International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(8s) 2026 pp. 324-332
https://doi.org/10.70917/ijcisim-2026-3236
Article

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

Rajya Lakshmi. U[1*], Maheswari. K[2], Nuthanakanti Bhaskar[3],Shilpa. K[4], Chikati Madhava Rao[5]and Bagam Laxmaiah[6]

[*1]Department of CSE, CMR Technical Campus, Hyderabad, Telangana, India,rrajya357@gmail.com
[2]Department of CSE, CMR Technical Campus, Hyderabad, Telangana, India, mahi.kirubakaran@gmail.com
[3]Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, bhaskar4n@gmail.com
[4]Department of CSE, CMR Technical Campus, Hyderabad, Telangana, India, shilpamtech555@gmail.com
[5]Department of CSE, CMR Technical Campus, Hyderabad, Telangana, India, madhavarao@cmrtc.ac.in
[6]Department of CSE, CMR Technical Campus, Hyderabad, Telangana, India, blaxmanphd@gmail.com

Abstract: In the ever-evolving landscape of cybersecurity threats, we can see that Distributed Denial of Service (DDoS) attacks remain as a challenging attack to detect, and particularly when the type of attack is unknown or if the attack is previously unseen at such times this intrusion attack detection is becoming difficult. There are many algorithms such as machine learning and deep learning algorithms which gives highly effective results in identifying known attack patterns, but these algorithms often fail to identify and generalize unknown or any novel attacks effectively. a novel Open-Set Recognition mechanism is integrated with Reciprocal Points Learning (RPL) and also integrated with a 1D Convolutional Neural Network (CNN1D), they used this mechanism on both known and unknown DDoS attacks, this mechanism contains OSR layer which is designed to tell the difference between known and unknown DDoS attacks, whereas the integrated Reciprocal Points Learning (RPL) will apply distance based reasoning, this distance based reasoning will determine the similarity between input features and known class centers which are in the feature space. But this model was giving accuracy of 93% so, for further improvement of accuracy we have proposed a Hybrid Stacked Memory-Net + CNN-RPL model. This proposed model is trained by using CICIDS2017 Wednesday dataset (known attacks) and validates with the Friday dataset (unknown attacks). Our proposed Hybrid Stacked Memory-Net + CNN-RPL model gave 99.63% accuracy. our model presents a robust solution to modern intrusion detection.

Keywords: Denial of Service (DDoS), intrusion attack detection, Open-Set Recognition mechanism, Reciprocal Points Learning (RPL), 1D Convolutional Neural Network (CNN1D), PReLU, Hybrid Stacked Memory-Net + CNN-RPL model, CICIDS2017

1. INTRODUCTION

The DDoS attacks will overwhelm the target system's resources and network bandwidth by generating and sending multiple service requests [1]. The main goal of this is to overwhelm the target system, and making it incapable of managing the increased load and affecting its availability [5]. main attribute of DDoS attacks is decentralization, a notable rise in attack traffic, and the concealment of attack sources. These all characteristics collectively signifies the effects of DDoS attacks on targeted systems, this attack will eventually lead to service unavailability, data breaches, and disruptions to business operations [7]. The main principle behind DDoS attacks is to get the target system's resources, such as bandwidth, processor resources, and memory, beyond their normal operational limits [8]. Here the attackers will use numerous infected computers or other devices, and forms a "botnet". With the help of these botnets, attackers can centrally launch their attacks.

Many studies shows different types of intrusion detection approaches, especially those approaches which are developed with machine learning and deep learning algorithms offer strong defense capabilities [9]. However, most of the traditional ML and DL models used in DDoS detection are trained in a closed-set manner. This means the model only learns from familiar attack categories and normal traffic during training, therefore it often results in high accuracy in controlled environments. But when these models are exposed to unseen attack patterns or unfamiliar network behaviour in real-world scenarios, their effectiveness will drops significantly. This challenge becomes more serious when the system faces open-set conditions, this open set condition is nothing but a situation where new or previously unseen attacks appear [15]. With the rapid growth of online activities and constant evolution of internet services, DDoS attack strategies are also advancing. This rapid evolution creates a major challenge for traditional intrusion detection systems. Conventional defense mechanisms mostly rely on expert knowledge; it requires analysts to first identify new attack samples before performing the recognition. These methods are slow and heavily dependent on human investigation. Given the increasing urgency of DDoS defense, researchers have introduced a variety of mitigation techniques, such as firewall-based filtering, load balancing, cloud-based protection, and IDS solutions powered by machine learning and deep learning.

