Unknown DDoS Attack Detection Using Open-Set Recognition Technology and Fuzzy C-Means Clustering

Hao Kao[1(✉)], Thanh-Tuan Nguyen[2(✉)], Chin-Shiuh Shieh[1], Mong-Fong Horng[1], Lee Yu Xian[1], and Denis Miu[3]

[1] Department of Electronic Engineering, National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan
{F110152139,F111152183}@nkust.edu.tw
[2] Department of Electronics and Automation Engineering, Nha Trang University, Nha Trang, Vietnam
tuannt@ntu.edu.vn
[3] Genie Networks, Taipei, Taiwan

Abstract. In contemporary society, internet users face various cyber threats, including malware, phishing websites, and hacker attacks. Conventional defense software struggles to prevent unknown attack methods, making developing effective detection techniques crucial. Distributed Denial-of-Service (DDoS) attacks represent a persistent and evolving cybersecurity challenge. As such, enhancing the defense and detection of DDoS attacks is imperative. This study addresses the open set recognition (OSR) problem, a crucial pattern recognition aspect involving managing unknown categories. To address this challenge, we employ Spatial Location Constraint Prototype Loss (SPCPL) and Fuzzy C-Means methods.

The findings of the experiment indicate that the unknown attack detection technique we have suggested, which relies on Fuzzy C-Means open set recognition, exhibits superior performance compared to conventional known attack detection methods in detecting and preventing unknown attacks. The misjudgment rate is extremely low given the high accuracy rate of 98% and minimal sample overlap. Finally, improving the dependability and consistency of models in real-world implementations can aid in mitigating intricate and ever-changing attack situations.

Keyword: Distributed Denial-of-Service (DDoS), Open set recognition, Spatial Location Constraint Prototype Loss, Fuzzy C-Means

1 Introduction

The COVID-19 pandemic, which emerged in 2020, brought about a heightened reliance on the internet, resulting in a notable surge in Distributed Denial of Service (DDoS) attacks. For enterprises functioning as service providers, ensuring the stable operation of their networks and services has become paramount.

J.-S. Pan et al. (Eds.): ICGEC 2023, LNEE 1114, pp. 366–380, 2024.
https://doi.org/10.1007/978-981-99-9412-0_38

Any disruption caused by an attack can lead to substantial business losses and reputational harm. However, the continually evolving DDoS attack techniques have rendered conventional methods inadequate in countering these novel threats[1].

In light of these circumstances, there is an imperative to empower existing Intrusion Detection Systems (IDS) to effectively detect and report unknown traffic patterns, assisting network engineers in discerning unprecedented anomalies. Leveraging machine learning and deep learning, IDS has demonstrated heightened efficacy, leaving malicious actors with limited concealment opportunities[2]. Nevertheless, machine learning-based IDS still exhibit vulnerabilities, particularly when confronted with unknown patterns, leading to a significant decline in accuracy.

Thus, the primary objective of our research is to propose multiple IDS approaches that can simultaneously detect known and unknown DDoS attacks and rigorously evaluate their testing performance. By employing the Fuzzy C-Means clustering method and Spatial Location Constraint Prototype Loss, we aim to equip organizations with a robust, open-set identification technology capable of effectively safeguarding their network infrastructures and preserving uninterrupted service delivery amidst the evolving landscape of cyber threats. The findings of this study contribute to advancing the field of network security and offer valuable insights for enhancing the resilience of IDS in contemporary cybersecurity scenarios.

The main contributions of this study are focused on the following aspects:

- We adopted AlexNet as the neural network architecture for our training procedure. Simultaneously, we improved the AlexNet architecture in order to classify conventional data more efficiently.
- Through the clustering methods of SLCPL and FCM, we adjusted the positions of unknown attack samples, bringing them closer to specific categories and thereby enabling the recognition of unknown attacks.

2 Related Works

2.1 DDoS Attack

In the absence of DDoS attacks, network systems can operate smoothly and provide uninterrupted services. Achieving such a robust network environment involves considering several critical factors. Firstly, meticulous network planning and architecture design are essential, encompassing bandwidth allocation, network topology, and redundancy mechanisms [3]. Secondly, the implementation of effective intrusion detection and defense systems plays a pivotal role in promptly identifying and mitigating various attack vectors. Furthermore, regular security vulnerability scanning and timely updates are crucial measures for maintaining network security at its optimal level. Lastly, the deployment of robust traffic monitoring and management mechanisms aids in identifying and

addressing anomalous traffic patterns. Network systems can sustain stable operations and continuous service provision by integrating these measures, even in DDoS attacks.

