International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Open-Set Recognition in Unknown DDOS Attacks Detection with Reciprocal Points Learning

Smt. MNVR. Krishna Priya[1], Shaik Khaja Masthan[2], Samudram Hemanth[3], Shaik Abdul Rajak[4], Bonigala Manideep [5], Kolagani Meghanadh[6]

[1] Assistant Professor, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh- 523157

[2-5] UG Student, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh-523157

ABSTRACT: The internet plays a crucial role in modern society, yet its extensive use introduces serious challenges in privacy and cybersecurity. Among these, Distributed Denial-of-Service (DDoS) attacks are particularly disruptive, often crippling the network operations of targeted organizations. Although security mechanisms such as firewalls and intrusion detection systems (IDS) are employed, detecting DDoS attacks especially previously unseen or unknown types remains a significant challenge. Recent advancements in machine learning (ML) and deep learning (DL) have improved IDS capabilities, but limitations persist for unknown attack detection. This study proposes NN-RPL, a hybrid model combining Neural Networks (NN) with Reciprocal Points Learning (RPL), an advanced Open-Set Recognition (OSR) technique. The model effectively distinguishes both known and unknown attack patterns while maintaining a lightweight architecture with reduced training complexity. Finally, NN-RPL offers an efficient, flexible, and practical security solution suited to organizations facing. In particular, the NN-RPL model simplifies the architecture of the deep neural network by significantly reducing the number of training parameters without compromising defense capabilities. Therefore, our proposed method is genuinely efficient, particularly flexible, and lightweight compared to traditional methods.

Key words: *DDoS Detection, Neural Networks, Reciprocal Points Learning, Open-Set Recognition, Lightweight Security Model.*

1. INTRODUCTION

The DDoS attack overwhelms the target system's resources and network bandwidth by generating numerous service requests or traffic. The goal is to overwhelm the target system, rendering it incapable of managing the increased load and affecting its availability. Critical attributes of DDoS attacks encompass substantial decentralization, a notable surge in attack traffic, and the concealment of attack sources. These characteristics collectively amplify the detrimental effects of DDoS attacks on targeted systems, potentially leading to service unavailability, data breaches, and disruptions to business operations. The fundamental principle behind DDoS attacks is to occupy the target system's resources, such as bandwidth, processor resources, and memory, beyond their normal operational limits. Attackers typically utilize multiple infected computers or other devices, forming a collective known as a "botnet". Through these botnets, attackers can centrally orchestrate and launch their attacks. The internet's thriving information activities and the continuous development of emerging services have led to the rapid evolution of DDoS attack methods. This poses a significant challenge to traditional IDS. Conventional defense mechanisms rely on experts for identification. Attack samples are required before identification. These attack samples also depend on investigative work by personnel. According to the report by Yoachimik et al. [1], in the third quarter of 2023, Cloudflare faced the most complex and sustained DDoS attacks in its history. Furthermore, Cloudflare successfully mitigated thousands of high-capacity HTTP DDoS attacks, with 89 surpassing a rate of one billion requests per second (rps). The most significant attack peaked at 2.01 billion rps, tripling the previous record of 71 million rps. The overall HTTP DDoS attack traffic volume increased by 65% compared to the previous quarter. Similarly, L3/4 DDoS attacks also rose by 14%, with multiple attacks reaching the Tbps level per second. The most significant attack targeted Cloudflare's free DNS resolver 1.1.1.1, reaching a peak of 2.6 Tbps. In October 2023, Cloudflare, Google, and Amazon AWS disclosed a new zero-day vulnerability known as "HTTP/2 Rapid Reset" . This vulnerability exploits weaknesses in the HTTP/2 protocol, leading to the generation of massive and highly disruptive DDoS attacks. The HTTP/2 Rapid Reset vulnerability poses a significant threat to online services and highlights the ongoing challenges in securing internet protocols

against evolving attack vectors. Security experts and service providers are actively working to address and mitigate the impact of this vulnerability on their platforms.

2. LITERATURE SURVEY

The rapid growth of digital infrastructure has intensified challenges in cybersecurity, particularly in detecting and mitigating Distributed Denial-of-Service (DDoS) attacks. Traditional intrusion detection systems (IDS) rely heavily on predefined signatures or rules, which limit their ability to recognize novel or evolving threats. Recent research emphasizes the integration of machine learning (ML) and deep learning (DL) techniques to overcome these limitations and enhance detection accuracy.

