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

Peer Reviewed, Referred & Indexed Journal

Intelligent Detection of Unknown DDoS Attacks through Open Set Recognition and Reciprocal Points Learning

[1]K.Gowtham Raju,[2]R.Harsha Vardhan,[3]T.Sirisha,[4]K.Manoj Kumar,[5]J.Sathvik

[1]Assistant Professor, Department of Computer Science & Engineering, Eluru College of Engineering and Technology

[2,3,4,5] B. Tech Student, Department of Computer Science & Engineering, Eluru College of Engineering and Technology

ABSTRACT

Distributed Denial of Service (DDoS) attacks continue to evolve in complexity and scale, making traditional closed-set intrusion detection systems ineffective against previously unseen attack patterns. Conventional machine learning models assume that all possible attack classes are known during training, which limits their ability to detect novel or zero-day DDoS attacks. To address this limitation, this study proposes an Open Set Recognition (OSR) framework for unknown DDoS attack detection using Reciprocal Points Learning (RPL). The proposed approach enhances the model's ability to distinguish between known traffic patterns and unseen malicious behaviors by learning compact decision boundaries and representative reciprocal points in feature space. By integrating deep feature extraction with reciprocal representation learning, the system effectively identifies unknown attack instances while maintaining high classification accuracy for known classes. Experimental evaluation on benchmark network intrusion datasets demonstrates improved detection performance, reduced false positives, and strong generalization capability compared to traditional closed-set models. The proposed framework provides a robust and scalable solution for next-generation intelligent network security systems capable of handling evolving cyber threats.

Keywords: Distributed Denial of Service (DDoS), Open Set Recognition (OSR), Reciprocal Points Learning (RPL), Unknown Attack Detection, Network Intrusion Detection, Deep Feature Extraction, Cybersecurity, Machine Learning.

INTRODUCTION

With the rapid growth of internet-based services, cloud computing, and IoT devices, network infrastructures have become increasingly vulnerable to cyber threats. Among these threats, Distributed Denial of Service (DDoS) attacks remain one of the most destructive and frequently occurring attacks in modern networks. DDoS attacks aim to overwhelm a target server, service, or network with massive volumes of malicious traffic, thereby disrupting normal operations and causing significant financial and reputational damage. As attackers continuously develop new strategies and traffic patterns, detecting these evolving threats has become a major challenge for traditional security systems.

Conventional intrusion detection systems (IDS) and machine learning-based approaches typically operate under a closed-set assumption, meaning that all possible attack categories are known during the training phase. However, in real-world scenarios, new and unknown DDoS variants frequently emerge, making closed-set models ineffective in identifying previously unseen attack patterns. These systems often misclassify unknown attacks as normal traffic or as known attack types, leading to

reduced detection accuracy and increased security risks.

To overcome this limitation, Open Set Recognition (OSR) has gained attention in recent years. OSR enables models to not only classify known categories but also identify and reject unknown or unseen instances. By incorporating OSR into DDoS detection, security systems can better handle zero-day attacks and novel traffic behaviors. In this context, Reciprocal Points Learning (RPL) provides an effective mechanism for learning compact class boundaries in the feature space. RPL introduces representative reciprocal points that help distinguish known classes from unknown samples by enforcing tighter decision margins and improving feature discrimination.

I. LITERATURE SURVEY

1. Open Set Recognition in Cybersecurity

Recent research emphasizes the importance of Open Set Recognition (OSR) in cybersecurity applications, particularly for handling unknown and zero-day attacks. Traditional classifiers operate under closed-set assumptions, which limit their ability to detect unseen threats. Bendale and Boult (2016) introduced the concept of open space risk and proposed methods to identify unknown classes effectively. Their work laid the foundation for applying OSR techniques in intrusion detection systems to improve robustness against evolving cyber threats.

2. Machine Learning-Based DDoS Detection

Machine learning approaches such as Support Vector Machines (SVM), Random Forest, and Deep Neural Networks have been widely used for DDoS attack detection. Studies show that deep learning models can automatically extract complex traffic patterns and achieve higher detection accuracy compared to traditional rule-based systems. However, these models typically assume that all attack types are known during training, making them vulnerable to new and unknown DDoS variants.

