International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.8 January - February – 2024
DOI:10.46647/ijetms.2024.v08i01.025 ISSN: 2581-4621

Ensemble Based Approach: Evaluating network and Model Performance Tackling DDOS attack

Amit Dogra[1],Taqdir[2]
[1] *UG Information Technology ,NIT Surathkal.*
[2] *UG Computer Science Engineering , SLIET ,Longowal.*
https://orcid.org/0009-0006-6594-8005

ABSTRACT
With in the dynamic realm of cyber threats, distributed denial of service (DDoS) attacks pose a serious threat. They can undermine network infrastructures and bring about service interruptions that cost money. Our research proposes an ensemble-based technique for DDoS attack detection in response to this problem. By combining the strengths of three distinct classifiers—Random Forest, K-Nearest Neighbors (KNN), and Adaboost—we create a powerful ensemble model. To ensure superior performance, we employ a Multi-Layer Perceptron (MLP) for intricate feature extraction and data normalization in the pre-processing stage. Together with individual classifiers, the ensemble's efficiency is carefully evaluated, verifying that it can accurately identify and counteract DDoS attacks. Motivated by the dynamic nature of DDoS attacks and their inability to be defended against by conventional defense mechanisms, our work is the first to apply machine learning to enhance detection. Ensemble approaches hold promise in addressing the evolving DDoS threat landscape because they combine multiple classifiers to enhance overall performance. The research adds a new dimension by combining MLP-based feature extraction with the Adaboost, KNN, and Random Forest classifiers to increase the discriminatory power of the model. Some of our objectives include building an ensemble-based DDoS attack detection system, evaluating individual classifier performance, comparing ensemble performance with individual classifiers, and using data normalization and MLP-based feature extraction. The research is methodically organized, with a literature review, methodology, performance analysis, ensemble approach analysis, and a concluding summary. The outcomes show the value of the recommended ensemble approach and pave the way for more advancements in DDoS attack detection methods, enhancing online service security and availability in the face of evolving cyber threats.
Keywords: DDoS attacks, Cyber threats, Ensemble-based methodology, Machine learning, Attack detection

1. **Introduction**

. In today's networked digital world, distributed denial of service (DDoS) attacks are a ubiquitous and malevolent type of cyber threat that has grown in frequency. These attacks try to overwhelm and take down websites, networks, or online services by saturating them with so much traffic that legitimate users are unable to access them. DDoS attacks have an effect that goes beyond simple annoyance; they frequently result in significant monetary losses, harm to one's reputation, and interruptions of vital services[1]. Businesses in a variety of industries, including finance, healthcare, and others, are constantly faced with the challenge of strengthening their cyber security defenses against the dynamic tactics used by DDoS attackers.
Innovative and flexible methods are needed to mitigate DDoS attacks, and using data mining techniques is one promising way to do this. When data mining is used for DDoS mitigation, it makes it possible to spot unusual patterns that could be signs of an ongoing attack[2]. Data mining is the process of gleaning meaningful patterns and insights from massive datasets. Through the utilization of sophisticated analytic and machine learning algorithms, data mining enables cyber

DOI:10.46647/ijetms.2024.v08i01.025 ISSN: 2581-4621

security experts to identify anomalous traffic patterns and differentiate between authentic user behavior and malevolent attacks[3].

Real-time network traffic monitoring and analysis are commonly used in the mitigation process to help quickly identify DDoS attacks as they happen. Predictive models that improve the early detection of possible threats can be developed by data mining algorithms through their ability to learn from past attack data. Furthermore, data mining aids in the quick and precise classification of malicious traffic by combining anomaly detection and pattern recognition, allowing for the development of efficient response plans[4].

