Hindawi
Security and Communication Networks
Volume 2022, Article ID 7585457, 10 pages
https://doi.org/10.1155/2022/7585457

Research Article

Light Weighted CNN Model to Detect DDoS Attack over Distributed Scenario

Harish Kumar,[1] **Yassine Aoudni**,[2] **Geovanny Genaro Reivan Ortiz**,[3] **Latika Jindal**,[4] **Shahajan Miah**,[5] **and Rohit Tripathi**[6]

[1]*Department of Computer Science, College of Computer Science, King Khalid University, Abha 61413, Saudi Arabia*
[2]*Department of Computers and Information Technology, College of Sciences and Arts in Turaif, Northern Border University, Arar, Saudi Arabia*
[3]*Laboratory of Basic Psychology, Behavioral Analysis and Programmatic Development PAD-LAB, Catholic University of Cuenca, Cuenca, Ecuador*
[4]*Department Computer Science Engineering, Medi-Caps University, Indore, India*
[5]*Department of EEE, Bangladesh University of Business and Technology (BUBT), Dhaka, Bangladesh*
[6]*Electronics Engineering Department, J C Bose University of Science and Technology YMCA, Faridabad, India*

Correspondence should be addressed to Shahajan Miah; miahbubt@bubt.edu.bd

Received 28 March 2022; Revised 8 May 2022; Accepted 17 May 2022; Published 13 June 2022

Academic Editor: Robertas Damaševičius

Copyright © 2022 Harish Kumar et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The minimal-degree distributed denial-of-service attack takes advantage of flaws in the adaptive mechanisms of network protocols, which could have a big impact on network service quality. It is very hard to find, has a low attack rate, and comes at a set time. Detection methods that have been used before have problems because they only use one type of detection and are not very good at identifying the object. In the end, a way to detect many sorts of minimal DDoS assaults that use deep hybrid learning is suggested. To construct multi-type limited DDoS threat data sets and mimic diverse sorts DDoS assaults and legitimate traffic in varying situations in the 5G setting, collect congestion at the networking entry and extract flow feature info are considered. From a statistical threshold and feature engineering point of view, these data sets show how many sorts of minimal DDoS assaults are there. This study aims to develop a deep hybrid learning-based multi-type low-rate DDoS attack detection solution for 5G networks which is the novel model that is recently deployed, and a hybrid deep learning algorithm was used to train the algorithm offline, and the algorithm's performance was compared to that of the LSTM-Light GBM and LSTM-RF algorithms. The CNN-RF revealing model was then used to detect minimal DDoS assaults at the gateway, so that multiple attacks could be detected at the same time. It can identify 4 sorts of low-rate DDoS assaults like Slow-Headers, Slow-Body, Slow-Read, and Shrew assaults, in a 120-second window. The false intercept rate is 11.03 percent. This means that 96.22 percent of traffic could be found. Using the strategy suggested can help cut down on the traffic concentration of minimal DDoS attacks at the net ingress. It can also be used in real-world situations.

1. Introduction

The DDoS assault is the large-scale distributed and very damaging network attack approach that may adversely damage service availability. It has progressively grown among the utmost severe security risks to the web. With the continual innovation and updating of attack technology, a new assault variation, called a low-rate DDoS attack, is developed. This attack makes use of flaws in the network protocol adaptive mechanism to deliver attack packets at a lower rate, lowering the victim's service quality. It has good concealment and a low attack rate. There are low-rate/minimal DDoS assaults of many protocols in the network environment as well as periodic and aperiodic attack methods [1]. As a result, effectively identifying many forms of minimal DDoS assault traffic is an important challenge that must be addressed.

This research primarily offers a multi-type low-rate DDoS assault revealing approach for networks in the 5G context based on deep hybrid learning. First, experimental data sets are obtained by simulating various sorts of low-rate assaults and normal communication behaviour; then, the characteristic information of various types of low-rate DDoS assaults is analyzed, and feature selection is performed based on the usual information; finally, the detection model is realized by combining the hybrid deep learning algorithm. Finally, the detection model is placed at the network's entry to enable online detection of many sorts of low-rate DDoS assaults.

This study's key contributions are as follows:

(1) Various forms of low-rate DDoS assaults and normal communication in diverse settings are simulated in the 5G environment, network traffic characteristic information during a specific time is gathered, and a tagged minimal-degree DDoS assault data set is generated.

(2) A multi-type low-rate DDoS assault feature set is suggested. The characteristic information of several forms of low-rate DDoS assaults and ordinary traffic is investigated from the standpoint of statistical thresholds and feature engineering, and 40 effective minimal-degree DDoS assault characteristics are derived.

(3) A multi-type low-rate DDoS assault detection approach is provided. The offline training, deployment, and detection of hybrid deep learning models are implemented using the low-rate DDoS assault feature set. The detection findings demonstrate that by choosing the ideal time frame, the approach presented in this study can efficiently identify four forms of minimal DDoS assaults, namely, Slow-Headers attack, Slow-Body attack, Slow-Read attack, and Shrew attack.

2. Related Work

For a long time, the research on minimal-degree DDoS assaults has received extensive attention from scholars at home and abroad. At the beginning of the 21st century, Kuzmanovic proposed the definition of Shrew attack, collected relevant data of minimal-degree DDoS assaults, and conducted appropriate analysis and research [2]. The research on minimal-degree DDoS assault revealing and defense mainly includes twofold methods. One is the detection method based on statistical analysis. The authors proposed a minimal-degree DoS assault revealing method centred on the Pearson relationship, which uses the Pearson coefficient of correlation based on the Hilbert spectrum net congestion, to characterize network traffic information, and compares this information with a threshold to detect low-rate attacks against TCP [3]. Author analyzed the sequence similarity between the minimal-degree DDoS assault pulses at the victim end from the perspective of sequence matching, used the Smith–Waterman algorithm, and designed a double-threshold rule to detect TCP-based low-rate attacks [4]. The authors proposed a method based on network self-similarity to analyze the impact of low-rate attacks on traffic self-similarity and used H-index combined with thresholds to identify attacks and legitimate traffic [5]. The deep neural model (DNN) is proposed as a deep learning technique for malware detection on a subset of frames acquired from data transfer [6]. The method suggested by the researchers limits the cost of interference in IoT transmitting data, and the network's smart use of training sets efficiently differentiates the conventional and threat sequences [7]. The above methods for detecting low-rate attacks only see low-rate attacks based on TCP and depend on the set of points, which are easily affected by the randomness of the network environment and cannot achieve excellent detection results.

