVM-RBF-PSO**
Precision	99.78	99.91
Recall	99.83	99.90
F1-Score	99.80	99.81
Accuracy	99.72	99.99

These results indicate that the SVM-RBF-PSO model, which integrates Particle Swarm Optimization (PSO) for feature selection, performed slightly better across all metrics compared to the SVM-RBF model without PSO integration. Moreover, the significant increase in accuracy demonstrates the effectiveness of the PSO algorithm in enhancing the performance of the SVM model for DDOS attack detection on the K99 dataset.

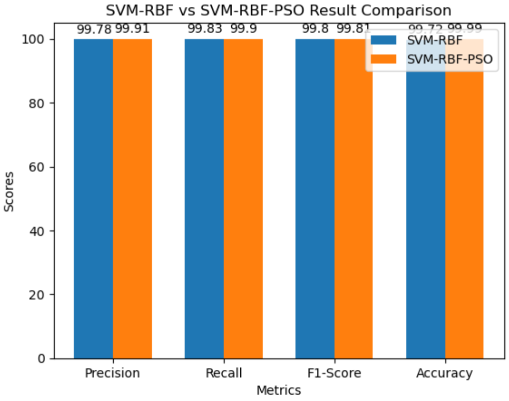


Figure 4.1: SVM models Performance.

Figure 4.1 Bar chart presents a comparison of the SVM-RBF and SVM-RBF-PSO performance metrics based on four evaluation metrics: accuracy, recall, F1-score, and precision. The x-axis shows each measure, while the y-axis

shows the scores that each model received. The SVM-RBF model and the SVM-RBF-PSO model have two bars next to each other for every metric. Each bar's height reflects the score that the corresponding model received for that specific metric. This visualization makes it easy to compare the two models quickly across a range of measures, revealing which model performs better overall and for each indicator in particular. The SVM-RBF-PSO model performs better than the SVM-RBF model in this particular instance on all measures, as shown.

4.4 SVM- RBF-PSO Comparison with Other Works

Given the meta-heuristic nature of the wrapper feature selection method employed in this approach, a comparative analysis was conducted to assess the efficacy of the SVM-RBF-PSO algorithm. This assessment involved a juxtaposition with some selected state-of-the-art algorithms that utilize meta-heuristic wrapper feature selection techniques specifically tailored for addressing DDoS attacks. The results of this comparative evaluation are presented in Table 5, shedding light on the performance of the SVM-RBF-PSO algorithm in relation to its counterparts in the domain of advanced algorithmic approaches.

Table 4.3: SVM-RBF-PSO comparison for DDOS attack

Authors	Dataset	Algorithm	Accuracy (%)
Malik and Aslam (2013)	KDD	RF-PSO	90.7
Li et al., (2018)	KDD	GBDT-PSO	78.48
Nazir and Khan (2021)	-	TS–RF	83.12
Current Study	**KDD**	**SVM-RBF-PSO**	**99.99**

Keys: Gradient boosting decision tree (GBDT) and particle swarm optimization (PSO), Tabu Search–Random Forest (TS–RF), Random Forest (RF) and Particle Swarm Optimization (PSO). SVM-RBF-PSO.

In Table 4.3, a comparative analysis is presented, evaluating the performance of various algorithms that considered meta-heuristic approaches for feature selection in addressing Distributed Denial of Service (DDoS) attacks. The algorithms under consideration include RF-PSO proposed by Malik and Aslam (2013) with an accuracy of 90.7% on the KDD dataset, GBDT-PSO introduced by Li et al. (2018) achieving an accuracy of 78.48% on the same dataset, and TS–RF by Nazir and Khan (2021) attaining an accuracy of 83.12%, although the specific dataset used is not mentioned.

Notably, the current study introduces the SVM-RBF-PSO algorithm, reporting a higher accuracy of 99.99% on the KDD dataset. This suggests that the SVM-RBF-PSO algorithm outperforms the compared algorithms in terms of accuracy for DDoS attack detection. The utilization of a Support Vector Machine (SVM) with a Radial Basis Function (RBF) kernel in conjunction with Particle Swarm Optimization (PSO) for feature selection appears to contribute to a more effective detection mechanism. Figure 19 shows the graphical presentation of the methods that applied metaheuristics approaches for feature selection.

