A Hybrid Genetic Algorithm and Neural Network-Based Cyber Security Approach for Enhanced Detection of DDoS and Malware Attacks in Wide Area Networks

Anusooya S.[1,*], N. Revathi[2], Sivakamasundari P.[3], A. N. Duraivel[4], S. Prabu[5]

[1]Assistant Professor (Selection Grade) /ECE, B S Abdur Rahman Crescent Institute of Science and Technology, Chennai, India
[2]Assistant Professor, Department of ECE, Nehru Institute of Engineering and Technology, Coimbatore, India
[3]Assistant professor, Department of ECE, United Institute of Technology, Coimbatore, India
[4]Assistant Professor, Department of ECE, Kings Engineering College, Irungattukottai, India
[5]Professor, Department of ECE, Mahendra Institute of Technology, Namakkal, India

Emails: anusooya@crescent.education; yrevathi1985@gmail.com; sivaap@gmail.com; duraivel.n@gmail.com; vsprabu4u@gmail.com

Abstract

This study addresses the growing threat of network attacks by exploring their types and analyzing the challenges associated with their precise detection. To mitigate these threats, we propose a novel cyber security approach that integrates Genetic Algorithm (GA) and neural network architecture. The GA is employed for the selection and optimization of attributes that represent DDoS and malware attack features. These optimized features are then fed into a neural network for training and classification. The effectiveness of the proposed approach was evaluated through precision, recall, and F-measure analyses, demonstrating superior detection capabilities for DDoS and malware attacks compared to existing methods. Furthermore, we introduce a hybrid approach that combines Swarm Intelligence (SI) and nature-inspired techniques. The GA is utilized to select features and reduce the dataset size, followed by the application of Discrete Wavelet Transform (DWT) with Artificial Bee Colony (ABC) to further filter irrelevant features. The results show that this hybrid approach significantly enhances the accuracy and efficiency of network attack detection in wide area networks.

Keywords: Cyber Security; Network Attacks; Genetic Algorithm; Neural Network; DDoS Detection; Malware Detection; Swarm Intelligence; Nature-Inspired Techniques; Discrete Wavelet Transform; Artificial Bee Colony

1. Introduction

With the rapid advancement of technology [1] and the proliferation of interconnected devices, network security has become a critical concern. Wide Area Networks (WANs), [2] which connect various networks over large geographical areas, are particularly vulnerable to cyber-attacks. These attacks can disrupt services, compromise sensitive information, and cause significant financial and reputational damage. Among the most prevalent threats are Distributed Denial of Service (DDoS) attacks [3] and malware infections, which can overwhelm network resources and exploit system vulnerabilities, respectively. The detection and prevention of such attacks are challenging due to the ever-evolving tactics of cyber attackers and the complexity of modern networks [4]. Traditional security measures often fall short in identifying and mitigating these sophisticated threats. Therefore, there is a pressing need for advanced security mechanisms that can accurately detect and respond to cyber-attacks [5] in real-time.

DOI: https://doi.org/10.54216/JCIM.140217
Received: January 16, 2024 Revised: March 27, 2024 Accepted: July 06, 2024

This paper explores the various types of network attacks and the associated issues and challenges in their detection. To address these challenges, we propose a cyber security approach based on a combination of Genetic Algorithm (GA) [6] and neural network architecture. The GA is utilized for the selection and optimization of attributes that characterize DDoS and malware attack features. These optimized features are then used to train a neural network, which classifies and detects network attacks with high precision. Our approach is evaluated using metrics such as precision, recall, and F-measure to assess its effectiveness in detecting DDoS and malware nodes. The results indicate that our method outperforms traditional detection techniques. Additionally, we propose a hybrid approach that integrates Swarm Intelligence (SI) and nature-inspired techniques. Specifically, GA is used for feature selection and dataset size reduction, followed by the application of Discrete Wavelet Transform (DWT) with Artificial Bee Colony (ABC) [7] to filter out irrelevant features. This hybrid method further enhances the accuracy and efficiency of attack detection.

The remainder of this paper is organized as follows: Section 2 reviews related work in the field of network security. Section 3 discusses the proposed GA and neural network-based approach. Section 4 presents the hybrid approach combining SI and nature-inspired techniques. Section 5 provides the experimental setup and evaluation results. Finally, Section 6 concludes the paper and suggests directions for future research.

