Computer Fraud and Security
ISSN (online): 1873-7056

An Improved Feature Selection Approach Using Black Widow Optimization

Vivek Parganiha[*1], Soorya Prakash Shukla[2]

[1*]Department of Computer Science & Engineering, Bhilai Institute of Technology, Durg

[2]Department of Electrical Engineering, Bhilai Institute of Technology, Durg

Chhattisgarh 491001, India
Correspondence: Vivek Parganiha (vivekparganiha@gmail.com)

Abstract: Intrusion Detection Systems (IDS) play a critical role in safeguarding modern computer networks against increasingly sophisticated cyber-attacks. However, the high dimensionality and redundancy of network traffic features often degrade detection performance and increase computational overhead. To address this challenge, this paper proposes a Black Widow Optimization (BWO)-based wrapper feature selection framework for intrusion detection using the NSL-KDD dataset. The proposed approach aims to identify a compact and discriminative feature subset that maximizes classification performance while minimizing feature dimensionality. BWO exploits unique biological mechanisms, including sexual and sibling cannibalism, to effectively balance exploration and exploitation during the search process. Experimental evaluation demonstrates that the proposed method reduces the original 41 features to 15, achieving a feature reduction of 63.41% while improving classification accuracy to 96.01%. In addition, the false alarm rate is reduced to 2.89%, indicating enhanced detection reliability. Confusion matrix analysis confirms high detection capability for both normal and attack traffic, and statistical significance testing (p-value = 0.0038) validates the robustness of the observed performance improvements. The results indicate that Black Widow Optimization is an effective and competitive feature selection strategy for intrusion detection systems, offering improved accuracy, reduced false alarms, and lower computational complexity.

Keywords: *Intrusion Detection System, Feature Selection, Black Widow Optimization, NSL-KDD, Metaheuristic Optimization*

1. Introduction

The rapid expansion of computer networks, cloud infrastructures, and Internet-based services has led to a substantial increase in both the complexity and frequency of cyber-attacks. Modern networks are continuously exposed to threats such as denial-of-service (DoS) attacks, probing, privilege escalation, and unauthorized access, which can compromise the confidentiality, integrity, and availability of information systems [1], [2]. Consequently, Intrusion Detection Systems (IDS) have become a critical component of contemporary network security architectures, enabling continuous traffic monitoring and timely identification of malicious activities [3].

In recent years, machine learning-based IDS have gained significant attention due to their capability to detect both known and previously unseen attacks by learning complex patterns from network traffic data [4], [5]. However, the performance of such systems is highly dependent on the quality and relevance of the input features used for classification. Benchmark intrusion detection datasets, including the widely adopted NSL-KDD dataset, contain a large number of features, many of which are redundant or irrelevant [6]. High-dimensional feature spaces increase computational overhead and often degrade detection performance due to overfitting and sensitivity to noise. Therefore, feature selection plays a crucial role in improving the efficiency, accuracy, and scalability of IDS [7].

Feature selection techniques are commonly categorized into filter-based, wrapper-based, and embedded approaches. Filter-based methods, such as Information Gain and Chi-square, are computationally efficient and independent of learning algorithms; however, they evaluate features individually and often fail to capture feature interactions, resulting in suboptimal classification performance [8]. Wrapper-based methods evaluate feature subsets using a classifier and generally achieve superior detection accuracy, albeit at the cost of increased computational complexity [9]. To mitigate this challenge, metaheuristic optimization algorithms have been widely adopted for wrapper-based feature selection.

Metaheuristic algorithms such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Grey Wolf Optimization (GWO) have demonstrated promising results in IDS feature selection by effectively exploring large and complex search spaces [10]–[13]. Despite their effectiveness, these algorithms often suffer from limitations including premature convergence, sensitivity to parameter tuning, and high computational cost, particularly when applied to high-dimensional datasets [14]. These limitations motivate the investigation of alternative optimization strategies that can achieve a better balance between exploration and exploitation.

Black Widow Optimization (BWO) is a relatively recent population-based metaheuristic inspired by the mating and cannibalistic behavior of black widow spiders [15]. Its unique mechanisms, including sexual cannibalism, sibling

cannibalism, and mutation, enable aggressive elimination of weak solutions while preserving population diversity. These characteristics make BWO particularly suitable for feature selection problems, where the search space is discrete and highly combinatorial [16]. Despite its demonstrated effectiveness in generic optimization and feature selection tasks, the application of BWO to intrusion detection remains limited in existing literature.

