An Adaptive F&WO Algorithm-Driven Model for Next-Generation Cyberthreat Detection and Response

Sreekanth Rallapalli[1], Weiwei Jiang[2]
[1]Lincoln University College, Malaysia / Department of MCA, Nitte Meenakshi Institute of Technology, Bengaluru, India
[2]Beijing University of Posts and Telecommunications, China

Abstract

The rapid expansion of cloud computing, Internet of Things (IoT), mobile platforms, and distributed digital infrastructures has significantly increased the complexity and scale of cybersecurity threats. Traditional intrusion detection systems (IDS) rely heavily on predefined rules and signatures, which often fail to detect evolving and sophisticated attacks. Additionally, many conventional detection systems suffer from high false positive rates and limited adaptability to dynamic network environments. This research proposes an intelligent cyberthreat detection and response framework using a hybrid Firefly and Whale Optimization (F&WO) algorithm integrated with machine learning. The model performs feature selection, hyperparameter tuning, and automated response prioritization to improve the efficiency of intrusion detection. By combining the exploration ability of the Firefly algorithm with the exploitation capability of Whale Optimization techniques, the proposed approach achieves improved optimization performance.

The framework is evaluated using widely used cybersecurity datasets including NSL-KDD, UNSW-NB15, and CICIDS2017. Experimental results demonstrate that the proposed F&WO-optimized model improves classification accuracy, precision, recall, and response efficiency while reducing false alarm rates compared with conventional approaches. The study highlights the potential of hybrid metaheuristic optimization techniques for building adaptive and intelligent cybersecurity defense systems capable of handling modern network threats.

Keywords: Cybersecurity, Intrusion Detection System, Hybrid Optimization, Firefly Algorithm, Whale Optimization Algorithm, IoT Security.

1. Introduction

The rapid digital transformation of modern organizations has resulted in extensive reliance on interconnected systems such as cloud computing platforms, IoT devices, mobile applications, and distributed networks. While these technologies enhance efficiency and scalability, they also introduce significant cybersecurity risks. Modern cyberattacks have evolved to become more sophisticated, adaptive, and difficult to detect using conventional security tools.

Traditional intrusion detection systems (IDS) are primarily based on signature detection or static rule-based mechanisms. These approaches are effective against known attacks but struggle to detect zero-day attacks, advanced persistent threats (APTs), and polymorphic malware. Furthermore, rule-based systems often generate a large number of false alarms, which increases the workload for security analysts and delays incident response.

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as promising approaches for improving cybersecurity systems. AI-based IDS can analyze large volumes of network traffic, detect hidden patterns, and identify anomalies that may indicate malicious activities. However, ML-based detection models require efficient feature selection and parameter optimization to achieve optimal performance.

Metaheuristic optimization algorithms such as Grey Wolf Optimization (GWO), Particle Swarm Optimization (PSO), Firefly Algorithm (FA), and Whale Optimization Algorithm (WOA) have been widely used to improve machine learning performance. These algorithms mimic natural behaviors to efficiently explore search spaces and identify optimal solutions.

In this research, a hybrid Firefly–Whale Optimization (F&WO) algorithm is proposed to enhance cyberthreat detection and automated response mechanisms. The hybrid approach combines the strengths of both algorithms to improve feature selection, reduce model complexity, and increase detection accuracy.

The key contributions of this work include:

1. Development of a hybrid F&WO optimization framework for cyberthreat detection.
2. Integration of optimization with machine learning for efficient feature selection and hyperparameter tuning.
3. Evaluation using multiple benchmark datasets including NSL-KDD, UNSW-NB15, and CICIDS2017.
4. Demonstration of improved performance in terms of accuracy, recall, precision, and false positive reduction.

---

2. Related Work

Several studies have explored AI-based techniques to improve intrusion detection systems. Machine learning models such as Random Forest, Support Vector Machines, Neural Networks, and Deep Learning architectures have been widely applied for detecting cyberattacks.

Optimization algorithms have also been integrated into IDS frameworks to improve feature selection and classification performance. For example, Grey Wolf Optimization (GWO) has been used to enhance intrusion detection in IoT environments by selecting optimal features from

network traffic data. Similarly, hybrid approaches combining optimization algorithms with ensemble learning techniques have demonstrated improvements in attack detection accuracy.

Whale Optimization Algorithm (WOA) has been applied in cybersecurity for optimizing machine learning models and improving anomaly detection. WOA simulates the bubble-net feeding strategy of humpback whales to perform efficient exploitation in optimization problems. Despite these advancements, many existing systems rely on a single optimization technique, which may limit their ability to explore the solution space effectively. Hybrid optimization approaches can address this limitation by combining complementary strategies. Recent studies have also highlighted the importance of automated response systems that can react to threats in real time. Intelligent response prioritization mechanisms can significantly reduce the time required to mitigate attacks. The proposed F&WO hybrid model addresses these challenges by integrating the exploration capability of the Firefly algorithm with the exploitation capability of Whale Optimization, enabling improved optimization for cyberthreat detection systems.

3. Proposed Methodology

3.1 Overview of the Proposed Framework

The proposed cybersecurity framework integrates data preprocessing, feature optimization, machine learning classification, and automated response mechanisms.

The system architecture includes the following stages:

1. Data Collection
2. Data Preprocessing
3. Feature Selection using F&WO Optimization
4. Machine Learning Classification
5. Threat Detection and Response Prioritization

The integration of optimization techniques enables the model to select relevant features from high-dimensional network traffic data, improving both detection accuracy and computational efficiency.

