Low-rate DDoS attacks detection method using data compression and behavior divergence measurement

Xinqian Liu , Jiadong Ren , Haitao He , Qian Wang , Chen Song

PII: S0167-4048(20)30380-1
DOI: https://doi.org/10.1016/j.cose.2020.102107
Reference: COSE 102107

To appear in: *Computers & Security*

Received date: 28 March 2020
Revised date: 2 November 2020
Accepted date: 3 November 2020

Please cite this article as: Xinqian Liu , Jiadong Ren , Haitao He , Qian Wang , Chen Song , Low-rate DDoS attacks detection method using data compression and behavior divergence measurement, *Computers & Security* (2020), doi: https://doi.org/10.1016/j.cose.2020.102107

Low-rate DDoS attacks detection method using data compression and behavior divergence measurement

Xinqian Liu[a,b], Jiadong Ren[a,b,*], jdren@ysu.edu.cn, Haitao He[a,b], Qian Wang[a,b], and Chen Song[c]

[a]Department of Information Science and Engineering, Yanshan University, Qinhuangdao 066001, China
[b]Hebei Key Laboratory of Software Engineering, Qinhuangdao 066001, China
[c]College of Artificial Intelligence, Tianjin University of Science and Technology, Tianjin 300457, China

Corresponding author:

Abstract

Distributed denial of service (DDoS) attacks have been a typical and extremely destructive threat to the Internet. DDoS attack detections suffer from the nonnegligible high complexity of massive traffic flow storage in the high-speed network. Besides, hidden low-rate DDoS (LDDoS) attacks evade the existing detection methods due to the similarity between LDDoS attack traffic and normal traffic. Focusing on these problems, this paper proposes a new **l**ow-rate **D**DoS attack **d**etection **m**ethod (LDDM) by designing the multidimensional sketch structure and novel measurement methods on network flows. First, the multidimensional sketch structure is designed to aggregate and compress network flows, which contributes to reduce the cost of data storage and enhance detection performance. Then, the improved behavior divergence measurement method based on daub 4 wavelet transform is proposed to calculate the energy percentage of each sketch divergence. This method obtains effective results in distinguishing the normal traffic and attack traffic. Furthermore, a modified weighted exponential moving average method is designed to construct the dynamic threshold of normal network. Meanwhile, a traffic freezing mechanism is proposed to ensure the standardization of the dynamic threshold. Finally, the effectiveness of the LDDM is evaluated using several real low-rate DDoS attack datasets. The comparisons with other methods illustrate our method has a lower false positive rate and false negative rate, as well as higher accuracy in the detection of stealthy low-rate DDoS attacks.

Keywords

Network security, Low-rate DDoS attack detection, Multidimensional sketch structure, Behavior divergence measurement, Daub 4 wavelet transform, Dynamic threshold mechanism

1、Introduction

Denial of service (DoS) is a typical flooding attack behavior. DDoS is a distributed format of DoS, which utilizes a group of connected devices as attackers (Vidal, 2017). This attack severely consumes the resources of servers or routers to make them unavailable partly or wholly. At the same time, DDoS also occupies network bandwidth to affect the overall network performance (Behal et al., 2017; Singh et al., 2018). According to the worldwide infrastructure security report (WISR), high-rate DDoS attacks, as a predominant attack mode, cause more than 600 Gbps traffic volume (2016). In short, DDoS attacks cause serious problems for network services. The hazard of DDoS attacks is related to not only the destructiveness for network performance but also the easy implementation (Alzahrani et al., 2018). At present, there are a variety of easy-to-operate DDoS attack tools, such as LOIC, Hyenae, and Hping3, which launch flooding attacks through different protocols (ICMP, UDP, and TCP) to fail victim services (David et al., 2019). To avoid the serious harm of DDoS attacks, it is necessary to detect and defend against DDoS attacks. However, due to the similarity between DDoS attack traffic and legitimate traffic, the detection of DDoS attacks is still quite difficult (Toklu et al., 2018).

