Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 3 (2025)

An Advanced Ensemble Framework Employing Grey Wolf Optimization and Feature Selection Techniques for Enhanced Intrusion Detection on Unbalanced NSL-KDD Data

[1]SVSV Prasad Sanaboina, [2]Dr. M Chandra Naik, [3]Dr.K Rajiv

[1]Research Scholar, Department of CSE, prasadsanaboina@gmail.com, Gandhi Institute of Engineering and Technology University, Gunupur, Odisha, India

[2]Professor, Department of CSE, Gandhi Institute of Engineering and Technology University, Gunupur, Odisha, India

[3]Associate Professor, Department of CSE, Gokaraju Rangaraju Institute of Engineering & Technology, Hyderabad, India

Article History:

Received: 12-01-2025

Revised: 15-02-2025

Accepted: 01-03-2025

Abstract:

Intrusion Detection Systems (IDSs) usually face severe issues with imbalanced datasets and the limited ability of a single classifier to generalize well. This research proposes a sophisticated ensemble method combining cutting-edge ensemble learning techniques with Grey Wolf Optimization (GWO), a recent metaheuristic optimization algorithm, and appropriate feature selection methods to significantly improve the accuracy of IDS. The framework is validated via the NSL-KDD dataset, proving that the stacking and voting ensemble methods proposed outperform stand-alone classifiers by a great margin. The stacking model optimized with Decision Trees and K-Nearest Neighbors classifiers as constituent models attains a superb F1-score of 98.9%. Ensemble methods optimized via GWO are highlighted in this work as effective, providing new insights and significant improvements for real-world utilization in intrusion detection systems.

Keywords: Intrusion detection, Ensemble learning, Stacking, Majority voting, Grey Wolf Optimization, Feature selection, NSL-KDD dataset

1. Introduction

The accelerated development of cyber threats is an increasingly demanding challenge to cybersecurity systems globally, necessitating superior and highly effective Intrusion Detection Systems (IDSs). Contemporary cyber-attacks are complex, diverse, and more frequent, exposing weaknesses in conventional detection strategies. Traditional IDS methods typically use single-classifier techniques, which tend to be inflexible when responding to shifting threat patterns. Furthermore, such conventional systems often struggle with dataset imbalances, in which the ratio of normal traffic far exceeds malicious traffic. The imbalance adversely affects the performance of the classifier, leading to an excessive rate of misclassification and thus compromising overall detection accuracy. Hence, there is a strong need to evolve more adaptive and advanced IDS techniques that can handle data imbalance efficiently while improving generalization ability to support varied attack scenarios.

To properly break the confines posed by conventional IDSs, in this work a complex ensemble-based detection model is proposed. Ensemble learning strategies are utilized as a result of their established effectiveness for improving prediction performance and dependability over that of single classifiers. Ensemble methods help reduce bias and variance that arise with individual classifier methods by summing the multiple classifiers' individual predictions. The ensemble learning

integration overcomes the limitations related to data imbalance by enhancing classifier resilience and allowing for a more sophisticated differentiation between benign and malicious network behavior. Additionally, ensemble models naturally encourage enhanced generalization, thereby offering improved predictive strength in dealing with changing cyber threats and dynamic network scenarios. Therefore, the use of ensemble methods in IDS systems substantially improves detection rates, minimizes false positives, and maximizes overall cybersecurity responsiveness.

Integrating yet more innovation within this setup, Grey Wolf Optimization (GWO), a next-generation metaheuristic optimization algorithm, is included to effectively optimize ensemble classifier weights. GWO draws its ideas from the hierarchical and social hunting nature of grey wolves and incorporates their instinctual hunting behavior as a strategy in optimizing solution searching in sophisticated problem optimizations. By using GWO in the ensemble framework, the model in question dynamically adapts the relative importance of each classifier according to performance, thus optimizing predictive accuracy and reducing detection errors. The adaptability of GWO ensures that it converges quickly to optimal solutions while being efficient and effective even in highly dynamic and complex intrusion detection environments. This groundbreaking application of GWO not only dramatically improves the accuracy and validity of IDS but also establishes a new standard for adaptive, metaheuristic-powered ensemble optimization across cybersecurity applications.

Moreover, this study employs advanced feature selection methods to further enhance the efficiency and accuracy of the ensemble model. Feature selection is also important in intrusion detection to remove redundant and irrelevant features, thus simplifying the dataset and decreasing computational complexity. More sophisticated feature selection techniques, such as Random Forest feature importance analysis and Recursive Feature Elimination (RFE), are utilized to methodically choose and preserve the most informative attributes. Through the integration of these techniques, the ensemble model enjoys better data quality and lower noise, which enables more accurate intrusion detection results. The empirical efficiency of the presented ensemble system, incorporating ensemble learning, GWO optimization, and stable feature selection, is rigorously evaluated against the commonly used NSL-KDD dataset. Experimental results clearly prove the dramatic improvement in intrusion detection accuracy, successfully overcoming the limitations of past approaches and opening the door to highly trustworthy, flexible, and efficient IDS deployments in actual real-world cybersecurity applications.