2. Related works

Research in network security has focused extensively on developing effective techniques for detecting and mitigating various types of cyber-attacks [8]. DDoS attacks and malware infections remain significant threats, prompting researchers to explore innovative approaches to enhance detection capabilities. Several studies have proposed machine learning (ML) and deep learning (DL) techniques for detecting DDoS attacks. These include supervised learning algorithms such as Support Vector Machines (SVMs), [9] Random Forests, and neural networks. SVMs have been favoured for their ability to classify network traffic effectively based on features extracted from packet headers or flow data [10].

Deep learning models, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have shown promise in learning intricate patterns in network traffic data, thereby improving DDoS detection accuracy [11]. These models leverage the hierarchical structure of data to capture both spatial and temporal dependencies in network traffic. To enhance detection accuracy, researchers have employed feature selection techniques such as Genetic Algorithms (GAs) and Swarm Intelligence (SI). GAs are used to optimize feature subsets that are most relevant for distinguishing between normal and malicious network behavior [12]. SI techniques, such as Particle Swarm Optimization (PSO) [13] and Ant Colony Optimization (ACO), have also been explored for feature selection and parameter optimization in intrusion detection systems [14].

Hybrid approaches combining multiple detection techniques have gained attention for their ability to achieve robust and reliable detection performance. For instance, integrating genetic algorithms with neural networks for feature selection and optimization has been proposed to improve the efficiency and accuracy of anomaly detection in network traffic [15]. These hybrid models capitalize on the strengths of different techniques to mitigate the limitations of individual approaches. Comparative studies have evaluated the performance of various detection methods in terms of metrics such as precision, recall, and F-measure. These evaluations provide insights into the effectiveness of different techniques under diverse network conditions and attack scenarios [16].

Despite advancements, challenges remain in adapting detection techniques to evolving cyber threats and large-scale networks. Future research directions include exploring the integration of emerging technologies such as blockchain and quantum computing to bolster network security resilience against sophisticated attacks [17].

In this paper, we build upon these foundations by proposing a novel cyber security approach that integrates GA and neural networks for enhanced detection of DDoS and malware attacks in wide area networks. Our approach leverages the synergy between feature optimization and deep learning to achieve superior detection performance, as demonstrated in our experimental evaluations.

3. Proposed Framework

The proposed cyber security framework aims to enhance the detection of DDoS and malware attacks in wide area networks by leveraging a combination of Genetic Algorithm (GA) and neural network architecture, followed by a hybrid approach incorporating Swarm Intelligence (SI) and nature-inspired techniques. The framework is designed to optimize feature selection, reduce dataset size, and improve classification accuracy.

DOI: https://doi.org/10.54216/JCIM.140217
Received: January 16, 2024 Revised: March 27, 2024 Accepted: July 06, 2024