In general, there are two types of DDoS attacks: high-rate DDoS (HDDoS) and low-rate DDoS (LDDoS) (Toklu et al., 2018). HDDoS attacks would cause a rapid growth of the network traffic, which present a significant difference from normal traffic in network volume and packet number. HDDoS is easy to be detected relatively (Al-Yaseen et al., 2017). On the other hand, because of the low attack speed, LDDoS attack traffic is more similar to normal traffic in network volume

and packet number. Hence, it is tougher to detect LDDoS. With a slow and seemingly unnoticeable process, LDDoS enables the performance of target system to gradually degrade until completely fail (Tang et al., 2011). As Wang et al. (2012), the sophisticated attackers are shifting their focus on more subtle and stealthy low-rate DDoS attacks. Therefore, facing the characteristics of high-incidence, concealment, and hard-to-detect of LDDoS, this paper focuses on low-rate DDoS attack detections.

In order to effectively detect DDoS attacks, a variety of measurement methods are applied to this field. These methods are mainly divided into five categories: probability based model (David et al., 2019; Park et al., 2016), information theory based one (Behal et al., 2017; Kumar et al., 2018; Marco et al., 2019), distance measurement based one (Tang et al., 2011; Tang et al., 2009; Wang et al., 2018), machine learning based one (Singh et al., 2018; Vidal et al., 2017; Indraneel et al., 2017), and signal process based one (Toklu et al., 2018; Callegari et al., 2011; Jiang et al., 2015). The existing methods mostly are used to detect HDDoS attacks, but few are applied to detect LDDoS attacks. Beside, most methods are not sensitive enough to perceive the slight changes of traffic features with the occurrence of LDDoS attacks. Therefore, these methods have higher false positive rates and false negative rates, as well as lower accuracy. Some researchers applied signal analysis methods to filter low-rate DDoS attacks, such as discrete wavelet analysis (Tang et al., 2011) and Fourier transform (Toklu et al., 2018). The research results have confirmed their ability in detecting LDDoS attacks. Tang et al. (2011) mentioned that the daub 4 wavelet transform, a kind of commonly used discrete wavelet transform, is very sensitive to capture small signal changes. Therefore, this paper designed the improved behavior divergence measurement method based on daub 4 wavelet transform to effectively detect low-rate DDoS attacks.

In addition, a major challenge about LDDoS attack detections is the storage complexity of massive traffic flow. In recent years, 100Gbps networking has become a standard, while 400Gbps is well accepted as the next milestone (Attig et al., 2011). In a 100Gbps networking, the number of concurrent flows reaches 50 million per minute. In the traditional per-item-state technique, the storage footprint can easily go beyond several gigabits. The analysis of massive traffic flow will greatly consume memory even on the risk of memory overflow (Tong et al., 2017). In order to alleviate this problem, sampling technique is widely used in network traffic monitoring. However, sampling will greatly reduce the accuracy of LDDoS attack detections (Jazi et al., 2017). Therefore, the sketch structure is introduced to solve this problem (Li et al, 2013). Sketch is a probabilistic storage structure, which can compress and summarize data via random hash functions. This technique can significantly reduce the storage and analysis consumption. For the above several gigabits data, only tens of megabytes of storage is required. Therefore, focusing on the high storage caused by massive network traffic, this paper proposes the multidimensional sketch technique to compress and summarize network flows to the maximum extent.