3. Deep Learning for Network Intrusion Detection

Recent advancements in deep learning, including Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, have significantly improved intrusion detection performance. Researchers have demonstrated that deep architectures can capture temporal and spatial traffic characteristics effectively. Despite their high accuracy, most deep learning models still follow a closed-set classification framework and struggle with unseen attack patterns.

4. Reciprocal Points Learning (RPL) for Open Set Classification

Reciprocal Points Learning has emerged as a promising approach for open set classification. RPL introduces representative reciprocal points in feature space to create compact decision boundaries and reduce open space risk. This technique enhances the model's ability to distinguish known classes from unknown samples. Studies applying RPL in image and pattern recognition domains show improved rejection of unseen classes, indicating its potential in cybersecurity applications.

5. Open Set Intrusion Detection Systems

Several recent works focus on integrating OSR techniques into intrusion detection systems to address zero-day attack challenges. Approaches such as threshold-based rejection mechanisms, distance-based classifiers, and generative modeling have been explored. These studies report improved detection of unknown attacks and reduced false positives. However, there is still a need for more robust and scalable frameworks specifically designed for unknown DDoS attack detection using advanced representation learning methods like RPL.

II. EXISTING SYSTEM

The existing DDoS detection systems mainly rely on traditional Intrusion Detection Systems (IDS) and closed-set machine learning models. These systems are trained using predefined attack categories and assume that all possible attack types are known during the training phase. Signature-based detection methods compare incoming traffic patterns with stored attack signatures, which makes them ineffective against new or modified DDoS attacks. Anomaly-based detection techniques attempt to identify deviations from normal traffic behavior, but they often produce high false positive rates.

Machine learning models such as Support Vector Machines, Random Forest, and Deep Neural Networks have improved detection accuracy for known DDoS attacks. However, these models operate under a closed-set assumption and cannot properly handle unknown or zero-day attacks. When unfamiliar traffic patterns appear, the system tends to misclassify them as either normal traffic or one of the known attack classes. This limitation reduces the reliability of the security framework in real-world dynamic network environments.

Therefore, existing systems lack the capability to effectively recognize and reject previously unseen DDoS attack patterns, highlighting the need for open set recognition-based solutions.

III. PROPOSED SYSTEM

The proposed system introduces an Open Set Recognition (OSR) framework for detecting unknown DDoS attacks using Reciprocal Points Learning (RPL). Unlike traditional closed-set models, the proposed approach is designed to identify both known and previously unseen attack patterns in dynamic network environments. The system focuses on learning discriminative feature representations that help separate known traffic classes from unknown malicious activities.

First, network traffic data is collected and preprocessed to remove noise, normalize features, and extract relevant traffic characteristics. Feature engineering techniques are applied to capture statistical and behavioral properties of network flows. These processed features are then fed into a deep learning-based feature extraction model to generate high-level representations of traffic patterns.

The core component of the proposed system is Reciprocal Points Learning. RPL introduces representative reciprocal points in the feature space for each known class. These reciprocal points help create compact decision boundaries, reducing open space risk and improving the system's ability to reject unknown samples. If a traffic instance falls far from the learned class boundaries, it is classified as an unknown attack rather than being forced into a known category.

IV. SYSTEM ARCHITECTURE

The Open Set DDoS Detection System using Reciprocal Points Learning (RPL) architecture begins with network traffic data collected from network devices such as servers, routers, and cloud systems. This raw traffic data first undergoes data preprocessing, where noise and irrelevant information are removed and features are scaled to improve data quality and model performance. After preprocessing, the system performs feature extraction using a deep learning model, which automatically learns important patterns and representations from the network traffic data. These extracted features are then passed to the Reciprocal Points Learning (RPL) module, which learns compact class boundaries for known traffic types and represents them using reciprocal points in the feature space. This helps the model clearly distinguish between known attack

patterns and unfamiliar behaviors. The open set classification stage then analyzes incoming samples and determines whether they belong to a known attack class or represent an unknown or zero-day attack. Finally, when a malicious or suspicious activity is detected, the system triggers alerts and mitigation actions, such as notifying administrators, blocking suspicious traffic, or activating security mechanisms, thereby enhancing the network's ability to defend against evolving DDoS threats.

