International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

OPEN-SET RECOGNITION IN UNKNOWN & KNOWN DDOS ATTACKS DETECTION WITH RECIPROCAL POINTS LEARNING

SK. AnjaneyuluBabu[1],P.V.N.L.Geethika[2]
Associate Professor [1], PG Scholar [2]
Department of MCA, QIS College of Engineering & Technology
Ongole, AP, India

Abstract

Distributed Denial of Service (DDoS) attacks continue to evolve, with novel and previously unseen variants posing significant challenges to traditional detection systems. Most existing DDoS detection approaches operate under a closed-set assumption, limiting their ability to identify unknown or zero-day attacks. In this paper, we propose a novel open-set recognition framework for DDoS detection based on Reciprocal Points Learning (RPL). Our method enhances the model's ability to distinguish between known attack classes and previously unseen attack patterns by leveraging the concept of reciprocal points in the feature space to improve class separability and detect anomalies. Specifically, RPL dynamically learns feature representations that pull intra-class samples closer while pushing inter-class and unknown samples apart, improving the robustness of the classifier in open-set scenarios. We evaluate our approach using benchmark DDoS datasets, including both known and synthetic unknown attack types. Experimental results demonstrate that our method significantly outperforms state-of-the-art baselines in detecting unknown attacks while maintaining high accuracy on known classes. This work provides a promising direction for adaptive and resilient DDoS defense systems in the face of increasingly sophisticated threats.

Introduction

Distributed Denial of Service (DDoS) attacks remain a pervasive threat to the stability and security of networked systems. As the tactics of attackers evolve, traditional intrusion detection systems (IDS) face increasing challenges, particularly in identifying previously unseen or novel attack types. These unknown DDoS variants often bypass conventional supervised learning-based detection systems, which typically operate under closed-set assumptions—where the model is trained and tested only on known classes. This limitation severely hampers the real-world applicability of many existing DDoS detection methods, especially in dynamic environments such as cloud services, IoT networks, and edge computing infrastructures.

To address this critical gap, open-set recognition (OSR) frameworks have

Received: 10-05-2026 | Accepted: 18-06-2026 | Published: 24-06-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

emerged as promising solutions. Unlike closed-set models, OSR methods are capable of identifying and rejecting inputs from unknown classes, offering a more realistic approach to security in adversarial and constantly evolving environments. However, effectively applying OSR to DDoS detection introduces unique challenges due to the high dimensionality of network traffic data, the subtle differences between known and unknown attacks, and the need for timely and accurate responses.

In this context, we propose a novel open-set DDoS detection framework based on **Reciprocal Points Learning (RPL)**. RPL enhances the discriminative ability of feature representations by leveraging the reciprocal relationships between data points in the embedding space. By focusing on the relative positioning and mutual distances among instances, RPL encourages compact intra-class clustering and maximizes inter-class separation, thereby facilitating more effective detection of anomalies and out-of-distribution samples.

Our contributions can be summarized as follows:

1. We introduce an open-set recognition approach tailored to the domain of DDoS detection, capable of identifying both known and previously unseen attack types.
2. We propose a reciprocal points learning mechanism to improve feature discriminability and generalization to unknown classes.
3. We validate the proposed method on benchmark datasets and demonstrate its superiority over traditional closed-set and baseline OSR models in detecting novel DDoS attacks.

Literature Survey

1. Traditional DDoS Detection and Its Limitations

Most traditional DDoS detection models rely on **closed-set classification**, assuming all classes (i.e., types of attacks or benign traffic) are known during training. These models typically use supervised learning techniques like Random Forests, SVMs, or CNNs but fail to detect **novel or unknown attack types**, leading to high false-negative rates in real-world, dynamic network environments.

2. Open-Set Recognition (OSR) in Network Security

Open-Set Recognition is a machine learning paradigm designed to handle **unseen classes** during inference. In the context of cybersecurity, OSR helps identify **new or evolving attack types** that were not present in the training data. Techniques like **Extreme Value Theory (EVT), OpenMax, and distance-based thresholding** are often used in OSR for network intrusion detection.