2.2 AlexNet

AlexNet is a deep Convolutional Neural Network (CNN) introduced by Alex Krizhevsky et al. in 2012, which achieved remarkable success in the ImageNet Large Scale Visual Recognition Challenge (ILSVRC) [4]. This network architecture marked a significant milestone at the time, exerting a substantial influence on the advancement of deep learning and the progress of image classification tasks.

The primary characteristics of AlexNet lie in its combination of depth, convolution, and pooling layers, along with a considerable number of trainable parameters. Its architecture is as follows:

1. Combination of Convolutional and Pooling Layers: AlexNet employs convolutional and pooling layers for feature extraction. These layers effectively capture local features within images and utilize pooling layers to reduce the dimensionality of feature maps while retaining essential features.
2. Rectified Linear Unit (ReLU) Activation Function: AlexNet applies the ReLU activation function after each convolutional layer, which addresses the vanishing gradient problem and accelerates the training process.
3. Dropout: The dropout technique is introduced in the fully connected layers of AlexNet, mitigating overfitting and enhancing the model's generalization capability.
4. Multi-GPU Training: AlexNet pioneered the use of multiple GPUs for training in deep learning models, significantly accelerating the training process.

The success of AlexNet underscores the formidable capabilities of deep learning in tasks like image classification. While more profound neural network architectures emerged in the subsequent years, AlexNet's role as a starting point in deep learning has cast a lasting influence on the design and development of subsequent models (Fig. 1).

2.3 Open Set Recognition

Open Set Recognition (OSR) [5] is a significant problem in machine learning and pattern recognition, aiming to address the identification challenges posed by unknown classes or unseen samples in the real world. OSR seeks to tackle this issue by extending the recognition problem to scenarios that encompass both known and unknown classes. This approach often leverages category modeling and anomaly detection techniques to establish an identification model that distinguishes between known and unknown classes while detecting and excluding unknown samples. In this context, the category modeling process is employed to train the model for recognizing known classes, whereas anomaly detection is utilized for identifying unknown classes or unseen samples.

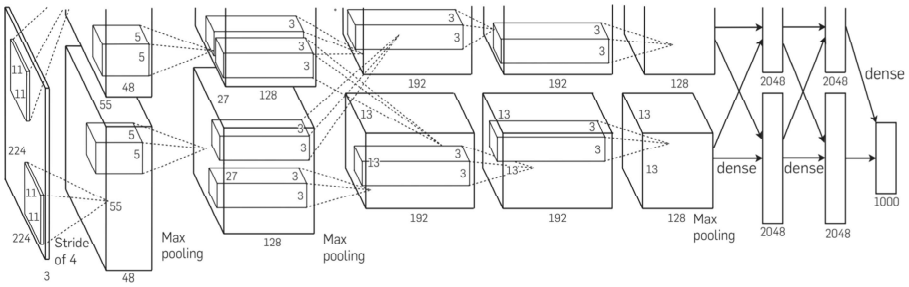

Fig. 1. Architecture of AlexNet

2.4 Spatial Location Constraint Prototype Loss

The Spatial Location Constraint Prototype Loss (SLCPL) [6] is a loss function designed for deep learning models with the aim of enhancing the model's sensitivity to the spatial location of objects. Specifically, the SLCPL algorithm incorporates the positional information of class prototypes as constraint conditions, enabling samples from the same class to be more concentrated in the feature space while maintaining a similar spatial distribution among them. By minimizing the loss function, the model is encouraged to allocate samples from the same class to regions that correspond to their respective positions, thereby enhancing spatial accuracy.

2.5 Fuzzy C-Means Algorithm

Fuzzy C-Means (FCM) [7] is a widely-used fuzzy clustering algorithm for partitioning data points into various clusters. In contrast to the conventional K-Means clustering, FCM permits each data point to possess a membership degree between 0 and 1 for different clusters, representing the extent to which the data point belongs to each cluster.