To address the above issues, this paper proposes a new low-rate DDoS attack detection method combining multidimensional sketch structure, the improved behavior divergence measurement method based on daub 4 wavelet transform and dynamic threshold mechanism. In the previous studies, sketch was usually deployed on the server device. Due to the unique destination of traffic flows, traffic flows are summarized only on the key of the source IP address. However, the proposed LDDM considers the bidirectional network flows in a local area network (LAN) or wide area network (WAN) environment. The distribution of both source IP address and destination IP address changes with network state. Therefore, multidimensional sketch structure from these two aspects is firstly constructed to compress traffic flows to the maximum extent. Meanwhile, this structure can facilitate LDDoS attack detections. In addition, the multidimensional sketch structure can be regarded as a data signal directly, which could greatly reduce the computational complexity of attack detection process. For the LDDoS attack detection process, previous studies independently analyzed a single-interval sketch structure by daub 4 wavelet transform. This method could not reflect the difference between LDDoS attacks and normal behaviors in the real detection process. To solve the problem, the LDDM proposes an improved behavior divergence measurement method based on daub 4 wavelet transform. Instead of measuring the single-interval sketch structure, the sketch divergences within continuous time intervals are rearranged and measured. To distinguish sketch divergences, the network baseline is required. Therefore, to evaluate the network baseline accurately and real-timely, the dynamic threshold mechanism is set up by employing the improved exponential weighted moving average method. Moreover, in order to prevent the network baseline from being polluted by attack traffic, the freezing mechanism is designed to ensure the standardization of network baseline and attack identification. Finally, several real low-rate DDoS attack datasets are adopted to test the availability, time feasibility and detection effectiveness of the LDDM. The comparisons with other methods illustrate that the LDDM has splendid detection results (such as a high accuracy, low false positive rate and false

negative rate) in the detection of stealthier low-rate DDoS attacks.

The rest of this paper is as follows. Section 2 introduces the background information concluding related works of DDoS attack detection methods and relevant basic technologies. Section 3 describes the overall framework of LDDM and shows the details of each component. Section 4 presents the experiment setting and performance evaluation in detail. Section 5 summarizes the whole paper.

2、Background

2.1 Related work

Considering the serious damage and easy operation of DDoS attacks, it is very important and meaningful to effectively detect DDoS attacks. At present, most of detection methods aim at high-rate DDoS attacks, and the researches on low-rate DDoS attacks are relatively small. Therefore, this section analyzes the existing DDoS attack detection methods about high-rate and low-rate DDoS attacks. There mainly concludes the following five categories.

Among the detection methods based on information theory, Kumar et al. (2018) proposed an early detection and mitigation framework of TCP SYN flooding attacks, which applied Shannon entropy to measure network flows. When the entropy value is lower than the given threshold, the SYN Flood attacks occur at this time. Among the detection methods based on distance measurement, Hellinger distance is widely used as a measurement index in the anomaly detection field (Tang et al., 2009; Wang et al., 2018). Tang et al. (2009) utilized Hellinger distance to measure SIP flooding attacks. When the deviation between some network traffic and normal network traffic is greater than the threshold, SIP flooding attacks occur. Entropy and distance measurements are widely utilized in DDoS attack detections, but the two measurement methods cannot effectively detect low-rate or hidden DDoS attacks (Sahoo et al., 2018).

Among the detection methods based on probability model, David et al. (2019) used the normal distribution model to describe network flow characteristics (such as packet number per second and the number of unique IP addresses) to detect DDoS flood attacks. In this method, the mean and variance of the normal distribution model are calculated. Further combining the mean and variance aims to construct a dynamic threshold. When the value of flow characteristic exceeds the constructed threshold, the current network flow is identified as an attack flow. Among the detection methods based on machine learning, Vidal et al. (2017) proposed a detection and mitigation method of DoS flood attacks based on behavior simulation of human immune system. Sreeram et al. (2017) utilized machine learning indexes and bat bio-inspired algorithm to detect HTTP flooding attacks at the application layer. CAIDA dataset was applied to verify the effectiveness of this algorithm. These two detection methods are similar. In order to detect the network deviation, the network flow characteristics are in-depth analyzed and modeled. However, the defects of these two methods lie in the complex process of network flow characteristic analysis and model construction, which makes these methods cannot meet the real-time requirement in the high-speed network. Besides, this method cannot be effectively extended and applied to the real network.

