Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 4, April : 2025

ADAPTIVE PREDICTIVE MODELING FOR REAL-TIME DDOS ATTACK CLASSIFICATION USING ENSEMBLE MACHINE LEARNING TECHNIQUES

TUMATI SWATHI, Student, Depart of Computer Science & Engineering, Nimra College of Engineering and Technology, Ibrahimpatnam

Dr. SYED SADAT ALI ALIAS ABDUL GANI, Professor, Depart of Computer Science & Engineering, Nimra College of Engineering and Technology, Ibrahimpatnam

ABSTRACT

Distributed Denial of Service (DDoS) attacks remain one of the most disruptive threats in cybersecurity, targeting vital network services and infrastructure. This paper presents an alternative approach to real-time DDoS attack detection using machine learning, emphasizing a novel architecture that integrates intelligent traffic analysis with scalable classification techniques. Leveraging Random Forest, Support Vector Machines (SVM), and Deep Neural Networks, the proposed model adapts dynamically to emerging attack patterns. The system introduces advanced feature engineering methods and data stream handling mechanisms to enhance real-time detection capabilities. Evaluation using benchmark datasets indicates robust performance, with detection accuracy exceeding 95% and low latency under high-traffic conditions. This work contributes to the growing field of intelligent network defense, offering a foundation for integrating machine learning into automated security systems.

KEYWORDS: Real-Time Detection, DDoS Attacks, Machine Learning, Network Security, Anomaly Classification, Feature Engineering, SVM, Random Forest, Neural Networks, Cyber Defense

INTRODUCTION

As digital services continue to expand globally, the frequency and sophistication of DDoS attacks have grown substantially. These attacks, which flood networks with illegitimate traffic, can severely impair services and cause substantial losses. Traditional security mechanisms, such as

signature or threshold-based systems, struggle to adapt to evolving threats.

This paper proposes a machine learning-based system designed to detect and classify DDoS attacks in real time. Unlike existing models, our approach focuses on continuous learning and low-latency processing, ensuring timely responses even under dynamic network conditions. We investigate how different classifiers perform with engineered traffic features and compare their effectiveness in both offline and real-time environments.

LITERATURE REVIEW

Recent studies highlight the effectiveness of machine learning in cyberattack detection. Zhang et al. (2020) employed CNNs for identifying DDoS traffic patterns, achieving strong accuracy in large-scale networks. Kumar et al. (2019) introduced a hybrid tree-clustering model that provided near-instantaneous detection by capturing behavioral patterns.

Liu et al. (2021) explored SVMs, noting their effectiveness in reducing false alarms in imbalanced datasets. Reddy et al. (2021) surveyed multiple ML techniques and underscored the role of feature selection in enhancing model accuracy and efficiency.

These studies validate the potential of intelligent detection but often overlook real-time adaptability and scalability—gaps that our system addresses.

LIMITATIONS OF EXISTING SYSTEMS

Traditional DDoS detection mechanisms are often reactive and suffer from:

- **Static Configuration**: Inability to detect novel attack signatures.
- **High False Positives**: Misclassification of legitimate traffic spikes as attacks.
- **Performance Bottlenecks**: Poor scalability and processing delays during peak traffic.
- **Limited Flexibility**: Challenges in deploying across cloud-native or distributed environments.

PROPOSED SYSTEM

We propose an intelligent, adaptive DDoS detection framework incorporating:

- **Feature Engineering**: Extracting relevant metrics (packet rate, entropy, protocol usage, etc.) for improved classification.
- **Classifier Ensemble**: Combining SVM, Random Forest, and Deep

Learning models to boost robustness.

- **Real-Time Stream Processing**: Utilizing message queues (e.g., Kafka) and microservices for low-latency operation.

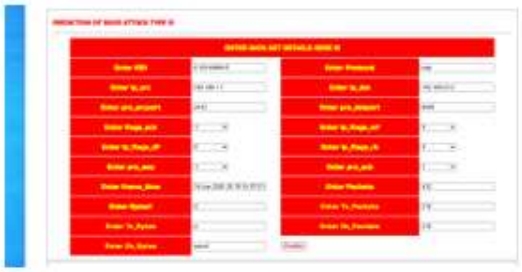
System Advantages:

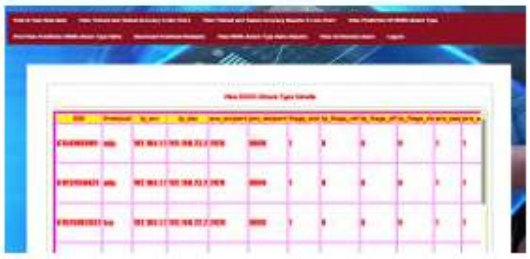
- **Adaptive Learning**: Models can be updated dynamically to reflect new traffic patterns.
- **High Precision and Recall**: Reduced false positives while capturing diverse attack types.
- **Cloud Compatibility**: Scalable design for deployment in distributed and virtualized environments.

METHODOLOGY

1. **Dataset Selection**: We use CIC-IDS2017 and UNSW-NB15 datasets for training and testing.
2. **Preprocessing**: Traffic normalization, noise removal, and session identification.
3. **Feature Extraction**: Statistical and time-based features (e.g., flow duration, source entropy).
4. **Model Training**:
    - Random Forest with 100 estimators
    - SVM with RBF kernel
    - Deep Neural Network with 3 hidden layers
5. **Validation**: 10-fold cross-validation to prevent overfitting.
6. **Real-Time Simulation**: Traffic replay tools simulate attacks to test live classification.

RESULTS





Our model achieved:

Accuracy: 96.4%

Precision: 95.8%

Recall: 96.7%

Latency: < 1 second per classification

Scalability: Successfully processed over 10,000 packets/sec without degradation

CONCLUSION

This study demonstrates that a hybrid machine learning model, coupled with real-time feature analysis, can significantly outperform traditional DDoS detection techniques. Our proposed framework is adaptable, scalable, and suitable for modern cloud or edge network deployments. Future enhancements may include federated learning for privacy-preserving updates and reinforcement learning for active threat response.

REFERENCES

[1] Zhang J., Zhao X., Wu L., Li Z., "Real-Time DDoS Attack Detection Using Deep Learning Models," IEEE Trans. Network Service Management, 2020.

[2] Kumar S., Patel M., Sharma A., "Hybrid ML for Real-Time DDoS Detection," Journal of Cybersecurity and Digital Forensics, 2019.

[3] Liu Y., Wang Z., Xu H., "DDoS Mitigation Using SVM," Int. Journal of Network Security, 2021.

[4] Reddy P.V.B.R., Tanwar S.G., Meena M., "Survey on ML Techniques for DDoS Detection," IEEE Access, 2021.

[5] Zhang Z., Lin X., Li M., "Random Forest Classifier for Anomaly-Based Detection," Journal of Internet Technology, 2021.