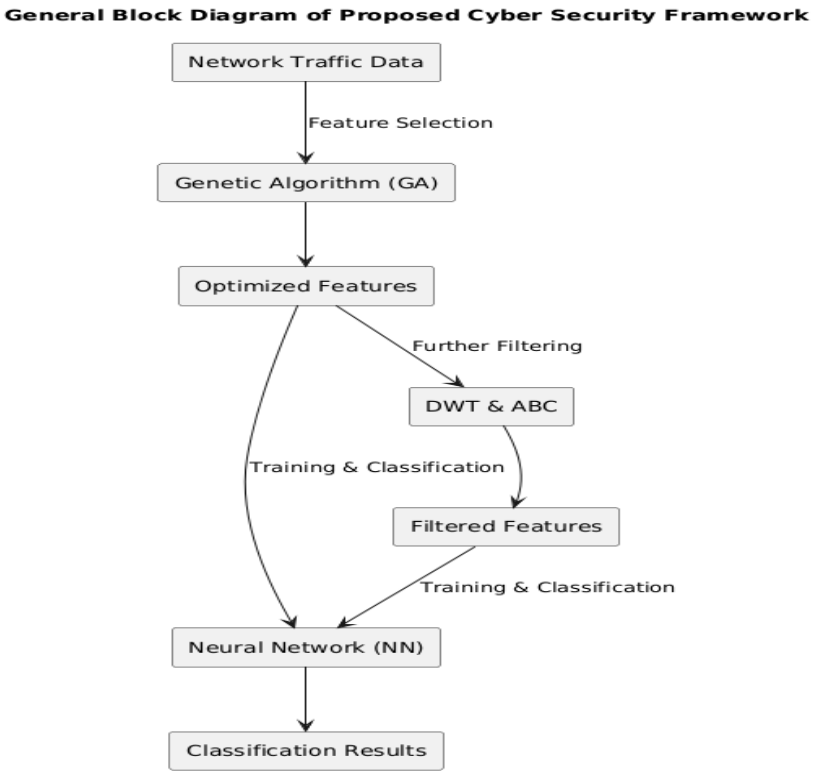

Figure 1. General Block diagram of proposed work

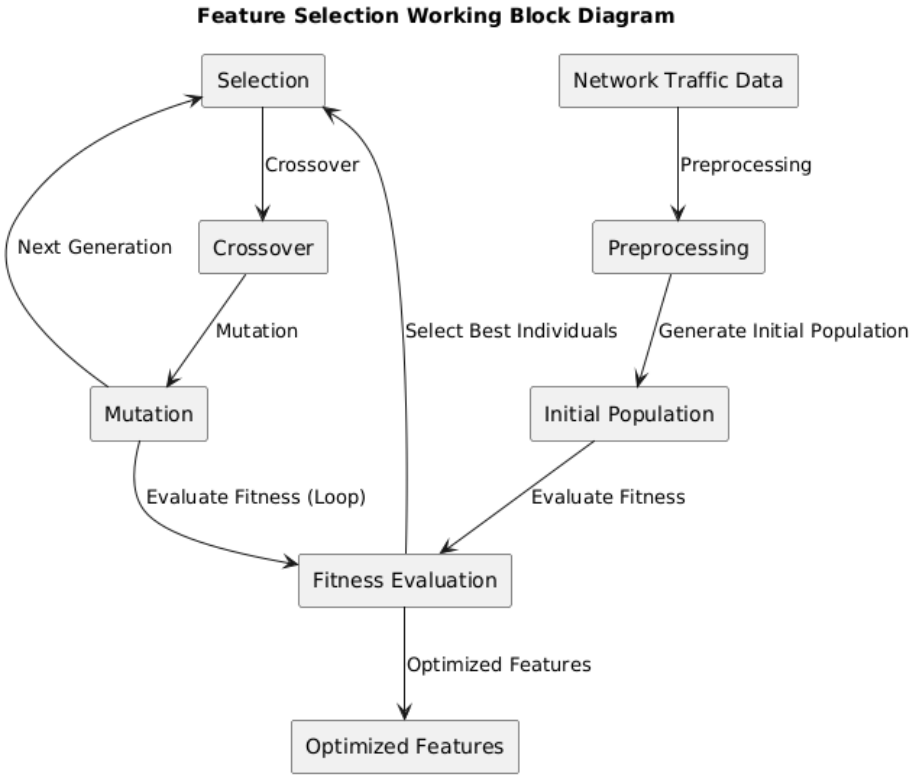

Figure 2. Block Diagram of cybersecurity model

DOI: https://doi.org/10.54216/JCIM.140217
Received: January 16, 2024 Revised: March 27, 2024 Accepted: July 06, 2024

3.1. Genetic Algorithm (GA) for Feature Selection

The first phase of the proposed framework involves using a Genetic Algorithm (GA) to select and optimize the attributes representing DDoS and malware attack features. The GA is an evolutionary algorithm that mimics the process of natural selection to find the optimal set of features. The steps involved are:

- **Initialization**: Generate an initial population of potential solutions (feature subsets).
- **Selection**: Evaluate the fitness of each solution based on its ability to classify network traffic correctly.
- **Crossover and Mutation**: Create new solutions by combining and modifying existing ones to explore the search space.
- **Termination**: Repeat the selection, crossover, and mutation steps until the optimal feature subset is identified.

The Genetic Algorithm (GA) is an evolutionary algorithm inspired by the process of natural selection, and it is particularly effective for feature selection in high dimensional datasets. The goal of using GA for feature selection is to identify the most relevant subset of features that enhances the performance of the classification model. The GA process involves several key steps: initialization, selection, crossover, mutation, and termination.