Among the detection method based on signal processing, this kind of methods is effectively applied in different DDoS attack detections. This is because signal processing method has a higher sensitivity to data changes. For example, Jiang et al. (2015) proposed a multi-scale continuous wavelet transform for analyzing network flow characteristics. And principal component analysis was applied to extract the properties of abnormal network traffic. Toklu et al. (2018) proposed a hybrid filtering scheme for both high-rate DDoS attacks and low-rate DDoS attacks. In this scheme, the average transform is used to filter network flows of high-rate DDoS attacks, and the Fourier transform is used to filter network flows of low-rate DDoS attacks. Tang et al. (2018) utilized the daub 4 wavelet analysis method to detect hidden SIP flooding attacks. Agrawal et al. (2018) proposed an LDDoS attack detection method based on power spectral density to detect and mitigate attacks in the frequency domain. For LDDoS attack flows, the attack spectrum is mainly distributed in the low frequency, while legitimate flows are uniformly distributed. According to the existing researches, the signal processing method can quickly perceive the weak signal change and is helpful for the LDDoS attack detections.

In addition, Bhushan et al. (2018) conducted probabilistic modeling on the size of network packets and identified LDoS attack flows through the hypothesis test of t-statistics in a cloud environment. In this method, there are some assumptions, such as attackers only use legitimate IP addresses to carry out attacks, and attackers have a fixed attack mode. Therefore, this method has great limitations in the actual application. Sahoo et al. (2018) proposed an early detection

scheme to detect low-rate DDoS attacks in the control layer of Software Defined Network. The scheme measured the generalized entropy difference of destination IP addresses. This paper further pointed out that statistical measurement methods such as Shannon entropy have a low accuracy in LDDoS attack detections. Considering the advantages and disadvantages of different metrics in LDDoS attack detections, this paper adopts an improved daub 4 wavelet transform method to detect LDDoS attacks.

2.2 Sketch

Sketch is a stream probability structure for data summarization and compression (Cormode et al., 2012). It builds a compact and constant-size summary for high dimensional data via random aggregation by hash functions. Intuitively, a sketch is a two-dimensional table of H rows and K columns. It is composed of H hash tables of size K as shown in Figure 1. $C[d, w]$ denotes the counter of the d^{th} row w^{th} column. In a sketch, each hash table corresponds to a separate hash function h_i that maps traffic flows to the corresponding hash space ($1,2,\ldots, K$). The coming data stream is considered as pairwise items encompassing a key and an associated value, represented by $item$=(key, $value$). The H independent hash functions map the incoming data to H rows by the keys. The buckets corresponding to the keys are updated by the associated value. $C[d,h_d(key)]$+=$value$, $d\in[1,H]$, $h_d(key)\in[1,K]$.Figure 1 presents the sketch structure and update process.

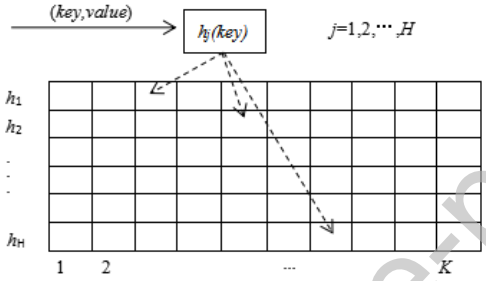


Figure.1 Sketch structure and the update processing of traffic flow

In the process of network traffic anomaly detections, the key is generally represented by source IP address or destination IP address. The value is represented by packet number or byte number. Sketch is an effective tool for summarizing and compressing data with a small tolerable error. Due to the randomness of hash functions, the distribution of normal traffic is relatively random in each hash table and keeps nearly stable in a short time. Therefore, when the network traffic significantly varies, the sketch distribution will greatly change to reflect anomalies.

2.3 Daub 4 wavelet transform

Daub 4 wavelet transform method is one common way of Discrete Wavelet Transform (DWT) (Tang et al., 2011). Due to the property of wavelet analysis, daub 4 wavelet transform can effectively detect the unexpected change, even the stealthy slow change. For a signal S consisting of K elements, it is decomposed into an approximating signal A and a detailed signal D by the daub 4 wavelet transform. Based on signals A and D, the energy percentage P^d of the signal S is obtained to reflect signal changes.