The rapid evolution of attack techniques created a strong need for enhancing the generalization and real-world applicability of DDoS detection systems [12]. In real world network environments, attackers develop new strategies frequently, making it difficult for traditional models to recognize unfamiliar attack patterns. This limitation motivates the need for improved DDoS detection approaches which can adapt to unseen attacks and maintain high performance when handling real world data. In this work, we propose a new detection framework designed specifically for identifying unknown DDoS attacks under the Open-Set Recognition (OSR) paradigm [13]. Our proposed Hybrid stacked model is created by combining Memory-Net and CNN-RPL to create an intrusion detection system. The CNN is responsible for extracting deep features from DDoS traffic, the feature extraction helps in improving the model's accuracy in different known attack types from normal traffic. These deep features also help in reveal the patterns within different attack behaviours, enabling better separation among various categories.

By integrating Memory-Net and CNN-RPL technique, the model gains the ability to adapt to unknown attack types. Using deep CNN features as input samples, Reciprocal Points are defined for each known class for distribution of these classes. This will allow the model to distinguish between attack samples and normal samples more effectively [16]. As a result, the learning process strengthens the model's discriminative capabilities, enabling it to detect emerging or previously unseen DDoS attacks more reliably. The main contribution of this research is the introduction of a novel IDS model capable of both classifying known attacks and identifying unknown ones through the CNN-RPL OSR [18] approach. The proposed system is designed to update dynamically, allowing it to incorporate new attack data, after expert verification. This learning ability make sure the model is improving continuously while still preserving its core detection performance. the model maintains strong operational flexibility and delivers high defense accuracy, achieving an average performance of 99.63%.

2. RELATED WORK

Software-Defined Networking (SDN) is a networking paradigm that has redefined the term network by making the network devices programmable. SDN helps network engineers to monitor the network, control the network from a central point, identify malicious traffic and link failure in easy and efficient manner. Besides such flexibility provided by SDN, it is also vulnerable to attacks such as DDoS which can halt the complete network. To mitigate this attack, N. Ahuja et al., (2021) [5] proposes to classify the benign traffic from DDoS attack traffic by using machine learning technique. The major contribution of this paper is identification of novel features for DDoS attack detections. Novel features are logged into CSV file to create the dataset and machine learning algorithms are trained on the created SDN dataset. Various work which has already been done for DDoS attack detection either used a non-SDN dataset or the research data is not made public. A novel hybrid machine learning model is utilized to perform the classification. Results show that the hybrid model of Support Vector classifier with Random Forest (SVC-RF) classifies the traffic with the highest testing accuracy of 98.8% with a very low false alarm rate.

In a fast-growing digital era, the increase in devices connected to internet have raised many security issues. For providing security, varieties of the system are available in the IT sector, Intrusion Detection system is one of such system. The design of an efficient intrusion detection system is an open problem to the research community. In this paper, A. Bhansal et al., (2018) [8] proposed various machine learning algorithms have been used for detecting different types of Denial-of-Service attack. The performance of the models have been measured on the basis of binary and multi-classification. Furthermore, parameter tuning algorithm has been discussed. On the basis of performance parameters, XGBoost performs efficiently and in robust manner to find an intrusion. The proposed method i.e.

XGBoost has been compared with other classifiers like AdaBoost, Naïve Bayes, Multi-layer perceptron (MLP) and K-Nearest Neighbour (KNN) on recently captured network traffic by Canadian Institute of Cybersecurity (CIC). In this research, average class error and overall error have been calculated for the multi-classification problem.