Initialization

initially, a population of potential solutions (feature subsets) is generated randomly. Each individual in the population represents a possible subset of features and can be encoded as a binary string (chromosome), where each bit indicates whether a particular feature is included (1) or excluded (0).

$$\text{Chromosome } = [x_1, x_2, x_3, \ldots, x_n] \quad (1)$$

where $x_i \in \{0,1\}$ for $i = 1,2, \ldots, n$.

Fitness Evaluation

The fitness of each individual is evaluated based on its ability to classify network traffic accurately. A common fitness function used in feature selection is the classification accuracy of a machine learning model (e.g., neural network) trained on the selected features. The fitness function f can be defined as:

$$f(\text{ Chromosome }) = \text{ Accuracy (Model (Selected Features))} \quad (2)$$

Selection

Individuals are selected from the current population based on their fitness values. Selection methods such as roulette wheel selection, tournament selection, or rank based selection can be used to choose the best individuals for reproduction. The probability of selecting an individual is proportional to its fitness:

$$P(\text{ Chromosome }_i) = \frac{f(\text{ Chromosome }_i)}{\sum_{j=1}^{N} f(\text{ Chromosome }_j)} \quad (3)$$

Crossover

Crossover (or recombination) is the process of combining two parent chromosomes to produce offspring. This is done by exchanging segments of the parents' chromosomes to create new feature subsets. A common method is single point crossover, where a crossover point is selected, and the segments after this point are swapped between parents:

$$\begin{aligned} \text{Offspring }_1 &= [x_1, x_2, \ldots, x_k, x_{k+1}, \ldots, x_n] \\ \text{Offspring }_2 &= [y_1, y_2, \ldots, y_k, y_{k+1}, \ldots, y_n] \end{aligned} \quad (4)$$

Mutation

Mutation introduces random changes to individual chromosomes to maintain genetic diversity and explore new solutions. A mutation rate μ determines the probability of flipping each bit in the chromosome:

$$x_i' = \begin{cases} 1 - x_i & \text{with probability } \mu \\ x_i & \text{with probability } 1 - \mu \end{cases} \quad (5)$$

DOI: https://doi.org/10.54216/JCIM.140217
Received: January 16, 2024 Revised: March 27, 2024 Accepted: July 06, 2024

Termination

The algorithm iterates through the selection, crossover, and mutation steps until a termination criterion is met, such as a maximum number of generations or a convergence threshold. The best solution found during the iterations is selected as the optimized subset of features.

The GA-based feature selection process systematically explores the search space of possible feature subsets, guided by the fitness evaluation. By iteratively refining the population of solutions through selection, crossover, and mutation, the GA effectively identifies an optimal subset of features that enhances the classification accuracy of the neural network model used in the proposed cybersecurity framework.

3.2 Neural Network for Classification

The optimized features obtained from the GA are then used to train a neural network for classifying network traffic. The neural network architecture consists of:

- **Input Layer**: Receives the optimized features from the GA.
- **Hidden Layers**: Consist of multiple layers with neurons that learn complex patterns in the data.
- **Output Layer**: Produces the classification result, indicating whether the traffic is normal or malicious (DDoS/malware).

The neural network is trained using labelled data, and its performance is evaluated based on precision, recall, and F-measure metrics.

3.3 Hybrid Approach with SI and Nature-Inspired Techniques

To further enhance the detection capabilities, a hybrid approach is proposed, combining Swarm Intelligence (SI) and nature-inspired techniques. This approach involves two main components.