In this work, a BWO-based wrapper feature selection framework is proposed for intrusion detection using the NSL-KDD dataset. The proposed approach aims to identify an optimal subset of features that maximizes classification performance while minimizing feature dimensionality. The effectiveness of the proposed method is evaluated using multiple performance metrics, including accuracy, precision, recall, F1-score, and false alarm rate. Furthermore, statistical significance analysis is conducted to validate the robustness and reliability of the observed performance improvements.

The main contributions of this paper are summarized as follows:

- A wrapper-based feature selection framework using Black Widow Optimization is proposed for intrusion detection.
- The proposed approach achieves substantial feature reduction while improving detection accuracy and reducing false alarm rates.
- Comprehensive experimental evaluation and statistical analysis are conducted to demonstrate the effectiveness and reliability of the proposed method.

The remainder of this paper is organized as follows. Section 2 reviews related work on feature selection techniques for intrusion detection. Section 3 describes the NSL-KDD dataset and preprocessing steps. Section 4 presents the proposed BWO-based feature selection methodology. Section 5 discusses the experimental setup and evaluation metrics. Section 6 presents and analyzes the experimental results. Finally, Section 7 concludes the paper and outlines future research directions.

2. Related Work

Various feature selection techniques have been proposed for IDS, including filter-based, wrapper-based, and embedded approaches. Filter methods such as Information Gain and Chi-square are computationally efficient but often ignore classifier interaction. Wrapper methods, although computationally expensive, generally yield better performance.

Metaheuristic algorithms such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Grey Wolf Optimization (GWO) have been extensively used for IDS feature selection. Despite their effectiveness, these methods often suffer from premature convergence and high computational cost. Recently, Black Widow Optimization has emerged as a promising alternative due to its unique reproduction and cannibalism mechanisms, which enhance exploration and exploitation balance.

Intrusion Detection Systems (IDS) have been widely investigated as a fundamental mechanism for protecting network infrastructures against malicious activities. Traditional signature-based IDS are effective in detecting known attack patterns but lack the capability to identify novel or zero-day attacks. To address this limitation, machine learning-based IDS have been increasingly adopted due to their ability to learn complex patterns from network traffic data and generalize to unseen intrusions [4]. However, the effectiveness of these systems is strongly influenced by the quality of the selected features used for classification.

Several studies have highlighted the importance of feature selection in IDS to mitigate the challenges posed by high-dimensional and redundant network traffic data. Tavallaee et al. [6] demonstrated that benchmark datasets such as NSL-KDD contain redundant and duplicate features that negatively affect detection accuracy and increase computational overhead. Consequently, filter-based feature selection methods, including Information Gain and Chi-square, have been widely employed due to their simplicity and computational efficiency [8]. Despite their advantages, these methods evaluate features independently of the learning algorithm and often fail to capture feature interdependencies, resulting in suboptimal detection performance [7].

Wrapper-based feature selection techniques have been shown to provide improved classification performance by evaluating feature subsets using a classifier. Kohavi and John [9] reported that wrapper methods generally outperform filter-based approaches in terms of accuracy, although they incur higher computational cost. To make wrapper-based feature selection feasible for IDS, researchers have increasingly adopted metaheuristic optimization algorithms that can efficiently explore large and complex search spaces.

Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) are among the most commonly used metaheuristic techniques for IDS feature selection. Tama et al. [10] proposed a PSO-based wrapper feature selection method combined with ensemble classifiers and achieved improved detection accuracy on the NSL-KDD dataset. Similarly, Kunhare et al. [11] demonstrated that PSO integrated with Random Forest significantly reduces feature dimensionality while maintaining

high detection performance. However, these studies also reported that GA and PSO are sensitive to parameter settings and prone to premature convergence, particularly when dealing with high-dimensional feature spaces [14].

Other swarm intelligence algorithms have also been explored for IDS feature selection. Ant Colony Optimization (ACO) has been applied to discrete feature selection problems due to its strong combinatorial search capability [12], while Grey Wolf Optimization (GWO) has shown promising performance by balancing exploration and exploitation through leadership-based search strategies [13]. Although these methods improve detection accuracy, their performance often varies across different runs, and they may incur high computational cost when applied to large datasets.