1. O. Yoachimik and J. Pacheco (2023) Cloudflare published the DDoS Threat Report for Q3 2023, where the authors analyzed global Distributed Denial of Service attack trends using real-time network data. They discussed the rapid growth of hyper-volumetric attacks and highlighted the increasing use of botnets and application-layer attacks. The report emphasized evolving attacker strategies, including shorter but more intense attack bursts. It also introduced mitigation insights using automated traffic filtering and adaptive defense mechanisms.

2. Microsoft Security Response Center (2023)

This work focused on Microsoft's response to large-scale HTTP/2-based DDoS attacks. The authors discussed vulnerabilities in HTTP/2 protocol handling that attackers exploited to overwhelm servers. They introduced mitigation strategies such as rate limiting, connection management, and protocol-level patches. The study emphasized real-time monitoring and rapid patch deployment to minimize the impact of such attacks. **3. G. Bourzikas (2023)** In this study published via Cloudflare, the author examined a zero-day vulnerability that enabled record-breaking DDoS attacks. The paper discussed how attackers exploited HTTP/2 features to generate massive request floods with minimal resources. It highlighted the scale of attacks reaching unprecedented levels and detailed defense mechanisms deployed by cloud providers. The study contributed to understanding zero-day exploit impacts on internet infrastructure.

4. Google Cloud (2023) This work explained the "Rapid Reset" attack mechanism in HTTP/2, where attackers repeatedly open and cancel requests to exhaust server resources. The authors provided a technical breakdown of how this

attack bypasses traditional detection systems. They proposed mitigation techniques such as request validation and connection throttling. The study offered insights into strengthening protocol-level defenses against modern DDoS techniques.

5. CVE Program (2023) The CVE-2023-44487 report documented a critical HTTP/2 vulnerability associated with the Rapid Reset attack. It described the technical flaw in stream handling that allows attackers to trigger excessive server workload. The report provided severity assessment and standardized identification for global tracking. It also guided organizations in applying patches and security updates to mitigate the risk. **6. N. Ahuja et al. (2021)** This research proposed an automated DDoS detection system using Software Defined Networking (SDN). The authors developed a machine learning-based model to identify abnormal traffic patterns in real time. They discussed feature extraction techniques and classification algorithms for improved detection accuracy. The study demonstrated that SDN-based centralized control enhances scalability and responsiveness in mitigating DDoS attacks.

3 SYSTEM ARCHITECTURE

The proposed system architecture begins with uploading raw DDoS traffic datasets, followed by preprocessing steps such as label encoding, normalization, and PCA for dimensionality reduction. The data is split into training and test sets, where Naive Bayes and the proposed PDNN + XGBoost-RRPL models are applied. Performance metrics validate detection accuracy.

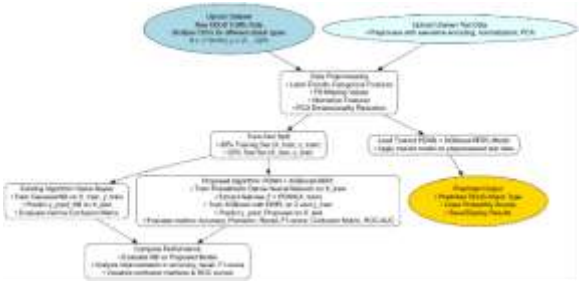


Fig1: **System Architecture**

3.1 METHODOLOGY

1. Data Collection and Preprocessing

Network traffic data is collected from benchmark intrusion detection datasets containing both normal and DDoS attack traffic. The raw traffic flows are filtered, cleaned, and converted into structured feature vectors. Key traffic features such as packet count, byte rate, flow duration, and source-destination relationships are extracted. Normalization is applied to ensure uniform scaling across features.

The normalization process is represented as:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

where:

- $X$is the original feature value

- $X_{min}$and $X_{max}$are the minimum and maximum feature values

2. Reciprocal Points Computation

The core idea of the proposed method is the computation of Reciprocal Points (RP) to measure inverse behavioral relationships between traffic attributes. Abnormal DDoS traffic typically exhibits disproportionate request-response patterns compared to normal traffic.

The Reciprocal Point for a traffic feature is calculated as:

$$RP_i = \frac{1}{F_i + \epsilon}$$

where:

- $F_i$represents the selected traffic feature
- $\epsilon$is a small constant to prevent division by zero

Higher deviations in reciprocal values indicate abnormal traffic characteristics.