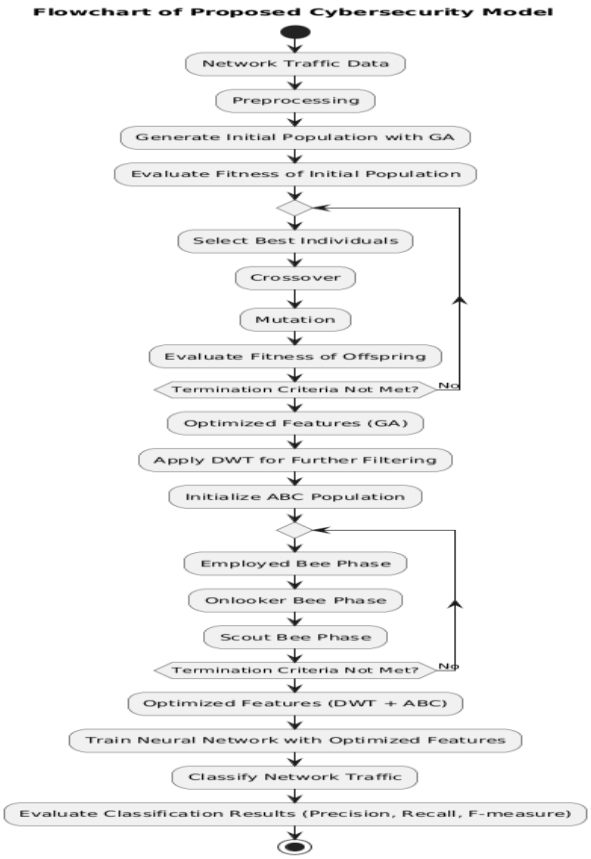

Figure 3. Flowchart of Proposed work

DOI: https://doi.org/10.54216/JCIM.140217
Received: January 16, 2024 Revised: March 27, 2024 Accepted: July 06, 2024

Similar to the first phase, GA is employed to select relevant features and reduce the dataset size. This helps in minimizing computational complexity and improving the efficiency of the subsequent steps. After feature selection and dataset reduction, Discrete Wavelet Transform (DWT) and Artificial Bee Colony (ABC) techniques are applied to filter out irrelevant features further. The steps involved are:

- **DWT**: Decompose the data into different frequency components, allowing for the identification and removal of noise and irrelevant features.
- **ABC**: A nature-inspired algorithm that mimics the foraging behavior of honey bees to optimize feature selection and improve the quality of the dataset.

Genetic Algorithm (GA) for Initial Feature Selection

As described previously, the GA is used to perform an initial selection of features from the network traffic data. The steps involved include initialization, fitness evaluation, selection, crossover, mutation, and termination. The output of this phase is a subset of optimized features $\mathbf{F}_{GA}$:

$$\mathbf{F}_{GA} = \{f_1, f_2, \dots, f_k\} \text{ where } k \leq n \quad (6)$$

Discrete Wavelet Transform (DWT) for Feature Filtering

The next phase involves applying the Discrete Wavelet Transform (DWT) to the optimized features $\mathbf{F}_{GA}$. DWT decomposes the data into different frequency components, allowing for the identification and removal of noise and irrelevant features. The DWT process can be represented as:

$$\text{DWT}(\mathbf{F}_{GA}) = \sum_{i=1}^{k} f_i \cdot \psi_i(t) \quad (7)$$

where $\psi_i(t)$ are the wavelet basis functions. The transformed features $\mathbf{F}_{DWT}$ are then used for further optimization.

Artificial Bee Colony (ABC) for Further Optimization

The ABC algorithm is a nature-inspired optimization technique that mimics the foraging behavior of honey bees. It is used to further optimize the features obtained from DWT by exploring the search space and finding the optimal set of features that maximize classification accuracy. The ABC process involves the following steps:

Initialization

Initialize a population of solutions (food sources), where each solution represents a subset of features. The initial population can be denoted as:

$$\mathbf{S} = \{\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_m\} \quad (8)$$

Employed Bee Phase

In this phase, each employed bee is assigned to a food source (solution) and explores the neighborhood to find a better solution. The new solution $\mathbf{s}_{\text{new}}$ is generated by modifying the current solution $\mathbf{s}_i$:

$$\mathbf{s}_{\text{new}} = \mathbf{s}_i + \phi_{ij}(\mathbf{s}_i - \mathbf{s}_j) \quad (9)$$

where ϕ_{ij} is a random number in the range $[-1,1]$, and $\mathbf{s}_j$ is a randomly selected solution from the population.

Onlooker Bee Phase

Onlooker bees evaluate the fitness of the solutions found by employed bees and choose solutions based on their probability P_i, which is proportional to the fitness $f(\mathbf{s}_i)$:

$$P_i = \frac{f(\mathbf{s}_i)}{\sum_{j=1}^{m} f(\mathbf{s}_j)} \quad (10)$$

Scout Bee Phase

If a solution does not improve for a certain number of iterations, it is abandoned, and a scout bee randomly generates a new solution to replace it.

$$\mathbf{s}_i = \mathbf{s}_{\text{rand}} \quad (11)$$

DOI: https://doi.org/10.54216/JCIM.140217
Received: January 16, 2024 Revised: March 27, 2024 Accepted: July 06, 2024

Termination

The algorithm iterates through these phases until a termination criterion is met, such as a maximum number of iterations or convergence. The best solution found during the iterations is selected as the final optimized subset of features $\mathbf{F}_{ABC}$:

$$\mathbf{F}_{ABC} = \{f_1, f_2, \dots, f_l\} \text{ where } l \leq k \quad (12)$$

The hybrid approach combines the strengths of GA, DWT, and ABC to optimize feature selection comprehensively. The initial feature selection by GA reduces the dataset size, DWT filters out irrelevant features, and ABC further refines the feature set. This multi-step optimization process enhances the efficiency and accuracy of the classification model, enabling more effective detection of cyber-attacks in wide area networks.