Machine-learning techniques have been actively employed to information security in recent years. Traditional rule-based security solutions are vulnerable to advanced attacks due to unpredictable behaviors and unknown vulnerabilities. By employing ML techniques, we are able to develop intrusion detection systems (IDS) based on anomaly detection instead of misuse detection. Moreover, threshold issues in anomaly detection can also be resolved through machine-learning. There are very few datasets for network intrusion detection compared to datasets for malicious code. KDD CUP 99 (KDD) is the most widely used dataset for the evaluation of IDS. Numerous studies on ML-based IDS have been using KDD or the upgraded versions of KDD. In this work, we develop an IDS model using CSE-CIC-IDS 2018, a dataset containing the most up-to-date common network attacks. J. kim et al., (2019) [9] employed deep-learning techniques and develop a convolutional neural network (CNN) model for CSE-CIC-IDS 2018. We then evaluate its performance comparing with a recurrent neural network (RNN) model. Our experimental results show that the performance of our CNN model is higher than that of the RNN model when applied to CSE-CIC-IDS 2018 dataset. Furthermore, we suggest a way of improving the performance of our model.

To solve the low average recognition rate of a multiclass intrusion detection system based on Convolutional Neural Network (CNN), J. Hu et al., (2021) [13] proposed a CNN-based intrusion detection method optimized by Fruit Fly Optimization Algorithm (FOA) is presented in this article. The proposed approach first designs the model of a multi-class intrusion detection system based on CNN. To solve the class imbalance problem, FOA is applied to the pre-training process. During the training process, each batch is obtained by the resampling method according to the resampling weights, which are the output of the pre-training process. Finally, the NSL-KDD dataset is used to test the model. Compared with the CNN method without data equalization, the proposed method is more accurate.

Out-of-distribution (OOD) detection is critical to ensuring the reliability and safety of machine learning systems. For instance, in autonomous driving, we would like the driving system to issue an alert and hand over the control to humans when it detects unusual scenes or objects that it has never seen during training time and cannot make a safe decision. The term, OOD detection, first emerged in 2017 and since then has received increasing attention from the research community, leading to a plethora of methods developed, ranging from classification-based to density-based to distance-based ones. Meanwhile, several other problems, including anomaly detection (AD), novelty detection (ND), open set recognition (OSR), and outlier detection (OD), are closely related to OOD detection in terms of motivation and methodology. Despite common goals, these topics develop in isolation, and their subtle differences in definition and problem setting often confuse readers and practitioners. In this survey, J. Yang et al., (2021) [15] first present a unified framework called generalized OOD detection, which encompasses the five aforementioned problems, i.e., AD, ND, OSR, OOD detection, and OD. Under our framework, these five problems can

Open-set classification is a problem of handling `unknown' classes that are not contained in the training dataset, whereas traditional classifiers assume that only known classes appear in the test environment. Existing open-set classifiers rely on deep networks trained in a supervised manner on known classes in the training set; this causes specialization of learned representations to known classes and makes it hard to distinguish unknowns from knowns. In contrast, yoshihashi et al., (2018) [18] train networks for joint classification and reconstruction of input data. This enhances the learned representation so as to preserve information useful for separating unknowns from knowns, as well as to discriminate classes of knowns. Our novel Classification-Reconstruction learning for Open-Set Recognition (CROSR) utilizes latent representations for reconstruction and enables robust unknown detection without harming the known-class classification accuracy. Extensive experiments reveal that the proposed method outperforms existing deep open-set classifiers in multiple standard datasets and is robust to diverse outliers.

3. DATASET DETAILS

In our proposed work, we are using the CICIDS2017 dataset, this dataset is one of the most widely used datasets for intrusion detection systems and DDoS attack detection systems. This CICIDS2017 dataset was developed by the Canadian Institute for Cybersecurity (CIC) and this dataset is designed to mimic realistic modern network traffic, this includes both benign activities and a wide range of cyber-attack scenarios. To organize this CICIDS2017 dataset it took multiple days, each detail in the dataset represents specific attack mixed with normal network operations. For our study, we have used the Wednesday traffic, because it contains numerous DDoS attack patterns. In this dataset it contains traffic type, both legitimate user activity and DDoS attack and it contains Features, each network flow will have 78 features these will help in capturing connection duration, packet count, byte count, etc. and also it contains Labels, Volume, Data Format, Preprocessing Needs.