Another kind is machine learning-based detection, which uses traffic properties and M-L procedures to identify minimum degree DDoS attacks. The authors recommended an approach on the fundamentals of principal factor investigation and S-V-M to sense minimal-degree TCP assaults. The major component analysis tactic effectively captures network communication properties while filtering noise from the environment [8]. The authors proposed a minimal-degree DDoS assault detection method for TCP in edge environments, which used local complex feature mining and deep CNN to acquire the finest trait distribution of raw info automatically, and deep reinforcement learning Q networks as decision-making to improve attack detection decision-making accuracy [9]. The authors constructed a minimal-degree DDoS assault detection system based on decomposition machines, offered a feature combination mechanism, established the correlation between feature samples, and detected HTTP-based low-rate assaults. J48, random tree, REP tree, random forest, multilayer perceptron, and support vector machine are six models that detect HTTP-based minimal-degree DDoS assaults, according to Reference, which proposes using machine learning approaches to identify low-rate DDoS assaults in the SDN situation [10]. DNN models can perform efficiently and precisely although with small samples since its architecture includes segmentation method and identification procedures, and also strands that upgrade themselves as they are programmed [6]. This method, however, has a higher false-positive rate than DDoS assaults. Hybrid deep learning algorithms may fully use the advantages of machine learning and deep learning algorithms. This article includes multiple machine learning models to anticipate application layer DDoS assaults in real time [11]. The authors have proposed CyDDoS architecture for an automated intrusion detection system (IDS) that blends a feature map synthesis algorithm with such a neural network [12].

A hybrid based on a long-short-term-memory network and a CNN was suggested by researcher. Therefore, successfully implementing security strategy to prevent a system from this danger is a significant issue since DDoS employs a variety of attack methods with numerous conceivable combinations [13]. The deep learning architecture detects Bot, Post Scan, and XSS threats in the CICIDS2017 data set. The detection system has been proved to have better detection capabilities [14]. The authors proposed a deep learning-based hybrid anomaly detection system that uses the limited Boltzmann machine and support vector machine methods to reduce the data's feature dimensions, but the data set used in the investigation was KDD99, which is incorrect. At a finer level, DoS assaults are categorized and identified. The authors proposed a hybrid time-series forecasting model for stock forecasting based on an extended short-term memory network and LightGBM, which performed well [15]. In terms of prediction, author proposes a hybrid deep learning model based on an extended short-term memory network and random forest (RF, random forest), which outperforms a single machine learning strategy [16]. Minimal-degree DDoS assault revealing approaches, such as the ones given above, can only identify a single sort of minimal DDoS assaults, which has the drawbacks of only detecting one type of attack and low detection accuracy. Given the aforementioned limitations, this research proposes a CNN-RF hybrid deep learning-based minimal-degree DDoS assault revealing system that can learn the characteristics of many kinds of attack traffic and improve the accuracy of online detection of numerous sorts of minimal-degree DDoS assaults.

3. Characteristic Analysis of Minimal-Degree DDoS Assaults

In this study, minimal-degree DDoS assaults are classified into two types: HTTP-based low-rate DDoS attacks and TCP-based minimal-degree DDoS assaults [17].

Slow-Headers, Slow-Body, along with Slow-Read assaults are examples of HTTP-based minimal-degree DDoS assaults [18]. This sort of assault exploits the weakness in the current HTTP Keep-Alive method, maintains the connection for an extended period of time, and continually consumes resources of server, ensuing in a service denial to the Web server. Among these, the Slow-Headers attacker sends an unfinished HTTP request ending with the character “rn,” causing the server to believe that the request was not delivered and continuing to wait. Finally, the number of connections approaches the server’s maximum capacity, and the new request is unable to be handled, resulting in a rejection-service assault. The sluggish body attacker makes a POST request to the server with a large content-length value. Even yet, the server only delivers a tiny amount of bytes each time, and the server’s resources are depleted when requests exceeds an assured threshold. Finally, Slow-Read attackers submit valid requests to the server to read huge data files while setting the TCP sliding window to a low number. As a consequence, establishing a communication link between the server and the attacker takes a lengthy time. When the number of connections exceeds a certain threshold, the service cannot be supplied.

TCP-based low-rate DDoS assaults come in a variety of flavors. This research focuses on the Shrew attack, which leverages the TCP timeout retransmission mechanism to transmit high-speed burst packets on a regular basis, lowering the victim’s quality of service and performance. The suggested model overcomes it by incorporating a novel position-oriented neural layer [19]. This article mostly replicates four forms of minimal-degree DDoS assaults using attack tools and Python scripts: Slow-Headers assaults, Slow-Body assaults, Slow-Read assaults, and Shrew assaults.

A typical analysis of minimal-degree DDoS attacks is mostly based on the original minimal-degree DDoS assaults. The CICFlowMeter feature extraction program extracts comprehensive bidirectional flows based on time frames, reflecting properties such as forward and reverse data flows. This technique is used as our research is mainly aimed on the attack tools namely as Slow-Headers attack, Slow-Body attack, Slow-Read attack, and Shrew attack; however, this work mostly replicates four forms of low-rate DDoS assaults. Aside from tag values, the device produces a total of 83 other types of feature information, such as flow ID, quintuple information, stream-level features, and package-level features. The flow ID is a penta-tuple consisting of the birthplace IP address, purpose IP address, port location, destiny port, and procedure that is used to uniquely identify the flow. Stream-level characteristics include statistics regarding the stream’s time, duration, and bytes per second. The amount of forwarding/reverse packets per second, statistical factors of packet length, SYN/FIN/RST flag bit count, and so on are all packet-level characteristics.

