International Journal of Information Technologies and Systems Approach
Volume 17 • Issue 1

An Adaptive Enhancement Method of Malicious Traffic Samples Based on DCGAN-ResNet System

Qiankun Li, Shijiazhuang University, China
Juan Li, Shijiazhuang University, China
Yao Li, Shijiazhuang University, China
Feng Jiu, Shijiazhuang University, China*
Yunxia Chu, Shijiazhuang University, China

ABSTRACT

A malicious traffic sample adaptive enhancement device based on Deep Convolutional Generative Adversarial Network (DCGAN) is designed to address the issue of imbalanced network traffic data distribution, aiming to enhance the accuracy and efficiency of anomaly detection. By leveraging generative adversarial network technology, this device can generate samples similar to real malicious traffic to balance the training dataset. It utilizes the generator and discriminator of the Deep Convolutional Generative Adversarial Network (DCGAN), combined with the residual network (ResNet) in the CNN model, to enhance the quality of generated samples. The device can switch states to adapt to various network environments and has been experimentally validated for its effectiveness and feasibility.Moreover, employing an adaptive device, the samples of malicious traffic are adjusted. Experimental analysis demonstrates that the device significantly enhances the accuracy of anomaly traffic detection, improves robustness, and provides robust support for network security protection.

KEYWORDS

DCGAN, Malicious Traffic, Malware, ResNet, Sample Bias

With the continuous expansion of network scale, there is a clear upward trend in the data traffic carried by various information systems. The importance of enhancing network risk management, reducing system risks, and ensuring business continuity is increasingly emphasized across various industries (Al-Abassi et al., 2020). However, the complexity and evolving nature of network attacks pose significant challenges to ensuring system network security.

During cyber security drills and routine defense, a highly imbalanced distribution of traffic from the internet can be observed (Kim et al., 2019). Machine learning models of defense devices are mostly suitable for typical network security scenarios (Sheet & Ibrahim, 2023). Existing methods for detecting abnormal traffic primarily rely on protective systems such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and web application firewalls (WAF), supplemented by manual analysis and judgment (Haddadpajouh et al., 2019; Sakhnini et al., 2019). These monitoring

DOI: 10.4018/IJITSA.343317 *Corresponding Author

system products have undergone years of development and iteration, possessing certain machine learning capabilities to learn patterns within the data based on embedded algorithms (Siddique et al., 2019). However, in practical production environments, the quantity of abnormal traffic data is much less than that of normal data, resulting in an extremely imbalanced distribution of data samples, which often hinders effective utilization of machine learning algorithms within these monitoring systems.

Addressing these challenges, this paper implements a malicious sample generation device focusing on abnormal information within traffic data to explore the distribution of external attacks across various network devices. This contributes to a better understanding of attackers' intentions and patterns, optimizing feature engineering methods for abnormal traffic detection and attack behavior analysis. The device adopts a data-adaptive enhancement method based on deep convolutional generative adversarial networks (DCGAN) to address the imbalance between attack samples and normal samples, improving the overall accuracy of detection models within monitoring systems. Furthermore, the DCGAN, based on generative adversarial network (GAN) (Ring et al., 2019; Kawai et al., 2019; Hu & Tan, 2017; Frid-Adar et al., 2018), introduces convolutional layers to enhance the quality of generated traffic and the training stability of the network (Jia et al., 2023). Through an automated parameter determination method, it further enhances the ability of various system models to detect unknown threats, strengthening the robustness of the model (Tang et al., 2023).

The main contributions of this article are summarized as follows:

1) **Specialized generation of malicious traffic data.** This solution addresses inherent issues between traditional detection methods and traffic data by enabling the creation of malicious traffic samples. It alleviates the model performance problems caused by imbalanced data sample distribution. It can automatically determine the number of generated malicious samples, achieving the maximum expected accuracy for each security system's anomaly detection.
2) **Control over the sample generation process.** We incorporated dynamically adjustable units into certain parts of the sample generation process. These adjustable units have default parameters, enabling automated generation of malicious traffic data and allowing adjustments to the dataset's scale as per the specific requirements.
3) **Organic integration of the sample adaptive enhancement system with existing detection systems.** Our designed sample adaptive enhancement system functions as a data generator, training the machine learning models within various detection systems. This enhances the ability of each network security protection system to defend against malicious traffic.
4) **Integration of DCGAN with residual network (ResNet).** The generator effectively addresses the imbalance between attack and normal sample distributions and mitigates issues such as gradient vanishing or exploding during deep network training, thereby enhancing the stability of the network.

LITERATURE REVIEW

Chuang & Wu (2019) proposed a novel method utilizing deep learning to generate data models aimed at balancing network intrusion detection datasets, thereby enhancing detection capabilities. This provides an effective solution to the deficiencies and imbalances in network intrusion detection. However, the training of deep learning models requires significant computational resources and time, which may limit their applicability in certain domains. Jiao et al. (2022) discuss machine learning model reconstruction and sample generation methods for malicious traffic detection, and according to the authors, existing machine learning models face issues like overfitting and underfitting in malicious traffic detection, affecting the accuracy and reconstruction rate of the models. They propose a solution based on model reconstruction and sample generation using a graph-based adaptive sample generation algorithm, quickly creating uniformly distributed generated samples in the input domain (Jiao et al., 2022). Although this method can generate and train reconstructed models like the target

model, it may not fully replicate all the features and behaviors of the target model due to the lack of all information and details.

Many studies use generative adversarial network (GAN) (Goodfellow et al., 2018) or their derivative structures to address sample imbalance issues. GAN essentially consists of a generator and a discriminator. Recently, GAN has gradually been applied to adversarial example generation tasks (Zhang et al., 2022). For example, Rathore et al. (2021) proposed a GAN-based malicious sample generation method and a sequence feature selection method combining variance and correlation analysis to address imbalance issues in PIoT trajectory data. Building different GAN models to handle different categories of malicious traffic can better address data imbalance issues, improving model generalization and robustness (Sharma et al., 2021). However, DCGAN uses deep convolutional neural networks, capturing data features better than GAN through fully connected layers, thus generating samples more effectively.

