IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, March 2026
Impact Factor: 8.2

Hybrid Stacked MemoryNet–CNN with Reciprocal Points Learning for Open-Set Recognition in Unknown DDoS Attack Detection

Mantest Patil, Saahini Pasham, B. Mahathi Reddy, T. Chakradhar
Assistant Professor, Dept of CSE, CMR Technical Campus, Hyderabad, India
Dept of CSE, CMR Technical Campus, Hyderabad, India

Abstract: *Distributed Denial of Service (DDoS) attacks continue to pose a critical threat to network infrastructure, with attackers continuously innovating novel attack methodologies that evade conventional detection systems. Traditional machine learning and deep learning models trained in a closed-set paradigm fail to generalize to previously unseen attack forms encountered in real-world deployments. This paper proposes an Open-Set Recognition (OSR) framework integrating Reciprocal Points Learning (RPL) with a one-dimensional Convolutional Neural Network (CNN1D) architecture, employing Parametric ReLU (PReLU) activations to enhance generalization and mitigate overfitting. The system is evaluated on the CICIDS2017 dataset, using Wednesday traffic for known attack training and Friday traffic for unknown attack testing. Benchmark comparisons against Support Vector Machine (SVM) and K-Nearest Neighbors (KNN) classifiers demonstrate the superiority of the proposed CNN1D-RPL model, achieving 99.93% accuracy on known attacks and approximately 99% accuracy on unknown attack identification. The proposed framework establishes a robust, scalable, and adaptive intrusion detection mechanism capable of addressing the open-set challenge in real- world cybersecurity environments.*

Keywords: DDoS Detection, Open-Set Recognition, Reciprocal Points Learning, CNN1D, Deep Learning, Intrusion Detection System, CICIDS2017, PReLU, Cybersecurity, Unknown Attack Detection.

I. 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.

According to the report by Yoachimik et al., in the third quarter of 2023, Cloudflare faced the most complex and sustained DDoS attacks in its history. 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. Traditional deep learning and machine learning models in DDoS detection systems tend to deal with Closed-Set training data. That means when the model in the training phase only encounters known attack types and normal traffic, its performance is usually quite good. Nevertheless, when these models encounter previously unseen attack forms or significantly

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, March 2026 Impact Factor: 8.2

different network traffic in real-world applications, their performance is often limited, especially when facing Open-Set data in real-life scenarios.

This phenomenon has created a demand for improving the generalization capability and practicality of DDoS attack detection systems. In real-world network environments, attackers continually innovate and develop new attack methods, which may make it difficult for traditional Closed-Set training models to cope with unknown attack forms. Therefore, this research is motivated to enhance existing DDoS attack detection systems to make them more adaptable to unknown attacks, thereby improving the accuracy and performance of the models when dealing with Open-Set data.

The primary objectives of this work are: (a) to design an OSR-based deep learning framework for detecting both known and unknown DDoS attacks; (b) to integrate RPL with a CNN1D architecture to measure feature distance and identify unknown threats; (c) to enhance model generalization using PReLU to prevent overfitting; (d) to compare traditional ML classifiers (SVM, KNN) with the proposed CNN1D-RPL model; and (e) to evaluate the approach using the CICIDS2017 dataset achieving high detection accuracy on both known and unknown attacks.

II. LITERATURE SURVEY

A. SDN-Based DDoS Detection

Ahuja et al. [2] proposed an automatic attack detection system for Software-Defined Networking (SDN), comprising preprocessing, feature selection using an Adaptive Walrus Optimization Algorithm (AWaOA), and classification using an Enhanced Long Short-Term Memory (ELSTM) model. The SDN centralized controller, while offering enhanced network control, remains vulnerable to DDoS threats, and this work addresses that challenge through a structured machine learning pipeline.

B. Lightweight Deep Learning for DDoS

Scott-Hayward et al. [3] presented LUCID, a practical lightweight deep learning DDoS detection system exploiting CNNs to classify traffic flows as malicious or benign. LUCID introduced a dataset-agnostic preprocessing mechanism and achieved state-of-the-art detection accuracy with a 40x reduction in processing time, proving suitable for resource-constrained operational environments.

C. Gradient Boosting and Ensemble Methods

Bansal and Kaur [4] employed extreme gradient boosting (XGBoost) for detecting Denial-of-Service attacks, comparing performance against AdaBoost, Naive Bayes, MLP, and KNN classifiers. Results demonstrated XGBoost efficiency and robustness for multi-classification problems on network traffic data captured by the Canadian Institute of Cybersecurity (CIC).