4. Minimal-Degree DDoS Assault Detection Framework

This section first introduces the composition of the detection framework, then introduces the principle and implementation of the data set generation module, and finally presents the specific performance and critical technologies of the offline training module and online detection module of the hybrid deep learning model detail. The detection framework comprises a data set generation module, feature analysis and selection module, a detached training unit, and a connected detection unit. The minimal-degree DDoS attack detection framework is shown in Figure 1. The framework is divided into data processing and deep hybrid learning. Figure 2 shows the flowchart for the proposed methodology.

The data processing part is responsible for preliminary processing of the acquired network traffic and is divided into a data set generation module and feature analysis and selection module. The data set generation module is used to obtain network traffic in a specified period, extract flow feature information, and perform data cleaning to get minimal-degree DDoS assault data set containing 4 types of minimal-degree DDoS attacks and regular traffic. The trait analysis and selection module analyzes the trait information of different kinds of minimal-degree DDoS assault from statistical thresholds and trait engineering and summarizes the valuable features of multiple types of minimal-degree DDoS assault.

The deep hybrid learning component detects many sorts of minimal-degree DDoS assaults and is separated into twofold segments: disconnected training and connected detection. The disconnected training unit selects valuable features from the data set for feature selection, uses a hybrid deep learning algorithm for training and testing, performs performance evaluation and related parameter optimization based on classification results, and selects the best attack detection model. By recording traffic in real time, the online

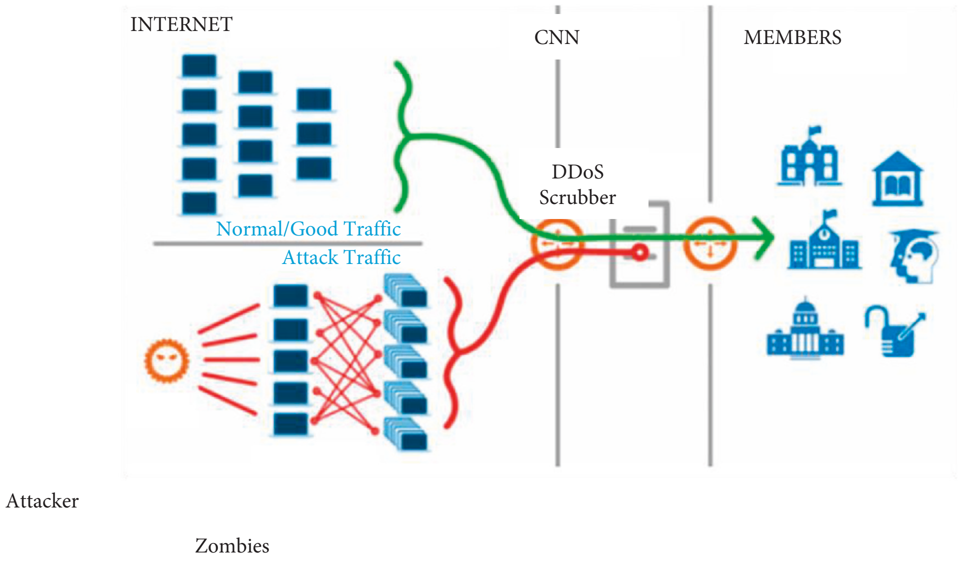

Figure 1: Minimal-degree DDoS assault detection framework.

detection module deploys the trained hybrid deep learning detection model to the network entry and achieves connected revealing of different forms of minimal-degree DDoS assaults. A model's output information is employed to recognize minimal-degree DDoS assaults on traffic to be detected—a particular sort of attack.

4.1. Data Processing Part

4.1.1. Data set Generation Module. The data set generation module is used to obtain the network traffic in a certain period. Then, the flow feature information is extracted by the flow feature extraction tool CICFlowMeter to get a minimal-degree DDoS assault data set. This data set contains multiple sorts of minimal-degree DDoS assaults and regular communication congestion in 5G environ, reflecting the traffic patterns in natural environments.

The generated a hefty figure of regular transmission simulation requests according to the third-generation cooperation project (3GPP) and IEEE for actual traffic laws of devices in different 5G application scenarios [20, 21]. This rule is obtained through the traffic data collected in the real scene. The result includes the influence of various environmental factors, which can reflect the request situation in the exact location. In this study, the method is improved to generate regular communication traffic. Combined with the four minimal-degree DDoS assault traffic generated by outbreak tools as well as scripts, a new minimal-degree DDoS assault data set will be obtained.

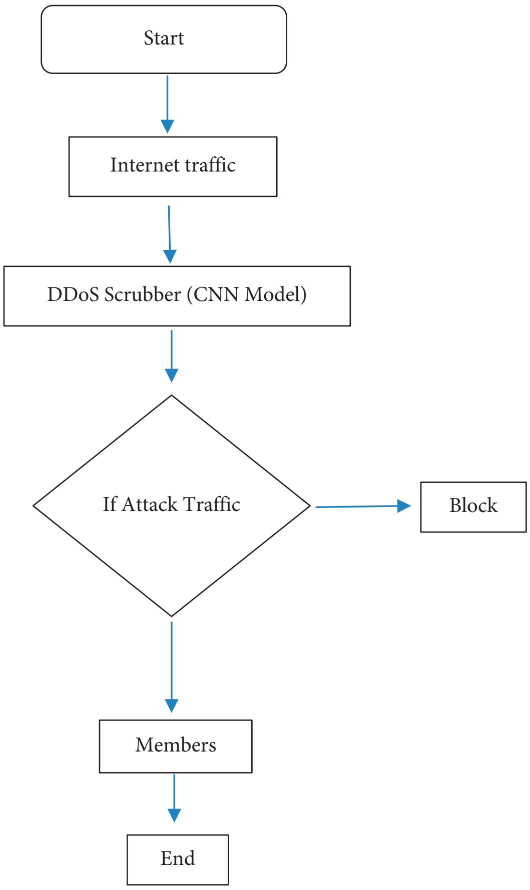

Figure 2: Flowchart.