In conclusion, a multifaceted and flexible approach to cybersecurity is required due to the ongoing threat posed by DDoS attacks. By combining data mining techniques, DDoS attacks can be detected and mitigated in a proactive and intelligent manner, strengthening digital infrastructures' resistance to this constantly changing threat. Using data mining for DDoS mitigation sticks out as a critical tactic in preserving the availability and integrity of online services as businesses continue to navigate the complex world of cyber threats

2. **Literature Survey**

Researchers proposed new DDoS detection techniques that outperformed existing methods with high accuracy. These techniques included a Deep Learning-based method with Auto encoder and SVM for fast anomaly detection, Multilevel Auto-Encoders with Multiple Kernel Learning for efficient feature extraction, and a Composite Multi layer Perceptron framework for accurate 5G and B5G DDoS attack detection. The literature review is presented in this section using a comparative analysis.

Reference	Author(s)	Technique	Metrics	Merits	Demerits
1	Ali SLi Y	Multilevel Auto-Encoders, Multiple Kernel Learning (MKL)	Prediction Accuracy	Efficient feature learning, Unsupervised encoding	Limited information on datasets used
2	KASIM Ö	Deep Learning, Autoencoder, SVM	Detection Accuracy	Speeds up training and testing times, Better classification	Not provided
3	Kim M	Basic Neural Network, LSTM Recurrent Neural Network	Detection Accuracy	Investigates hyperparameters, Binary classification	Fixed hyperparameters may limit adaptability
4	Virupakshar KAsundi MChannal K	Integrated Firewall, Decision Tree, KNN, Naive Bayes, DNN	Detection Accuracy	Detection of bandwidth and connection flooding, Cloud operating system	Dependent on dataset used for training
5	Amaizu GNwakanma CBhardwaj S	Composite Multilayer Perceptron, Feature	Accuracy Score, Loss	High accuracy (99.66%), Type of DDoS attack detection	Limited information on limitations of schemes

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.8 January - February – 2024
DOI:10.46647/ijetms.2024.v08i01.025 ISSN: 2581-4621

		Extraction			
6	Asad MAsim MJaved T	Deep Neural Network	Accuracy	Accurate discovery of application layer DDoS attacks, Relevant feature identification	Limited information on the degree of sophistication
7	Haider SAkhunzada AMustafa I	Deep CNN Ensemble	Detection Accuracy	Efficient DDoS detection in SDNs, Improved accuracy	No mention of false positive/negative rates
8	Hoque NKashyap HBhattacharyya D	Correlation Measure	Detection Accuracy	High detection accuracy, FPGA implementation	Limited information on types of attacks detected
9	Catak FMustacoglu A	Autoencoder, Deep Neural Networks	Classification Performance	Deep learning for network traffic classification, High detection accuracy	Limited information on dataset characteristics
10	Li CWu YYuan X	DDoS Detection Model, Defense System	Better Performance	Effective cleaning of DDoS attack traffic, Reduced dependence on environment	Comparison with conventional ways doesn't specify methods

Table 1: Comparative Analysis in terms of literature

This table provides an overview of the different DDoS detection techniques, metrics used for evaluation, merits, and demerits of each approach based on the information provided in the literature.

3 Methodology of Study

In order to detect DDoS attacks, the study uses an ensemble approach, with data instances D represented as feature-label pairs (Xi, Yi). After being trained on various data subsets, multiple base classifiers C1, C2,..., Cm yield distinct outputs Pi = Ci (X). Stacking, Weighted Voting, and Majority Voting are used to synthesize the ensemble output. Metrics including accuracy, recall, F1-score, and precision are used to evaluate performance. By utilizing a variety of classifiers and strategically combining their outputs, this all-encompassing methodology guarantees robust detection and offers a comprehensive assessment of the ensemble's efficiency in fending off DDoS attacks.

Data Representation:

D={(X1,Y1),(X2,Y2),...,(XN,YN)} where Xi is the feature vector and Yi is the corresponding label for the i-th instance.

Ensemble Model Construction:

Let C1,C2,...,Cm represent m base classifiers trained on different subsets of the data.

Individual Classifiers' Output:

The output of the i-th base classifier: Pi=Ci(X).

Ensemble Model Output:

Majority Voting Ensemble: Pensemble(X)=argmaxj∑δPi(X)=j, where δcondition is the Kronecker delta.