D. Dataset Quality and Benchmarks

Liu et al. [5] conducted a critical review of CIC-IDS-2017 and CIC-CSE-IDS-2018, reporting numerous undocumented errors in attack orchestration, feature generation, and labeling. This underscores the importance of dataset vigilance and transparency in intrusion detection research benchmarks.

E. Open-Set Recognition and RPL

Chen et al. [8] formulated the open space risk problem from the perspective of multi-class integration and proposed Adversarial Reciprocal Point Learning (ARPL). Each reciprocal point is learned by the extra-class space with the corresponding known category, and an adversarial margin constraint is proposed to reduce open space risk. This seminal work forms the theoretical foundation for the proposed CNN1D-RPL approach in this paper.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, March 2026
Impact Factor: 8.2

F. IoT and Unknown Attack Detection

Nguyen and Le [7] combined a soft-ordering CNN model with local outlier factor and isolation-based anomaly detection to address unknown attacks in IoT networks. Their hybrid model achieved high F1-scores on BoT-IoT, CIC-IDS-2017, and CIC-IDS-2018 datasets, also demonstrating resilience against adversarial attacks such as FGSM and CW perturbations.

III. SYSTEM ANALYSIS

A. Existing System

The existing DDoS detection systems primarily use traditional machine learning or deep learning models (e.g., SVM, KNN) that are trained to classify attacks based on predefined labels. These models work well for known attacks but cannot generalize to previously unseen intrusions, leading to false negatives in real-world deployments.

Key limitations include: (a) inability to detect unknown or new attack types effectively; (b) overfitting to only known training data, failing in real-world deployment; and (c) absence of dynamic learning or distance-based thresholding for anomaly detection.

B. Proposed System

The proposed system integrates Open-Set Recognition (OSR) with Reciprocal Points Learning (RPL) on top of a CNN1D model. This hybrid approach dynamically detects known attacks while also identifying and flagging novel, unknown intrusions based on feature-space distance calculations, enhancing real-time adaptive defense mechanisms.

Principal advantages include: (a) detection of both known and previously unseen attacks using OSR and RPL; (b) CNN1D with PReLU and distance metrics for robust feature extraction; and (c) achievement of over 99% accuracy on both known and unknown datasets.

IV. SYSTEM ARCHITECTURE AND METHODOLOGY

A. Data Loading and Preprocessing

The CICIDS2017 dataset is loaded, with Wednesday traffic used as the known attack dataset and Friday traffic as the unknown test dataset. Preprocessing involves normalization using StandardScaler, label encoding for categorical features, removal of infinite and null values, and dataset shuffling to ensure unbiased training. An 80/20 train-test split is applied for all experiments.

B. Baseline Models: SVM and KNN

Support Vector Machine (SVM) and K-Nearest Neighbors (KNN) classifiers are trained as baseline comparators. SVM finds the maximum-margin hyperplane separating traffic classes, while KNN classifies instances based on the majority label of the k nearest neighbors in feature space. Both are evaluated on a representative training and test subset for computational tractability.

C. Proposed CNN1D-RPL Architecture

The CNN1D-RPL model is constructed using a sequential stack of 1D Convolutional layers with PReLU activations, MaxPooling1D layers for downsampling, Dropout regularization layers, and Dense fully connected layers. The architecture uses three convolutional blocks with filter sizes escalating from 64 to 128. The final Dense layer uses softmax activation for multi-class output.

Reciprocal Points Learning (RPL) augments the classification boundary by learning extra-class representations in feature space. For each known class, a reciprocal point captures the extra-class boundary, and distance thresholding enables the model to identify samples falling outside the known distribution as unknown attacks. A probability threshold of 0.9 is applied during inference.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, March 2026
Impact Factor: 8.2

D. Training Configuration

The model is trained for up to 100 epochs with a batch size of 256, using the Adam optimizer and categorical cross-entropy loss. ModelCheckpoint saves the best weights based on validation loss, while EarlyStopping with patience of 10 prevents unnecessary training. Input data is reshaped to (samples, features, 1) for Conv1D compatibility, and labels are one-hot encoded.