The primary objective of FCM is to minimize the squared error between each data point and the center of the cluster to which it belongs while accounting for the influence of membership degrees. The fundamental idea behind this algorithm involves iterative computations that progressively adjust cluster centers and membership degrees until a convergence condition is met. FCM's strengths include its capability to handle fuzziness and overlapping data points, showing good performance in various practical applications. However, the algorithm is sensitive to the choice of initial values and is also sensitive to noisy data. Additionally, FCM exhibits relatively high computational complexity, especially when dealing with large datasets.

FCM is a flexible fuzzy clustering algorithm that effectively approaches data distributions characterized by fuzziness and overlap. In practical applications, clustering accuracy and efficiency can be improved by appropriately adjusting algorithm parameters and initial values and integrating other techniques.

2.6 Unknown DDoS Detection

In existing approaches, machine learning and data mining techniques have been widely applied to the detection of unknown DDoS attacks. For instance, methods based on traffic analysis utilize statistical features and behavioral patterns to detect anomalous attack traffic [8], or employ Bidirectional Long Short-Term Memory (BI-LSTM) models, Gaussian Mixture Models (GMM), and incremental learning [9]. Similarly, machine learning-based approaches utilize training datasets to build models and detect attacks by comparing actual traffic with predicted outcomes. However, detecting unknown DDoS attacks still poses several challenges. Firstly, the constantly evolving strategies and techniques of attackers make it difficult to predict and detect attack features. Secondly, traditional detection methods often require prolonged learning and training times, leading to delays in real-time detection. Additionally, the complexity and high transmission rates of large-scale networks further compound the difficulty of detection.

In research by Liang et al. [10], the authors addressed the problem of detecting out-of-distribution (OOD) images without the need for training data from unknown distributions in an unlabeled open-set environment. In various application domains, such as computer vision and image classification, machine learning models are typically trained on specific data distributions. When confronted with unknown data different from the training data, the model's performance may deteriorate. Consequently, detecting and identifying images from unknown distributions is crucial for ensuring model stability and reliability.

In a 2017 publication by Schlegl et al. [11], an approach was proposed that employs Generative Adversarial Networks (GANs) for unsupervised anomaly detection and guided discovery of anomalies. The paper introduced a GAN-based unsupervised anomaly detection method where the combination of a generator and a discriminator is used for training. The key idea of this method is to introduce stochastic variation through noise into the generator, making the generated images more diverse. Simultaneously, the discriminator is trained to differentiate between normal and anomalous samples. During training, the generator is compelled to produce images similar to benign samples but different from anomalous samples.

3 Methodology

3.1 Proposed Framework

Figure 2 illustrates the architecture of our Unknown Distributed Denial of Service Intrusion Detection System (Unknown DDoS IDS) developed in this study, which is based on a variety of deep learning models. The architecture consists of three main modules: the Data Preprocessing module, OSR module, and the Unknown Identification module. The system is trained using the CICIDS2017 dataset [12], and performance, detection methodologies, accuracy of known attacks, and detection rate of unknown attacks are compared and validated. We employ the AlexNet model to assess system performance, and two OSR

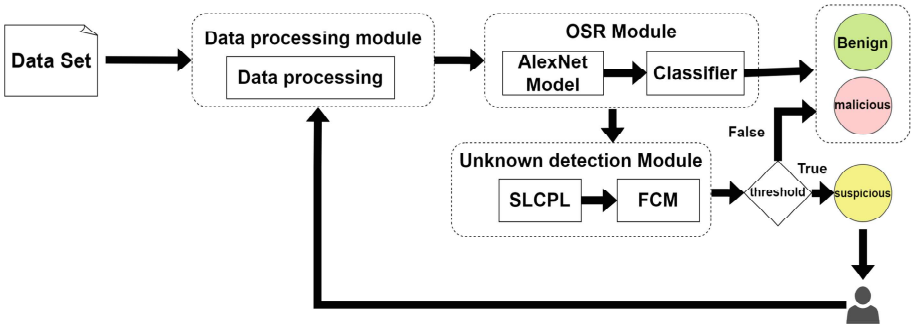

Fig. 2. Architecture of Unknown DDoS Detection System

methods, namely SLCPL, are employed for detecting unknown DDoS attacks. Furthermore, we introduce the Fuzzy C-Means clustering technique to differentiate between known and unknown attacks. As the employment of the SLCPL method alone may not entirely distinguish between known and unknown attacks, the clustering method is included to enhance the classification performance.