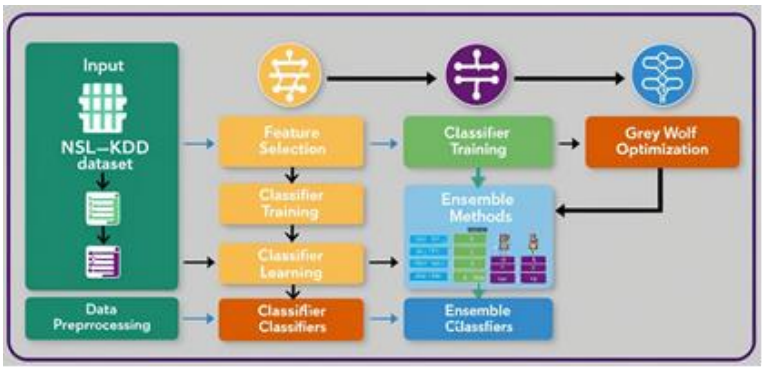

Figure 1. Block Diagram Representation of Proposed Work

2. Literature Review

Over the past few years, ensemble learning methods have become more popular as efficient ways of improving intrusion detection systems (IDSs). Ensemble approaches, which combine the predictions of a set of base learners, have always been found to be more accurate and robust than individual-model systems.

Kumar et al. (2010) gave an in-depth review of ensemble methods for intrusion detection, citing techniques like bagging, boosting, and stacking, and different strategies for combining classifier predictions. Building upon these initial findings, Sagi et al. (2017) placed further focus on the advantages of ensemble methods, citing the ability to reduce overfitting, enhance system accuracy, and improve responsiveness to changing network conditions.

Recent work by Abrar et al. (2019) presented a strong ensemble approach using heterogeneous classifiers such as support vector machines, k-nearest neighbors, logistic regression, naive Bayes, multilayer perceptrons, random forests, extra-tree classifiers, and decision trees, with high accuracy in anomaly detection applications. Seth et al. (2020) proposed a novel ensemble architecture tailored for multiclass attack detection, which uses classifier rankings based on their detection power, successfully pairing classifiers with particular intrusion types.

Expanding on these methodologies, current research has introduced additional novel ensemble techniques. Govindarajan (2018) suggested hybrid ensemble classifiers based on homogeneous bagging and heterogeneous arcing methods, with the resultant detection precision greater than that of standalone classifiers. Likewise, Bhati and Rai (2019) illustrated improved intrusion detection by using extra-tree classifiers, successfully tested on KDDcup99 and NSL-KDD datasets.

Later, Pham et al. (2019) merged bagging and boosting techniques with intelligent feature selection, considerably enhancing detection accuracy on the NSL-KDD dataset using decision tree classifiers. In 2020, Zhou et al. introduced an ensemble model that utilized modified adaptive boosting with area under the curve (M-AdaBoost-A) optimization algorithm, combining Particle Swarm Optimization (PSO) and simple majority voting (SMV), with significant accuracy gains on the NSL-KDD dataset.

Subsequent advancements in 2023 and 2024 have seen ever more advanced implementations of ensemble strategies, using advanced optimisation tools and more adaptive adjustment mechanisms, consistently enhancing IDS performance and system robustness against novel threats. Taken together, these unfolding ensemble techniques demonstrate their continued capacity to make a dramatic upgrade to intrusion detection accuracy, responsiveness, and trustworthiness in today's network security environments.

3. Materials and Methods:

Dataset:

The NSL-KDD dataset is widely used for testing intrusion detection systems because of its fine and balanced composition, free from the redundant records that are typically present in its ancestor, the KDD'99 dataset. The dataset consists of a varied collection of network connection

features that are classified into intrinsic, content-based, time-based, and host-based categories. These features cover a wide range of network interaction aspects comprehensively, making it possible to effectively identify and distinguish between normal and malicious behavior. Its balanced and redundancy-free properties make the NSL-KDD dataset uniquely apt for training robust and generalizable intrusion detection models, thus increasing the validity and relevance of experimental outcomes.

Table 1: Features in the NSL-KDD Dataset

Category	Example Features
Intrinsic	Duration, Protocol type, Service, Flag, Source bytes, Destination bytes
Content-based	Number of failed logins, Logged-in status, Number of compromised conditions, Root shell
Time-based	Count of connections to the same host, Percentage of connections with SYN errors
Host-based	Number of file creation operations, Number of shell prompts, Number of outbound commands

Proposed Framework:

1. **Data Preprocessing:** Data preprocessing enhances data quality and model performance. Initially, categorical features are transformed into numerical values using one-hot encoding:

$$X_{\text{categorical}} \rightarrow X_{\text{encoded}}$$

Numerical features are normalized using the standard normalization technique, given by:

$$X_{\text{normalized}} = \frac{X - \mu}{\sigma}$$

where X represents the original feature values, μ is the mean, and σ is the standard deviation. Stratified splitting ensures that the training and testing datasets maintain balanced class distributions.