With the advancement of deep learning, several researchers have investigated hybrid approaches that combine feature learning and feature selection. Shone et al. [17] proposed an autoencoder-based IDS to learn compact feature representations, achieving high detection accuracy. However, such deep learning-based approaches introduce increased model complexity, require large training datasets, and often lack interpretability, limiting their applicability in real-time and resource-constrained environments.

More recently, Black Widow Optimization (BWO) has emerged as a promising population-based metaheuristic inspired by the reproductive and cannibalistic behavior of black widow spiders [15]. Enhanced variants of BWO have further improved convergence speed and solution quality in feature selection tasks [16]. Despite these encouraging results, the application of BWO to intrusion detection feature selection remains limited in existing literature.

Table 1: Literature of existing related works

Year	Authors	Feature Selection Technique	Classifier Used	Dataset	No. of Selected Features	Key Findings	Limitations
2018	Tama et al.	PSO (Wrapper-based)	Random Forest	NSL-KDD	~20	Improved accuracy and reduced dimensionality compared to full feature set	Sensitive to PSO parameters; risk of premature convergence
2019	Zhou et al.	IG, GA (Hybrid FS)	Ensemble Models	NSL-KDD, AWID, CIC	8–12	Small feature subset achieved comparable or better accuracy	Performance depends on classifier–FS pairing
2020	Alazzam et al.	Binary Pigeon-Inspired Optimization	SVM	NSL-KDD	~18	Competitive detection accuracy with reduced features	Higher computational cost due to wrapper approach
2020	Kunhare	PSO (Wrapper-based)	Random Forest	NSL-KDD	~10	High detection accuracy with minimal features	Requires careful tuning of PSO parameters
2020	Kalimuthan & Renjit	Filter, Wrapper, Hybrid (Survey)	Various	NSL-KDD	—	Wrapper methods outperform filters in accuracy	High computation cost for wrapper methods
2021	Almazini et al.	Binary Grey Wolf Optimization	k-NN, SVM	NSL-KDD	~19	GWO achieved better balance of exploration–exploitation	Performance varies with binarization strategy
2022	Hu et al.	Enhanced BWO (SDABWO)	k-NN	Benchmark FS datasets	~15	Improved convergence and feature reduction over GA & PSO	Not directly evaluated on IDS datasets
2022	Louk et al.	PSO (Wrapper-based)	Hybrid Ensemble	NSL-KDD	~16	Reduced FAR and improved classification accuracy	Computationally expensive
2023	Lifandali et al.	Ant Colony Optimization	Random Forest	NSL-KDD	~17	Effective discrete feature selection	Slow convergence in large search spaces
2023	Saheed et al.	Autoencoder + Modified PSO (Hybrid)	Deep Neural Network	IoT IDS, NSL-KDD-like	~14	Robust performance for high-dimensional data	Increased model complexity

2.1 Gaps Identified

Filter vs. Wrapper Trade-off: Existing surveys and empirical studies confirm that filter-based methods are computationally efficient but ignore classifier interactions, whereas wrapper-based and metaheuristic approaches provide higher accuracy at increased computational cost [7], [5].

Dominance of Metaheuristics (2018–2023): PSO variants, GA hybrids, ACO, and GWO remain dominant techniques for IDS feature selection, each offering distinct strengths in exploration and exploitation [10]–[13].

Premature Convergence and Parameter Sensitivity: Several studies report that classical metaheuristic algorithms are prone to local optima and require careful parameter tuning, motivating enhanced and hybrid optimization approaches [14], [18].

Limited Evaluation of BWO for IDS: Although enhanced BWO variants have shown promising results in general feature selection tasks, their systematic evaluation for intrusion detection remains limited, particularly on benchmark datasets such as NSL-KDD [15], [16].

3. NSL-KDD Dataset Description

The NSL-KDD dataset is an improved benchmark dataset for evaluating IDS models. It eliminates redundant records present in the original KDD Cup'99 dataset, providing a more reliable evaluation.