Daub 4 wavelet transform method has two sets of coefficients, the scaling coefficients $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and the wavelet coefficients $\{\beta_1, \beta_2, \beta_3, \beta_4\}$. The coefficients are pre-defined constants and satisfy the relationship $\beta_k = (-1)^{k-1}\alpha_{4-(k-1)}$. According to the scaling coefficients, the daub 4 scaling signal $\boldsymbol{V}$ is represented as a $2/K*K$ matrix.

$$V=\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_3 & \alpha_4 & 0 & 0 & 0 & 0 & \cdots & \alpha_1 & \alpha_2 \end{pmatrix}. \quad (1)$$

Similarly, according to the wavelet coefficients, the daub 4 wavelet signal $\boldsymbol{W}$ is expressed as a $2/K*K$ matrix.

Applying $\boldsymbol{V}$ and $\boldsymbol{W}$ to transform signal S, the trend signal and fluctuation signal are obtained.

$$a_i = \sum_{j=1}^{K} S_j V_{ij} \quad i \in \{1,2,\cdots,\frac{K}{2}\}, \tag{2}$$

$$d_i = \sum_{j=1}^{K} S_j W_{ij} \quad i \in \{1,2,\cdots,\frac{K}{2}\}. \tag{3}$$

Using the trend signal and fluctuation signal, the approximating signal A and detailed signal D are received.

$$A_j = \sum_{i=1}^{\frac{K}{2}} a_i V_{ij} \quad j \in \{1,2,\cdots,K\}, \tag{4}$$

$$D_j = \sum_{i=1}^{\frac{K}{2}} d_i W_{ij} \quad j \in \{1,2,\cdots,K\}. \tag{5}$$

The energy percentage of the signal S is calculated.

$$P^d(S) = \frac{\sum_{j=1}^{K}(D_j)^2}{(\sum_{j=1}^{K}(A_j)^2 + \sum_{j=1}^{K}(D_j)^2)}. \tag{6}$$

When the signal keeps relatively stable, P^d remains at a low level. When the signal mutates, P^d rapidly increases. Hence, P^d keeps at a low level under normal network conditions. However, P^d rapidly varies under abnormal network state. In a word, the P^d contributes to monitor network traffic changes and quickly identify attack behaviors.

3、The proposed low-rate DDoS attacks detection method LDDM

3.1 System overview

Figure 2 shows the overall process of LDDM. This method is utilized to detect low-rate DDoS attacks in network environment, not a server side. At the initial moment, network traffic of each detection interval is captured and preprocessed, and traffic packets are aggregated into flows. Network flows are applied into the whole detection process. In the sketch compress component, network flows are mapped into the multidimensional sketch structure with keys of the source IP address and destination IP address. The divergence between the multidimensional sketch of the current detection interval and that of the previous normal interval is measured to obtain an energy percentage P^d on the LDDoS detection component. The P^d value serves as the input of the next component. In the dynamic threshold component, according to the existing P^d set, the improved exponential weighted moving average method is adopted to estimate the detection threshold *Th*. The input P^d is compared with the estimated threshold *Th* to distinguish whether the detection result is an attack. The new P^d is stored into the P^d set. When the detection result is an attack, the freezing mechanism is triggered to freeze normal sketch, thresholds, and some variables which are used to estimate the dynamic threshold.

3.2 Multidimensional sketch structure

To our knowledge, due to the attack detection system based on sketch usually building on the server device, the current studies only focus on received requests. Since the destination of individual requests is unique, it is enough to hash individual requests into sketch taking source IP address as the key. However, the LDDM is constructed on network environment based on network flows. Both the uplink request traffic and downlink response traffic reflect network changes. Hence, there will be a large deviation to illustrate network traffic changes only by source IP address. For the low-rate DDoS attack traffic, distributions of source and destination IP addresses are very similar to the IP addresses' distributions of normal traffic. Mapping and detecting attack traffic with only one feature would cause a serious error. Combining with the source IP and destination IP address, attack traffic can is found more accurately. Therefore, in order to monitor DDoS attacks more accurately, the vector <*SIP*, *DIP*> is applied as a key vector to describe the constantly coming network flows, where SIP is the source IP address, and DIP is the destination IP address. The value is set as 1 which represents the number of traffic flows.