Jamoos et al. (2023) state that the performance of traditional machine learning methods largely depends on dataset balance. However, many IDS datasets exhibit imbalanced class distributions, making threat detection challenging in some minority classes. To address this, a new model based on GAN – temporal dilated convolutional generative adversarial network (TDCGAN) – has been proposed. Moti et al. (2021) introduced a novel malicious software detection and generation framework called MalGAN for the Internet of Things (IoT) network edge. Unlike traditional feature-based methods, MalGAN does not require prior knowledge of malicious software and can automatically learn and generate new malicious software samples from raw bytecode. Nevertheless, redundant data may lead to storage wastage, especially when dealing with large datasets.

Additionally, Daniyal used DCGAN to deceive malicious software classifiers into believing they are normal entities. In this work, issues related to model collapse, instability, and vanishing gradients in the DCGAN were addressed by the proposed hybrid Aquila optimizer-Mine burst and harmony search (AO-MBHS) (Alghazzawi et al., 2022). However, there are many improved algorithms for the Aquila optimizer that require further research and optimization.

When dealing with highly imbalanced data distributions, normal samples typically outnumber abnormal ones significantly. Directly modeling and analyzing imbalanced data can lead to model bias, thereby affecting model accuracy (Yang et al., 2023). The innovative design of the malicious traffic sample enhancement system in this paper includes the use of a DCGAN to construct the generator, coupled with the ResNet from the CNN model. This design enables deep neural networks to train without encountering gradient disappearance issues. Additionally, the system utilizes a state-switching button to control the status of the malicious traffic sample enhancement system, providing two modes: PASS and WORKING. Such a sample enhancement system helps address certain biased traffic data issues, enhancing the effectiveness of detection models.

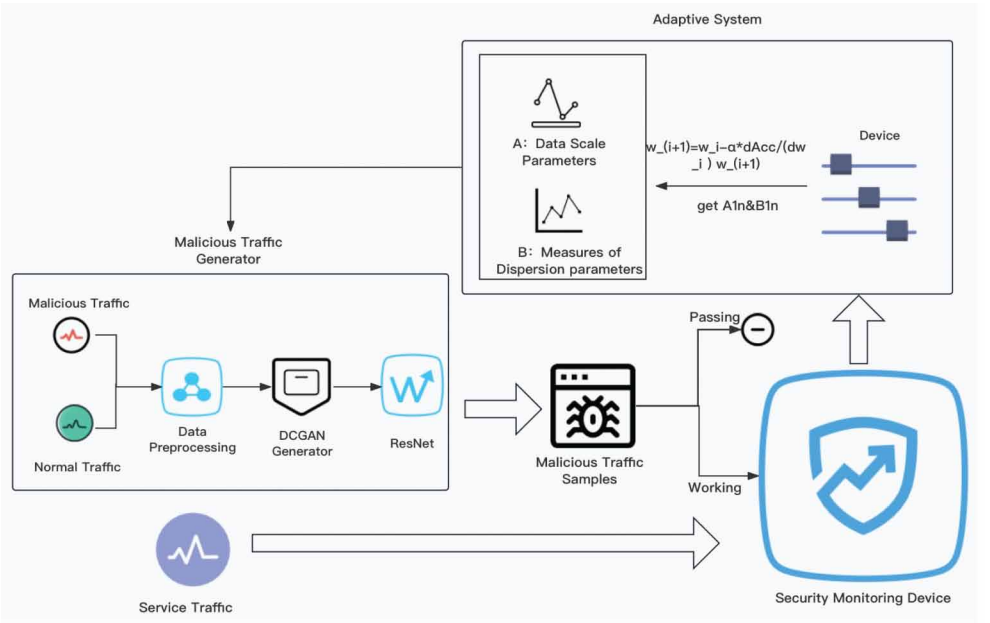
METHODS

Figure 1 illustrates the overall model architecture of this paper. As shown, the apparatus is divided into two parts. The left block consists of a malicious traffic generator composed of the DCGAN+ResNet algorithm. The generator has two states, working and passing, which can be adjusted according to service requirements. The upper right block contains the adaptive adjustment device for the malicious traffic generator. The following sections provide a detailed description of the structure and methodology of this device.

Overview of the Proposed Methods

To enhance the effectiveness of malicious traffic detection, this paper proposes an adaptive augmentation system tailored to malicious traffic samples. This system serves as the front-end unit of enterprise network security protection systems. It generates malicious samples, combines them with original samples to construct a new training set, and then inputs them into existing network security

Figure 1. Novelty Work



protection systems. Subsequently, the system calculates the enhancement effect of anomaly detection for each security system and feeds back the results to the augmentation system. Through the system's adaptive module, parameters are adjusted, enabling multiple feedback adjustments to incentivize the augmentation system. Moreover, it trains machine learning modules within each system to achieve optimal detection performance for the entire system. The position of the system within the network modules is shown in Figure 2.