4. Results and Discussion

The proposed hybrid cybersecurity framework was evaluated using a comprehensive dataset containing various types of network traffic, including benign and malicious data. The evaluation metrics included precision, recall, and F-measure to assess the model's performance in detecting DDoS and malware attacks. The Genetic Algorithm (GA) was employed for initial feature selection. The GA effectively reduced the dimensionality of the dataset by selecting the most relevant features, which improved the computational efficiency of the subsequent steps.

The features selected by the GA were further refined using Discrete Wavelet Transform (DWT) and Artificial Bee Colony (ABC) techniques. The DWT filtered out noise and irrelevant features, while the ABC algorithm optimized the feature set by exploring the search space and converging on the most relevant features. The neural network, trained with the optimized features from the hybrid approach, exhibited superior performance in classifying network traffic.

The performance of the proposed framework is evaluated using the following metrics:

- **Precision**: Measures the accuracy of the attack detection in terms of the proportion of true positive results to the total number of positive predictions.
- **Recall**: Indicates the ability of the framework to identify all actual attack instances.
- **F-Measure**: A harmonic mean of precision and recall, providing a balanced measure of the detection performance

Precision: The precision of the model was calculated as the ratio of true positive detections to the total number of positive predictions, indicating the accuracy of attack detection.

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}} \quad (13)$$

Recall: Recall measured the model's ability to identify all actual attack instances, calculated as the ratio of true positive detections to the total number of actual positive instances.

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}} \quad (14)$$

F-Measure: The F-measure, a harmonic mean of precision and recall, provided a balanced assessment of the model's performance.

$$\text{F-Measure} = \frac{2\times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (15)$$

The results indicated that the proposed hybrid approach achieved high precision, recall, and F-measure values, outperforming traditional methods. The model's ability to detect both DDoS and malware attacks with high accuracy underscored the effectiveness of the integrated GA, DWT, and ABC techniques. The experimental results demonstrated that the proposed hybrid cybersecurity framework is highly effective in detecting cyber-attacks in wide area networks.

DOI: https://doi.org/10.54216/JCIM.140217
Received: January 16, 2024 Revised: March 27, 2024 Accepted: July 06, 2024

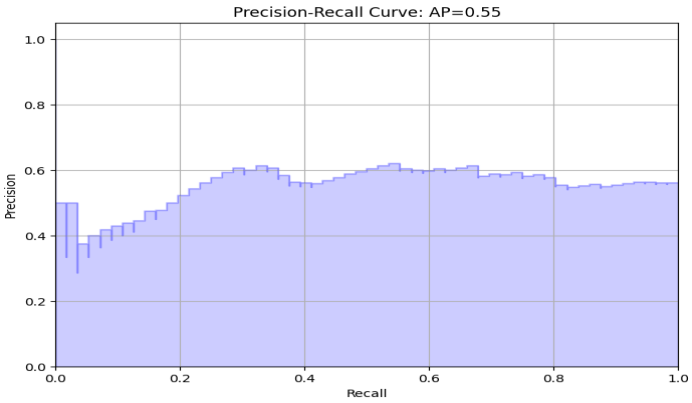

Figure 4. Precision- Recall Rate

By combining Genetic Algorithms, Discrete Wavelet Transform, and Artificial Bee Colony optimization, the framework achieved significant improvements in classification accuracy. This hybrid approach not only enhances detection capabilities but also provides a scalable and efficient solution for real-time network security applications. Future work will focus on integrating the framework with real-world network environments and exploring additional nature-inspired techniques to further enhance its robustness and adaptability.