As per this study, attack is realized by sending traffic through attack tools. Considering the security of the network environment, the capture of low-rate network traffic is recognized based on the VMware vSphere virtualization experimental platform. The realistic environment is close to the natural environment, reflecting the traffic statistics in the virtual environment. Thereafter, the traffic collection tool Tcpdump is deployed and installed to capture the data packets in the network. The data set collection point is at the access gateway of the network entrance, which can completely capture the communication traffic in the network. Finally, CICFlowMeter is used to extract characteristic information of network traffic. At the same time, according to the attack plan in Table 1, the extracted feature information

Table 1: Minimal-degree DDoS attack plan.

Attack time	Source IP	Destination IP	Traffic type
2021.5.25	23.1.0.22	23.1.1.22	Slow-Headers
	23.1.0.12	23.1.1.23	Slow-Body
	23.1.0.13	23.1.1.24	Slow-Read
15 : 35–16 : 15	23.1.0.14	23.1.1.25	Shrew
	23.1.0.20~23.1.0.29	23.1.1.73	Normal flow

is labeled, and the labeled data set is used for the training and verification of the detection model. This article includes multiple machine learning models to anticipate application layer DDoS assaults in real time. The authors have proposed CyDDoS, an architecture for an automated intrusion detection system (IDS) that blends a feature map synthesis algorithm with such a neural network [22]. The three types of minimal-degree DDoS attack methods, Slow-Headers assault, Slow-Body assault, and Slow-Read assaults studied in this article, send the attack traffic by modifying the parameters of the slow Http test and slow HTTP attack tool, and the Shrew attack realizes the sending attack by writing Python scripts flow. Python scripts are used for regular communication requests based on the statistical laws of different scenarios in the 5G environment to simulate sending massive connection regular request traffic. Based on the above implementation methods, this study collects traffic and automatically extracts flow feature information under minimal-degree DDoS assault and normal communication behaviour [23]. In our investigation, the capture period starts at 08:00 on May 19, 2021 and ends at 17:00 on May 24, 2021. During this period, different attacks were launched, including low-rate DDoS assaults, DDoS network stratum assaults, DDoS application stratum assaults, and distributed reflection amplification attacks. Table 1 shows the attack plan for minimal-degree DDoS assaults.

Based on the network traffic pcap file obtained by the above attack plan, the traffic feature extraction tool CIC-FlowMeter is employed to excerpt the traffic trait info, and a multi-type minimal-degree DDoS assault data set is obtained. Table 2 depicts the quantity of data samples of every single traffic type in the data set and the ratio of standard traffic samples. It can be seen that the number of data samples of regular traffic is plentiful superior than the count of data samples of each minimal-degree DDoS attack, reflecting the minimal-degree DDoS attacks.

5. Experiment and Result Analysis

This study simulates various minimal-degree DDoS attacks and regular communication requests in the 5G environment. It conducts performance evaluations of different hybrid deep learning detection models and online detection performance tests under other detection time windows. Table 2 displays the number of data samples from each traffic category in the data set as well as the ratio of regular traffic data. Figure 3with Tables 3 and 4depicts the efficiency and $F1$ value of the three models. As shown in Figure 4, for detecting Slow-Headers attack traffic, the CNN-RF model outperforms the other two models in terms of effectiveness and F1 value for identifying ordinary benign traffic.

Table 2: Number and proportion of data samples for each traffic type.

Traffic type	Number of data samples	The proportion of attack traffic to normal traffic
Slow-Headers	100 793	01 : 04.5
Slow-Body	110 044	01 : 04.5
Slow-Read	68 074	01 : 04.5
Shrew	45 389	01 : 04.5
Normal flow	460 619	—

5.1. Experimental Environment. To authenticate the revealing effect of the technique in this research on multi-type low-rate DDoS attacks, a related test platform is built on the network platform using actual network equipment.

In this study, a virtual platform based on Vmware vSphere is set up as the experimental environment. A total of nine hosts were used in the experiment, including two routers, one client host, four dummy hosts, and two web servers. The investigation in this study builds a hybrid deep learning model based on the TensorFlow framework. The programming language is Python3.8, and the machine learning library of TensorFlow2.1 and Keras2.2.4 is used to build the model. The Ubuntu18.04 is software background in server operating structure, and the number of virtual cores is 8, the memory is 8 GB, four hosts are used as puppet hosts, and two virtual machines built with web servers are used as attacked servers. This is critical to halt fraudulent activity since they have a long-term influence on financial circumstances. Outlier detection has several essential applications for fraud prevention [24]. Detection is performed at the network entry router, and data collection and cleaning functions are provided.

The simulation includes public services, smart homes, PC Internet access, and MTC communication based on this connection.

The four transmission scenarios generated a large number of regular communication data requests. Minimal-degree DDoS assault attacker controls four puppet hosts to periodically send minimal-degree DDoS attacks based on HTTP protocol and TCP protocol to the web server. The experimental minimal-degree DDoS assault types select HTTP-based Slow-Headers assaults, Slow-Body assaults, Slow-Read assaults, and TCP-based Shrew assaults [25].