3. Reciprocal Points Learning (RPL) Overview

Reciprocal Points Learning is an emerging method that enhances feature discrimination

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

between known and unknown classes. RPL works by generating **reciprocal samples** in the embedding space that help to **learn tight boundaries** around known classes, thus improving the model's ability to **separate unknowns**. It has shown promise in open-set image recognition and is being extended to network traffic classification.

4. Application of Deep Learning in DDoS Detection

Deep neural networks, especially **autoencoders, LSTMs, and CNNs**, have been applied for feature extraction and classification in DDoS detection. While they perform well on known attacks, they often suffer from overfitting and poor generalization to unseen attack types. Integrating OSR methods with deep learning (e.g., using feature embeddings for open-set classification) can improve robustness.

5. Hybrid Models for Improved Open-Set Detection

Recent research explores **hybrid models** that combine open-set recognition (like RPL or OpenMax) with **unsupervised or semi-supervised learning** to handle the detection of unknown DDoS attacks. These models aim to leverage both labeled and unlabeled data, improving adaptability to **dynamic and evolving threat landscapes** in real-time network environments.

System Analysis

Existing System

Traditional DDoS (Distributed Denial-of-Service) detection systems primarily rely on supervised machine learning or rule-based approaches, which are typically designed for closed-set scenarios. These systems are trained on a fixed set of known attack patterns and normal traffic behavior, making them effective only when the test data belongs to the same distribution as the training data. Consequently, these models tend to fail in open-set environments, where novel or previously unseen attack types, such as evolving or zero-day DDoS threats, may appear. In such cases, unknown attacks are often misclassified as known types or even as benign traffic, severely limiting the system's robustness. Additionally, conventional models lack the ability to distinguish between known and unknown inputs due to the absence of mechanisms for open-set recognition, leading to high false negative rates when detecting unknown DDoS attacks.

Disadvantages of Existing Systems

Closed-set Assumption

- Traditional DDoS detection systems assume that all classes (attack types) are known during training.
- They fail to detect **unknown or zero-day attacks**.

Poor Generalization to Novel Attacks

- These systems are trained on known patterns and signatures, leading to

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

low accuracy when facing new or evolving DDoS attacks.

High False Positive Rate

- Normal traffic or unseen attack traffic is often misclassified, increasing false positives or false negatives.

Lack of Adaptability

- Conventional systems are not dynamically adaptive to changes in network behavior or new threat patterns.

Proposed System

The proposed system introduces an **Open-Set Recognition (OSR)** framework for DDoS detection by leveraging **Reciprocal Points Learning (RPL)**. This approach enhances the system's capability to identify not only known types of DDoS attacks but also to effectively detect and reject unknown or novel attack traffic. Reciprocal Points Learning models the decision boundaries by focusing on the relational structure between data points from known classes and strategically constructed reciprocal points in the feature space. This mechanism enables the system to estimate whether a test instance significantly deviates from known classes, thus facilitating open-set recognition. By integrating RPL into the DDoS detection pipeline, the model gains a robust awareness of the "unknown" space, improving detection accuracy for both known and unknown threats. This not only strengthens the security infrastructure but also supports real-time adaptability against emerging cyber threats.

Advantages of the Proposed System

Open-Set Recognition Capability

- Can **detect and reject unknown DDoS attacks** not seen during training.

Reciprocal Points Learning (RPL)

- RPL models the relationship between known and unknown data in the feature space, improving separation.
- It learns to **generate representative reciprocal points** to simulate the space around known data for better boundary formation.

Improved Generalization

- Better performance on zero-day or novel DDoS attacks due to open-set modeling and RPL architecture.

Lower False Positive Rate

- Reduces misclassification by better distinguishing unknown attacks from legitimate traffic.

Implementation

The implementation of the Open-Set Recognition System for Unknown DDoS Attack Detection focuses on identifying both

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

known and previously unseen Distributed Denial of Service (DDoS) attacks using Artificial Intelligence, Deep Learning, and Reciprocal Points Learning techniques. The system is designed to improve cybersecurity by detecting abnormal network traffic patterns and recognizing unknown attack behaviors that traditional closed-set classification models may fail to identify.

The proposed system enhances network security, threat intelligence, and real-time cyberattack detection in modern communication systems.