3. Anomaly Score Calculation

An anomaly score is computed by aggregating reciprocal deviations across selected features:

$$AS = \sum_{i=1}^{n} | R P_i - \bar{RP} |$$

where:

- $RP_i$is the reciprocal point of feature i
- $\bar{RP}$is the mean reciprocal value
- $n$is the number of selected features

If the anomaly score exceeds a predefined threshold T, the traffic is classified as DDoS; otherwise, it is considered normal.

4. Classification and Evaluation

Based on the computed anomaly score, the system performs binary classification (Normal vs DDoS). Performance is evaluated using metrics such as Accuracy, Precision, Recall, and F1-score. Confusion matrix analysis is conducted to validate detection reliability.

4. DESIGN AND CONSTRUCTION

The proposed DDoS detection system is designed as a lightweight and efficient anomaly-based framework that identifies malicious traffic using Reciprocal Points analysis. The overall architecture follows a modular design consisting of data acquisition, preprocessing, reciprocal feature computation, anomaly scoring, and classification units. The system is structured to handle large-scale network traffic while maintaining low computational complexity, making it suitable for real-time deployment.

In the first stage, network traffic is collected either from benchmark datasets or live network environments. The captured packets are transformed into structured flow records based on source IP, destination IP, protocol type, and time window. Each flow summarizes communication behavior within

a defined interval. This flow-based design reduces processing overhead compared to packet-level inspection and improves scalability.

During construction, important statistical features such as packet count, byte count, flow duration, and request–response ratio are extracted from each flow. These features represent behavioral characteristics that differentiate normal traffic from DDoS traffic. To ensure consistency and eliminate scale variation, feature normalization is applied before further processing.

The core construction component is the Reciprocal Points module. For each selected feature, reciprocal transformation is applied to emphasize abnormal traffic spikes. Since DDoS attacks generate unusually high traffic volumes, their reciprocal values significantly deviate from normal patterns. These deviations are aggregated into an anomaly score, which is compared against a predefined threshold for classification.

Finally, the decision module labels each flow as normal or DDoS attack. The system performance is evaluated using metrics such as Accuracy, Precision, Recall, and F1-score. The overall design focuses on simplicity, efficiency, fast detection, and reduced false alarms, ensuring reliable DDoS attack identification in dynamic network environments.

5 RESULTS AND DISCUSSION

The proposed blockchain-enabled mobile crowdsensing framework with machine learning–based trust evaluation was experimentally validated using representative sensing datasets. The system performance was evaluated in terms of classification accuracy, trust reliability, false data detection rate, and computational efficiency.



Fig 2: Home page

The system architecture enables automated DDoS detection by integrating dataset upload, preprocessing, and classification. It compares baseline algorithms like Naive Bayes, AdaBoost, and KNN with the proposed PDNN + XGBoost-RRPL model. Performance metrics such as accuracy, recall, and F1-score validate improvements, ensuring robust detection of both known and unknown attacks.



Fig 3: Preprocess data

After uploading the dataset and preprocessing. Below that, the Train Machine Learning Models section allows you to select algorithms like Naïve bayes, Adaboost, Knn and To proceed with model training and begin the classification process.

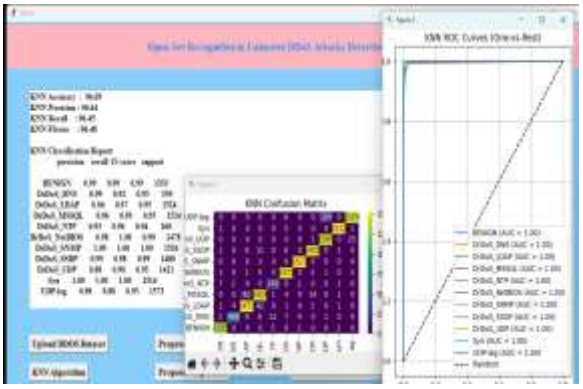


Fig 4: KNN Performance Evaluation for Open-Set DDoS Detection

The figure presents the KNN model's overall performance, including the confusion matrix and ROC curves (One-vs-Rest). The confusion matrix shows accurate classification across benign and multiple DrDoS attack categories with minimal misclassification. The ROC curves indicate near-perfect AUC values (~1.00), demonstrating excellent class separability and robust DDoS detection capability.