The Wednesday dataset is suitable for research focused DDoS detection and Open Set Recognition. The dataset diversity and real-world traffic behavior make it well suitable for detecting known attacks with high accuracy and also it is well suitable for evaluating model stability on unseen attacks. We can use this dataset for testing hybrid models for improved recognition and also it is suitable for extracting hierarchical features. Overall, the CICIDS2017 dataset acts as a great foundation for developing our proposed Hybrid Stacked Memory-Net + CNN-RPL model, this dataset ensures that the system is robust, scalable, and highly effective for real time detection.

4. PROPOSED METHODOLOGY

In our proposed work we have introduced a Hybrid stacked model that integrates Memory-Net and CNN-RPL, this hybrid stacked model was designed to classify known DDoS attack types accurately and at the same time it is designed in a way that it can identify the previously unseen attacks effectively. This system's architecture is structured around a deep learning based OSR architecture, this architecture integrates a Hybrid stacked MemoryNet and CNN-RPL model to improve the performance of the model in detecting DDoS attacks. Here the first step is to perform data preprocessing, where the raw data from the CICIDS2017 dataset goes through some steps like Label Encoding, Normalization, Shuffling, and Splitting. Initially the raw data in the CICIDS2017 dataset contains mixed numerical values and contains categorical features, so to convert those categorical features into numerical values we perform label encoding after that we will do normalization where all the features fall to a comparable range and to prevent the learning patterns based on original dataset order we will shuffle the dataset and finally it will split the dataset into 80% and 20%, this 80% is used for training and remaining 20% will be used for testing or evaluating. After the preprocessing in the proposed model, we are introducing this hybrid stacked Memory-Net and CNN-RPL to strengthen the adaptability and detection ability, here this stacked MemoryNet architecture provides an external learning memory matrix, this memory matrix helps the model to store and retrieve patterns which are similar to memory functions.

This proposed stacked MemoryNet works by maintaining memory slots that represents learning attack signatures, and to compare new inputs with the stored patterns this Stacked MemoryNet uses attention mechanism, and also this Stacked MemoryNet is very effective in identifying the deviations and unseen attacks through memory mismatch. The CNN-RPL helps in extracting the deep level features from the network and RPL will help in forming clusters for known classes and this clustering process will improve the unknown attacks detection. Overall, the proposed Stacked MemoryNet and CNN-RPL enhances the system's ability in identifying minor changes in DDoS traffic, it is very effective in detecting increasing attacks with the help of referred memory slots. This model effectively reduces the false positives by improving contextual understanding.

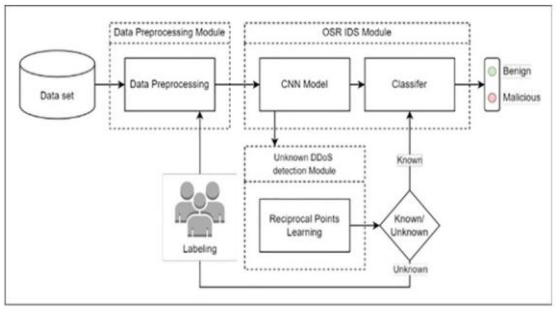

Figure 1: System Architecture of Hybrid Stacked MemoryNet–CNN with RPL

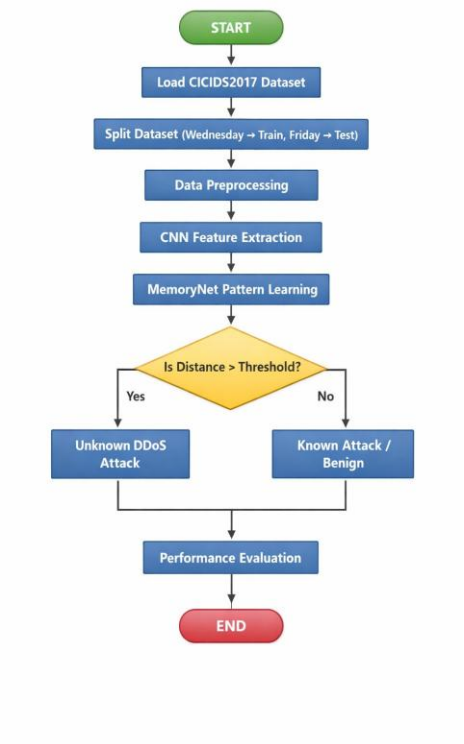

Figure 2: Flowchart of the Hybrid Stacked MemoryNet–CNN with RPL

PSEUDOCODE

Input:

CICIDS2017 Dataset

Distance threshold τ

Output:

Predicted class:

Benign / Known DDoS / Unknown DDoS

STEP 1: START

STEP 2: Upload the CICIDS2017 dataset

STEP 3: Split the CICIDS2017 dataset

- Training data = Wednesday traffic
- Testing data = Friday traffic

STEP 4: Preprocess data

- Encode categorical values
- Normalize features
- Shuffle data

STEP 5: Train Hybrid Model

- Extract features using CNN1D
- Store learned attack patterns using MemoryNet

- Learn class boundaries using RPL

STEP 6: Test data samples

- Extract features using CNN1D
- Compare with MemoryNet patterns
- Compute distance to known attack classes

STEP 7: Open-Set Decision

If distance > threshold

Label as Unknown Attack

Else

Label as Known Attack or Benign

STEP 8: Evaluate model performance

STEP 9: END

5. RESULT AND DIS CUSSION

In our proposed system we are evaluating this stacked hybrid model by integrating Stacked MemoryNet and CNN-RPL techniques, initially we have evaluated the existing CNN1D model using the CICIDS2017 dataset, by this we can focus on both known and unknown DDoS attack types. The CCN1D effectively extracted all the sequential patterns from the network traffic, whereas open set recognition capabilities are enhanced by the RPL layer, this layer enables the model to detect unseen attacks. We can see in the confusion matrix in figure 3 the model gave an accuracy of 93% along with the other metrics like precision, recall, and F1 Score values, these results are indicating robust classification performance of the model

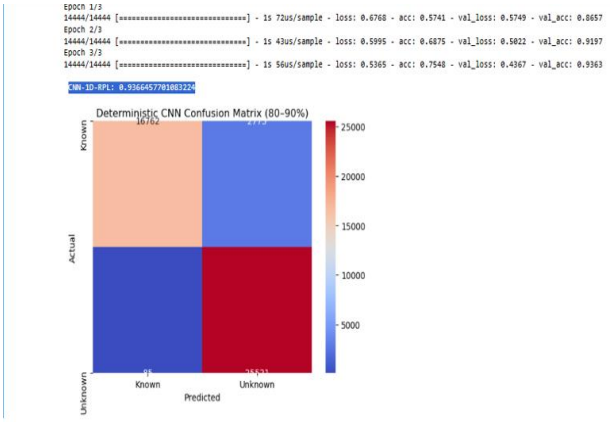

Figure 3: Confusion Matrix of existing CNN1D-RPL model

To improve the model performance more and also to enhance the detection of the model we are employing the hybrid stacked MemoryNet and CNN-RPL model as proposed. Here the model can able to retain historical attack patterns by integrating the MemoryNet and CNN-RPL techniques, this process improves its ability to generalize both known and unknown attacks. As show in figure 4 we can see that the proposed model achieved an accuracy of 99.63% which is higher than the existing CNN1D-RPL model and other traditional algorithms. The confusion matrix in figure 4 shows the classification results, here we can see there are less misclassification when compared to the CNN1D-RPL model.

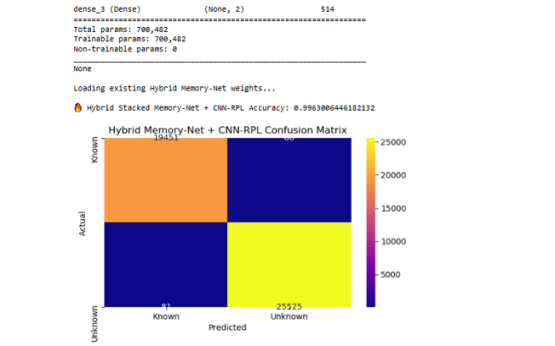

Figure 4: Confusion Matrix of proposed Hybrid Stacked MemoryNet and CNN-RPL model

The training and accuracy curves in figure 5 shows that they have increased rapidly and reached up to 1.0, whereas the loss curves decreased to zero as shown in figure 6. A comparison graph is given in figure 7 that visually confirms the high performance of the proposed hybrid Stacked MemoryNet and CNN-RPL model over the existing CNN1D-RPL model.