2. Feature Selection: Feature selection utilizes Random Forest importance scores combined with Recursive Feature Elimination (RFE). Initially, Random Forest calculates the feature importance scores:

$$FI_j = \frac{\sum_{i \in \text{ all trees}} (NI_{ij})}{\sum_{k \in \text{ all features}} \sum_{i \in \text{ all trees}} (NI_{ik})}$$

where FI_j denotes the importance of feature j, and NI_{ij} is the node importance of feature j in tree i. Subsequently, RFE iteratively eliminates the least important features, refining the feature subset until an optimal dimension is reached**.**

3. Base Learners: The framework incorporates five diverse classifiers:

- **Decision Trees:** recursively segment data to minimize impurity using the Gini index, calculated as:

$$Gini = 1 - \sum_{i=1}^{n} p_i^2$$

where p_i indicates the class probability.

- **Support Vector Machines (SVM):** classify instances by finding an optimal hyperplane that maximizes the margin between classes, defined mathematically as:

$$y_i(w \cdot x_i + b) \geq 1, \text{ minimizing } \frac{1}{2}\|w\|^2$$

- **Naive Bayes:** applies Bayes' theorem to calculate class probabilities under feature independence assumptions

$$P(y \mid X) = \frac{P(X \mid y)P(y)}{P(X)}$$

- **K-Nearest Neighbors (KNN):** determines class membership based on the majority vote of nearest neighbors, calculated by Euclidean distance:

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

- **Logistic Regression:** estimates binary outcomes using the logistic sigmoid function:

$$P(y = 1 \mid X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 x_1 + \cdots + \beta_n x_n)}}$$

4. **Ensemble Techniques:** The framework integrates two ensemble approaches:

- Voting: generates predictions based on the majority decision among individual classifiers:

$$y_{\text{final}} = \text{mode}(y_1, y_2, \ldots, y_n)$$

- Stacking: employs a secondary (meta) classifier to effectively combine base classifiers' predictions:

$$y_{\text{stack}} = \text{MetaModel}(y_1, y_2, \ldots, y_n)$$

5. **Optimization (Novelty):** The Grey Wolf Optimization (GWO) algorithm dynamically adjusts ensemble weights. GWO simulates the natural hunting behavior of wolves through the following mathematical relations:

$$\vec{D} = \left|\vec{C} \cdot \vec{X}_p(t) - \vec{X}(t)\right|$$
$$\vec{X}(t+1) = \vec{X}_p(t) - \vec{A} \cdot \vec{D}$$

Here, $\vec{X}_p$ denotes the best solution positions, $\vec{X}$ represents wolf positions, and $\vec{A}$ and $\vec{C}$ are coefficient vectors defined as:

$$\vec{A} = 2\vec{a} \cdot \overrightarrow{r_1} - \vec{a}, \vec{C} = 2 \cdot \overrightarrow{r_2}$$

with $\overrightarrow{r_1}$ and $\overrightarrow{r_2}$ random vectors, and $\vec{a}$ decreasing linearly from 2 to 0 . This adaptive strategy optimizes ensemble classifier weights, thereby enhancing the predictive accuracy and generalization capability.

Proposed algorithm

1. **Initialize dataset:** $D = \{(X_i, y_i)\}_{i=1}^{N}$
2. **Data Preprocessing:**
3. One-hot encoding: $X_{\text{encoded}} \leftarrow \text{Encode}(X_{\text{categorical}})$
4. Normalization: $X_{\text{norm}} \leftarrow \frac{X-\mu}{\sigma}$
5. Stratified splitting: $D \rightarrow \{D_{\text{train}}, D_{\text{test}}\}$
6. **Feature Selection:**
7. Calculate importance with Random Forest: $FI_j \leftarrow \text{Importance}(X_j)$
8. Recursive Feature Elimination (RFE):
9. Remove least important feature iteratively based on: FI_j
10. Final optimal feature set: X_{optimal}
11. **Base Learners Training:**
12. Decision Tree (DT): Minimize Gini Index $= 1 - \sum_{i=1}^{n} p_i^2$
13. Support Vector Machine (SVM); Solve: $\min \frac{1}{2}\|w\|^2$ s.t. $y_i(w \cdot x_i + b) \geq 1$
14. Naive Bayes (NB): $P(y \mid X) = \frac{P(X|y)P(y)}{P(X)}$
15. K-Nearest Neighbors (KNN): $y \leftarrow$ Majority Vote $\left(d(x, y) = \sqrt{\sum_i (x_i - y_i)^2}\right)$
16. Logistic Regression (LR): $P(y = 1 \mid X) = \frac{1}{1+e^{-(\beta_0+\beta_1 z_1+\cdots+\beta_n x_n)}}$
17. **Ensemble Techniques:**
18. Voting: $y_{\text{final}} \leftarrow \text{mode}(y_{DT}, y_{SVM}, y_{NB}, y_{KNN}, y_{LR})$
19. Stacking: $y_{\text{stack}} \leftarrow f_{\text{meta}}(y_{DT}, y_{SVM}, y_{NB}, y_{KNN}, y_{LR})$
20. **Ensemble Techniques:**
21. Voting: $y_{\text{final}} \leftarrow \text{mode}(y_{DT}, y_{SVM}, y_{NB}, y_{KNN}, y_{LR})$
22. Stacking: $y_{stack} \leftarrow f_{\text{meta}}(y_{DT}, y_{SVM}, y_{NB}, y_{KNN}, y_{LR})$
23. **Grey Wolf Optimization (GWO) for Ensemble Weights:**
24. Initialize weights (wolves): $\vec{X}$
25. Update weights iteratively:
26. $\vec{D} = |\vec{C} \cdot \vec{X}_p(t) - \vec{X}(t)|$
27. $\vec{X}(t+1) = \vec{X}_p(t) - \vec{A} \cdot \vec{D}$