5.2. Evaluation Indicators. The minimal-degree DDoS assault detection framework implements offline training and online detection for various kinds of minimal-degree DDoS assault data based on hybrid learning procedure [26]. Offline activity mainly analyzes the model's classification performance through six evaluation indicators: accuracy, precision, recall, $F1$ value, detection time, and confusion matrix. Among them, the rate of exactness symbolizes the ratio of

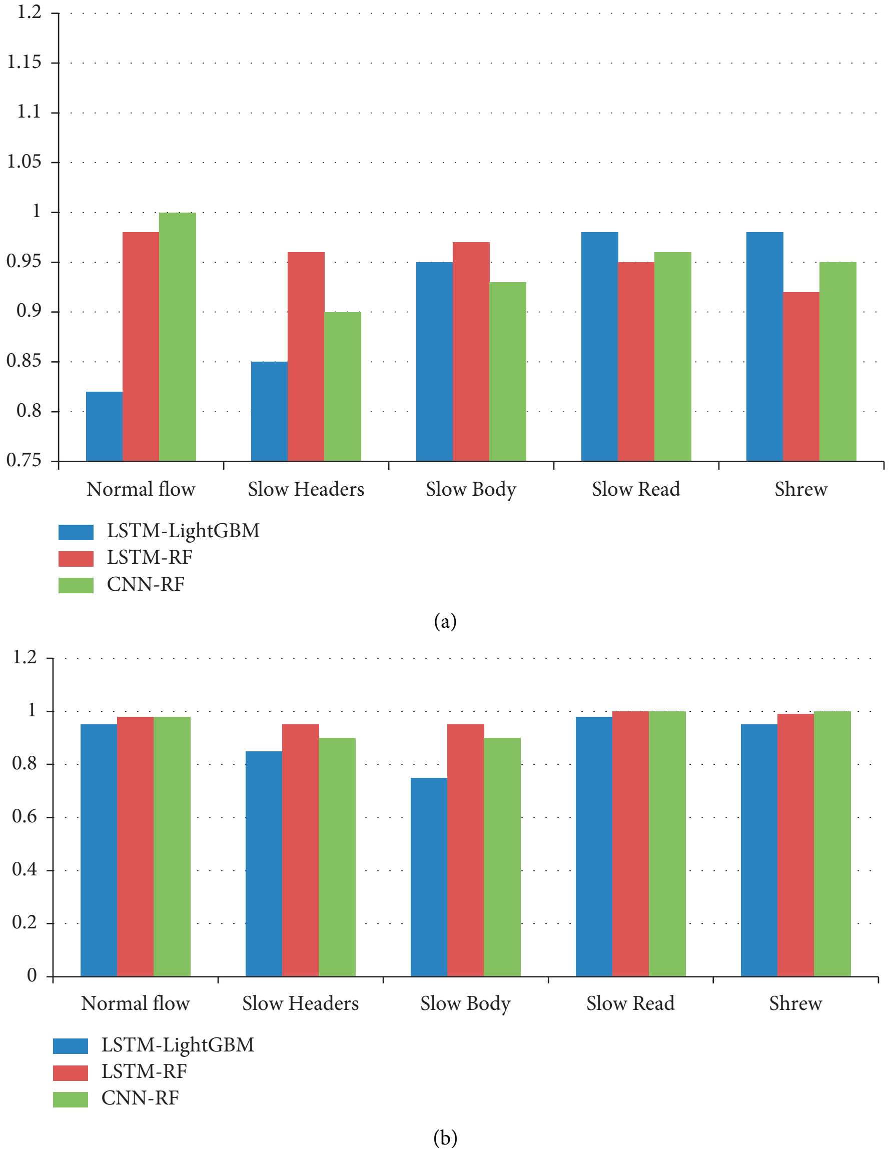

FIGURE 3: Comparison of precision and *F*1 scores of different models. (a) Comparison of the accuracy of different models. (b) Comparison between *F*1 of different models.

TABLE 3: Comparison of the accuracy of different models.

*F*1 value	LSTM-LightGBM	LSTM-RF	CNN-RF
Normal flow	0.82	0.98	1
Slow-Headers	0.85	0.96	0.9
Slow-Body	0.95	0.97	0.93
Slow-Read	0.98	0.95	0.96
Shrew	0.98	0.92	0.95

TABLE 4: Comparison between *F*1 of different models.

*F*1 value	LSTM-LightGBM	LSTM-RF	CNN-RF
Normal flow	0.95	0.98	0.98
Slow-Headers	0.85	0.95	0.9
Slow-Body	0.75	0.95	0.9
Slow-Read	0.98	1	1
Shrew	0.95	0.99	1

the amount of exact samples classified through the prototype to the overall quantity of pieces; the exactness degree represents the proportion for an amount of samples suggested by prototype as an attack category and the count of samples that are assault kinds; and the recall rate represents the prototype suggested as an attack category [27]. The share of the sum of pieces to all the examples of this assault type are as follows: the *F*1 value combines the results of precision and recall, representing the harmonic average of the two, which can more accurately reflect model performance; detection time reflects the time complexity of the model. It is used to measure the time efficiency of the model; the classification effect of the prototype is examined by employing confusion matrix as well as the grade to which the predicted label matches the actual label, which corresponds to the recall rate numerically [28].

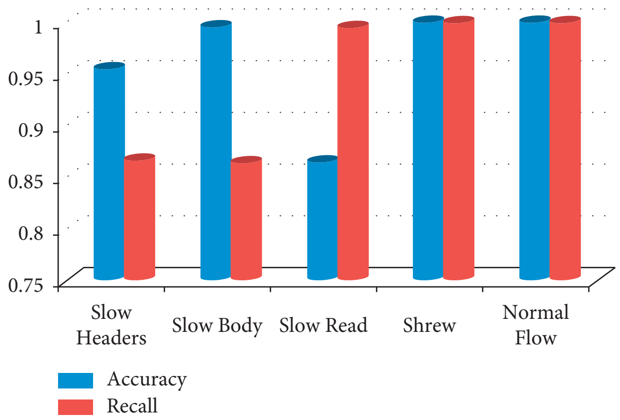

Figure 4: Detection performance.