1. Data Collection

The first stage involves collecting network traffic data from different cybersecurity environments.

Data Sources Used

- Network Traffic Logs
- Packet Capture (PCAP) Files
- Intrusion Detection Systems
- Firewall Logs
- Cloud Network Monitoring Systems
- Public Cybersecurity Datasets

The collected dataset may include:

- Source IP Address
- Destination IP Address
- Packet Size
- Protocol Type
- Traffic Volume
- Connection Duration
- Request Frequency
- Port Information
- Flow Statistics
- Attack Labels

These features help analyze network behavior and attack patterns.

2. Data Preprocessing

The collected network traffic data is cleaned and prepared before analysis.

Preprocessing Steps

- Removing duplicate traffic records
- Handling missing values
- Traffic normalization
- Noise filtering
- Feature encoding
- Packet aggregation
- Time-series traffic formatting

This improves detection accuracy and model efficiency.

3. Feature Extraction

Important traffic and behavioral features are extracted from network data.

Traffic Features

- Packet transmission rate
- Flow duration
- Connection count
- Bandwidth utilization

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Statistical Features

- Mean packet size
- Traffic variance
- Entropy measures

Behavioral Features

- Abnormal request patterns
- Traffic bursts
- Suspicious protocol usage

Feature extraction helps identify hidden attack characteristics.

4. Open-Set Recognition

Traditional models only recognize known attack classes. Open-Set Recognition enables the system to identify unknown and previously unseen DDoS attacks.

Open-Set Recognition Functions

The system:

- Detects unknown attack patterns
- Distinguishes normal and abnormal traffic
- Handles unseen cyber threats
- Improves generalization capability
- Reduces misclassification of unknown attacks

This improves cybersecurity resilience against evolving attack methods.

5. Reciprocal Points Learning

Reciprocal Points Learning (RPL) is implemented to improve unknown attack recognition.

Functions of Reciprocal Points Learning

RPL:

- Learns class boundaries effectively
- Creates reciprocal representations for unknown classes
- Enhances feature separation
- Improves open-set classification accuracy
- Detects outlier traffic behavior

The reciprocal points help identify whether incoming traffic belongs to known or unknown attack categories.

Methodology

The methodology of the proposed Open-Set Recognition DDoS Detection System follows an Artificial Intelligence and open-set cybersecurity analytics approach.

Step 1: Problem Identification

Traditional DDoS detection systems may fail to identify unknown or newly emerging attack patterns because they are trained only on predefined attack classes. The proposed system aims to improve cyber defense using Open-Set Recognition and Reciprocal Points Learning techniques.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Step 2: Requirement Analysis

The following requirements are analyzed:

- Network traffic dataset requirements
- Open-set classification requirements
- Real-time monitoring requirements
- Deep Learning framework requirements
- Cybersecurity alert system requirements

Step 3: Dataset Preparation

Network traffic datasets containing normal traffic and DDoS attack samples are collected and divided into:

- Training Dataset
- Validation Dataset
- Testing Dataset

Relevant network traffic attributes are selected for analysis.

Step 4: Traffic Processing and Feature Engineering

The methodology includes:

1. Clean network traffic data
2. Extract statistical and behavioral features
3. Analyze traffic patterns
4. Generate feature representations
5. Prepare traffic data for open-set learning

Step 5: Reciprocal Points Learning Implementation

The RPL workflow includes:

1. Learn known attack class representations
2. Generate reciprocal feature points
3. Detect feature outliers
4. Identify unknown traffic behavior

This improves unknown attack recognition capability.