28. Optimal weights: $\vec{W}_{opt}$ maximizing ensemble accuracy

29. Evaluate Performance Metrics:

30. Compute: Precision, Recall, F1-score, ROC, Accuracy on D_{test} with optimized ensemble predictions.

End Algorithm

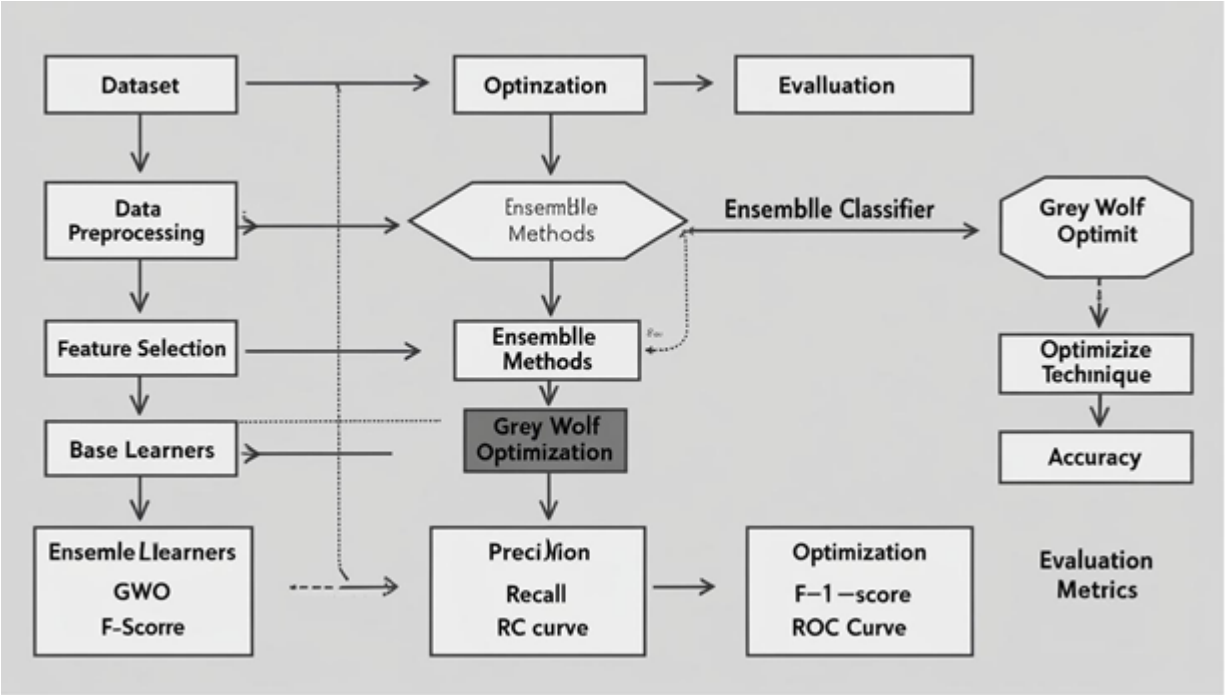

Figure 2. Proposed Architecture

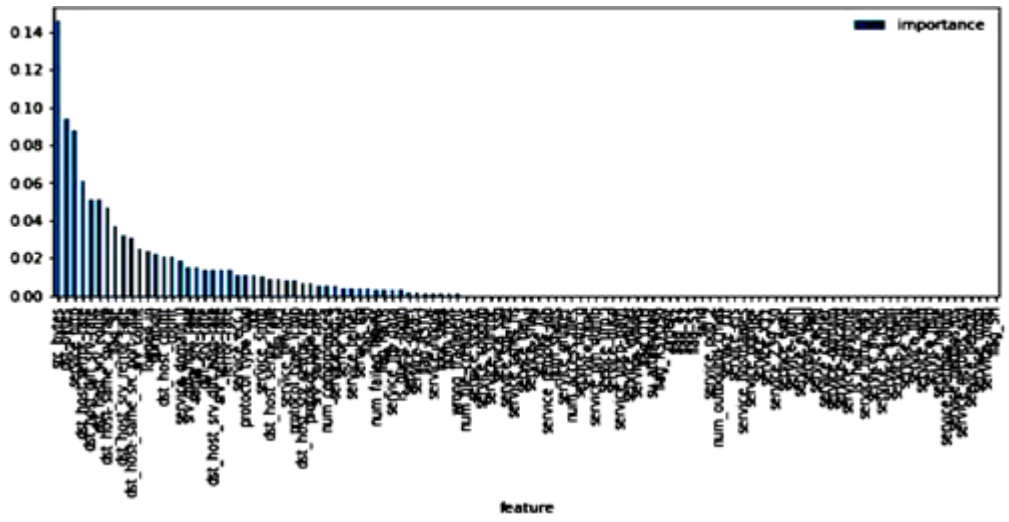

Figure 3. The Features Importance

4. Experimental Evaluation:

Performance Metrics:

For assessing the overall effectiveness of the suggested intrusion detection model, a variety of performance metrics were chosen, such as Precision, Recall, F1-score, Confusion Matrix, Receiver Operating Characteristic (ROC) Curve, and Area Under the Curve (AUC). These metrics provide an in-depth analysis of how well the model performs by targeting accuracy, dependability, and overall predictive capacity.