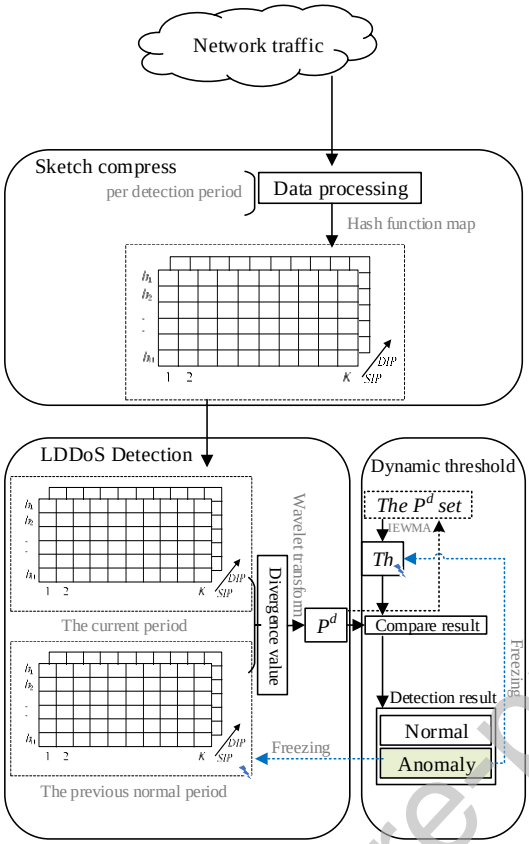


Figure.2 Framework of the proposed low-rate DDoS attacks detection method

In sketch, the hash function is required to keep network flows uniform and independent distribution. The general hash function family can well meet these requirements, which has the pretty ability of avoiding collision and controlling the conflict probability within a certain range. Due to these advantages, the general hash function can ensure the uniform distribution of data items. Meanwhile, this function does not have the complex encryption ability and computing consumption like the encryption hash function. In this paper, the selected hash function is as follows (cormode et al., 2012).

$$h_d(key) = (a_i key + b_i) \bmod p \bmod K \quad (7)$$

Where p is a prime number greater than the value of the maximum key. For a faster mapping, p is set as 2^{31}-1 that is a Mersenne prime. $a, b \in [1, p\text{-}1]$ are two random values.

Since the hash functions in a sketch are built via separate random seeds, they are independent of each other. In addition, due to the confidentiality of random seeds, the multidimensional sketch structure remains security, even if the attacker knows detection results. The multidimensional sketch structure allows a separate summarization of the network flow characteristics on each attribute to identify attacks.

3.3 The improved behavior divergence measurement method based on daub 4 wavelet transform

The improved behavior divergence measurement method aims to discover the divergence between attack sketch and normal sketch. Meanwhile, this method should also ensure the divergence large enough to distinguish LDDoS attacks. Therefore, this paper proposes the improved behavior divergence measurement method based on daub 4 wavelet transform to magnify the attack divergence and keep the normal divergence at a low level.

Before introducing the detailed method, the following definitions are given.

Definition 1 (abnormal hash table). A hash table corresponds to a row data in a sketch. When the energy percentage of the signal deviation of a hash table is not within the range of the threshold, the hash table is defined as an abnormal hash table.

Definition 2 (abnormal sketch). A sketch is defined as an abnormal sketch with more than $H/2$ abnormal hash tables.

Definition 3 (abnormal time). If there is at least one abnormal sketch in the multidimensional sketch structure at time interval t^{th}, the time interval t^{th} is defined as an abnormal time.