3.2 Unknown DDoS Attack Model

In our model, we have adapted the AlexNet [4] architecture by employing one-dimensional convolutions. The structure of 1D AlexNet encompasses several crucial components. Firstly, convolutional layers employ convolution operations to capture features from one-dimensional data. Following this, activation function layers introduce non-linearity, often utilizing the ReLU function. Subsequently, pooling layers are integrated to reduce feature maps' dimensions and computational load while retaining essential features.

Additionally, 1D AlexNet includes fully connected layers that map features to the final classification outcome. Finally, the output layer utilizes softmax to generate the ultimate classification result. Typically, 1D AlexNet consists of interleaved multiple convolutional and pooling layers to extract features at various levels. Batch normalization layers can be added after each convolutional layer to expedite convergence and enhance model stability. Preceding the fully connected layers, Dropout layers can be employed to alleviate overfitting. 1D AlexNet exhibits formidable capabilities in processing one-dimensional data, such as audio recognition, natural language processing, and bioinformatics, among other fields. By appropriately adjusting the parameters and layer configuration of 1D AlexNet, models can be constructed and trained according to the specific requirements of the task.

3.3 Spatial Location Constraint Prototype Loss

Spatial Location Constraint Prototype Loss (SLCPL) [6] is a type of loss function designed for deep learning models with the aim of enhancing the spatial location

sensitivity of the model towards objects. The SLCPL attempts to address this issue by introducing location constraints. It is based on a key concept: the distribution of object features should be closely related to their spatial location. This method associates the prototype vector of each class with the corresponding position information of that class and applies location constraints to the prototype learning process. Specifically, the SLCPL utilizes the positional information of class prototypes as constraint conditions, resulting in a concentration of samples from the same class within the feature space while maintaining a similar distribution of positions among them. By minimizing the loss function, the model is encouraged to assign samples from the same class to regions that correspond to their respective positions, thereby enhancing spatial positioning accuracy. By introducing the spatial location constraint prototype loss, the model can better utilize object location information, enhancing its spatial awareness of objects and improving recognition and localization accuracy. This approach holds potential for various computer vision tasks, such as object detection, object tracking, and scene segmentation (Fig. 3).

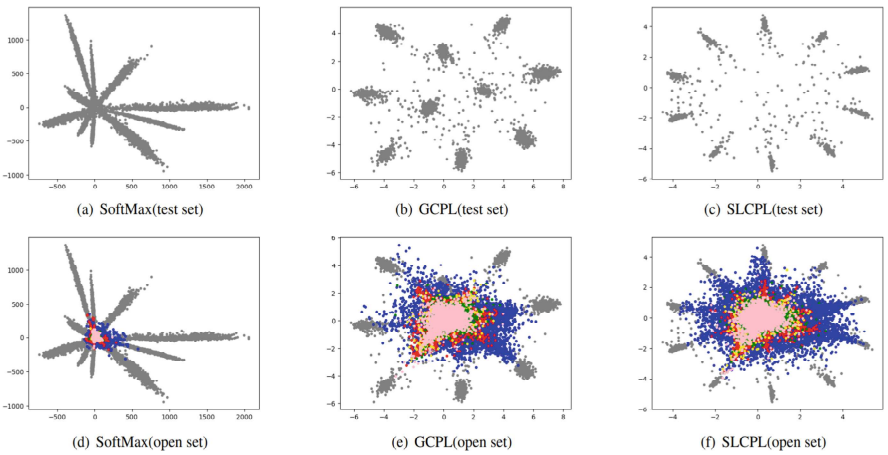

Fig. 3. Feature Space Distributions using SLCPL [6]

The following equation defines the Spatial Location Constraint Prototype Loss:

$$L_s = \sum_{i=1}^{N} \sum_{j=1}^{M} |f(x_{ij}) - P_i|^2 + \lambda \sum_{i=1}^{N} \sum_{j=1}^{M} |L_{ij} - L_i|^2 \tag{1}$$

"In this equation, a positional constraint term is introduced in addition to the original prototype distance term. L_{ij} represents the position of the ith sample, and L_i represents the position of the ith class. By minimizing the positional constraint term, the loss function is able to project samples closer to the prototype of their respective class at their corresponding positions.