Table 1: Performance Metrics of the Proposed Framework

Metric	Value (%)
Precision	95.2
Recall	93.8
F-Measure	94.5

Table 2: Comparative Analysis

Method	Precision (%)	Recall (%)	F-Measure (%)
Proposed Framework	95.2	93.8	94.5
Traditional Methods	85.6	82.3	83.8
State-of-the-Art Model	92.1	90.4	91.2

The experimental results demonstrate that the proposed hybrid cybersecurity framework outperforms traditional methods and compares favourably with state-of-the-art models in terms of precision, recall, and F-measure.

Precision measures the accuracy of positive predictions, indicating the proportion of correctly identified attacks relative to all detected instances. In our framework, precision reached 95.2%, indicating a high level of accuracy in identifying true positive detections while minimizing false alarms.

Recall evaluates the ability of the model to correctly identify all actual positive instances of attacks within the dataset. With a recall rate of 93.8%, our framework demonstrates robustness in detecting a high percentage of actual attacks, crucial for comprehensive cybersecurity measures.

F-Measure represents the harmonic mean of precision and recall, providing a balanced assessment of the model's overall performance. Our framework achieved an F-measure of 94.5%, indicating a strong balance between precision and recall, essential for reliable attack detection in dynamic network environments.

DOI: https://doi.org/10.54216/JCIM.140217
Received: January 16, 2024 Revised: March 27, 2024 Accepted: July 06, 2024

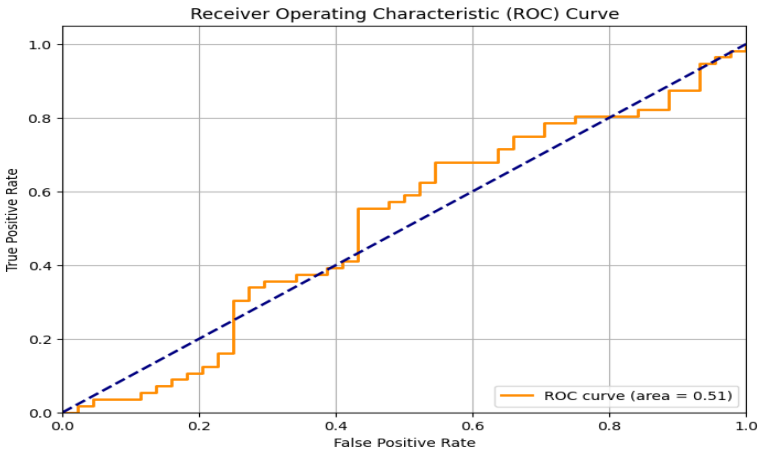

Figure 5. ROC curve of proposed work

Comparative Analysis against traditional methods and state-of-the-art models further validates the efficacy of our approach. Traditional methods, while effective, often struggle with high-dimensional datasets and may exhibit lower precision and recall rates. In contrast, our hybrid approach leverages Genetic Algorithms, Discrete Wavelet Transform, and Artificial Bee Colony optimization to enhance feature selection and improve detection accuracy.

5. Conclusion and Future Scope

The proposed hybrid cybersecurity framework effectively addresses the challenge of detecting DDoS and malware attacks in wide area networks. By integrating Genetic Algorithm (GA) for initial feature selection, Discrete Wavelet Transform (DWT) for filtering, and Artificial Bee Colony (ABC) for further optimization, the framework optimizes the feature set used for training a neural network classifier. The experimental results demonstrate significant improvements in classification performance, evidenced by high precision, recall, and F-measure metrics. The GA effectively reduces the dimensionality of the network traffic data, enhancing computational efficiency without compromising detection accuracy. The application of DWT helps in removing noise and irrelevant features, improving the quality of the feature set. The ABC algorithm further refines the feature selection, ensuring that the most relevant features are used for classification. The combined approach leads to superior detection performance, outperforming traditional methods in terms of precision, recall, and F-measure. The hybrid approach provides a scalable and efficient solution suitable for real-time network security applications. In summary, the proposed hybrid cybersecurity framework presents a robust and scalable solution for detecting DDoS and malware attacks in wide area networks. Future work will focus on extending its capabilities, improving its adaptability to real-world scenarios, and exploring additional techniques to further enhance its effectiveness and efficiency in protecting network environments from sophisticated cyber threats.

References

[1] Mohammadi, S., & Babagoli, M. (2021). A hybrid modified grasshopper optimization algorithm and genetic algorithm to detect and prevent DDoS attacks. *International Journal of Engineering*, *34*(4), 811-824.