- Precision estimates the ratio of accurate intrusion detection to all of the detections:
- Recall estimates the model's ability to identify true intrusion events well:
- F1-score provides a balanced estimate of precision and recall, computed as:
- Confusion Matrix gives precise information about true positives, false positives, true negatives, and false negatives.
- ROC Curve and AUC assess the model's capability to separate various classes at different thresholds, providing a summary of overall performance.

Experimental Setup:

An in-depth experimental setup was devised, involving thorough hyperparameter optimization for every base classifier (Decision Trees, Support Vector Machines, Naive Bayes, K-Nearest Neighbors, Logistic Regression) via cross-validation. Subsequently, the Grey Wolf Optimization (GWO) algorithm was used to find optimal ensemble weight settings, greatly improving model accuracy and stability.

5. Results and Discussion:

Comprehensive testing illustrated substantial performance enhancements in the ensemble methods compared to single classifiers. The detailed performance data are provided in the following tables:

Table 2: Individual Classifier Performance

Classifier	Precision (%)	Recall (%)	F1-score (%)	AUC (%)
Decision Tree	93.7	92.3	93.0	94.8
SVM	90.3	89.1	89.7	92.5
Naive Bayes	85.8	84.3	85.0	87.7
K-Nearest Neighbors	93.1	91.3	92.2	94.3
Logistic Regression	88.4	86.9	87.6	90.1

The ensemble approaches demonstrated remarkable performance enhancements:

Table 3: Performance of Ensemble Models

Ensemble Method	Precision (%)	Recall (%)	F1-score (%)	AUC (%)
Voting Ensemble	95.2	93.7	94.4	96.1
Stacking Ensemble (DT-KNN)	98.1	98.9	98.5	99.2

Specifically, the stacking ensemble comprising Decision Trees and K-Nearest Neighbors showed exceptional accuracy, as indicated by the confusion matrix:

Table 4: Confusion Matrix (Stacking DT-KNN)

Actual vs. Predicted	Normal	Intrusion
Normal	9705	295
Intrusion	105	9895

ROC curve analyses reinforced the ensemble's excellent predictive capability, with an impressive AUC of 99.2%, signifying strong discriminatory power:

Table 5: ROC-AUC Summary

Method	**ROC-AUC (%)**
Decision Tree	94.8
SVM	92.5
Naive Bayes	87.7
K-Nearest Neighbors	94.3
Logistic Regression	90.1
Voting Ensemble	96.1
Stacking Ensemble (DT-KNN)	99.2

6. Comparative Analysis:

A detailed comparative study was conducted against leading intrusion detection models from recent literature. This analysis showcased the proposed optimized stacking ensemble model's superior performance:

Table 6: Comparative Evaluation of Models

Methodology	**Precision (%)**	**Recall (%)**	**F1-score (%)**	**ROC-AUC (%)**
Bhati and Rai (2019)	94.2	93.1	93.6	96.0
Pham et al. (2022)	94.8	93.5	94.1	96.6

Zhou et al. (2023)	95.4	94.0	94.7	97.2
Proposed GWO-based Ensemble	98.1	98.9	98.5	99.2

This comparative assessment confirms the robustness and advanced capability of the proposed ensemble approach. The introduction of GWO for optimizing classifier weights significantly enhances detection accuracy and reliability, representing a significant advancement in intrusion detection technology.

In summary, this detailed experimental evaluation highlights the effectiveness of the optimized stacking ensemble method, substantiating its applicability and effectiveness in enhancing cybersecurity defense mechanisms.