Figure 2. Position of the System in the Network Module

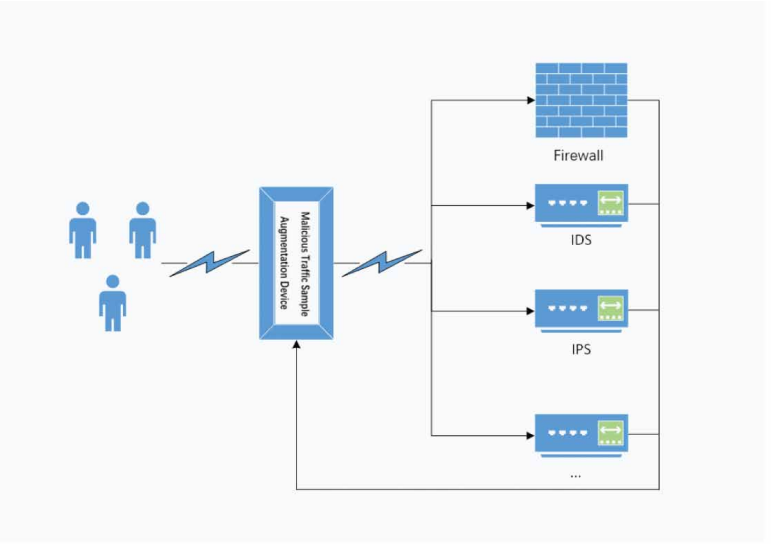
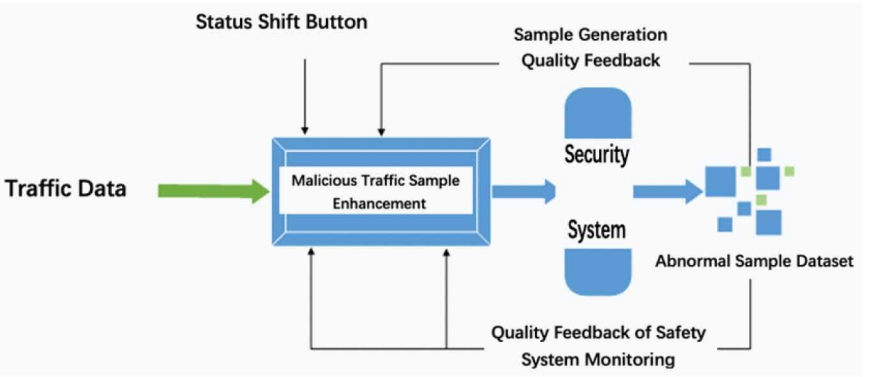


Figure 3. Following Data for Input and Output



More specifically, the following figure illustrates the data input and output directions of the malicious traffic sample adaptive enhancement system.

The data in the Figure 3 flows from left to right, with business traffic data highlighted in green and synthesized data in blue. Upon enabling the device, business traffic data first passes through and is combined with data generated by the device before flowing into various security protection systems. As these security protection systems process the traffic data, they detect anomalous samples, which are collected and stored in an anomalous sample dataset. The data from this dataset continues to flow into the malicious traffic sample adaptive augmentation system for analysis to obtain new malicious traffic data. Subsequently, based on the actual detection performance, the correct detection rate of each system is fed back to the adaptive parameter module within the sample augmentation system to regulate the scale of the generated data as well as the discrete degree of the data.

Status Switch Buttons

The status switch button controls the status of this malicious traffic sample enhancement system with two modes: PASS and WORKING.

The PASS state is the pass-through mode, which means that the enhancement system is turned off and all traffic data passes through directly without any processing. In pass-through mode, the device is completely inactive and does not change the original network structure. It is recommended that the device be placed in PASS state to avoid any impact on the service when there is a large amount of business traffic data.

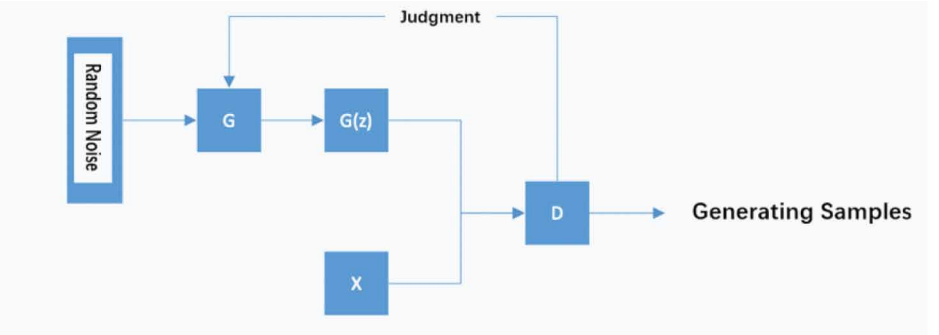
The WORKING state is the working mode, which represents that this enhancement system is turned on and the device enhances the malicious samples in the traffic data. In the working mode, the device learns the patterns of the data in the malicious sample set and constructs new malicious samples, which are merged with the previous original data and fed into each network security defense system as new training data for training, thereby enhancing the detection capability of each system for unknown malicious samples.

System Architecture

The internal structure of the malicious traffic sample enhancement system is shown in Figure 4.

The base sample is X, which represents the malicious traffic dataset collected by each security system in the augmented system; G is the generative model generating module used to generate anomalies based on the malicious traffic dataset; $G\left(z\right)$ is the sample generated by the generating module; D is the discriminative model discriminative module used to judge the anomaly degree to which the generated $G\left(z\right)$ can be faked or not and feed the discriminative result to D for judgment

Figure 4. Internal Structure of the Malicious Traffic Sample Enhancement System



; X is the raw data that is mixed with $G\left(z\right)$ and input to D for judgment. Whether it can be false or not and feedback the discriminative result to the generative model; X is the original data, which is mixed with $G\left(z\right)$ and input to D for judgment. Based on Goodfellow et al. (2018), we generally set the objective function of GAN as:

$$\min_{G}\max_{D}V\left(D,G\right)=E_{x\sim p_{data}\left(x\right)}\left[\log D\left(x\right)\right]+E_{z\sim p_{z}\left(z\right)}\left[\log(1-D\left(G\left(z\right)\right)\right) \tag{1}$$

where G is the generative model, D is the discriminant model, $G\left(z\right)$ is the generative data, $G\left(z\right)p_{data}\left(x\right)$ is the data distribution of the real sample, and z is the random noise.

G (generator) and D (discriminator) are two processes that can be implemented using various network structures. In this system, a DCGAN is employed to build the generator (Radford et al., 2015; Yu et al., 2017), while the GAN network's discriminative model utilizes ResNet (He et al., 2016) from the CNN model. In this paper, the DCGAN-ResNet method was chosen to address the issue of vanishing gradients during neural network training. This phenomenon occurs during the backpropagation process of neural networks, where gradients gradually decrease as the network depth increases, making it difficult to effectively adjust the weights of earlier network layers. Consequently, with the increase in network depth, training errors also increase, leading to deteriorated performance during both the training and testing phases, a phenomenon known as network degradation. The ResNet effectively resolves this issue.