3.2 Firefly Optimization Algorithm

The Firefly Algorithm is a nature-inspired metaheuristic technique based on the flashing behavior of fireflies. In this algorithm, each firefly represents a potential solution, and its brightness corresponds to the quality of the solution.

Key characteristics include:

• Attraction between fireflies based on brightness
• Movement toward better solutions
• Random exploration for diversity

This approach allows efficient exploration of the search space to identify optimal feature subsets.

3.3 Whale Optimization Algorithm

The Whale Optimization Algorithm mimics the bubble-net hunting strategy of humpback whales. It includes three main phases:

1. Encircling prey
2. Bubble-net attacking strategy
3. Random search for prey

WOA is particularly effective for exploitation and fine-tuning solutions during optimization.

3.4 Hybrid F&WO Optimization

The proposed hybrid algorithm combines both techniques to improve optimization performance.

• Firefly algorithm performs global exploration
• Whale optimization performs local exploitation

The hybrid process includes:

1. Initial population generation
2. Feature subset evaluation
3. Firefly-based exploration phase
4. Whale optimization refinement phase
5. Selection of optimal feature subsets

This approach improves model accuracy while reducing redundant features.

4. Experimental Setup

4.1 Datasets

The model was evaluated using three widely used cybersecurity datasets:

NSL-KDD – A refined version of the KDD Cup 1999 dataset used for intrusion detection research.

UNSW-NB15 – A modern dataset containing diverse attack categories and realistic network traffic.

CICIDS2017 – A comprehensive dataset containing multiple attack types including DDoS, brute force, botnet, and infiltration attacks.

4.2 Performance Metrics

The system performance was evaluated using standard classification metrics:

- Accuracy
- Precision
- Recall
- F1-Score
- False Positive Rate

These metrics provide a comprehensive evaluation of the detection capability of the model.

5. Results and Analysis

Experimental results demonstrate that the proposed F&WO optimized model achieves significant improvements compared with traditional IDS models.

Key observations include:

- Higher detection accuracy across all datasets
- Improved precision and recall values
- Reduction in false positive rates
- Faster decision-making for automated responses

The hybrid optimization process improves feature selection and reduces unnecessary attributes, which enhances the overall performance of the machine learning classifier.

Compared with single optimization algorithms, the F&WO model provides better convergence and more stable results. The integration of automated response prioritization also improves the practical usability of the system in real-world network environments.

6. Discussion

The results indicate that hybrid metaheuristic optimization techniques can significantly improve cybersecurity detection systems. By combining exploration and exploitation strategies, the proposed algorithm effectively identifies optimal features for classification.

The framework is also scalable and can be applied to large-scale IoT networks and cloud infrastructures. Furthermore, integrating automated response mechanisms enables faster mitigation of cyber threats.

Future improvements may include:

- Integration with deep learning models
- Deployment in real-time network monitoring systems
- Integration with federated learning for distributed cybersecurity systems

7. Conclusion

This study proposed a hybrid Firefly and Whale Optimization (F&WO) algorithm-based cyberthreat detection framework to enhance intrusion detection and response mechanisms. The model integrates optimization techniques with machine learning to improve feature selection and classification performance. Evaluation using multiple benchmark datasets demonstrated that the proposed model achieves high detection accuracy, improved recall and precision, and reduced false positive rates. The hybrid optimization approach also improves computational efficiency and response speed. The findings suggest that hybrid metaheuristic optimization techniques can play a significant role in developing next-generation intelligent cybersecurity defense systems capable of adapting to evolving cyber threats.

References

Alqahtany, S. S., et al. (2025). Enhanced Grey Wolf Optimization and Random Forest for IDS in IoT Networks. *Scientific Reports.*

Hussien, S. A. S., et al. (2025). Enhanced IoT cyberattack detection using GWO and SMOTE. *Mesopotamian Journal of Computer Science.*

Hybrid whale-gray wolf optimization for intrusion detection in IoT. (2025). *Journal of Engineering and Applied Science.*

Ensemble feature selection using BGSA and BGWO for cyberthreat detection. (2023). *Decision Analytics Journal.*

Federated learning client selection using Grey Wolf Optimization. (2024). *arXiv Preprint.*

AI-based anomaly detection in smart grids using LSTM and RF. (2025). *Scientific Reports.*

ML-based intrusion detection for IoT networks. (2025). *Future Generation Computer Systems.*

DNS tunneling detection using reinforcement learning and optimization. (2025). *Frontiers in Computer Science.*

Optimized ensemble ML models for IIoT cybersecurity. (2026). *Frontiers in Artificial Intelligence.*

Privacy-preserving federated AI framework for cyberthreat detection. (2025). *Scientific Reports.*

Zero-day threat detection using flow-based telemetry. (2022). *arXiv Preprint.*

Deep learning-based IDS for modern network traffic classification. (2023). *IEEE Access.*

A survey on AI-driven cyber defense systems. (2022). *ACM Computing Surveys.*

Optimized feature selection methods for intrusion detection datasets. (2024). *Computers & Security.*

Intelligent response automation in cybersecurity using AI. (2024). *Springer Cybersecurity Journal.*

Hybrid metaheuristic approaches for IDS in cloud and IoT. (2026). *IEEE Transactions on Network Science and Engineering.*