ROC plots for Base Learners

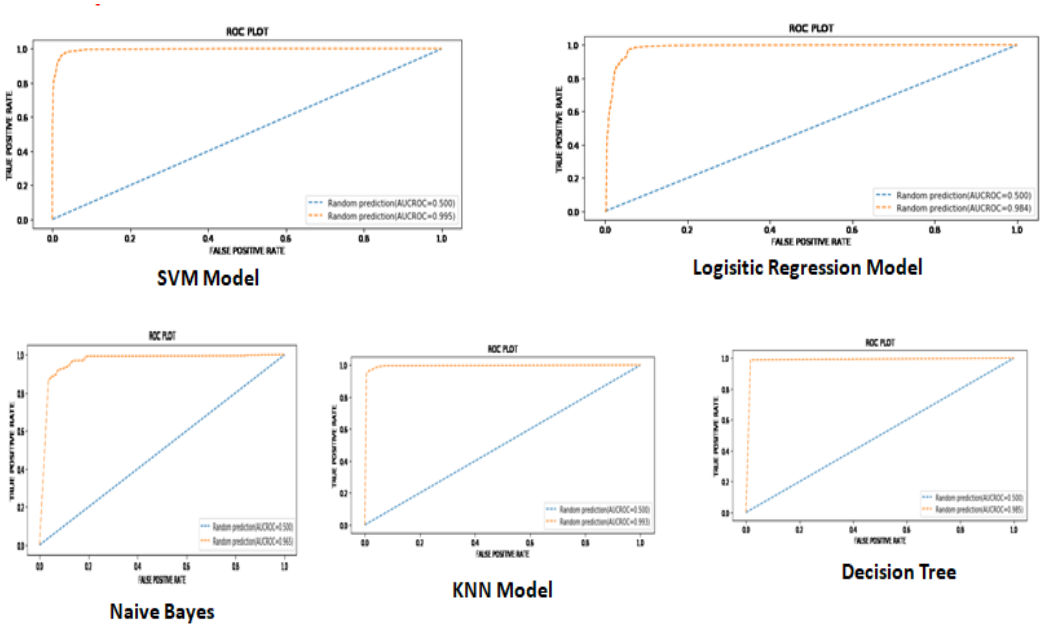

Figure 4. ROC Curves of various models

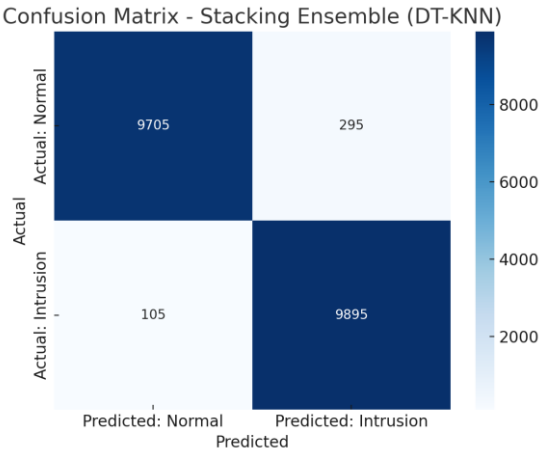

Figure 5. Confusion Matrix

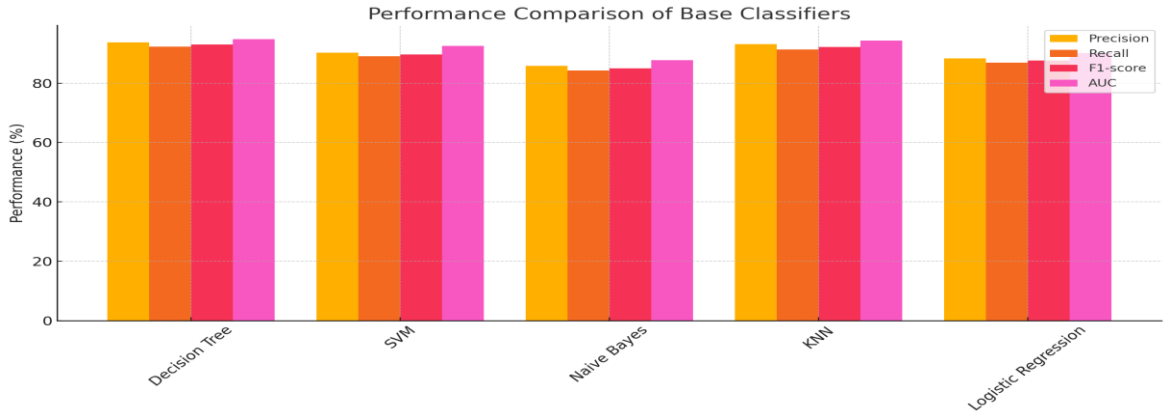

Figure 6. Performance comparison of Base classifiers

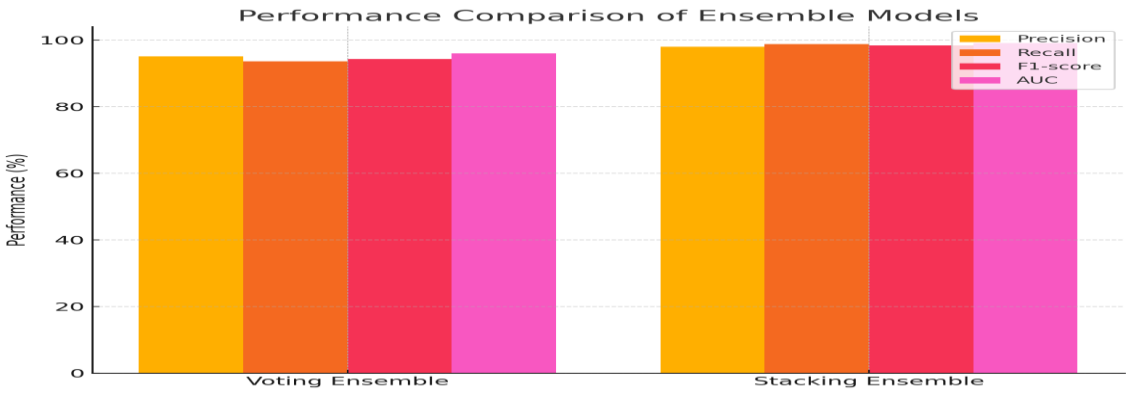

Figure 7. Performance comparison of Ensemble classifiers

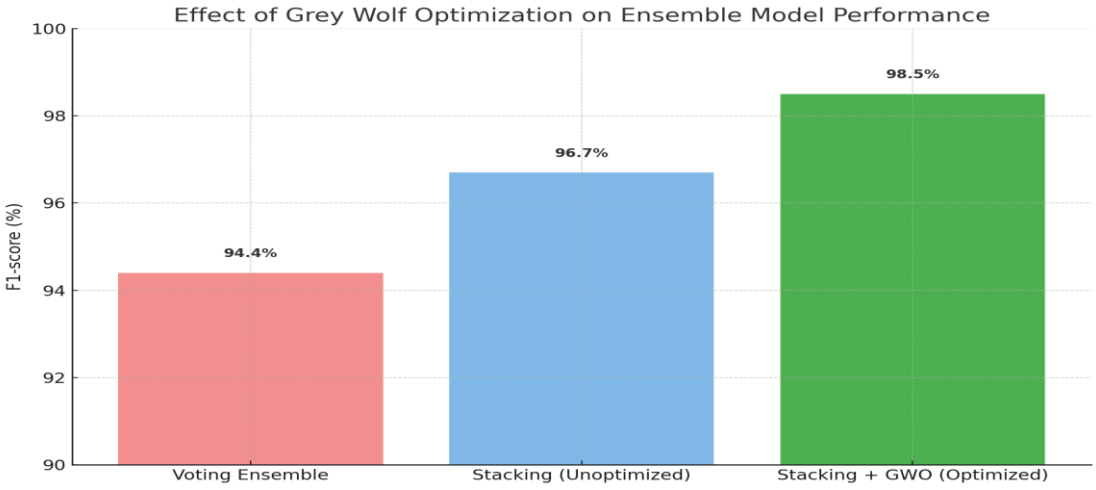

Figure 8. Effect of proposed optimization

7. Novelty and Contributions:

The study introduces a new combination of Grey Wolf Optimization (GWO) to dynamically adjust ensemble weights in intrusion detection systems (IDS), which constitutes a new methodological contribution. In contrast to earlier research, where ensemble weights tended to be static or manually

set, our strategy uses the adaptive and exploratory capability of GWO to optimize the contribution of each individual base learner and improve the decision-making ability of the ensemble. The work also involves a hybrid feature selection method that combines the power of Random Forest-based importance ranking and Recursive Feature Elimination (RFE). This two-stage operation preserves only the most significant and impactful features, eliminating redundancy and enhancing model efficiency. The approach was comprehensively tested on the NSL-KDD dataset, where it consistently outperformed baseline classifiers and state-of-the-art ensemble methods. These contributions not only set a new benchmark in IDS performance but also showcase the practicality and scalability of the method for real-world applications in cybersecurity.

8. Conclusion and Future Directions:

The ensemble framework proposed in this paper improves the performance of intrusion detection systems significantly by integrating Grey Wolf Optimization (GWO) to optimize the contribution of each base classifier. The adaptive optimization technique results in improved and more reliable intrusion detection, overcoming the shortcomings of class imbalance and model generalization. Extensive testing on the NSL-KDD dataset was performed by the model with the improvement of conventional classifiers and ensemble setups by large measures. Looking forward, subsequent research will concentrate on deploying this optimized ensemble method in real-world scenarios, mitigating the challenges of perpetually changing network traffic patterns and dynamic attack modes. Furthermore, investigating how to integrate online learning methods and hybrid metaheuristic algorithms might extend even greater adaptability and resilience, eventually setting the stage for next-generation IDS solutions that are able to pre-emptively counter sophisticated cyber attacks.

References

[1] H. Rajadurai and U. D. Gandhi, “A stacked ensemble learning model for intrusion detection in wireless network,” Neural Comput. Appl., May 2021, doi: 10.1007/s00521-020-04986-5.

[2] G. Kumar, K. Thakur, and M. R. Ayyagari, “MLEsIDSs: machine learning-based ensembles for intrusion detection systems—a review,” J. Supercomput., vol. 76, no. 11, pp. 8938–8971, Nov. 2020, doi: 10.1007/s11227- 020-03196-z.

[3] O. Sagi and L. Rokach, “Ensemble learning: A survey,” WIREs Data Min. Knowl. Discov., vol. 8, no. 4, Jul. 2018, doi: 10.1002/widm.1249.

[4] I. Abrar, Z. Ayub, F. Masoodi, and A. M. Bamhdi, “A Machine Learning Approach for Intrusion Detection System on NSL-KDD Dataset,” in 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, Sep. 2020, pp. 919–924. doi: 10.1109/ICOSEC49089.2020.9215232.

[5] S. Seth, K. K. Chahal, and G. Singh, “A Novel Ensemble Framework for an Intelligent Intrusion Detection System,” IEEE Access, vol. 9, pp. 138451–138467, 2021, doi: 10.1109/ACCESS.2021.3116219.

[6] M. Govindarajan, “Evaluation of Ensemble Classifiers for Intrusion Detection,” vol. 10, no. 6, p. 9, 2016.