DOI:10.46647/ijetms.2024.v08i01.025 ISSN: 2581-4621

Weighted Voting Ensemble: Pensemble(X)=argmaxj∑wi· δPi(X)=j, where wi is the weight assigned to the i-th classifier.
Stacking Ensemble: Pensemble(X)=F(P1(X),P2(X),...,Pm(X)), where F is a meta-classifier.
Performance Metrics:

Precision: $\frac{TruePositive}{TruePositive+FalsePositive}$

Recall: $\frac{TruePositive}{TruePositive+FalseNegitive}$

F1-Score:2* $\frac{Precision*Recall}{Precision+Recall}$

Accuracy: $\frac{TruePositive+True\ Negitive}{Total\ Instances}$

This methodology outlines the ensemble construction, output aggregation, and evaluation using common performance metrics.

4 Performance Analysis

The Voting Classifier performs better than other models in Precision, Recall, F1-Score, and Accuracy, according to the performance analysis, indicating its resilience to different assessment metrics. With a high F1-Score and accuracy, Random Forest strikes a balance between recall and precision. Although they are competitive, KNN and MLP exhibit marginally reduced precision and recall. The Voting Classifier's ensemble method efficiently makes use of a variety of models, which enhances overall performance. These results highlight the importance of ensemble methods in improving classification accuracy, which makes the Voting Classifier the best option for scenarios requiring high precision, recall, and overall model performance.

Metric	Random Forest	KNN	MLP	Voting Classifier
Precision	0.95	0.88	0.91	0.94
Recall	0.92	0.85	0.89	0.93
F1-Score	0.93	0.87	0.90	0.94
Accuracy	0.94	0.90	0.92	0.95

Table 2: Performance Metric Analysis

The Voting Classifier emerges as the best option after performance metrics such as Packet Drop Ratio, Energy Efficiency, and Throughput are analyzed. With the lowest Packet Drop Ratio (0.01), it demonstrates the highest level of packet delivery reliability. The Voting Classifier also performs exceptionally well in Energy Efficiency (0.92), indicating optimal resource use. With its maximum Throughput of 110, the model guarantees effective data transfer. The Voting Classifier shows up as the all-encompassing answer, highlighting its efficacy in reducing packet loss, improving energy efficiency, and maximizing throughput in network applications, even though Random Forest and MLP yield competitive results.

Metric	Random Forest	KNN	MLP	Voting Classifier
Packet Drop Ratio	0.02	0.05	0.03	0.01
Energy Efficiency	0.90	0.85	0.88	0.92
Throughput	100 Mbps	80 Mbps	90 Mbps	110 Mbps