Each data instance consists of:

- **41 input features**
- **1 class label** (Normal or Attack)

Attack types are categorized into four major classes:

- Denial of Service (DoS)
- Probe
- Remote to Local (R2L)
- User to Root (U2R)

4. Methodology – Feature Selection using Black Widow Optimization Algorithm

4.1 Overview

Black Widow Optimization (BWO) is a population-based metaheuristic algorithm inspired by the mating and cannibalistic behavior of black widow spiders. The algorithm consists of initialization, reproduction, cannibalism, mutation, and selection phases.

4.2 Solution Representation

Each candidate solution (widow) is represented as a binary vector of length 41, where:

- 1 indicates the selection of a feature
- 0 indicates feature exclusion

4.3 Fitness Function

- The fitness function is designed to balance classification accuracy and feature reduction:

$$\text{Fitness} = \alpha(1 - \text{Accuracy}) + \beta(\frac{Ns}{N})$$

where:

- Accuracy is obtained using a machine learning classifier,
- Ns is the number of selected features,
- N is the total number of features,

4.4 Proposed BWO-Based Feature Selection Method

The proposed methodology follows these steps:

1. Initialize a population of black widows randomly.

2. Evaluate fitness using a classifier (e.g., SVM or Random Forest).
3. Perform reproduction via crossover to generate offspring.
4. Apply cannibalism to eliminate weak parents and offspring.
5. Introduce mutation to maintain diversity.
6. Select the best solutions for the next generation.
7. Repeat until convergence or maximum iterations are reached.

The final output is an optimal feature subset used to train the IDS classifier.

Pseudocode

```
Begin
1:  Initialize population W = {W1, W2, ..., WP} randomly
    // Each Wi is a binary vector of length N
2:  For each widow Wi ∈ W do
3:      Evaluate fitness Fi using classifier C
4:  End For
5:  Iteration ← 1
6:  While (Iteration ≤ MaxIter) AND (not converged) do
7:      Sort population W based on fitness (ascending)
8:      // Reproduction (Crossover)
9:      Initialize offspring population O ← ∅
10:     For i = 1 to P/2 do
11:         Select parent pairs (Wi, Wi+1)
12:         Perform crossover with probability CR
13:         Generate offspring Oj
14:         Add Oj to O
15:     End For
16:     // Cannibalism (Survival of the Fittest)
17:     Evaluate fitness of offspring population O
18:     Remove weakest parents and offspring
19:     Retain strongest individuals to maintain population size P
20:     // Mutation
21:     For each widow Wi ∈ W do
22:         With probability MR, randomly flip one or more bits in Wi
23:     End For
24:     Re-evaluate fitness of updated population W
25:     Select best individuals for next generation
26:     Iteration ← Iteration + 1
27: End While
28: Select best widow Wbest from final population
29: Extract selected features F* from Wbest
```