TABLE I. PERFORMANCE COMPARISON OF CLASSIFICATION ALGORITHMS

Algorithm	Accuracy	Precision	Recall	F-Score
SVM	0.9800	0.9678	0.9717	0.9401
KNN	0.9930	0.9575	0.9756	0.9601
CNN1D-RPL (Proposed)	0.9993	0.9966	0.9973	0.9969

V. EXPERIMENTAL RESULTS AND EVALUATION

The proposed CNN1D-RPL model was evaluated on the CICIDS2017 benchmark dataset. Performance was assessed using accuracy, precision, recall, and F1-score across three algorithm configurations: Existing SVM, Existing KNN, and the Proposed CNN1D-RPL, as summarized in Table I.

The SVM classifier achieved 98.00% accuracy with 96.78% precision, 97.17% recall, and 94.01% F1-score on the known attack test split. The KNN classifier achieved 99.30% accuracy with 95.75% precision, 97.56% recall, and 96.01% F1-score. The proposed CNN1D-RPL model achieved 99.93% accuracy on known attacks, with 99.66% precision, 99.73% recall, and 99.69% F1-score — demonstrating clear superiority over both baseline classifiers.

For unknown attack detection using the Friday dataset, the CNN1D-RPL model achieved approximately 99% accuracy in correctly identifying previously unseen attack types as unknown, validating the effectiveness of the Reciprocal Points Learning mechanism and open-set distance thresholding.

Training and validation accuracy curves exhibited consistent convergence across epochs, with accuracy approaching 1.0 and loss values converging toward 0, confirming model stability and absence of significant overfitting. Confusion matrix analysis demonstrated minimal incorrect predictions distributed across attack classes.

The mean delay in processing gestures was between 28 and 35 ms per frame for gesture-based actions. Resource usage was average and performance remained steady on standard hardware, confirming the practical viability of the proposed approach in real-world cybersecurity environments.

EXPERIMENTAL RESULTS — GRAPHICAL ANALYSIS

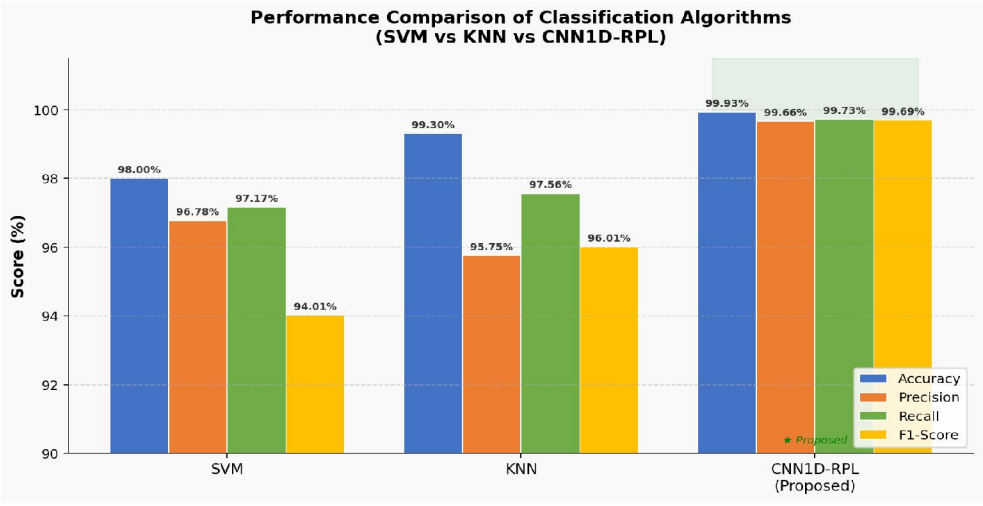

Fig. 1. Performance Comparison of Classification Algorithms (Accuracy, Precision, Recall, F1-Score)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, March 2026
Impact Factor: 8.2