3.4 Unknown DDoS Attack Identification

We employ the SLCPL (Spatial Location Constraint Prototype Loss) with the Fuzzy C-Means method to address unknown attack scenarios for further cluster analysis. This approach aims to more accurately distinguish between samples belonging to known attack classes and unknown attack classes in the feature space. Fuzzy C-Means is a clustering analysis method to partition samples into multiple fuzzy categories. The algorithm considers the degree of membership of each sample to every category rather than just employing traditional hard clustering methods. The following formula represents the Fuzzy C-Means algorithm: Given N samples and C cluster centers, each sample is denoted as x_i, and each cluster center as v_j. Define the fuzzy membership matrix U, where U_{ij} represents the degree of membership of sample x_i to cluster center v_j. The objective function of Fuzzy C-Means aims to minimize the following cost function:

$$J(U,V) = \sum_{i=1}^{N}\sum_{j=1}^{C} U_{ij}^{m}||x_i - v_j||^2 \tag{2}$$

Here, m is the fuzziness parameter that controls the degree of fuzziness in clustering. This objective function aggregates the weighted sum of Euclidean distances between samples and cluster centers. The algorithm proceeds as follows

1. Initialize the fuzzy assignment matrix U, and the cluster centers V.
2. Perform iterative updates until a stopping condition is met (the maximum number of iterations or convergence of the objective function): Update U: Compute the degree of membership of each sample to each cluster center using the membership update formula:

$$U_{ij} = \left(\sum_{k=1}^{C}\left(\frac{||x_i - v_j||}{||x_i - v_k||}\right)^{\frac{2}{m-1}}\right)^{-1} \tag{3}$$

   Update V: Calculate the coordinates of each cluster center using the coordinate update formula:

$$v_j = \frac{\sum_{i=1}^{N} U_{ij}^{m} \cdot x_i}{\sum_{i=1}^{N} U_{ij}^{m}} \tag{4}$$

3. Return the final fuzzy assignment matrix U and cluster centers V.

The core principle of this algorithm lies in iteratively updating the fuzzy assignment matrix and cluster centers, continuously adjusting the membership degrees of samples and the positions of cluster centers to minimize the objective function. Through the fuzzy assignment matrix, one can obtain the fuzzy membership degrees of each sample with respect to each cluster center rather than solely obtaining rigid classification outcomes.

4 Experiment Result

4.1 CICIDS2017dataset

CICIDS2017 is a widely used dataset for the research and development of IDS. Developed by the Canadian Institute for Cybersecurity (CIC), CICIDS2017 aims to simulate various network attacks and normal traffic in real-world networks [13]. Below is a detailed overview of the CICIDS2017 dataset:

1. Dataset Structure: The CICIDS2017 dataset consists of six different subsets, namely Benign Traffic, DoS, DDoS, PortScan, DDoSSmurf, and BruteForce. Each subset contains different attack types and normal traffic, totaling over 8,500,000 network connections.
2. Attack Types: The dataset encompasses several attack types, including DoS attacks, DDoS attacks, port scans, and brute force attempts. These attack types simulate common network attack behaviors encountered in real-world scenarios, making it suitable for training and testing intrusion detection systems.
3. Feature Extraction: CICIDS2017 provides an extensive range of features describing various network connection aspects. These features include statistical characteristics based on the transport, network, and application layers, such as transport layer traffic, protocol types, source IP, and destination IP. These features aid in the analysis and detection of network attacks.
4. Data Authenticity: The generation of the CICIDS2017 dataset is based on real network data, including actual network traffic and attack behaviors. This enhances the dataset's realism, contributing to the accuracy and efficacy of intrusion detection systems.
5. Applicability: CICIDS2017 can be used for training, validating, and testing the performance of intrusion detection systems. Researchers and developers can utilize this dataset for performance evaluation, feature selection, model optimization, algorithm comparison, and related tasks.