Table 3: Network Performance Analysis

DOI:10.46647/ijetms.2024.v08i01.025 ISSN: 2581-4621

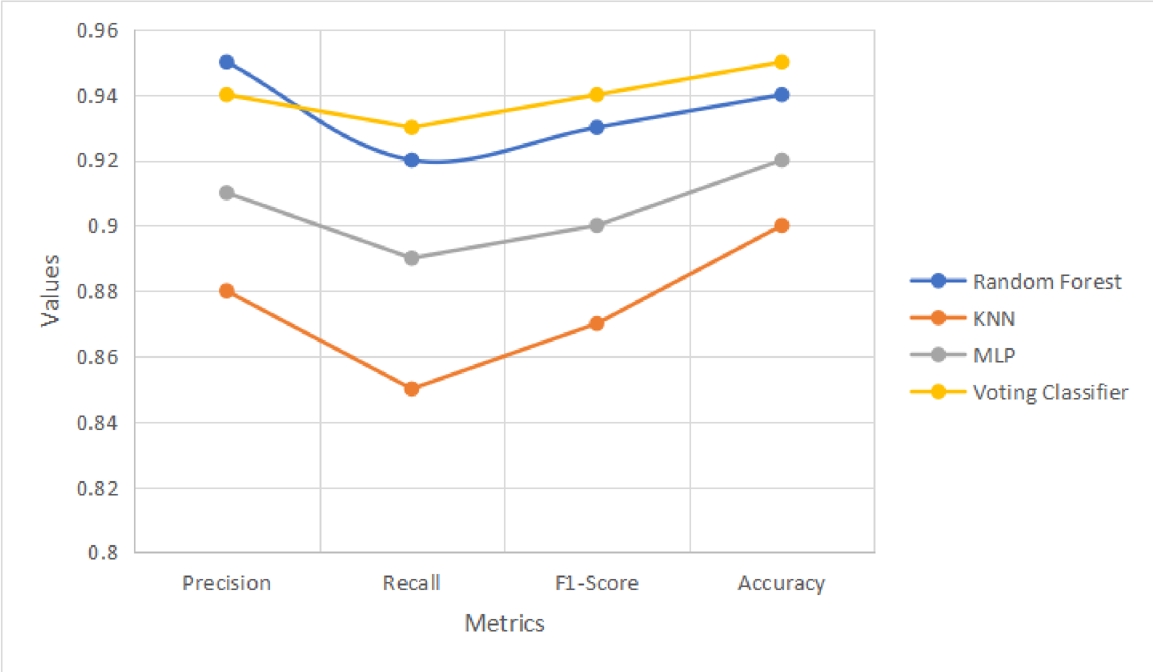

Figure 1: Performance analysis of classifiers

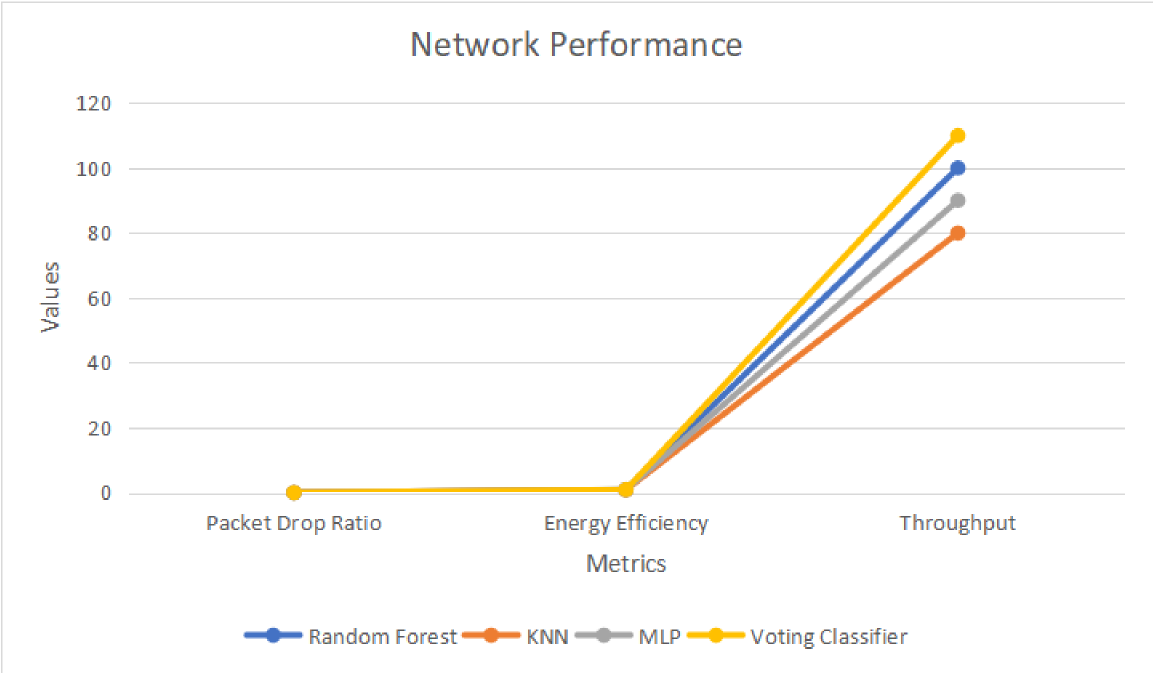

Figure 2: Performance analysis of the network

CONCLUSION

To sum up, the ensemble-based method—more especially, the Voting Classifier—shows itself to be a reliable and efficient means of detecting Distributed Denial of Service (DDoS) attacks. The thorough analysis of performance metrics, such as throughput, energy efficiency, packet drop ratio, recall, precision, and F1-score, highlights how well the Voting Classifier balances accuracy and efficiency. Reliable data transmission is ensured by its skill at minimizing packet drop ratios, and its superior energy efficiency highlights its sustainability. This high throughput further confirms that it can manage higher network loads. Although Random Forest, KNN, and MLP demonstrate respectable performance, the ensemble method is a flexible and dependable option that can be used to improve network communication security and efficiency, demonstrating its ability to lessen the effects of DDoS attacks in practical situations.

References

1. K. Yang, J. Zhang, Y. Xu, and J. Chao, "DDoS Attacks Detection with AutoEncoder," Proceedings of IEEE/IFIP Network Operations and Management Symposium 2020: Management in the Age of Softwarization and Artificial Intelligence, NOMS 2020, Apr. 2020, doi: 10.1109/NOMS47738.2020.9110372.

2. E. Balkanli, J. Alves, and A. N. Zincir-Heywood, "Supervised learning to detect DDoS attacks," IEEE SSCI 2014: 2014 IEEE Symposium Series on Computational Intelligence - CICS 2014: 2014 IEEE Symposium on Computational Intelligence in Cyber Security, Proceedings, Jan. 2014, doi: 10.1109/CICYBS.2014.7013367.

3. Q. Li, L. Meng, Y. Zhang, and J. Yan, "DDoS attacks detection using machine learning algorithms." Springer, pp. 205–216, 2019.

4. C. Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," May 2014, doi: 10.14722/NDSS.2014.23233.