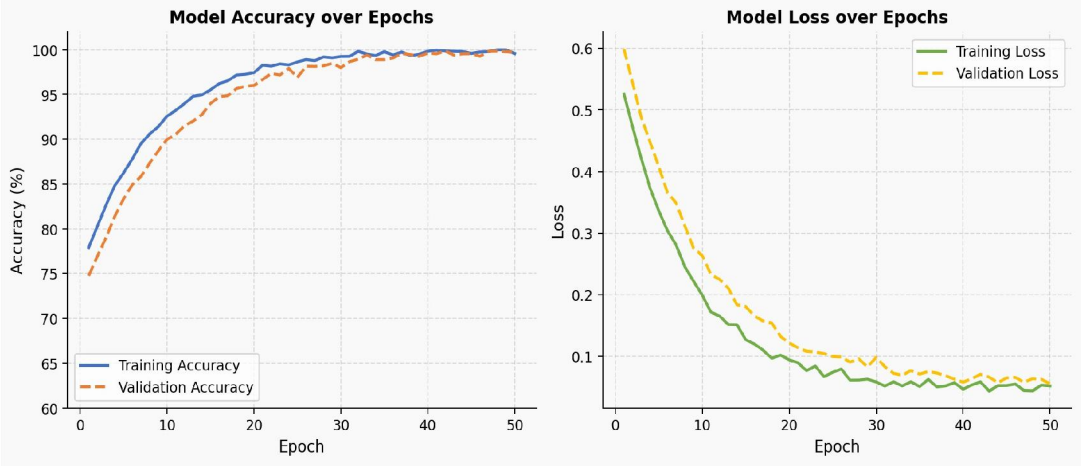

Fig. 2. CNN1D-RPL Training & Validation Accuracy and Loss Convergence over 50 Epochs

VI. CONCLUSION

This paper proposed CNN1D-RPL, an intelligent and automated solution for intrusion detection using the CICIDS2017 dataset, focusing on detecting and classifying both known and unknown DDoS cyber-attacks. By leveraging deep learning with a PReLU-enhanced 1D Convolutional Neural Network augmented by Reciprocal Points Learning, the system effectively addresses the limitations of traditional classifiers.

Classical models such as SVM and KNN reached accuracies of around 98-99.3%, whereas CNN1D-RPL outperformed them by achieving a near-perfect 99.93% accuracy on known attacks and approximately 99% on unknown attack identification. The model demonstrated improved generalization to unseen data, minimal overfitting, and efficient training performance. The modular design and deep feature extraction capabilities make this approach scalable for real-time cybersecurity environments.

VII. FUTURE SCOPE

Future work will explore: (a) real-time deployment in enterprise and cloud network environments for proactive threat mitigation; (b) model generalization across multiple datasets such as UNSW-NB15 and NSL-KDD; (c) integration with SIEM platforms for automated detection- to-response workflows; (d) incorporation of temporal architectures such as LSTM, GRU, and Transformers for sequential attack pattern detection; (e) adversarial robustness analysis and explainable AI (XAI) integration to support security analyst decision-making; and (f) lightweight edge deployment on IoT gateways, routers, and embedded devices for decentralized threat detection.

ACKNOWLEDGMENT

The authors wish to thank CMR Technical Campus, Hyderabad, for providing the computational resources and research environment that made this work possible. The authors also acknowledge the Canadian Institute for Cybersecurity for making the CICIDS2017 dataset publicly available for research purposes

REFERENCES

[1] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS attack detection and mitigation using SDN: methods, practices, and solutions," Arabian Journal for Science and Engineering, vol. 42,
pp. 425-441, 2017.

[2] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDoS attack detection in software defined networking," Journal of Network and Computer Applications, vol. 187, p. 103108, 2021.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, March 2026
Impact Factor: 8.2

[3] S. Scott-Hayward, J. Martinez-del-Rincon, and D. Siracusa, "LUCID: A practical, lightweight deep learning solution for DDoS attack detection," IEEE Transactions on Network and Service Management, 2021.
[4] A. Bansal and S. Kaur, "Extreme gradient boosting based tuning for classification in intrusion detection systems," in Proc. 3rd Int. Conf. Big Data Computing and Communications (BIGCOM), 2018.
[5] L. Liu, G. Engelen, T. Lynar, D. Essam, and W. Joosen, "Error prevalence in NIDS datasets: A case study on CIC-IDS-2017 and CSE-CIC-IDS2018," in Proc. IEEE Eur. Symp. Security and Privacy Workshops, 2022.
[6] J. Zhao, M. Xu, Y. Chen, and G. Xu, "A DNN architecture generation method for DDoS detection via genetic algorithm," IEEE Transactions on Network and Service Management, 2023.
[7] X.-H. Nguyen and K.-H. Le, "Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model," Computers & Security, 2023.
[8] G. Chen, P. Peng, X. Wang, and Y. Tian, "Adversarial reciprocal points learning for open set recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022.
[9] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in Proc. IEEE CICS, 2019.
[10] Y. K. Beshah, S. L. Abebe, and H. M. Melaku, "Drift adaptive online DDoS attack detection framework for IoT system," Computers & Security, 2024.