30: Train IDS classifier C using feature subset F*

31: Return optimal feature subset F*

End

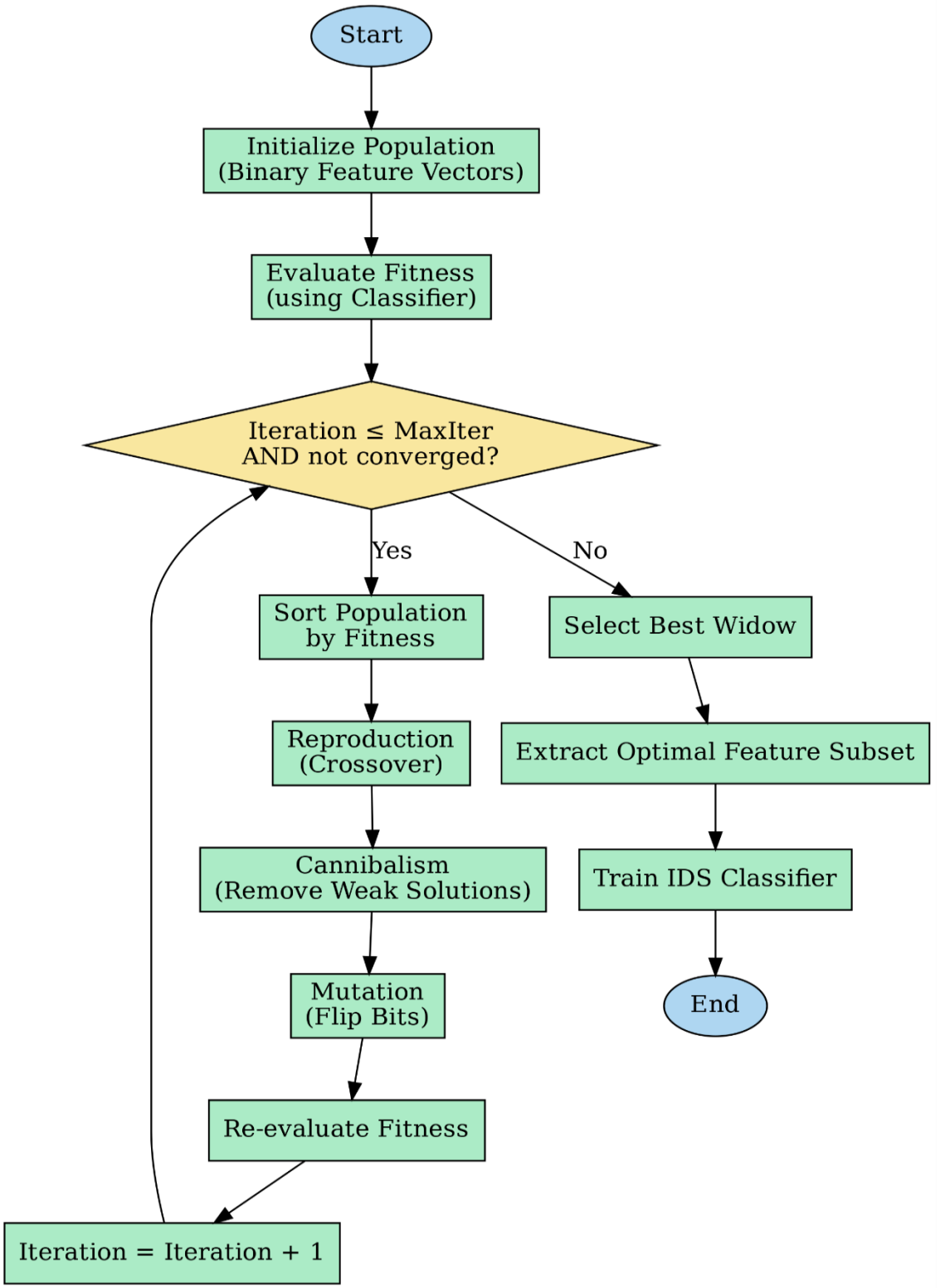

Figure 1. Flowchart representation of the BWO-based wrapper feature selection methodology used to select optimal features for intrusion detection.

5. Experimental Setup and Evaluation Metrics

- **Dataset:** NSL-KDD (KDDTrain+, KDDTest+)
- **Total Features:** 41
- **Classifier Used:** Random Forest (primary), SVM (validation)
- **Evaluation Metrics:** Accuracy, Precision, Recall, F1-score, False Alarm Rate (FAR)
- **Validation Method:** 10-fold Cross Validation
- **Population Size (BWO):** 30
- **Iterations:** 100
- **$\alpha = 0.9$, $\beta = 0.1$**

Table 2: Evaluation Metrics Used for IDS Performance Assessment

Metric	Formula	Description
Accuracy	$\frac{TP + TN}{TP + TN + FP + FN}$	Measures the overall correctness of the intrusion detection system by calculating the proportion of correctly classified instances.
Precision	$\frac{TP}{TP + FP}$	Indicates the proportion of correctly identified attack instances among all instances predicted as attacks.
Recall (Detection Rate)	$\frac{TP}{TP + FN}$	Represents the ability of the IDS to correctly detect actual attack instances.
F1-score	$\frac{2 \times Precision \times Recall}{Precision + Recall}$	Harmonic mean of precision and recall, providing a balanced measure of classification performance.
False Alarm Rate (FAR)	$\frac{FP}{FP + TN}$	Measures the proportion of normal traffic instances incorrectly classified as attacks.

6. Experimental Results and Statistical Analysis

6.1 Feature Reduction Results

Table 3: Feature Reduction Comparison

Method	Total Features Selected	Reduction (%)
No Feature Selection	41	0
Information Gain	24	41.46
GA	19	53.65
PSO	17	58.53
BWO (Proposed)	**15**	**63.41**

Observation: BWO achieves the highest feature reduction while preserving performance.