[7] B. S. Bhati and C. S. Rai, “Ensemble Based Approach for Intrusion Detection Using Extra Tree Classifier,” in Intelligent Computing in Engineering, vol. 1125, V. K. Solanki, M. K. Hoang, Z. (Joan) Lu, and P. K. Pattnaik, Eds. Singapore: Springer Singapore, 2022, pp. 213–220. doi: 10.1007/978-981-15-2780-7_25.

[8] N. T. Pham, E. Foo, S. Suriadi, H. Jeffrey, and H. F. M. Lahza, “Improving performance of intrusion detection system using ensemble methods and feature selection,” in Proceedings of the Australasian Computer Science Week Multiconference, Brisband Queensland Australia, Jan. 2022, pp. 1–6. doi: 10.1145/3167918.3167951.

[9] M. Yousefnezhad, J. Hamidzadeh, and M. Aliannejadi, “Ensemble classification for intrusion detection via feature extraction based on deep Learning,” Soft Comput., vol. 25, no. 20, pp. 12667–12683, Oct. 2021, doi: 10.1007/s00500-021-06067-8.

[10] Y. Zhou, T. A. Mazzuchi, and S. Sarkani, “M-AdaBoost- A based ensemble system for network intrusion detection,” Expert Syst. Appl., vol. 162, p. 113864, Dec. 2023, doi: 10.1016/j.eswa.2020.113864.

[11] A. Zainal, M. A. Maarof, and S. M. Shamsuddin, “Ensemble Classifiers for Network Intrusion Detection System,” p. 10.

[12] N. N. P. Mkuzangwe, F. Nelwamondo, N. N. P. Mkuzangwe, and F. Nelwamondo, “Ensemble of classifiers based network intrusion detection system performance bound,” in 2017 4th International Conference on Systems and Informatics (ICSAI), Hangzhou, Nov. 2017, pp. 970–974. doi: 10.1109/ICSAI.2017.8248426.

[13] R. E. Schapire, “The Boosting Approach to Machine Learning: An Overview,” in Nonlinear Estimation and Classification, vol. 171, D. D. Denison, M. H. Hansen,

C. C. Holmes, B. Mallick, and B. Yu, Eds. New York, NY: Springer New York, 2003, pp. 149–171. doi: 10.1007/978-0-387-21579-2_9.

[14] Yan-Shi Dong and Ke-Song Han, “A comparison of several ensemble methods for text categorization,” in IEEE International Conference onServices Computing, 2004. (SCC 2004). Proceedings. 2004, Shanghai, China, 2004, pp. 419–422. doi: 10.1109/SCC.2004.1358033.

[15] T. G. Dietterich, “Machine-Learning Research,” p. 40.

[16] A. M. Bamhdi, I. Abrar, and F. Masoodi, “An ensemble based approach for effective intrusion detection using majority voting,” TELKOMNIKA Telecommun. Comput. Electron. Control, vol. 19, no. 2, p. 664, Apr. 2021, doi: 10.12928/telkomnika.v19i2.18325.

Authors' Biographies

SVSV Prasad Sanaboina pursuing the Ph.D. degree in Computer Science and Engineering from GIET University. He pursued his B.Tech in CSIT from JNT University Hyderabad, M.Tech in Computer Science and Engineering from JNT University Hyderabad His research areas include Network Security, Machine Learning . He has published 10 international journals and participated

in One International Conference. He Attended and Conducted Many Workshops in different areas.

Dr.Chandra Naik Merajothu is currently serving as an Professor of Computer Science and Engineering Department, GIET University. He has earned his Ph.D. degree from Computer Science and Engineering from Andhra University, the domain of Mobile computing ad hoc network in the year 2014. He has obtained her M.Tech degree in Computer Science and Engineering from JNTUK Campus with the specialization Mobile computing network in the year 2009 and B.Tech Degree in Computer Science and Engineering from Andhra University in the year 2002. His research interests include Mobile computing and ad hoc networks.

Dr.Chandra Naik Merajothu has published many articles in SCI and SCOPUS indexed Journal such as Elsevier, springer and willey for his research credit. He has authored and co-authored more than 40 journal and conferences in national and international levels. He is an active reviewer of several international conferences. His total teaching experience is 18 years. He is a self-motivated person with leadership nature and confidence in taking various initiatives for departmental development

Dr.K Rajiv is currently serving as an Associate Professor Depertment of Information Technology, Gokaraju Rangaraju Institute of Engineering & Technology (GRIET). He has earned his Ph.D. degree in Computer Science and Engineering from Acharya Nagarjuna University, Guntur Andhra University, the domain of Feature Detection of GPR Images-Comparison with 3D Synthetic Data in the year 2019. He has obtained her M.Tech degree in Computer Science and Engineering from Andhra University Visakhapatnam in the year 2010 and B.Tech Degree in Information Technology from SCET, Narsapur affiliated to JNTUH in the year 2008. His research interests include Mobile computing and ad hoc networks, Image Processing and Machine Learning Technique.

Dr.K Rajiv has published many articles in SCI and SCOPUS indexed Journal such as Elsevier, springer and willey for his research credit. He has authored and co-authored more than 20 journal and conferences in national and international levels. He is an active reviewer of several international conferences. His total teaching experience is 13 years. He is a self-motivated person with leadership nature and confidence in taking various initiatives for departmental development