In addition, to analyze the classification of online detection, new evaluation indicators are defined: false intervention degree and malicious congestion revealing degree used to evaluate an online detection of normal and malicious traffic, respectively. Among them, the false interception rate represents the proportion of misjudging regular traffic as diverse kinds of minimal-degree DDoS assaults, and the calculation is shown in formula (1); the malicious traffic detection rate represents the proportion of detected malicious traffic to the overall count of negative traffic samples, and the calculation is shown in formula (2).

$$\text{false}_{\text{interception}_{\text{rate}}} = \sum_{i=1}^{4} \frac{G_i}{M}, \quad (1)$$

$$\text{Malicious}_{\text{trafficdetection}_{\text{rate}}} = 1 - \sum_{i=1}^{4} \frac{T_i}{\sum_{i=1}^{4} B_i}, \quad (2)$$

where G_i represents the number of data samples that misjudge the regular traffic in the network environment as a further four forms of minimal-degree DDoS assault traffic after online detection; M represents the total number of data samples of regular traffic in the network environment; T_i represents the number of undetected data samples of minimal-degree DDoS assault congestion within the network environment after detection; B_i represents the total number of data samples of different types of minimal-rate DDoS assault congestion within the network environment.

5.3. Offline Training Analysis. Based on the minimal-degree DDoS assault data set obtained by the data set generation module in Section 3, data cleaning is performed, including processing the feature data with null feature values and processing feature data with infinite feature values. Feature selection is carried out according to the 40 useful features shown in Figure 3 and is distributed in a dual sets as training as well as test in a ratio of 7 : 3. The data set is shown in Table 5. The total number of data samples in the minimal-degree DDoS assault data set is 794,919, including 556,444 in the preparation set as well as 238,475 in the training set.

Table 5: Minimal-degree DDoS assault data set.

Data set type	Normal flow samples	Number of attack traffic samples
Training set	288555	267800
Test set	129832	108943

The CNN-RF model showed optimal performance through hyperparameter search, given the same minimal-degree of DDoS assault data set and eigenvalues. At the same time, the CNN-RF prototype projected in this study is associated with the LSTM-LightGBM prototype and the LSTM-RF prototype, and the optimum hybrid deep learning prototype is nominated to identify the connected revealing of multi-type minimal-rate DDoS assaults. This study uses four evaluation indicators: detection time, precision rate, $F1$ value, and confusion matrix. Figure 3 shows the confusion matrix performance of the three hybrid deep learning models. It may be perceived that the recognition precision of LSTM-Light-GBM model for each traffic type varies greatly, especially the recognition accuracy of the Slow-Body attack is only 0.5565, and the false-positive rate of the Slow-Headers attack is 0.2695. The recognition accuracy of the LSTM-RF model for the five types of traffic is better than that of the LSTM-LightGBM prototype, especially the recognition accuracy of the Slow-Read attack is about 0.9992, but it will produce a false-positive rate of 0.0788 when identifying the Slow-Body attack. The accuracy of the CNN-RF model overperforms the LSTM-RF, especially the recognition accuracy of Slow-Read assaults and Shrew attack can reach 0.9999. The recognition accuracy of Slow-Headers attack traffic can also get 0.9566.

Figure 3 with Tables 3 and 4 shows the evaluation of the three prototypes in terms of exactness and $F1$ value. As can be seen from Figure 3, for the identification of regular benign traffic, the CNN-RF prototype outperforms the other two designs in terms of accuracy and $F1$ value; for the detection of Slow-Headers attack traffic, the accuracy of the CNN-RF design is the best. Excellent: the LSTM-RF and LSTM-LightGBM models have similar performance in $F1$ value; for detecting Slow-Body and Slow-Read assault congestion in net, the LSTM-LightGBM design has poor performance in both accuracy and $F1$ score, and the CNN-RF model's performance is poor. Best performing: for Shrew, the detection of attack traffic in the three models is in the two evaluation indicators of good performance.

The detection time comparison of different hybrid deep learning ideas is presented in Table 5. It may be seen from Table 6 that the detection time of the CNN-RF model is 268.3689 s, which is about 9 s longer than that of the LSTM-LightGBM design, and about 40 s more minor than that of the LSTM-RF model. However, the LSTM-LightGBM design is significantly lower than the CNN-RF design in detection accuracy and $F1$ score. Therefore, while the detection time is shorter, the CNN-RF design has better accuracy and $F1$ value for various forms of minimal-rate DDoS assaults and regular congestion.

Combining the above evaluation indicators, it can be concluded that the distinction of LSTM-LightGBM model

Table 6: Comparison of detection time of different models.

Model category	LSTM-LightGBM	LSTM-RF	CNN-RF
Detection time/s	259.8986	308.5964	268.3689

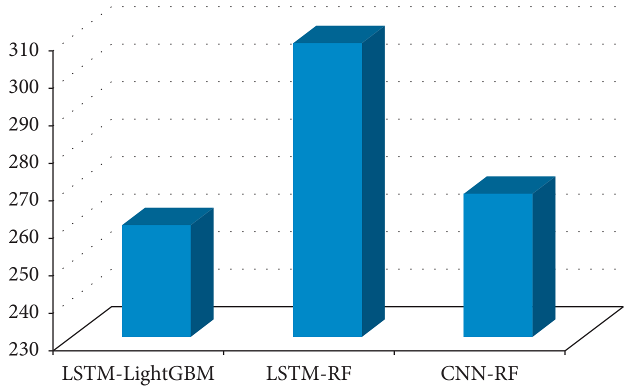

Figure 5: Comparison of detection time.

along with the LSTM-RF model, the CNN-RF model proposed in this article has better performance in regular traffic. Slow-Headers assault, Slow-Body assault, Slow-Read assault and Shrew's assault traffic detection as well as classification all show excellent performance and can accurately detect different types of low-rate DDoS attacks.

5.4. Online Inspection and Verification. The offline training experiments and analysis in Section 4 show that the CNN-RF model has excellent detection performance. To further illustrate that the model version is still the best in online detection, this section compares the performance of LSTM-LightGBM, LSTM-RF, and CNN-RF models in expressions of precision, error interception degree, and malicious traffic detection degree. The contrast of detection time is shown in Figure 5.