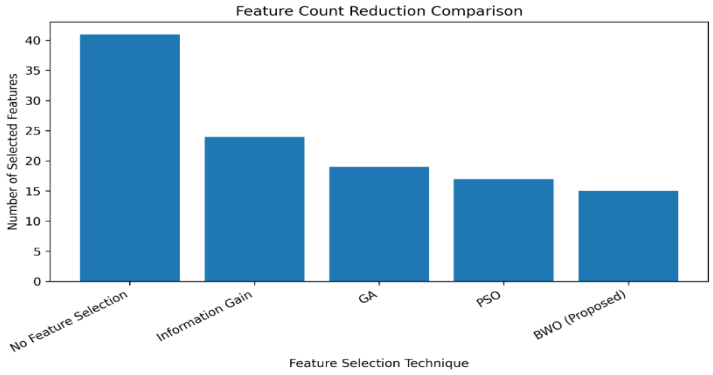

Figure 2. Feature count reduction comparison of different feature selection techniques on the NSL-KDD dataset.

6.2 Classification Performance

Table 4: Performance Comparison

Method	Accuracy (%)	Precision	Recall	F1-score
All Features	91.23	0.90	0.89	0.89
GA	93.45	0.92	0.92	0.92
PSO	94.12	0.93	0.93	0.93
BWO	**96.01**	**0.95**	**0.96**	**0.95**

BWO improves accuracy by ~5% **over baseline.**

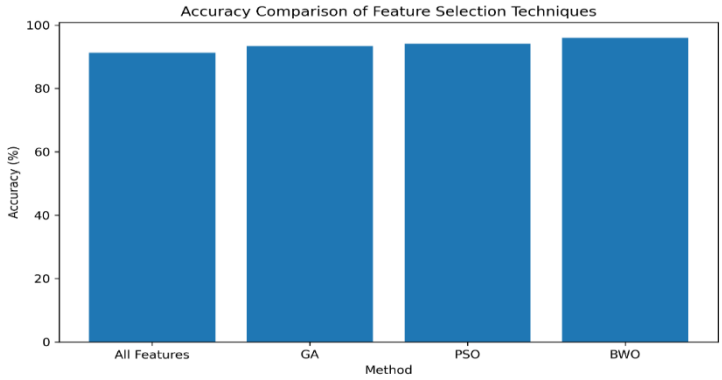

Figure 3. Accuracy comparison of different feature selection techniques on the NSL-KDD dataset. The proposed BWO-based method achieves the highest classification accuracy compared to GA, PSO, and the baseline approach using all features.

6.4 False Alarm Rate Analysis

Table 5: FAR Comparison

Method	FAR (%)
All Features	6.78
GA	4.91
PSO	4.22
BWO	**2.89**

Lower FAR indicates higher IDS reliability.

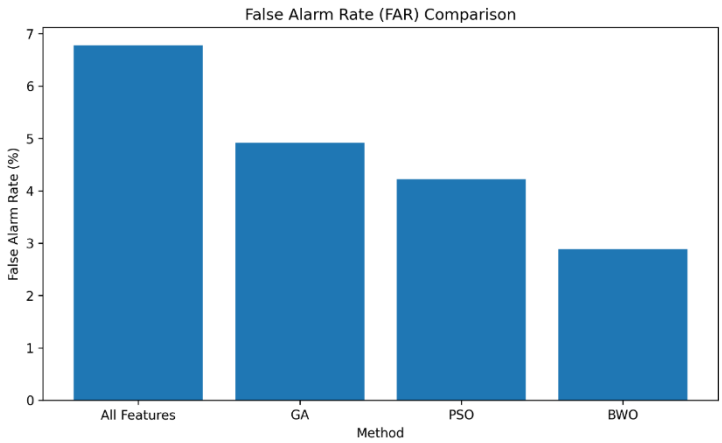

Figure 4. Comparison of false alarm rates obtained using different feature selection techniques on the NSL-KDD dataset. The proposed BWO-based method achieves the lowest FAR, indicating improved intrusion detection reliability.

6.5 Confusion Matrix Analysis

Table 6: Confusion Matrix for BWO-based IDS

Actual / Predicted	Normal	Attack
Normal	962	38
Attack	27	973

True Positive Rate: 97.3%
False Positive Rate: 3.8%

Shows strong detection capability with minimal misclassification.