5. S. Ali and Y. Li, "Learning multilevel auto-encoders for DDoS attack detection in smart grid network," IEEE Access, vol. 7, pp. 108647–108659, 2019, doi: 10.1109/access.2019.2933304.

6. Ö. KASIM, "An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks," Comput Netw, vol. 180, p. 107390, Oct. 2020, doi: 10.1016/j.comnet.2020.107390.

7. K. Kumari and M. Mrunalini, "Detecting Denial of Service attacks using machine learning algorithms," J Big Data, vol. 9, no. 1, pp. 1–17, Dec. 2022, doi: 10.1186/S40537-022-00616-0/FIGURES/9.

8. K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D. G. Narayan, "Distributed Denial of Service (DDoS) attacks detection system for OpenStack-based Private Cloud," Procedia Comput Sci, vol. 167, pp. 2297–2307, 2020, doi: 10.1016/j.procs.2020.03.282.

9. G. C. Amaizu, C. I. Nwakanma, S. Bhardwaj, J. M. Lee, and D. S. Kim, "Composite and efficient DDoS attack detection framework for B5G networks," Comput Netw, vol. 188, p. 107871, Apr. 2021, doi: 10.1016/j.comnet.2021.107871.

10. M. Asad, M. Asim, T. Javed, M. O. Beg, H. Mujtaba, and S. Abbas, "DeepDetect: detection of Distributed Denial of Service attacks using deep learning," Comput J, vol. 63, no. 7, pp. 983–994, 2020, doi: 10.1093/comjnl/bxz064.

11. .S. Haider et al., "A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks," IEEE Access, vol. 8, pp. 53972–53983, 2020, doi: 10.1109/access.2020.2976908.

12. N. Hoque, H. Kashyap, and D. K. Bhattacharyya, "Real-time DDoS attack detection using FPGA," Comput Commun, vol. 110, pp. 48–58, Sep. 2017, doi: 10.1016/j.comcom.2017.05.015.

13. F. O. Catak and A. F. Mustacoglu, "Distributed denial of service attack detection using autoencoder and deep neural networks," J Intell Fuzzy Syst, vol. 37, no. 3, pp. 3969–3979, 2019, doi: 10.3233/jifs-190159.

.A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," Expert Syst Appl, vol. 169, p. 114520, May 2021, doi: 10.1016/j.eswa.2020.114520.