Finally, the best-performing and trained model under the optimal time window is selected, and the fine-grained online detection of multi-type low-rate DDoS attacks is deployed. First, multiple types of minimal-degree DDoS assault traffic files online are replayed, Tcpdump is used to internment network congestion inside the specified detection time window, and flow feature information is extracted through CICFlowMeter; then, the structure and parameters of the trained detection model are read and implemented for online detection. The model outputs detection classification labels, actual labels, and malicious traffic IP addresses; finally, based on statistical methods, the model's detection accuracy rate and negative traffic detection rate and other indicators are viewed.

This section compares the performance of the benchmark detection time window of 60 s with the detection time window of 120 s and 180 s and compares the LSTM-LightGBM, LSTM-RF, and CNN-RF models, respectively, and selects the optimal detection model. The optimal detection time window below is the final online detection parameter. Table 7 shows the performance comparison of the accuracy, false interception rate, and malicious traffic detection rate of different models under different time windows.

Table 7: Comparison of online detection performance of different models under different time windows.

Model name	Time window/s	Accuracy	False interception rate	Malicious traffic detection rate
LSTM-LightGBM	70	0.85394	0.28498	0.85244
	110	0.89384	0.20312	0.87258
	190	0.87698	0.21015	0.88593
LSTM-RF	70	0.90894	0.20591	0.96852
	110	0.92438	0.17419	0.95478
	190	0.89394	0.19875	0.92574
CNN-RF	70	0.9569	0.17058	0.87244
	110	0.95347	0.11789	0.88574
	190	0.98397	0.20591	0.98657

It can be seen from Table 7 that under the time window of 120 s, the LSTM-LightGBM, LSTM-RF, and CNN-RF models all show relatively optimal detection performance. The accuracy of the LSTM-RF model reaches 0.9243, and the malicious traffic detection rate is 0.9193. When the detection time window is 180 s, the accuracy of the LSTM-RF model drops to 0.897 6; simultaneously, the false interception rate increases to 0.192 7, indicating that a huge quantity of regular, benign transportation is misjudged as malicious traffic. Under the time window of 120 s, the LSTM-LightGBM model performed the worst, with an accuracy of only 0.896 5 and a false intercept rate of 0.203 1. For the CNN-RF model, when the online detection time window is 120 s, the minimum false intercept rate is 0.110 3. That is, the proportion of regular traffic being misjudged as malicious traffic is the lowest; at the same time, the negative traffic data samples detected by this detection mechanism are highest. The ratio of the number is 0.962 2. After analysis, the detection time window of 120 s altogether includes the characteristic information of different sorts of minimal-rate DDoS attacks, reflecting the complete minimal-degree DDoS assault activities, thus effectively distinguishing different kinds of minimal-rate DDoS attacks from regular traffic.

Consequently, the detection time window is set to 120 s, and the CNN-RF model with the best performance is deployed to realize online detection. The detection performance for diverse categories of minimal-rate attacks and regular traffic is obtained through the detection, as shown in Table 8. From Table 8 and Figure 4, it can be seen that the precision rate of the CNN-RF hybrid deep learning model for Slow-Headers assaults, Shrew attack, and regular traffic is above 0.95; and for Slow-Read attack and Slow-Body attack traffic, the precision and recall rate are both above 0.86, resulting in fewer misjudgments between the dual attack categories. In summary, detection exactness of the CNN-RF hybrid deep learning model for every kind of minimal-degree DDoS assaults and regular congestion in traffic reaches 0.965 2, which can accurately detect different types of low-rate DDoS attacks online.

Table 8: Online detection performance under 120-s time window.

Traffic type	Accuracy	Recall
Slow-Headers	0.9546	0.8666
Slow-Body	0.9952	0.8639
Slow-Read	0.8647	0.9948
Shrew	0.9998	0.9994
Normal flow	0.9999	0.9995

It can be seen from the above analysis that the CNN-RF hybrid deep learning model proposed in this article has excellent online detection performance and can realize connected revealing of four kinds of minimal-degree DDoS assaults. At the same time, the accuracy degree of each minimal-degree DDoS assaults is above 0.85, which can prevent the attack from causing more damage to the network; the malicious traffic detection rate reaches 0.962 2, and the detection accuracy rate reaches 0.965 2, which can effectively detect the web online. The malicious traffic in the network reduces the concentration of minimal-degree DDoS assault traffic at the ingress network.

6. Conclusion

Aiming at four types of minimal-degree DDoS assaults, this study obtains minimal-degree DDoS assault data sets, analyzes and obtains 40 effective traits of minimal-degree DDoS assaults, and proposes a variable-kind minimal-degree DDoS based on CNN-RF hybrid learning. The attack detection method and online deployment of this model realize connected revealing of variable types of minimal-degree DDoS assaults. Furthermore, an online detection time window is proposed, and the online detection performance is evaluated using false intervention degree and malicious network congestion revealing rate. Experiments show that the prototype based on CNN-RF hybrid deep learning algorithm can accurately detect different types of minimal-degree DDoS assaults. At the identical interval, the revealing method in this study is highly portable, and the minimal-degree DDoS assault data set is used close to the actual situation, which can be deployed and applied in practical environments when the hybrid deep learning model implements training and detection for multi-type low-rate DDoS attacks. The online detection accuracy in different scenarios decreases related to the attack traffic sending rate and the duty cycle of regular traffic in the detection window. In the future, we will study the optimization model and time window and analyze the relationship between time window and data set and feature selection so that the model can better adapt to the environment and have higher accuracy and detection efficiency.

Data Availability

The data shall be made available on request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the King Khalid University Researchers Supporting Project Number (GRP/326/42).

References

[1] S. Yeom and K. Kim, "Improving performance of collaborative source-side DDoS attack detection," in *Proceedings of the 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pp. 239–242, Daegu, Korea (South), September 2020.

[2] W. Sun, Y. Li, and S. Guan, "An Improved Method of DDoS Attack Detection for Controller of SDN," in *Proceedings of the 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET)*, pp. 249–253, Beijing, China, August 2019.

[3] B. Jia and Y. Liang, "Anti-D chain: a lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain," *China Communications*, vol. 17, no. 9, pp. 11–24, 2020.