In general, in two consecutive time intervals, the corresponding two hash tables of two sketches are regarded as signals S_1 and S_2. Attacks are detected by calculating the divergence between signals S_1 and S_2. For continuous normal network traffic, sketch distributions remain relatively stable, and the divergence between S_1 and S_2 is small. However, when DDoS attacks occur, the sketch distributions significantly change to cause a much greater divergence. According to this viewpoint, LDDoS can be identified by measuring the divergence magnitude. Note that even under continuous normal network, sketch distributions still have a small divergence due to the influence of network dynamics. Although the overall network traffic remains relatively stable in a certain time scale, requests of individual users still have a great change, such as request time and request number. Since the sketch maps requests of each individual user into a single bucket, the divergence of sketch distributions has been resulted.

In order to effectively measure the divergence magnitude, this paper proposes the improved behavior divergence measurement method based on daub 4 wavelet transform. This method measures the energy percentage of the signal divergence to describe the divergence magnitude. In the real detection process, the detection time interval is set as a fixed value ΔT that is an adjustable parameter. Suppose in the t^{th} time interval, the i^{th} row in a sketch is represented as a signal $S_{t,i}=<n_{i1},n_{i2},n_{i3}, \ldots,n_{iK}>$, where n_{ij} is the counter of the i^{th} row j^{th} bucket. The signal of the i^{th} row in the $t+1^{th}$ time interval is represented as $S_{t+1,i}=<m_{i1},m_{i2},m_{i3}, \ldots,m_{iK}>$. The divergence of these two signals is $S_{dev} = |S_{t+1,i} - S_{t,i}|$. Due to the uncertainty of individual network requests, even under the normal network, individual requests still have a small divergence. However, when the individual requests greatly vary, the signal divergence also significantly changes. At this time, the approximating signal A and detailed signal D cannot be effectively identified based on the divergence S_{dev}. The energy percentage is overestimated resulting in a higher false positive rate. On the other hand, continuous overestimation of the normal P^d leads to an increase of standard threshold, so that attacks cannot be effectively identified resulting in a high false negative rate. To solve this problem, S_{dev} is sorted in ascending order $S_{dev}' = sort(S_{dev}, ascending)$, which can help to effectively distinguish the approximating signal A and detailed signal D. The $P^d(S_{dev}')$ is obtained according to formulas (1-6), which can reasonably reflect the magnitude of signal divergence. The whole calculating process of the improved behavior divergence measurement method based on daub 4 wavelet transform is shown in algorithm 1.

Algorithm 1. The improved behavior divergence measurement method based on daub 4 wavelet transform

Input: the sketches of the t^{th} time interval, the sketches of the $t+1^{th}$ time interval
Output: the P^d_set
(1) Initialize P^d_set = ø
(2) For each sketch in multidimensional sketch
(3) PD = ø
(4) For each row S_i in a sketch
(5) $S_{dev} = |S_{t+1,i} - S_{t,i}|$
(6) Sort S_{dev} ascendingly
(7) Calculate P^d_i of S_{dev}
(8) Add P^d_i to PD
(9) End for
(10) Add PD to P^d_set
(11) End for

By tracking changes of the signal divergence, the whole network traffic is monitored. In each time interval, the abnormal hash table and sketch are obtained to distinguish whether the time interval is an attack time. If it is an attack time, the attack detection model will send an alarm. Otherwise, the detection of the next interval is conducted. This method continuously calculates traffic changes of each time interval and automatically adapts to the real-time change of network traffic. Compared with the popular machine learning methods, our method does not need to generate a fixed training model

according to the predefined dataset. Hence, the proposed LDDM is more adaptive and meets the network dynamic characteristic.