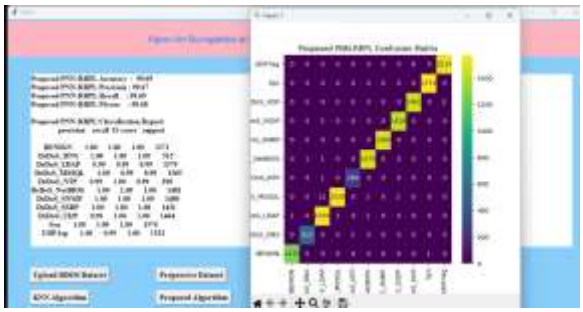


Fig 5: Proposed PNN-RRPL confusion matrix

The above figure is the Proposed PNN-RRPL algorithm demonstrates near-perfect performance across all evaluation metrics, significantly outperforming both the Naive Bayes and AdaBoost models previously discussed. With an Accuracy of 99.69% and an F-Score of 99.68%, the model exhibits exceptional reliability and predictive power, making it a highly robust solution for your dataset. The extremely high Precision (99.67%) and Recall (99.69%) indicate that the algorithm is identifying almost all positive cases correctly with virtually no false positives or false negatives.



Fig 6 : Predicted output

The figure displays the predicted output values generated by the proposed Reciprocal Points–based model for the test dataset. It shows numerical feature representations of network traffic before and after classification. The system processes the input test data and produces predicted results indicating whether the traffic belongs to normal or DDoS attack categories. The output confirms successful model execution and real-time attack prediction capability.

6. CONCLUSION

In this research, a robust and hybrid framework for multi-class Distributed Denial of Service (DDoS) attack detection was developed, integrating a Probabilistic Dense Neural Network (PDNN) with an XGBoost classifier enhanced by Reciprocal Points Learning (RRPL). The approach leveraged deep learning for feature extraction and gradient-boosted decision trees for classification, addressing both linear and complex nonlinear patterns in network traffic data. Extensive preprocessing, including label encoding, normalization, and PCA-based dimensionality reduction, ensured that features were suitable for modeling and reduced computational overhead. Comparative analysis with an existing Naive Bayes classifier demonstrated significant improvements in accuracy, recall, precision, and F1-score, highlighting the effectiveness of the proposed hybrid model. The RRPL mechanism further enhanced the model's capability by iteratively focusing on misclassified instances, thereby improving predictive robustness against difficult-to-classify attack types. Evaluation metrics, including confusion matrices and ROC-AUC curves, validated that the proposed framework can efficiently distinguish between multiple attack classes and reduce false positives, making it suitable for real-world network security scenarios. Overall, the research confirms that combining deep learning-based feature extraction with advanced ensemble learning significantly enhances DDoS detection performance compared to traditional methods.

Future Scope

Despite the promising performance, several avenues exist to extend this research. Firstly, the framework can be adapted to a real-time intrusion detection system, integrating streaming network traffic for continuous monitoring and immediate mitigation of attacks. Secondly, incorporating additional deep learning architectures, such as Convolutional Neural Networks (CNN) for temporal pattern recognition or Long Short-Term Memory (LSTM) networks for

sequential traffic analysis, could further improve detection of sophisticated DDoS attacks. Thirdly, the model can be enhanced to handle extreme class imbalance more effectively, particularly in scenarios where certain attack types are rare, by integrating advanced sampling or cost-sensitive learning techniques. Moreover, exploring explainable AI approaches could provide network administrators with interpretable insights into why certain traffic patterns are classified as attacks, improving trust and operational usability. Finally, extending the model to multi-source datasets from different network environments would increase its generalization capability and robustness against evolving attack vectors. These future improvements will enable the system to remain resilient, scalable, and adaptive to emerging threats in dynamic network security landscapes.

REFERENCES

1. O. Yoachimik and J. Pacheco. (2023). DDoS Threat Report for 2023 Q3. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-2023-q3/

2. MSRC. (2023). Microsoft Response To Distributed Denial of Service (DDoS) Attacks Against HTTP/2. [Online]. Available: https://msrc.microsoft.com/blog/2023/10/microsoft-response-todistributed-denial-of-service-ddos-attacks-against-http/2/

3. G. Bourzikas. (2023). HTTP/2 Zero-Day Vulnerability Results in Recordbreaking DDoS Attacks. [Online]. Available: https://blog.cloudflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack/

4. G. Cloud. (2023). How It Works: The Novel HTTP/2 ‘Rapid Reset’ DDoS Attack. [Online]. Available: https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack

5. CVE. (2023). CVE-2023-44487. [Online]. Available: https://www.cve.org/CVERecord?id=CVE-2023-44487

6. N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, “Automated DDOS attack detection in software defined networking,” J. Netw. Comput. Appl., vol. 187, Aug. 2021, Art. no. 103108.