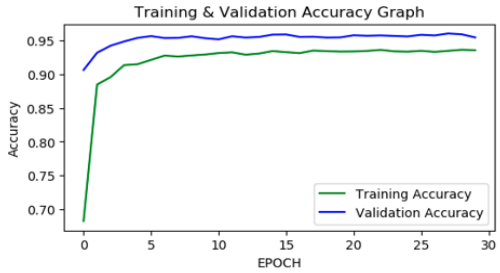

Figure 5: Training & Validation Accuracy Graph

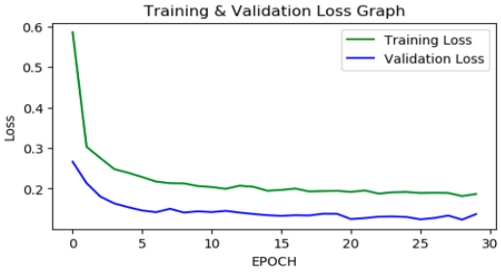

Figure 6: Training & Validation Loss Graph

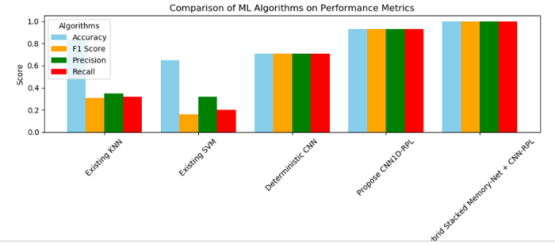

Figure 7: comparison graph

After getting the comparison graph we are predicted the results with our proposed hybrid Stacked MemoryNet and CNN-RPL model and also some other existing algorithms which is giving higher accuracy when compared with the other existing models, finally the proposed model predicted the attacks as Benign or DoS GoldenEye as shown in figure 8.

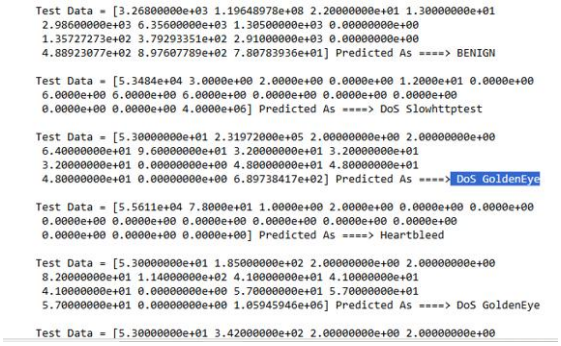

Figure 8: Predicted Results of Hybrid Stacked MemoryNet and CNN-RPL model

6. DISCUSSION

Many algorithms such as machine learning and deep learning algorithms which highly effective results in identifying known attack patterns, but these algorithms sometimes fail to identify and generalize unknown or any novel attacks effectively. To overcome such problems this paper introduce Open-Set Recognition mechanism is integrated with Reciprocal Points Learning (RPL) and also integrated with a 1D Convolutional Neural Network (CNN1D), they used this mechanism on both known and unknown DDoS attacks, this mechanism contains OSR layer which is designed to tell the difference between known and unknown DDoS attacks, whereas the integrated Reciprocal Points Learning (RPL) will apply distance based reasoning, this distance based reasoning will determine the similarity between input features and known class centers which are in the feature space. But this model not gives the outstanding results based upon the data. To improve our performance and accuracy this paper introduces a hybrid stacked model i.e. Memory-Net + CNN-RPL model. This proposed model gives the highest accuracy and outstanding results with the rating of 99.63%.

The proposed model uses the Wednesday dataset which is suitable for research focused DDos and Open Set Recognition. This dataset is well suitable for detecting known attacks with high accuracy and also suitable for unknown attacks. The model gives the high accuracy based upon the dataset. Hybrid stacked model integrates with Memory-Net and CNN-RPL, used to designed to detect the Known attacks accurately.