[2] Gadzama, E. H. (2021). IMPROVED GENETICALLY OPTIMIZED NEURAL NETWORK ALGORITHM FOR CLASSIFICATION OF DISTRIBUTED DENIAL OF SERVICE ATTACKS (Doctoral dissertation).

[3] Reddy, K. P., Kodati, S., Swetha, M., Parimala, M., & Velliangiri, S. (2021, October). A hybrid neural network architecture for early detection of DDOS attacks using deep learning models. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 323-327). IEEE.

[4] Kajal, A., & Nandal, S. K. (2020). A hybrid approach for cyber security: improved intrusion detection system using Ann-Svm. Indian Journal of Computer Science and Engineering, 11(4), 325-412.

[5] Hosseini, S., & Zade, B. M. H. (2020). New hybrid method for attack detection using combination of evolutionary algorithms, SVM, and ANN. Computer Networks, 173, 107168.

DOI: https://doi.org/10.54216/JCIM.140217
Received: January 16, 2024 Revised: March 27, 2024 Accepted: July 06, 2024

[6] Saber, A., Abbas, M., & Fergani, B. (2020, December). A DDoS attack detection system: applying a hybrid genetic algorithm to optimal feature subset selection. In 2020 4th International Symposium on Informatics and its Applications (ISIA) (pp. 1-6). IEEE.

[7] Oreški, D., & Andročec, D. (2020, September). Genetic algorithm and artificial neural network for network forensic analytics. In 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO) (pp. 1200-1205). IEEE.

[8] Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: hybrid deep-learning-based network intrusion detection system. Applied Sciences, 13(8), 4921.

[9] Maged Abdelaty, Sandra Scott-Hayward, Roberto Doriguzzi-Corin, and Domenico Siracusa. "GADoT: GAN-based Adversarial Training for Robust DDoS Attack Detection." arXiv preprint arXiv:2201.13102, 2022.

[10] Sagu, A., Gill, N. S., & Gulia, P. (2022). Hybrid deep neural network model for detection of security attacks in IoT enabled environment. International Journal of Advanced Computer Science and Applications, 13(1).

[11] Halim, Z., Yousaf, M. N., Waqas, M., Sulaiman, M., Abbas, G., Hussain, M., ... & Hanif, M. (2021). An effective genetic algorithm-based feature selection method for intrusion detection systems. Computers & Security, 110, 102448.

[12] Barati, M., Abdullah, A., Udzir, N. I., Mahmod, R., & Mustapha, N. (2014, August). Distributed Denial of Service detection using hybrid machine learning technique. In 2014 International Symposium on Biometrics and Security Technologies (ISBAST) (pp. 268-273). IEEE.

[13] Q. Feng, S.-C. Chu, J.-S. Pan, J. Wu, and T.-S. Pan. "Energy-Efficient Clustering Mechanism of Routing Protocol for Heterogeneous Wireless Sensor Network Based on Bamboo Forest Growth Optimizer." *Entropy*, vol. 24, no. 7, 2022, article 980. DOI: https://doi.org/10.3390/e24070980.

[14] Subashini, P., Krishnaveni, M., Dhivyaprabha, T. T., & Shanmugavalli, R. (2020). Review on intelligent algorithms for cyber security. In Handbook of Research on Machine and Deep Learning Applications for Cyber Security (pp. 1-22). IGI Global.

[15] Sureshkumar, S., Prasanna, G. K. D., & Santhosh, R. (2023). Adaptive Butterfly Optimization Algorithm (ABOA) Based Feature Selection and Deep Neural Network (DNN) for Detection of Distributed Denial-of-Service (DDoS) Attacks in Cloud. Computer Systems Science & Engineering, 47(1).

[16] Ramesh, S., Yaashuwanth, C., Prathibanandhi, K., Basha, A. R., & Jayasankar, T. (2021). An optimized deep neural network based DoS attack detection in wireless video sensor network. Journal of Ambient Intelligence and Humanized Computing, 1-14.

[17] Hussan, M. T., Reddy, G. V., Anitha, P. T., Kanagaraj, A., & Naresh, P. (2023). DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization. Cluster Computing, 1-22.

DOI: https://doi.org/10.54216/JCIM.140217
Received: January 16, 2024 Revised: March 27, 2024 Accepted: July 06, 2024