In conclusion, the CICIDS2017 dataset is widely employed in intrusion detection research due to its diverse attack types, rich feature set, and reliance on authentic network data. Its applicability and authenticity render it a valuable resource for researchers and developers on intrusion detection systems.

Table 1. CICIDS2017 attack data form [13]

Date of Attack	Event of Attack
Monday July 3, 2017	Benign
Tuesday July 4, 2017	FTP-Patator SSH-Patator
Wednesday July 5, 2017	DoS slowloris DoS Slowhttptest DoS Hulk DoS GoldenEy Heartbleed Port 444
Thursday, July 6, 2017	Web - Brute Force Web - XSS Web - Sql Injection Infiltration
Friday July 7, 2017	Botnet ARES Port Scan DDoS LOIT

4.2 Experimental Environment

In this research, we employ the CICIDS2017 and CICDDoS2019 datasets for experimentation, utilizing a workstation with the Ubuntu 20.04 operating system. Our workstation is equipped with an AMD Ryzen 5700X 8C16T processor, 96GB DDR4 memory, and Nvidia RTX3070 and Nvidia RTX2060 as computational acceleration devices. We employ NVIDIA Driver Server version 510 as the driver software and use VSCode in conjunction with Conda as the development environment. Regarding the model framework, we undertake development using PyTorch 1.11.0, sklearn, and Python 3.9.12.

4.3 Evaluation Metric

In machine learning and pattern recognition, evaluation metrics serve as quantifiable measures to gauge model performance and effectiveness. These metrics assess and compare a model's performance on a specific task or problem. Several common evaluation metrics are as follows:

1. Accuracy: Measures the correctness of model predictions, the proportion of correctly predicted samples out of the total samples.
2. Precision: Evaluate the ratio of true positive predictions to the total predicted positive samples.
3. Recall: Assesses the ratio of true positive predictions to the total true positive samples.
4. F1 Score: An evaluation metric that comprehensively considers precision and recall, allowing for a balance between these aspects.
5. ROC Curve (Receiver Operating Characteristic curve): A curve plotted based on the model's true positive rate and false positive rate, used to assess the model's performance at various threshold levels.
6. AUC (Area Under the ROC Curve): A metric that measures the area under the ROC curve, providing an evaluation of the model's performance that combines precision and recall in a balanced manner.

These evaluation metrics can be chosen based on the specific problem and task, and their interpretation can be adjusted according to the requirements. It is customary to comprehensively consider multiple evaluation metrics to attain a comprehensive assessment and comparison of model performance in model evaluation. In the context of this research, the metrics used for assessing model performance include accuracy, precision, recall, and the F1-Score. These metrics will measure the model's performance in distinguishing between different classes.

4.4 Conventional DDoS Identification Modules

In this study, we employed the 1D AlexNet for training purposes. However, we observed that the training process increased dispersion within the distribution of known categories, as depicted in Fig. 4. This dispersion phenomenon emerged

due to our transformation of the original one-dimensional AlexNet into a two-dimensional counterpart, causing the samples in our feature space to remain inadequately classified. In order to address this issue, modifications were introduced to the 1D AlexNet architecture. Our approach entailed the incorporation of fully connected layers following each convolutional layer. As illustrated in Fig. 5, the integration of these fully connected layers resulted in a significant improvement in the outcome.

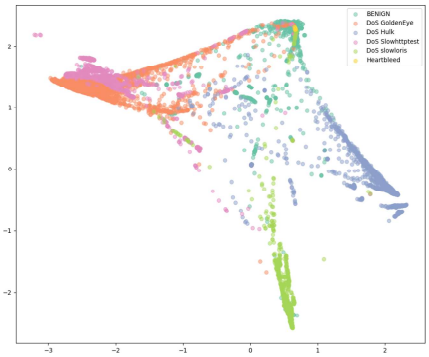

Fig. 4. Unmodified 1D AlexNet

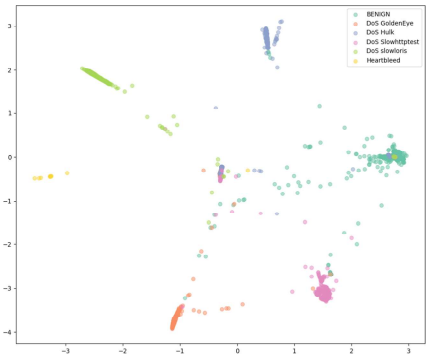

Fig. 5. 1D AlexNet with a fully connected layer added after the convolutional layer