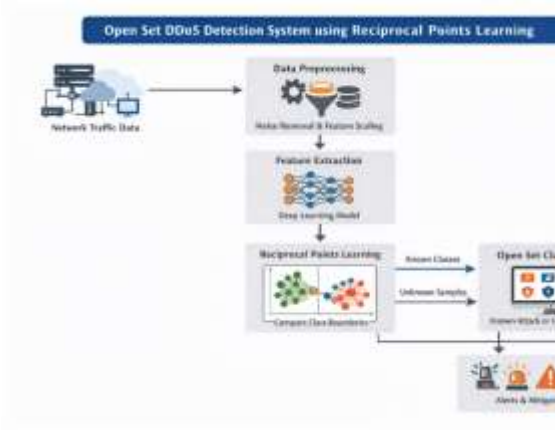

Fig 5.1: Structure of the Proposed System

V. IMPLEMENTATION

Fig 6.1: Home Page

Fig 6.2: Model Training Page

Fig 6.3: Comparison Graph

Fig 6.4: Prediction inputs Page

Fig 6.5: Result Page

VI. CONCLUSION

The proposed system for Intelligent Detection of Unknown DDoS Attacks through Open Set Recognition and Reciprocal Points Learning demonstrates a significant advancement in modern cybersecurity defense mechanisms. Traditional intrusion detection systems often struggle to identify previously unseen or unknown attack patterns, especially in dynamic network environments. By integrating Open Set Recognition (OSR) with Reciprocal Points Learning, the system can effectively distinguish between known network traffic patterns and previously unseen malicious activities.

The approach enhances the detection capability by allowing the model to classify unknown attack behaviors instead of forcing them into predefined categories. This reduces misclassification and improves overall detection accuracy. Additionally, the system leverages machine learning techniques to analyze traffic patterns, identify anomalies, and respond to suspicious activities in real time.

The implementation of this intelligent detection framework contributes to stronger network resilience, improved threat identification, and proactive mitigation of distributed denial-of-service (DDoS) attacks. By enabling more adaptive and intelligent network monitoring, the proposed solution supports secure digital infrastructures and helps organizations protect critical systems from evolving cyber threats.

VII. FUTURE SCOPE

Future research can focus on extending the proposed framework by integrating advanced deep learning architectures such as transformer-based models and graph neural networks to improve detection accuracy and adaptability in large-scale network environments. These models may better capture complex traffic relationships and evolving attack strategies.

Another promising direction is the integration of federated learning to enable collaborative training across distributed network environments while preserving data privacy. This approach would allow multiple organizations to improve attack detection models without sharing sensitive network data directly.

Furthermore, incorporating edge computing could enhance real-time detection capabilities by processing network traffic closer to the data source, thereby reducing latency and improving response time during active attacks.

Future work may also explore the use of blockchain-based frameworks to ensure secure and transparent logging of network events, which can enhance trust and auditability in cybersecurity systems.

Additionally, the system can be improved by incorporating adaptive adversarial training techniques to increase resilience against sophisticated attack strategies designed to evade detection systems. Continuous evaluation with real-world network datasets and deployment in hybrid or multi-cloud infrastructures will also be crucial to validate the scalability and robustness of the proposed solution.

Overall, these enhancements can make the

intelligent detection framework more scalable, secure, and effective in combating emerging and unknown DDoS attack patterns in modern network ecosystems.

VIII. REFERENCES

[1] K. G. Liakos, P. Busato, D. Moshou, S. Pearson, and D. Bochtis, "Machine learning applications and techniques in network security and intrusion detection: A review."
[2] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in IEEE Symposium on Security and Privacy, 2010.
[3] A. Bendale and T. Boult, "Towards open set deep networks," in IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.
[4] C. Geng, S. Huang, and S. Chen, "Recent advances in open set recognition: A survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021.
[5] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, 2018.
[6] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," in Network and Distributed System Security Symposium (NDSS), 2018.
[7] W. Wang, Y. Sheng, J. Wang, et al., "HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks for intrusion detection," IEEE Access, 2017.
[8] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in International Conference on Information Systems Security and Privacy (ICISSP), 2018.
[9] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
[10] T. Boult and A. Bendale, "Open world recognition," in IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017.