[4] J. He, Y. Tan, W. Guo, and M. Xian, "A Small Sample DDoS Attack Detection Method Based on Deep Transfer Learning," in *Proceedings of the 2020 International Conference on Computer Communication and Network Security (CCNS)*, pp. 47–50, Xi'an, China, August 2020.

[5] Z. Liu, Y. He, W. Wang, and B. Zhang, "DDoS attack detection scheme based on entropy and PSO-BP neural network in SDN," *China Communications*, vol. 16, no. 7, pp. 144–155, 2019.

[6] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," *Expert Systems with Applications*, vol. 169, Article ID 114520, 2021.

[7] M. H. Ali, M. M. Jaber, S. K. Abd et al., "Threat analysis and distributed denial of service (DDoS) attack recognition in the Internet of things (IoT)," *Electronics*, vol. 11, no. 3, p. 494, 2022.

[8] S. Dong and M. Sarem, "DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks," *IEEE Access*, vol. 8, pp. 5039–5048, 2020.

[9] Y. Chen, X. Chen, H. Tian, T. Wang, and Y. Cai, "A Blind Detection Method for Tracing the Real Source of DDoS Attack Packets by Cluster Matching," in *Proceedings of the 8th IEEE International Conference on Communication Software and Networks (ICCSN)*, pp. 551–555, Beijing, China, June 2016.

[10] X. Liang and T. Znati, "An empirical study of intelligent approaches to DDoS detection in large scale networks," in *Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC)*, pp. 821–827, Honolulu, HI, USA, February 2019.

[11] J.-H. Jun, H. Oh, and S.-H. Kim, "DDoS Flooding Attack Detection through a Step-by-step Investigation," in *Proceedings of the 2011 IEEE 2nd International Conference on Networked Embedded Systems for Enterprise Applications*, pp. 1–5, Perth, WA, Australia, December 2011.

[12] M. J. Awan, U. Farooq, H. M. A. Babar et al., "Real-time DDoS attack detection system using big data approach," *Sustainability*, vol. 13, no. 19, Article ID 10743, 2021.

[13] I. Ortet Lopes, D. Zou, F. A. Ruambo, S. Akbar, and B. Yuan, "Towards effective detection of recent DDoS attacks: a deep learning approach," in *Security and Communication Networks*, W. Li, Ed., vol. 2021, Article ID 5710028, 14 pages, 2021.

[14] V. Popovskyy and V. Skibin, “Entropy Methods for DDoS Attacks Detection in Telecommunication Systems,” in *Proceedings of the 2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology*, pp. 182–185, Kharkov, Ukraine, October 2014.

[15] D. Erhan and E. Anarim, “Istatistiksel Yöntemler Ile DDoS Saldırı Tespiti DDoS Detection Using Statistical Methods,” in *Proceedings of the 2020 28th Signal Processing and Communications Applications Conference (SIU)*, pp. 1–4, Gaziantep, Turkey, October 2020.

[16] L. Wang and Y. Liu, “A DDoS Attack Detection Method Based on Information Entropy and Deep Learning in SDN,” in *Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 1084–1088, Chongqing, China, June 2020.

[17] A. Sanmorino and S. Yazid, “DDoS Attack detection method and mitigation using pattern of the flow,” in *Proceedings of the 2013 International Conference of Information and Communication Technology (ICoICT)*, pp. 12–16, Bandung, Indonesia, March 2013.

[18] L. Luo, J. Wang, and L. Jia, “A CGAN-based DDoS Attack Detection Method in SDN,” in *Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 1030–1034, Harbin City, China, June 2021.

[19] K. Mahajan, U. Garg, and M. Shabaz, “CPIDM: a clustering-based profound iterating deep learning model for HSI segmentation,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 7279260, 12 pages, 2021.

[20] R. Arthi and S. Krishnaveni, “Design and Development of IOT Testbed with DDoS Attack for Cyber Security Research,” in *Proceedings of the 2021 3rd International Conference on Signal Processing and Communication (ICPSC)*, pp. 586–590, Coimbatore, India, May 2021.

[21] D. Ushakov, M. Vinichenko, and E. Frolova, “Environmental capital: a reason for interregional differentiation or a factor of economy stimulation (the case of Russia),” *IOP conference series: earth and environmental science*, vol. 272, no. 3, p. 032111, 2019.

[22] Y. Chen, J. Hou, Q. Li, and H. Long, “DDoS attack detection based on random forest,” in *Proceedings of the 2020 IEEE International Conference on Progress in Informatics and Computing (PIC)*, pp. 328–334, Shanghai, China, December 2020.

[23] S. Nguyen, J. Choi, and K. Kim, “Suspicious Traffic Detection Based on Edge Gateway Sampling Method,” in *Proceedings of the 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pp. 243–246, Seoul, Korea (South), September 2017.

[24] S. Sanober, I. Alam, S. Pande et al., “An enhanced secure deep learning algorithm for fraud detection in wireless communication,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6079582, 14 pages, 2021.

[25] D. Erhan, E. Anarım, and G. K. Kurt, “DDoS attack detection using matching pursuit algorithm,” in *Proceedings of the 2016 24th Signal Processing and Communication Application Conference (SIU)*, pp. 1081–1084, Zonguldak, Turkey, May 2016.

[26] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, “A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis,” in *Proceedings of the 2016 8th International Conference on Communication Systems and Networks (COMSNETS)*, pp. 1-2, Bangalore, India, January 2016.

[27] N. R. Nayak, S. Kumar, D. Gupta, A. Suri, M. Naved, and M. Soni, “Network mining techniques to analyze the risk of the occupational accident via Bayesian network,” *International Journal of System Assurance Engineering and Management*, vol. 13, pp. 1–9, 2022.

[28] K. Hong, Y. Kim, H. Choi, and J. Park, “SDN-assisted slow HTTP DDoS attack defense method,” *IEEE Communications Letters*, vol. 22, no. 4, pp. 688–691, 2018.