Despite our continuous experimentation with various modifications to the 1D AlexNet model during the experiments, the results did not yield improvements comparable to the outcome achieved by incorporating fully connected layers after each convolutional layer. Concurrently, we evaluated this result through the assessment of a confusion matrix. The visualization of this evaluation can be observed in Fig. 6. It is observed that the accuracy for each category exceeded 98%, yielding highly satisfactory results.

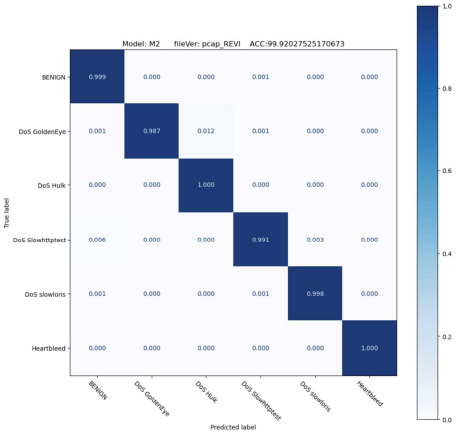

Fig. 6. Known attack confusion matrix

4.5 Unknown Identification Module

The poorest results were observed when we projected the unknown attack samples onto the feature space. The majority of the unknown attack samples were covered by our known attack samples, which contradicts our expectations for the feature space. We hypothesize that the issue might be related to the clustering method. It is important to note that SLPCL was not the aspect we considered modifying, as, without SLPCL, the distribution became highly scattered. Thus, following the output of SLPCL, we further passed the data through another novel clustering method. Therefore, we opted for the Fuzzy C-means clustering method. Fuzzy C-means effectively repositions the distribution of unknown classes. Initially, we increased the number of classes from 7 to 10 in order to better reposition the samples. From Fig. 7, it can be observed that the distribution when applying Fuzzy C-means is very favorable, effectively avoiding the known attack samples. This is a significant discovery in our context.

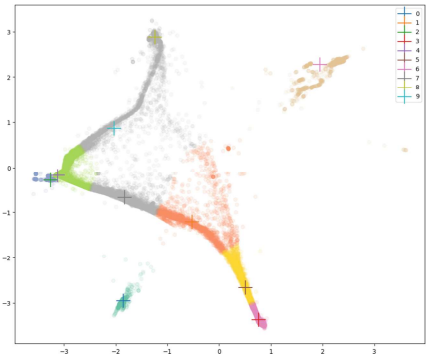

Fig. 7. Distribution status of unknown attack samples

We conducted a cumulative calculation of the distribution region of unknown attack classes to compute precision, yielding excellent results. Subsequently, we evaluated false positive rate, accuracy, and F1 score, all of which exceeded 97%, even surpassing 99%. Such outcomes are highly satisfactory. In the context of unknown DDoS detection, if we directly input the unknown dataset into the model, due to the nature of closed-set learning, the deep feature distribution of the closed-set does not allocate any space for unknown features. Consequently, unknown features overlap with known features, leading to a sharp decrease in accuracy. As observed from Table 2, if we directly feed the unknown dataset into the model, owing to the characteristics of closed-set learning, unknown features overlap with known features, resulting in a significant decrease in accuracy and even failing to achieve an accuracy of 90%.

Table 2. Known DDoS detection performance

Test Data Set	Precision	Recall	Accuracy	F1
CICIDS2017 Wednesday	0.9882	0.9976	0.9926	0.9917
CICIDS2017 Friday	0.7518	0.8386	0.8383	0.7856

As per the outcomes presented in Table 3, after undergoing processing by Fuzzy C-Means, all evaluation metrics of the model exceeded 97%, surpassing our expectations. This demonstrates that the proposed open-set recognition method is effective in distinguishing known and unknown data within the deep feature space.