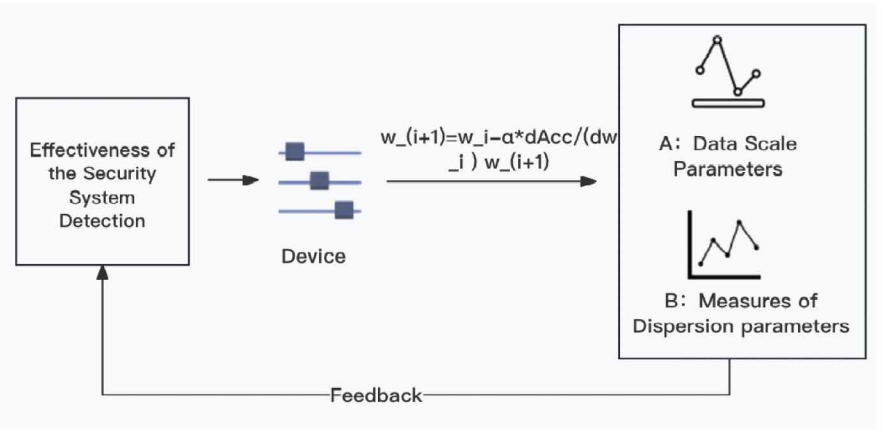
After several rounds of training and reaching the termination criteria of the model, D outputs the current data samples, which are subject to constraints imposed by the data size adjustment button and the data discretization adjustment button. The data size adjustment button regulates the quantity of samples outputted by D based on its setting. Meanwhile, the data discretization adjustment button adjusts the cosine similarity between the malicious traffic samples output by D and each sample in the original malicious traffic dataset. If the data falls below the set threshold, it will be discarded.

Adaptive System Architecture

The structure of the adaptive parameter module is shown in Figure 5.

In this paper, all the effectiveness of the security system detection is input into the adaptive device for calculation. Next, the data scale parameters and the measures of dispersion parameters are obtained, and overall system optimization is gradually achieved through multiple reciprocal operations.

Figure 5. Structure of Adaptive Parameter Module



Each system involves two parameters: the data generation scale parameter and the data discretization parameter. If there are N systems in total, then there are 2N parameters in total.

The data scale parameter controls the proportion of data generated by the enhancement device. This parameter can adjust the amount of generated data and blend it into the original data. In this proposal, the adjustment value for data scale is determined by the adaptive device, and set this value to be A.

The measures of dispersion parameter controls the deviation level between the data generated by the sample enhancement device and the anomaly samples, with the button's value range being (0, 1]. A higher value indicates a greater degree of deviation, meaning that the generated anomaly samples differ more from the original malicious traffic data. In this proposal, the adjustment of data discretization is determined by the adaptive device, and this value is set to be B.

The device uses cosine similarity to evaluate the degree of similarity between two traffic data samples. If there are two flow sample vectors X and Y, then the cosine similarity of these two vectors is calculated as:

$$\cos\left(\theta\right) = \frac{\sum_{i=1}^{n}\left(X_i \times Y_i\right)}{\sqrt{\sum_{i=1}^{n}\left(X_i\right)^2} \times \sqrt{\sum_{i=1}^{n}\left(Y_i\right)^2}} \tag{2}$$

The measures of dispersion parameter serves as an upper threshold, capable of filtering out data with cosine similarity less than B.

For N systems, there will be 2N parameters in the process of malicious sample enhancement: $A1,\ A2,\ ...,\ An\ ;\ B1,\ B2,\ ...,\ Bn$. It is necessary to analyze these parameters to obtain the optimal parameter corresponding to each system in order to achieve the optimal detection efficiency of the entire system.

In order to obtain the values of these parameters, correspondences need to be established:

$A1,\ B1 \rightarrow \mathrm{Acc}_1$
$A2,\ B2 \rightarrow \mathrm{Acc}_2$
$An,\ Bn \rightarrow \mathrm{Acc}_n$

The following is an example of $A1$, B1 $\rightarrow Acc1$ to show how the parameters are calculated.

The data scale control parameter A represents the size of the generated data, with a range of 0% to 300%.

The measures of dispersion parameter B regulates the degree of dispersion of the generated data, with a range of (0, 1].

First, sample A and B randomly select several value pairs to be used as parameters for generating malicious sample data. Then, these generated malicious samples are input into Security Protection System 1, and the accuracy of System 1 is calculated as Acc1. After multiple generations, several three-dimensional datasets will be obtained, which will then undergo polynomial fitting.

Let the fitting curve for the generated parameters of the first security system be:

$$x1 * A1n + x2 * B1n + C = Acc1n$$

$A1n$ and $B1n$ are the required parameters and C is a constant. The subscript 1 denotes the first security system, and the subscript n denotes that n points were randomly sampled. The meaning of the fitted curve is to use the distribution of A and B sampling to obt the accuracy of the corresponding system.

For $x1 * A1n + x2 * B1n + C = Acc1n$, use the mean square error minimization method to calculate the weight values of x.

Given the mean-square error (MSE):

$$MSE\left(Acc^{*}\right) = E\left(Acc^{*} - Acc\right)^{2} \tag{3}$$

where Acc^{*} denotes the estimated value of system accuracy, Acc denotes the actual value of system accuracy, and E denotes the expectation of both.

The smaller the mean square error, the better the fit of the curve $x1 * A1n + x2 * B1n + C = Acc1n$, so the values of $A1n$ and $B1n$ corresponding to the smallest mean square error are required, which are the parameter values of the malicious traffic sample enhancement system corresponding to the security detection system.

The fitted curves were solved using the gradient descent method:

$$w_{i+1} = w_{i} - \alpha * \frac{dAcc}{dw_{i}} w_{i+1} \tag{4}$$

For the initial trial value of the weights, w_{i} denotes the initial trial value of weights, denotes the updated weight value, α denotes the learning rate, and $\frac{dAcc}{dw_{i}}$ denotes the partial derivative of the accuracy. The weights are solved by several iterations, and the resulting $A1n$ and $B1n$ are the optimal parameters of the generated samples corresponding to the first security system.

Similarly, sample parameters can be calculated for all security systems, and with the relevant sample parameters, the next stage of sample generation can be carried out.