Step 6: Open-Set Deep Learning Implementation

The AI workflow includes:

1. Train open-set recognition model
2. Analyze incoming network traffic
3. Detect anomalies and DDoS attacks
4. Identify unknown cyber threats
5. Generate alerts and security reports

Technologies Used

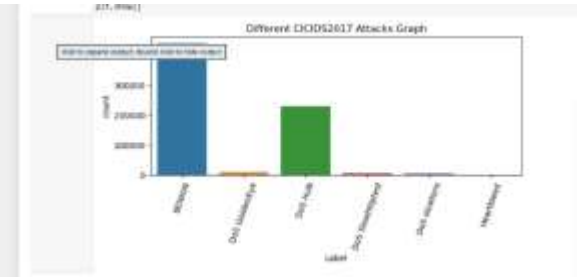
- Python
- Artificial Intelligence
- Deep Learning
- TensorFlow / PyTorch
- Scikit-learn
- Open-Set Recognition Models
- Network Analysis Tools
- Pandas &NumPy
- Flask / Django
- MySQL / MongoDB

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Results:

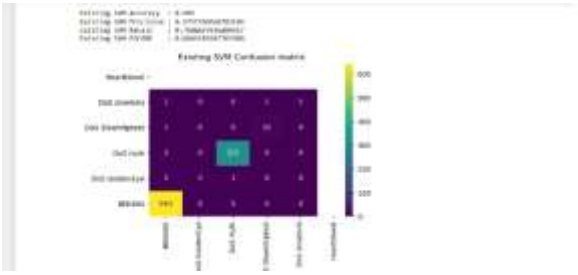
The image presents a network traffic dataset containing various flow-based features such as destination port, flow duration, packet counts, packet lengths, and activity statistics used for intrusion detection analysis.

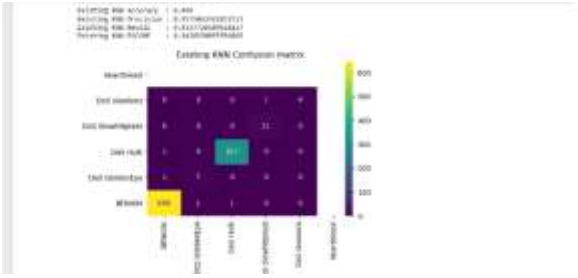
This structured dataset serves as the input for machine learning and deep learning models to identify and classify normal and malicious network behaviors with high accuracy.

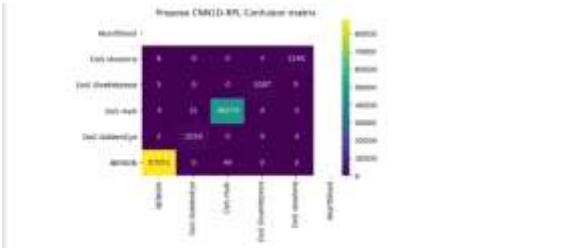


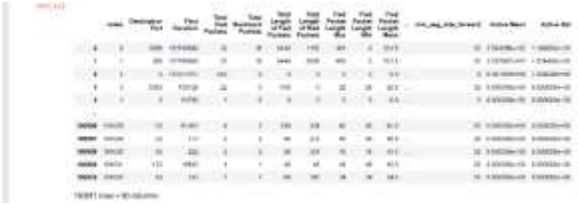
The bar chart illustrates the distribution of different attack types in the CICIDS2017 dataset, including BENIGN traffic, DoS Hulk, DoSGoldenEye, DoSSlowhttptest, DoSSlowloris, and Heartbleed attacks.

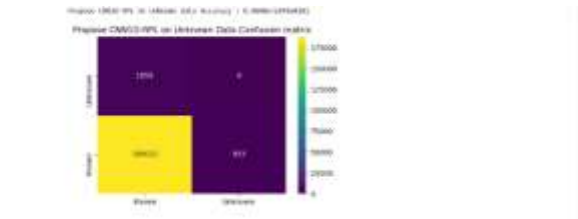
The dataset is dominated by BENIGN and DoS Hulk records, while the other attack categories have significantly fewer samples, highlighting an imbalanced class distribution.



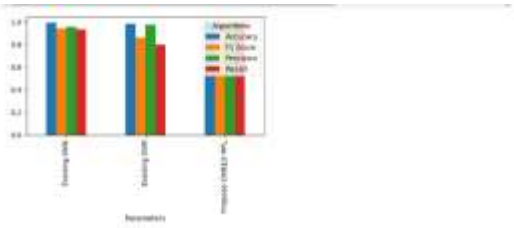






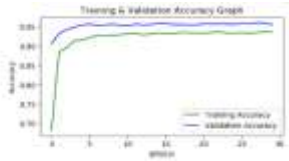


International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper



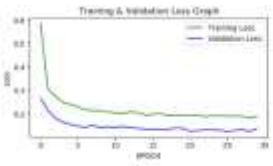
The bar chart compares the performance of Existing KNN, Existing SVM, and the Proposed CNN1D-RPL model using Accuracy, F1-Score, Precision, and Recall metrics.