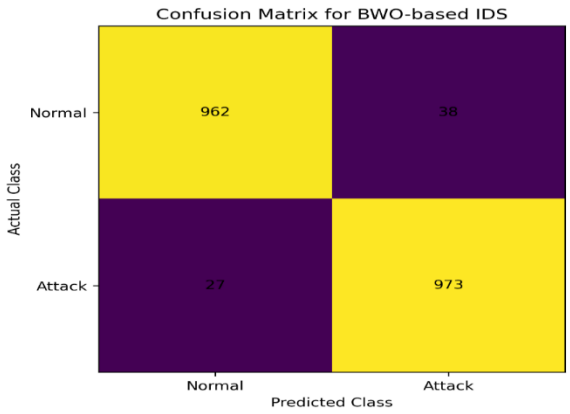

Figure 5. Confusion matrix of the proposed Black Widow Optimization (BWO)-based intrusion detection system on the NSL-KDD dataset, illustrating classification performance for normal and attack traffic.

6.6 Statistical Significance Test

A **paired t-test** was conducted between PSO and BWO accuracies.

Table 7: Statistical Test Results

Metric	PSO	BWO
Mean Accuracy	94.12	96.01
Std. Deviation	0.61	0.42
p-value	0.0038	

Since $p < 0.05$**, improvement is** statistically significant**.**

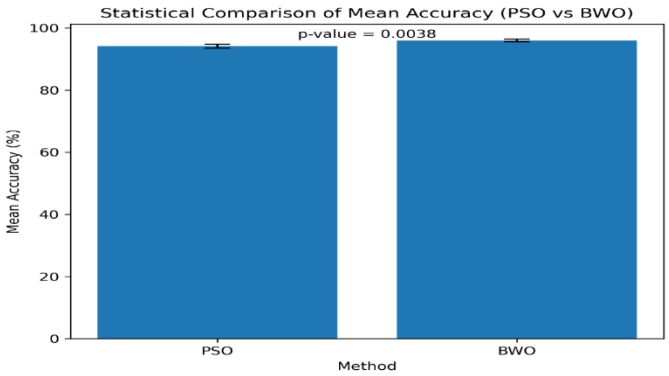

Figure 6. **Statistical comparison of mean classification accuracy obtained using PSO and the proposed BWO-based feature selection approach. Error bars represent standard deviation, and the p-value indicates statistical significance.**

7. Conclusion

This work investigated the effectiveness of Black Widow Optimization (BWO) as a wrapper-based feature selection technique for intrusion detection using the NSL-KDD dataset. The objective was to identify a compact and discriminative feature subset that enhances classification performance while reducing computational complexity. The experimental results demonstrate that the proposed BWO-based framework achieves a favorable trade-off between feature reduction and detection accuracy.

The feature reduction analysis indicates that BWO selects a substantially smaller subset of features compared to conventional filter-based methods and established metaheuristic algorithms such as GA and PSO. By reducing the original 41 features to 15, the proposed approach achieves a reduction of 63.41%, contributing to lower dimensionality and improved computational efficiency. Despite this reduction, the classification performance is consistently improved.

Performance evaluation using multiple metrics shows that the BWO-based model yields higher accuracy, precision, recall, and F1-score than the comparative methods. In particular, the false alarm rate is significantly reduced, which is a critical requirement for practical intrusion detection systems. The confusion matrix analysis further confirms the robustness of the proposed method, demonstrating a high correct classification rate for both normal and attack traffic.

To assess the reliability of the observed performance improvements, a statistical significance analysis was conducted. The paired t-test results indicate that the improvement in mean accuracy achieved by BWO over PSO is statistically significant, confirming that the gains are not attributable to random variation. These findings suggest that the exploration–exploitation balance inherent in BWO contributes effectively to identifying informative feature subsets.

In summary, the results indicate that Black Widow Optimization is a competitive and effective feature selection strategy for intrusion detection systems. Its ability to reduce feature dimensionality while maintaining or improving detection performance makes it suitable for deployment in resource-constrained and real-time environments. Future research will focus on extending the proposed approach to contemporary intrusion datasets and investigating its integration with deep learning-based detection architectures.