EXPERIMENTAL ANALYSIS

Experimental Setup

To prevent the experimental process from influencing the actual business operations, the experiment was built based on TensorFlow 2.5.0 and Keras 2.5.3 deep learning architecture for experimental

Table 1. Number of Packets of Each Type of Attack Traffic in the Training Data Set

Type of attack traffic	Frequency	Proportion
Scan	231	39.55%
DDos	129	22.09%
Botnet	110	18.84%
Spam	39	6.68%
Backdoor	75	12.84%
Total	584	100.00%

simulation; the operating system is Windows 10, using i7-12700H processor; the size of the memory is 16G, using the RTX3060 graphic card to increase the execution speed of the deep neural network.

The experiments were conducted to export some of the anomaly samples labeled by the probes as a training set to be input into the DCGAN-ResNet network for learning and generation.

A total of 584 PACP data were selected for the generation experiments, containing five attack categories and 84 attack types of character data. The five attack categories used were:

Scan: Scanning is a network attack where an attacker scans the ports or vulnerabilities of a target system to find opportunities for exploitation. Network scanners can help attackers discover open ports, unpatched vulnerabilities, and potential security weaknesses on the target system.

DDos: Distributed denial-of-service (DDoS) attack is a common network attack that aims to make the target system or network unable to provide services. Attackers control multiple computers or network zombies to send a large number of invalid or high-traffic network requests to the target, thereby exhausting the resources of the target system and crashing it.

Botnet: Botnet is a special kind of malware that exploits victims' computer resources to mine encrypted currency (such as Bitcoin). This virus typically runs in hiding on the victim's computer, consuming a large amount of CPU and GPU resources, and reducing system performance and battery life.

Spam: Spam is a network attack where attackers send large numbers of advertisements, junk messages, or other useless emails to harass recipients. Spam usually contains deceptive, misleading, or enticing content aimed at persuading recipients to click malicious links or download malware.

Backdoor: Backdoor is a network attack where attackers install hidden programs or command-line tools on the victim's computer to allow them to remotely control it. Backdoors allow attackers to access the victim's computer secretly and steal sensitive information, execute malware, or perform other malicious activities. Figure 6 depicts a pie chart illustrating the percentage of each type of attack traffic in the training dataset.

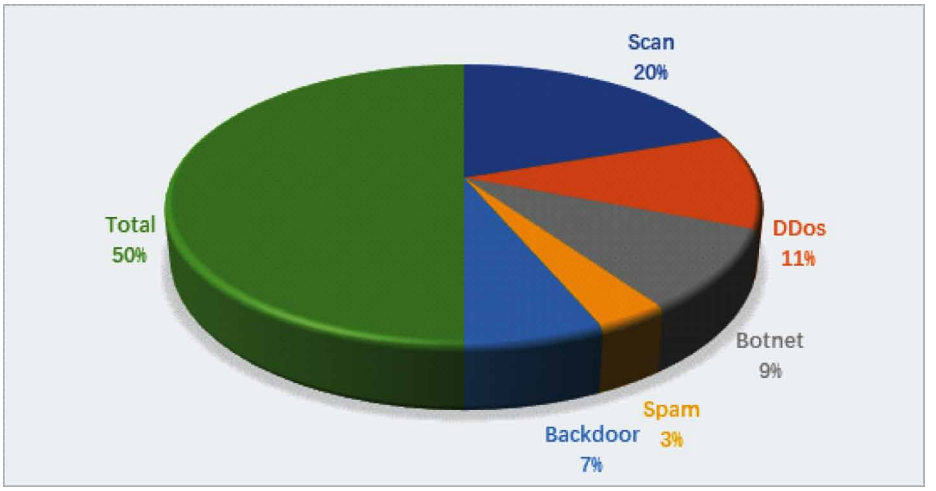
Evaluation Indicators

The main criteria for evaluating algorithm performance are outlined below:

True Positive (TP) represents correctly classified positive class samples.
True Negative (TN) denotes accurately classified negative class samples.
False Positive (FP) indicates negative class samples mistakenly classified as positive.
False Negative (FN) reflects positive class samples mistakenly classified as negative.

The experiments are theoretically verified on four models and compared by four evaluation indexes: accuracy, orecision, recall and F1-score. The specific calculation method is shown below:

Figure 6. Percentage of Each Type of Attack Traffic in the Training Dataset



Accuracy indicates the ratio of correctly predicted samples to the total number of samples.

$$Accuracy = \frac{TP + TN}{TP + FP + FN + PN} \tag{5}$$

Precision indicates the proportion of correctly predicted sample instances to the total predicted sample instances.

$$Precision = \frac{TP}{TP + FP} \tag{6}$$

Recall represents the ratio of predicted samples to the total samples in the dataset.

$$Recall = \frac{TP}{TP + FN} \tag{7}$$

F1-score is the weighted average of precision and recall.

$$F1 - Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{8}$$

Validation of Sample Imbalance

The experiment compares the performance of the sample equalized dataset and the original dataset on four machine learning algorithms – Decision Tree, Random Forest, Plain Bayes and AdaBoost – and verifies the effectiveness of malicious encrypted traffic enhancement based on DCGAN-ResNet sample enhancement in conjunction with evaluation metrics. The experimental results are shown in

Table 2. Evaluation Metrics After Balancing the Dataset

	Accuracy	Detection Rate	Recall Rate	F1-Score
Decision Tree	0.9451	0.9420	0.9630	0.9524
Random Forest	0.9785	0.9919	0.9740	0.9829
Plain Bayes	0.6195	0.9992	0.5558	0.7143
AddBoost	0.8476	0.8665	0.9987	0.9279