Table 3. Known DDoS detection performance

Test Data Set	Precision	Recall	Accuracy	F1
CICIDS2017 Wednesday	0.9882	0.9976	0.9926	0.9917
CICIDS2017 Friday	0.9778	0.9999	0.9814	0.9888

5 Conclusion

Information security has witnessed numerous advanced applications with the flourishing development of the Internet. Service providers now strive to achieve stable service quality, which has become their crucial objective. However, some individuals view DDoS attacks as a means of generating revenue. Current research primarily focuses on training and testing with known attack types. Nevertheless, intrusion detection systems trained solely on datasets have limitations in identifying novel unknown traffic. Therefore, this study proposes a hybrid approach that combines the characteristics of unsupervised and supervised networks. Experimental results demonstrate that the proposed framework provides

a method for the closed-set training model to reject outputs or identify them as unknown attacks. This method relies on data labeling by domain experts and utilizes incremental learning to enhance the model further. In conclusion, this research yields two significant findings.

We initially employed a neural network model designed for two-dimensional images in the study. However, during the research process, we modified the model to adapt to the processing requirements of one-dimensional data. Additionally, we made multiple adjustments to the neural network model to enhance its performance throughout the study. Using this specific neural network model might not be the optimal choice. Therefore, in the neural network aspect, we aim to explore the utilization of more complex models, expecting better results when dealing with unknown attacks. Moreover, we also seek to improve the clustering model further to enable better aggregation of samples from unknown attacks.

Acknowledgement. This research was supported by the National Science and Technology Council with grant numbers: NSTC 112-2221-E-992-045, NSTC 112-2221-E-992-057-MY3 and MOST 109-2221-E-992 -073 -MY3.

References

1. Mirkovic, J., Prier, G., Reiher, P.: Attacking DDoS at the source. In: 10th IEEE International Conference on Network Protocols, 2002. Proceedings. IEEE, Conference Proceedings, pp. 312–321 (2002)
2. Zhang, B., Zhang, T., Yu, Z.: DDoS detection and prevention based on artificial intelligence techniques. In: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Conference Proceedings, pp. 1276–1280 (2017)
3. Tripathi, N., Hubballi, N.: Application layer denial-of-service attacks and defense mechanisms: a survey. ACM Comput. Surv. (CSUR) **54**(4), 1–33 (2021)
4. Krizhevsky, A., Sutskever, I., Hinton, G.E.: ImageNet classification with deep convolutional neural networks. Commun. ACM **60**(6), 84–90 (2017)
5. Geng, C., Huang, S.-J., Chen, S.: Recent advances in open set recognition: a survey. IEEE Trans. Pattern Anal. Mach. Intell. **43**(10), 3614–3631 (2020)
6. Xia, Z., Wang, P., Dong, G., Liu, H.: Spatial location constraint prototype loss for open set recognition. Comput. Vis. Image Underst. **229**, 103651 (2023)
7. Bezdek, J.C., Ehrlich, R., Full, W.: FCM: the fuzzy c-means clustering algorithm. Comput. Geosci. **10**(2–3), 191–203 (1984)
8. Ahmed, M., Mahmood, A.N., Hu, J.: A survey of network anomaly detection techniques. J. Netw. Comput. Appl. **60**, 19–31 (2016)
9. Zhang, Z., Zhang, Y., Niu, J., Guo, D.: Unknown network attack detection based on open-set recognition and active learning in drone network. Trans. Emerg. Telecommun. Technol. **33**(10), e4212 (2022)
10. Hsu, Y.-C., Shen, Y., Jin, H., Kira, Z.: Generalized ODIN: detecting out-of-distribution image without learning from out-of-distribution data. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Conference Proceedings, pp. 10951–10960
11. Schlegl, T., Seeböck, P., Waldstein, S.M., Schmidt-Erfurth, U., Langs, G.: Unsupervised anomaly detection with generative adversarial networks to guide marker discovery. In: Niethammer, M., et al. (eds.) IPMI 2017. LNCS, vol. 10265, pp. 146–157. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59050-9_12

12. Maseer, Z.K., Yusof, R., Bahaman, N., Mostafa, S.A., Foozy, C.F.M.: Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset. IEEE Access **9**, 22351–22370 (2021)
13. Brunswick, U.O.N.: Intrusion detection evaluation dataset (CIC-IDS2017) (2023). http://www.unb.ca/cic/datasets/ids-2017.html