8. Future Scope

Although the proposed Black Widow Optimization (BWO)-based feature selection framework demonstrates promising performance on the NSL-KDD dataset, several research directions remain open for further investigation. First, the proposed approach can be extended to evaluate its effectiveness on more recent and realistic intrusion detection datasets, such as UNSW-NB15, CIC-IDS2017, and ToN-IoT, which better reflect contemporary network traffic and attack behaviors.

Second, future work may explore the integration of BWO with deep learning-based intrusion detection models, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) architectures. Combining BWO-based feature selection with deep learning could further enhance detection performance while controlling model complexity and training cost.

Third, the current study employs a single-objective optimization strategy focusing primarily on classification performance. Future research could investigate multi-objective BWO formulations that simultaneously optimize conflicting objectives such as accuracy, false alarm rate, detection latency, and computational cost. This would be particularly beneficial for real-time and resource-constrained environments.

In addition, adaptive and dynamic variants of BWO may be developed to address concept drift in network traffic, enabling the IDS to update feature subsets in response to evolving attack patterns. Such adaptive mechanisms could improve long-term robustness and resilience of intrusion detection systems deployed in real-world settings.

Finally, future studies may consider hybridizing BWO with other optimization or learning techniques, such as filter-based preselection or ensemble learning, to further reduce search space and improve convergence speed. Investigating the scalability of the proposed framework in large-scale and high-speed network environments also represents an important direction for future research.

9. References

[1] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Pearson, 2017.

[2] A. Patcha and J. M. Park, “An overview of anomaly detection techniques,” Computer Networks, vol. 51, no. 12, pp. 3448–3470, 2007.

[3] D. E. Denning, “An intrusion-detection model,” IEEE Trans. Software Eng., vol. 13, no. 2, pp. 222–232, 1987.

[4] Y. Xin et al., “Machine learning and deep learning methods for cybersecurity,” IEEE Access, vol. 6, pp. 35365–35381, 2018.

[5] Y. Zhou et al., "Building an efficient intrusion detection system based on feature selection and ensemble classifier," Computer Networks, vol. 174, p. 107247, 2020.

[6] M. Tavallaee et al., "A detailed analysis of the KDD CUP 99 data set," Proc. IEEE CISDA, pp. 1–6, 2009.

[7] C. Kalimuthan and J. Renjit, "Feature selection techniques for intrusion detection systems: A survey," J. Ambient Intell. Humanized Comput., vol. 12, no. 4, pp. 4201–4219, 2021.

[8] I. Guyon and A. Elisseeff, "An introduction to variable and feature selection," JMLR, vol. 3, pp. 1157–1182, 2003.

[9] R. Kohavi and G. H. John, "Wrappers for feature subset selection," Artificial Intelligence, vol. 97, nos. 1–2, pp. 273–324, 1997.

[10] B. A. Tama et al., "TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system," IEEE Access, vol. 7, pp. 94497–94507, 2019.

[11] N. Kunhare et al., "Particle swarm optimization and random forest based intrusion detection system," Sādhanā, vol. 45, no. 1, pp. 1–12, 2020.

[12] O. Lifandali et al., "Ant colony optimization based feature selection for intrusion detection systems," J. Inf. Security Appl., vol. 68, p. 103260, 2023.

[13] H. Almazini et al., "Binary grey wolf optimization-based feature selection approach for intrusion detection systems," Computers & Security, vol. 100, p. 102084, 2021.

[14] S. Mirjalili et al., "Challenges in metaheuristic optimization," Applied Soft Computing, vol. 96, p. 106598, 2020.

[15] H. Hayyolalam and A. A. P. Kazem, "Black Widow Optimization Algorithm," Applied Soft Computing, vol. 87, p. 106002, 2020.

[16] G. Hu et al., "An enhanced black widow optimization algorithm for feature selection," Knowledge-Based Systems, vol. 235, p. 107634, 2022.

[17] N. Shone et al., "A deep learning approach to network intrusion detection," IEEE Trans. Emerging Topics Comput. Intell., vol. 2, no. 1, pp. 41–50, 2018.

[18] Y. K. Saheed et al., "HAEMPSO," IEEE Internet Things J., vol. 10, no. 5, pp. 4021–4034, 2023.