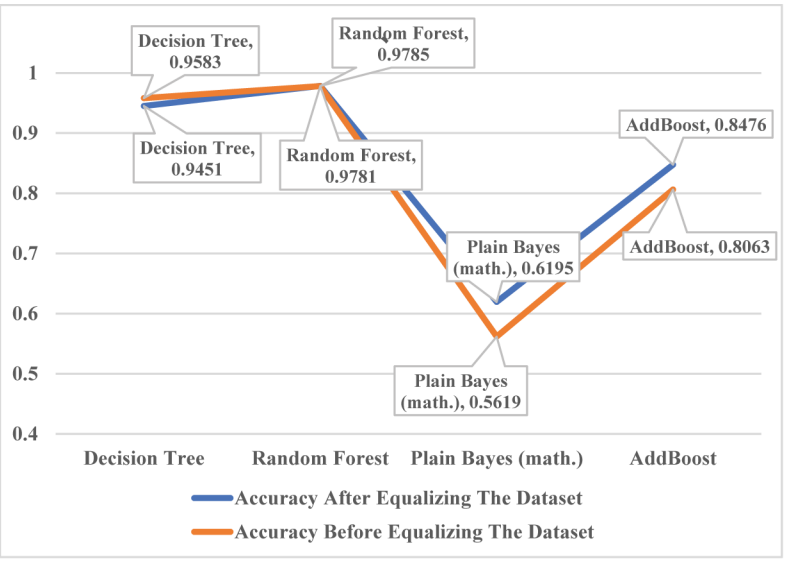
Table 3. Evaluation Metrics after Training on the Original Dataset

	Accuracy	Detection Rate	Recall Rate	F1-Score
Decision Tree	0.9583	0.9594	0.9590	0.9589
Random Forest	0.9781	0.9791	0.9789	0.9790
Plain Bayes	0.5619	0.9997	0.4892	0.6569
AddBoost	0.8063	0.8718	0.9352	0.9024

Table 2 and Table 3. Figure 7 is line chart, based on data from Table 2 and Table 3, and it demonstrates the comparison of recognition accuracy before and after training.

From the above table, we can see that compared to the original dataset, the equalized dataset has a slight decrease in the prediction index on the Decision Tree model, and an improvement on the Plain Bayes, Random Forest and AdaBoost models; this is because the original dataset has a huge proportion of normal traffic samples, and the classifier is inclined to the learning of normal traffic samples, which in turn makes more than 90% of the predicted data correctly classified normal traffic samples. After the dataset is equalized, there is an equal proportion of normal and malicious traffic samples, and the ability of the classifier to learn normal and malicious traffic is roughly the same,

Figure 7. Comparison of Recognition Accuracy Before and After Training



so the predicted correctly classified data has the same proportion of normal and malicious traffic. $F1-\text{Score}$ It can be seen as the overall performance; the detection effect obtained using the DCGAN-ResNet sample enhancement method has a relatively large improvement in this indicator, which verifies the effectiveness of the malicious encrypted traffic detection method based on the DCGAN-ResNet sample enhancement proposed in the paper and solves the problem of data imbalance.

COMPARISON WITH OTHER ADVANCED METHODS

In their research, Wang et al. (2020) demonstrated the classification of malicious websites using the Naive Bayes model. They categorized website features based on traffic data and classified the websites into two groups: malicious and benign using NB. Meanwhile, Miller et al. (2020) proposed a computational model to address the limitations of current VPN traffic detection. They utilized a neural network trained on Multilayer Perceptron (MLP), analyzing traffic statistics from TCP headers of captured network packets to create a VPN-usage detection model. In experiments using OpenVPN with tenfold cross-validation, the accuracy in identifying VPN traffic reached 93.71%. Additionally, Mohammad et al. (2021) introduced an improved DDoS attack detection model based on induction of rules from instances (IRI). The primary aim of Alam et al. (2020) was to develop an attack detection model for defending against phishing attacks using machine learning algorithms such as Random Forest and Decision Trees. Their model employed principal component analysis (PCA) for feature selection and achieved an accuracy of 97% using the RF algorithm (Alam et al., 2020). Sethi et al. (2020), using the same cloud dataset, proposed an intrusion detection system (IDS) to protect cloud networks from cyber-attacks. They applied a double deep Q-learning (DDQN) algorithm, achieving an accuracy of 96.87%. Using the RF algorithm, this study achieved an accuracy of 97.85% after training with the DCGAN-ResNet system, as shown in Table 4.

Figure 8 shows the recognition accuracy in this study significantly exceeds that of other studies.

Visualization Analysis

During the training process, the loss function keeps decreasing; Figures 9(a) and (b) below show the 8th and 317th training. The results of some of the data generated after the completion of training are plotted in Figure 9(c). As can be seen from the two figures (a) and (b), the loss function decreased from 2.6033 to 0.813, showing an obvious decline.

Figure 10 shows the change of the loss function during nearly 500 training sessions during the experiment. The value of the loss function decreases rapidly at the beginning of the training and becomes stable between 0.8-0.9, after about 400 sessions of training.

After approximately 400 sessions, the experiment transformed the generated data in PACP format and used the Scapy tool to transform the packets into traffic incorporated into as well as prepared models to simulate the process of training a learning model on a cyber security device machine.

Table 4. Comparison of the Results of Different Methods

Author	Problem Domain	Techniques	Results Accuracy
Wang et al. (2020)	Malicious Traffic	NB	90%
Miller et al. (2020)	Malicious Traffic	Neural Network	93.71%
Mohammad et al. (2021)	IDS	NB and HW	93.90%
Alam et al. (2020)	Phishing Attacks	RF, DT	97%
Sethi et al. (2020)	Malicious Traffic	DDQA	96.87%
Our paper	Malicious Traffic	RF	97.85%