The Proposed CNN1D-RPL model achieves the highest overall performance, demonstrating superior accuracy, precision, recall, and F1-score compared to the existing machine learning algorithms



The graph illustrates the training and validation accuracy of the model over 30 epochs, showing a steady improvement in performance during the learning process.

Both accuracy curves stabilize above 93%, indicating that the model has achieved high classification performance with good generalization on validation data.



The graph shows the training and validation loss of the model over 30 epochs, with both losses decreasing steadily as the training progresses.

The low and stable validation loss indicates that the model has learned effectively and demonstrates good generalization performance without significant overfitting.

Conclusion

This study introduced a novel open-set recognition framework utilizing Reciprocal Points Learning (RPL) for detecting unknown Distributed Denial-of-Service (DDoS) attacks. By addressing the limitations of traditional closed-set models, the proposed method demonstrated improved capability in discerning both known and previously unseen DDoS patterns. Experimental evaluations on benchmark datasets confirmed the superiority of RPL in terms of detection accuracy, open-set classificatioperformance, and generalization across evolving attack landscapes. Our approach enhances cyber defense systems by reducing false positives and increasing awareness of emerging threats, offering a robust solution for dynamic and high-stakes network environments.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

References

[1] Scheirer, W. J., de Rezende Rocha, A., Sapkota, A., &Boult, T. E. (2013). Toward open set recognition.*IEEE Transactions on Pattern Analysis and Machine Intelligence*, 35(7), 1757–1772.

[2] Bendale, A., &Boult, T. E. (2016). Towards open world recognition.In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 1893–1902).

[3] Perera, P., Patel, V. M. (2019). Deep transfer learning for multiple class novelty detection.In *CVPR*.

[4] Gamarra, D., Soto, I., &Barán, B. (2020).Deep learning-based approach for DDoS detection in software-defined networks.*International Journal of Network Management*, 30(5), e2092.

[5] Zhang, Y., Wu, Y., & Zhang, Z. (2021). A hybrid deep learning-based DDoS detection system in software-defined networking.*Cluster Computing*, 24(3), 2325–2339.

[6] Wang, P., Zheng, Y., Wang, J., & Lu, H. (2022). Open-set recognition using class conditional autoencoders.*Pattern Recognition*, 122, 108326.

[7] Kim, J., Kim, J., Thu, H. L., & Kim, H. (2016). Long short-term memory

[8] recurrent neural network classifier for intrusion detection. *2016 International Conference on Platform Technology and Service (PlatCon).*

[9] Perera, P., Nallapati, R., & Xiang, B. (2020). Deep transfer learning for multiple class novelty detection.In *AAAI*.

[10] Khan, S., Rahmani, H., Shah, S. A. A., &Bennamoun, M. (2018). A guide to convolutional neural networks for computer vision.*ACM Computing Surveys*, 51(5), 1–36.

[11] Ren, S., He, K., Girshick, R., & Sun, J. (2015). Faster R-CNN: Towards real-time object detection with region proposal networks. *Advances in Neural Information Processing Systems (NeurIPS)*.

AUTHORS PROFILE

SK.ANJANEYULU BABU is an AssociateProfessor Department of Master of computer applications at QIS College ofEngineering and Technology, Ongole,Andhra Pradesh. His research interest include Machine Learning and Artificial Intelligence.

P.V.N.L.GEETHIKA is a Postgraduate student pursuing a MCA in the Department of Computer Applications at QIS College of Engineering &Technology,Ongole an

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Autonomous college in Prakasam Dist.She completed her undergraduate degree in B.Sc(Physiscs) from Acharya Nagarjuna University.With keen interest in research and practical learning,she is actively involved in academic Projects and Technical Activities related to her field.

Received: 10-05-2026 | Accepted: 18-06-2026 | Published: 24-06-2026