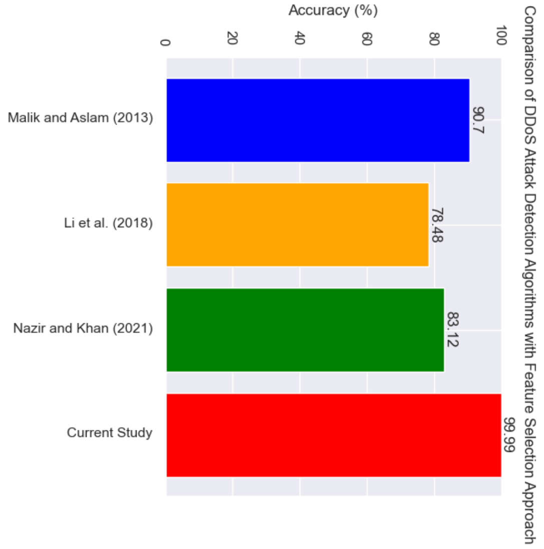


Figure 4.2: FS Meta Heuristics Approach Comparison

5.0 Conclusion

In conclusion, this study presents a comprehensive approach to address the challenge of detecting Distributed Denial of Service (DDOS) attacks in network traffic. By integrating machine learning techniques, specifically the SVM algorithm with the RBF kernel, and optimizing feature selection using the PSO algorithm, the proposed model aims to enhance the accuracy and reliability of DDOS attack detection. The empirical evaluation conducted on the KDD-99 dataset demonstrates the effectiveness of the SVM-RBF-PSO model compared to the SVM-RBF model without PSO integration. Across multiple performance metrics including precision, recall, F1-score, and accuracy, the SVM-RBF-PSO model consistently outperforms the SVM-RBF model. Notably, the SVM-RBF-PSO model achieves a notably higher accuracy of 99.99%, indicating its superior performance in identifying network intrusions. Furthermore, a comparative analysis with state-of-the-art algorithms employing meta-heuristic approaches for feature selection highlights the efficacy of the SVM-RBF-PSO algorithm. Compared to other algorithms such as RF-PSO, GBDT-PSO, and TS-RF, the SVM-RBF-PSO algorithm achieves the highest accuracy of 99.99%, showcasing its effectiveness in detecting DDOS attacks. In summary, the integration of SVM with RBF kernel and PSO for feature selection presents a robust solution for DDOS attack detection, offering superior performance compared to existing methods. The findings of this study contribute valuable insights into the application of advanced machine learning techniques for enhancing cybersecurity in network environments. Further research can explore additional datasets and fine-tune the proposed model for real-world deployment, ultimately strengthening network defence mechanisms against evolving cyber threats.

Reference

Agboola, O. P., Bashir, F. M., Dodo, Y. A., Mohamed, M. A. S., & Alsadun, I. S. R. (2023). The influence of information and communication technology (ICT) on stakeholders' involvement and smart urban sustainability. Environmental Advances, 13, 100431.

Aggarwal, P., & Sharma, S. K. (2015). Analysis of KDD dataset attributes-class for intrusion detection. Procedia Computer Science, 57, 842-851.

Awadallah, M. A., Hammouri, A. I., Al-Betar, M. A., Braik, M. S., & Abd Elaziz, M. (2022). Binary Horse herd optimization algorithm with crossover operators for feature selection. Computers in biology and medicine, 141, 105152.

Gaye, B., Zhang, D., & Wulamu, A. (2021). Improvement of support vector machine algorithm in big data background. Mathematical Problems in Engineering, 2021, 1-9.

Ibor, A. E., &Epiphaniou, G. (2015). A hybrid mitigation technique for malicious network traffic based on active response. International Journal of Security and Its Applications, 9(4), 63-80.

Kaur Chahal, J., Bhandari, A., & Behal, S. (2019). Distributed denial of service attacks: A threat or challenge. New Review of Information Networking, 24(1), 31-103.

Khaire, U. M., & Dhanalakshmi, R. (2022). Stability of feature selection algorithm: A review. Journal of King Saud University-Computer and Information Sciences, 34(4), 1060-1073.

Malik, A. J., & Khan, F. A. (2013). A hybrid technique using multi-objective particle swarm optimization and random forests for PROBE attacks detection in a network. In 2013 IEEE International Conference on Systems, Man, and Cybernetics (pp. 2473-2478). IEEE.

Paniri, M., Dowlatshahi, M. B., & Nezamabadi-Pour, H. (2020). MLACO: A multi-label feature selection algorithm based on ant colony optimization. Knowledge-Based Systems, 192, 105285.

Rostami, M., Forouzandeh, S., Berahmand, K., & Soltani, M. (2020). Integration of multi-objective PSO-based feature selection and node centrality for medical datasets. Genomics, 112(6), 4370-4384.

Rostami, O., & Kaveh, M. (2021). Optimal feature selection for SAR image classification using biogeography-based optimization (BBO), artificial bee colony (ABC) and support vector machine (SVM): a combined approach of optimization and machine learning. Computational Geosciences, 25, 911-930.

Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-8). IEEE.

Shukla, M., Tupsamudre, H., & Lodha, S. (2022). Enterprise Security: Modern Challenges and Emerging Measures. In Research Anthology on Business Aspects of Cybersecurity (pp. 441-470). IGI Global.

Nazir, A., & Khan, R. A. (2021). A novel combinatorial optimization-based feature selection method for network intrusion detection. Computers & Security, 102, 102164.

Li, L. Yang, Y., ShenshenBai, J.C., Xiaoyun, C. (2018). Towards Effective Network Intrusion Detection: A Hybrid Model Integrating Gini Index and GBDT with PSO. Journal of Sensors, 1-10

J. Ren, J. Guo, W. Qian, H. Yuan, X. Hao, H. Jingjing (2019). Building an effective intrusion detection system by using hybrid data optimization based on machine learning algorithms. *Secur Commun Netw*, 2019