Figure 8. Comparison with Other Research

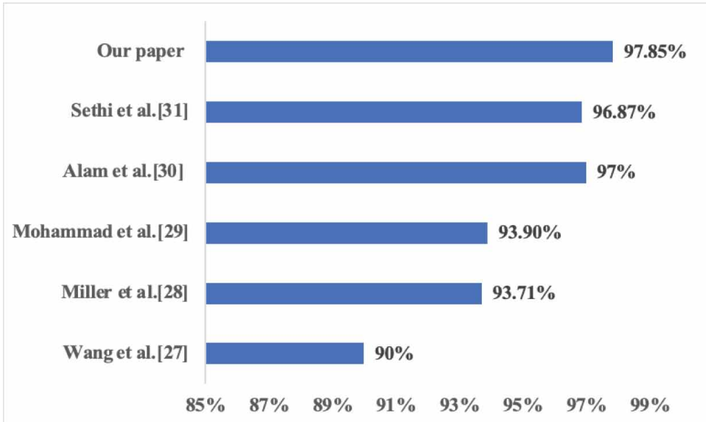
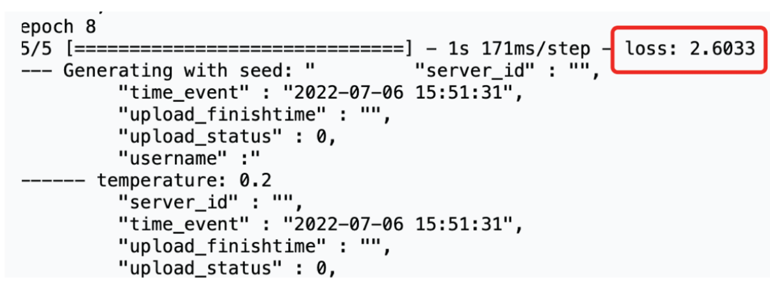
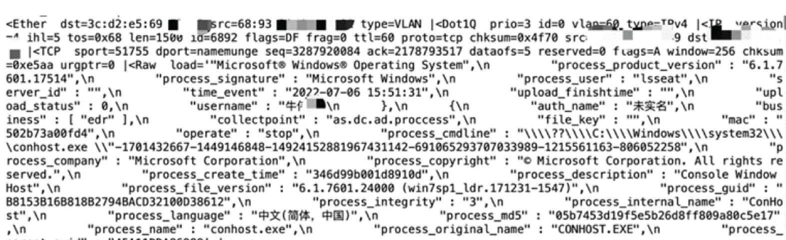


Figure 9. Training Results



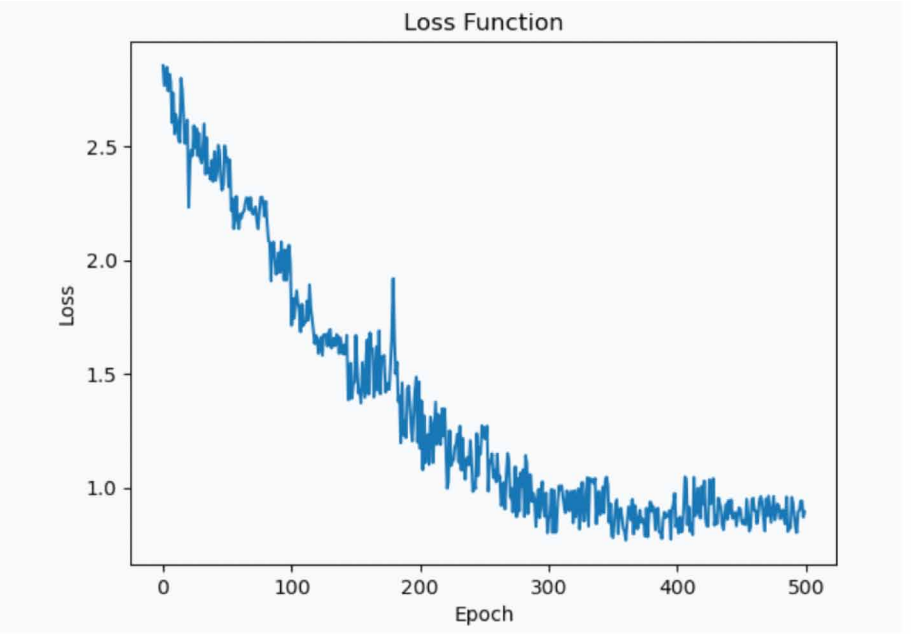
(a) 8th Training Results

(b) 317th Training Results



(c) Results After Training

Figure 10. Change of the Loss Function



CONCLUSION AND OUTLOOK

This article introduces a sample enhancement system based on DCGAN-ResNet to improve the detection effectiveness of network security devices and address the imbalance between "normal" and "malicious" sample distributions in current traffic data. The system utilizes the detection status of current network security devices and dataset conditions to automatically acquire parameters for generating malicious traffic data, establishing an adaptive model. With these parameters, the system learns and generates relevant features from malicious traffic samples. It further employs a Python program integrated with the Scapy tool to automate the distribution of PACP packets. Experimental results demonstrate that the sample enhancement system based on DCGAN-ResNet can to some extent resolve the issue of biased traffic data and enhance the effectiveness of the detection model. This sample enhancement system can be used in network security monitoring devices to train security monitoring devices to maintain sensitivity. When new 0-day vulnerabilities are discovered, this sample enhancement system can be used to quickly grasp and form effective protection.

However, there are still some issues. First, due to the unique nature of the technology, the system has not been widely applied and has only undergone limited experiments and simple applications in a small scope. Second, there is the issue of model training. When facing new types of malicious traffic attacks, retraining the model to learn and simulate the features of these new malicious samples requires considerable time and performance input. As a solution, the next step involves exploring data stream processing, gradually optimizing the model, and adopting a stream training method to better address the challenges posed by new types of attacks.

PROCESS DATES

Received: 1/25/2024, Revision: 3/6/2024, Accepted: 3/19/2024

FUNDING

No funding was received for this work.

CONFLICTS OF INTEREST

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

REFERENCES

Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 83965–83973. doi:10.1109/ACCESS.2020.2992249

Alam, M. N., Sarma, D., Lima, F. F., Saha, I., Ulfath, R. E., & Hossain, S. (2020). Phishing attacks detection using machine learning approach. *The 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT),* 1173-1179.

Alghazzawi, D. M., Hamid Hasan, S., & Bhatia, S. (2022). Optimized generative adversarial networks for adversarial sample generation. *Computers, Materials & Continua*, *72*(2), 3877–3897. doi:10.32604/cmc.2022.024613

Chuang, P., & Wu, D. (2019). Applying deep learning to balancing network intrusion detection datasets. *The 2019 IEEE 11th International Conference on Advanced Infocomm Technology (ICAIT),* 213-217.