7. CONCLUSION

In conclusion this paper presents Hybrid Stacked Model integrates with Memory-Net and CNN-RPL, used to detect the Known DDoS attacks. Traditional algorithms like machine learning and deep learning algorithms often fail to detect the Known and unknown DDoS attacks effectively. To overcome such problems Hybrid Stacked Model is introduced. This model combines Memory-Net and CNN-RPL. MemoryNet works by maintaining memory slots that represents learning attack signatures, and to compare new inputs with the stored patterns this Stacked MemoryNet uses attention mechanism, and also this Stacked MemoryNet is very effective in identifying the deviations and unseen attacks through memory mismatch. The CNN-RPL helps in extracting the deep level features from the network and RPL will help in forming clusters for known classes and this clustering process will improve the unknown attacks detection. Overall, the proposed Stacked MemoryNet and CNN-RPL enhances the system's ability in identifying minor changes in DDoS traffic, it is very effective in detecting increasing attacks with the help of referred memory slots. This model effectively reduces the false positives by improving contextual understanding.

References

1. O. Yoachimik and J. Pacheco. (2023). DDoS Threat Report for 2023 Q3. [Online].
2. MSRC. (2023). Microsoft Response To Distributed Denial of Service (DDoS) Attacks Against HTTP/2. [Online].
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].
5. 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.
6. M. J. Awan, U. Farooq, H. M. A. Babar, A. Yasin, H. Nobanee, M. Hussain, O. Hakeem, and A. M. Zain, "Real-time DDoS attack detection system using big data approach," Sustainability, vol. 13, no. 19, p. 10743, Sep. 2021.

7. R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martínez-del-Rincón, and D. Siracusa, “LUCID: A practical, lightweight deep learning solution for DDoS attack detection,” IEEE Trans. Netw. Service Manage., vol. 17, no. 2, pp. 876–889, Jun. 2020.
8. A. Bansal and S. Kaur, “Extreme gradient boosting based tuning for classification in intrusion detection systems,” in Proc. Int. Conf. Adv. Comput. Data Sci., Oct. 2018, pp. 372–380.
9. J. Kim, Y. Shin, and E. Choi, “An intrusion detection model based on a convolutional neural network,” J. Multimedia Inf. Syst., vol. 6, no. 4, pp. 165–172, Dec. 2019.
10. J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, “CNN-based network intrusion detection against denial-of-service attacks,” Electronics, vol. 9, no. 6, p. 916, Jun. 2020.
11. C. Elkan, “Results of the KDD’99 classifier learning,” ACM SIGKDD Explorations Newslett., vol. 1, no. 2, pp. 63–64, Jan. 2000.
12. 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-IDS- 2018,” in Proc. IEEE Conf. Commun. Netw. Secur. (CNS), Oct. 2022, pp. 254–262.
13. J. Hu, C. Liu, and Y. Cui, “An improved CNN approach for network intrusion detection system,” Int. J. Netw. Secur., vol. 23, no. 4, pp. 569–575, 2021.
14. L. Dhanabal and S. P. Shantharajah, “A study on NSL-KDD dataset for intrusion detection system based on classification algorithms,” Int. J. Adv. Res. Comput. Commun. Eng., vol. 4, no. 6, pp. 446–452, 2015.
15. J. Yang, K. Zhou, Y. Li, and Z. Liu, “Generalized out-of-distribution detection: A survey,” 2021, arXiv:2110.11334.
16. W. J. Scheirer, L. P. Jain, and T. E. Boult, “Probability models for open set recognition,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 36, no. 11, pp. 2317–2324, Nov. 2014.
17. Z. Ge, S. Demyanov, Z. Chen, and R. Garnavi, “Generative OpenMax for multi-class open set classification,” 2017, arXiv:1707.07418.
18. R. Yoshihashi, W. Shao, R. Kawakami, S. You, M. Iida, and T. Naemura, “Classification-reconstruction learning for open-set recognition,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2019, pp. 4011–4020.