Frid-Adar, M., Diamant, I., Klang, E., Amitai, M. M., Goldberger, J., & Greenspan, H. (2018). GAN-based synthetic medical image augmentation for increased CNN performance in liver lesion classification. *Neurocomputing*, *321*, 321–331. doi:10.1016/j.neucom.2018.09.013

Goodfellow, I., Pouget-Abadie, J., & Mirza, M. (2018). Generative adversarial networks. *IEEE Signal Processing Magazine*, *35*(1), 53–65. doi:10.1109/MSP.2017.2765202

Haddadpajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2019). A survey on Internet of Things security: Requirements, challenges, and solutions. *Internet of Things : Engineering Cyber Physical Human Systems*, *14*, 100129. doi:10.1016/j.iot.2019.100129

He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. *The 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* 770-778. https://www.doi.org/10.1109/CVPR.2016.90

Jamoos, M., Mora, A. M., Alkhanafseh, M. Y., & Surakhi, O. M. (2023). A new data-balancing approach based on generative adversarial network for network intrusion detection system. *Electronics (Basel)*, *12*(13), 2851. doi:10.3390/electronics12132851

Jia, N., Tian, X., Gao, W., & Jiao, L. (2023). Deep graph-convolutional generative adversarial network for semi-supervised learning on graphs. *Remote Sensing (Basel)*, *15*(12), 3172. doi:10.3390/rs15123172

Jiao, L., Fei, J., & Zhao, M. (2022). Malicious traffic detection model refactor method based on adaptive sample generation. *The 2022 IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 5,* 845-851.

Kawai, M., Ota, K., & Dong, M. (2019). Improved MalGAN: Avoiding malware detector by leaning cleanware features. *The 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC),* 40-45.

Kim, J. S., Maeng, Y., & Jang, M. (2019). Becoming invisible hands of national live-fire attack-defense cyber exercise. *The 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* 77-84.

Miller, S., Curran, K., & Lunney, T. F. (2020). Detection of virtual private network traffic using machine learning. *International Journal of Wireless Networks and Broadband Technologies*, *9*(2), 60–80. doi:10.4018/IJWNBT.2020070104

Mohammad, R. M., & Alsmadi, M. K. (2021). Intrusion detection using highest wins feature selection algorithm. *Neural Computing & Applications*, *33*(16), 9805–9816. doi:10.1007/s00521-021-05745-w

Moti, Z., Hashemi, S., Karimipour, H., Dehghantanha, A., Jahromi, A. N., Abdi, L., & Alavi, F. (2021). Generative adversarial network to detect unseen Internet of Things malware. *Ad Hoc Networks*, *122*, 102591. doi:10.1016/j.adhoc.2021.102591

Rathore, S., Park, J. H., & Chang, H. (2021). Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 90075–90083. doi:10.1109/ACCESS.2021.3077069

Ring, M., Schlör, D., Landes, D., & Hotho, A. (2019). Flow-based network traffic generation using generative adversarial networks. *Computers & Security*, *82*, 156–172. doi:10.1016/j.cose.2018.12.012

Sakhnini, J., Karimipour, H., Dehghantanha, A., Parizi, R. M., & Srivastava, G. (2019). Security aspects of Internet of Things aided smart grids: A bibliometric survey. *Internet of Things : Engineering Cyber Physical Human Systems*, *14*, 100111. doi:10.1016/j.iot.2019.100111

Seo, E., Song, H. M., & Kim, H. K. (2018). GIDS: GAN based intrusion detection system for in-vehicle network. *The 2018 16th Annual Conference on Privacy, Security and Trust (PST),* 1-6.

Sethi, K., Kumar, R., Mohanty, D., & Bera, P. (2020). *Robust adaptive cloud intrusion detection system using advanced deep reinforcement learning*. SPACE. doi:10.1007/978-3-030-66626-2_4

Sharma, P., Jain, S., Gupta, S., & Chamola, V. (2021). Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Networks*, *123*, 102685. doi:10.1016/j.adhoc.2021.102685

Sheet, O. I., & Ibrahim, L. M. (2023). Design and implement machine learning tool for cyber security risk assessment. *Journal of Education and Science*.

Siddique, K., Akhtar, Z., Aslam Khan, F., & Kim, Y. (2019). KDD Cup 99 data sets: A perspective on the role of data sets in network intrusion detection research. *Computer*, *52*(2), 41–51. doi:10.1109/MC.2018.2888764

Tang, X., Yin, P., Zhou, Z., & Huang, D. (2023). Adversarial perturbation elimination with GAN based defense in continuous-variable quantum key distribution systems. *Electronics (Basel)*, *12*(11), 11. doi:10.3390/electronics12112437

Wang, S., Wang, Y., & Tang, M. (2020). Auto malicious websites classification based on Naive Bayes classifier. *The 2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE),* 443-447.

Yang, C., Gan, X., Peng, A., & Yuan, X. (2023). ResNet based on multi-feature attention mechanism for sound classification in noisy environments. *Sustainability (Basel)*, *15*(14), 10762. doi:10.3390/su151410762

Yu, Y., Gong, Z., Zhong, P., & Shan, J. (2017). *Unsupervised representation learning with deep convolutional neural network for remote sensing images*. Springer., doi:10.1007/978-3-319-71589-6_9

Zhang, Q., Yang, J., Zhang, X., & Cao, T. (2022). Generating adversarial examples in audio classification with generative adversarial network. *The 2022 7th International Conference on Image, Vision and Computing (ICIVC),* 848-853.

Qiankun Li, MS degree from Worcester Polytechnic Institute, lecturer at Shijiazhuang University. Her current research interests include data security and safety management.

Juan Li, master of computer application technology, lecturer at Shijiazhuang University. Her research interests include new information technology engineering curriculum system.

Yao Li, master of telecommunications from Hong Kong University of Science and Technology, work at Shijiazhuang University. Her research interest include Internet of Things and smart agriculture.

Jiu Feng, master of Computer Application Technology from Taiyuan University of Science and Technology, work at College of Future Information Technology, Shijiazhuang University. His research interests include information security and data security.

Yunxia Chu, master from Hebei Normal University, professor at the Hebei Internet of Things Intelligent Perception and Application Technology Center. Her research interests include Internet of Things and modern educational technology.