3.4 Dynamic threshold mechanism

The dynamic threshold mechanism means that the threshold is not preset and fixed, but varies with network state. It can say that the dynamic threshold mechanism satisfies the dynamic characteristics of network traffic. The proposed dynamic threshold has two important functions: (1) to avoid the detection inaccuracy caused by a too large or too small static threshold; (2) to perfectly reflect the change range of normal flows. Besides, to smoothly implement the dynamic threshold, the freezing mechanism is proposed to ensure the standardization of the dynamic threshold and prevent abnormal flows from polluting the dynamic threshold.

Due to the inherent dynamic of network traffic, the energy percentage of the signal divergence is not fixed in normal network. Therefore, the fixed threshold will lead to a high false positive rate and false negative rate. To solve this problem, the improved exponential weighted moving average method (IEWMA) (Indraneel et al., 2017) is used to calculate the dynamic threshold. When attacks occur, due to the pseudo-random technology of DDoS attacks, distributions of source IP addresses are more uniform. A smoother signal is presented to make a smaller P^d by daub 4 wavelet transform. However, because DDoS attacks usually point to a single destination IP address, distributions of destination IP address present a more prominent change, and the P^d value increases. Therefore, dynamic thresholds of these two properties are calculated via different operations as shown below. The threshold at the t+1th time interval is estimated according to a real value and an estimated value of P^d at the t^{th} time interval. Specifically, P_t^d and $\hat{P}_t^d$ is the real value and the estimated value of the energy percentage at time interval t, respectively. $\hat{P}_{t+1}^d$ is the estimated value at time interval t+1. The threshold of the time interval t+1 is calculated as follows.

$$\hat{P}_{t+1}^d = \alpha P_t^d + (1-\alpha)\hat{P}_t^d, \tag{8}$$

$$d_t = \left|P_t^d - \hat{P}_t^d\right|, \tag{9}$$

$$\sigma_{t+1}^2 = \beta d_t^2 + (1-\beta)\sigma_t^2, \tag{10}$$

$$Th_{t+1} = \begin{cases} \hat{P}_{t+1}^d + \lambda\sigma_{t+1} \; sketch.attribute = DIP \\ \hat{P}_{t+1}^d - \lambda\sigma_{t+1} \; sketch.attrobute = SIP' \end{cases} \tag{11}$$

Where Th_{t+1} is the threshold at the time interval t+1, σ, β, and λ are adjustable parameters. Considering the capacity of anomaly detection of the P^d value, appropriate parameters σ, β, and λ would greatly reduce the detection errors. Hence, parameters σ, β and λ would be set based on the literature (Vidal, 2017) and further be modified according to massive experiments. Note that in the initial time, $\hat{P}_1^d = P_1^d$, $\sigma_1 = 0$. According to the estimated threshold and the actual P^d at time interval t+1, the detection rules are defined as follows.

For source IP address, the rule is as follows.

$$\delta_{t+1} = \begin{cases} 1 \; Th_{t+1} > P_{t+1}^d \\ 0 \; Th_{T+1} < p_{t+1}^d \end{cases} \tag{12}$$

For destination IP address, the rule is as follows.

$$\delta_{t+1} = \begin{cases} 1 \; Th_{t+1} < P_{t+1}^d \\ 0 \; Th_{T+1} > p_{t+1}^d \end{cases} \tag{13}$$

When the actual P^d exceeds the range of the estimated threshold, an abnormal hash table is defined at this time. When an anomaly time is identified, anomaly detection system would arise an alarm.

In the continuous attack detection process, if an abnormal P^d is used to estimate the threshold in the next time interval, the network threshold would be polluted and increased. Thus, a high false negative rate is produced. In order to avoid the problem and accurately describe normal network, when an attack is detected, the freezing mechanism is proposed to freeze both the threshold and the signal. Until attacks disappear, the update of the threshold is resumed. This freezing mechanism keeps the threshold at a relatively stable level and prevents attack traffic polluting the network threshold. Algorithm 2 takes

a destination IP address as an example to describe the implementation of freezing mechanism.

Algorithm 2. Freezing Mechanism

Input: P_t^d of the t^{th} time interval, Th_t of the t^{th} time interval, σ, β, λ

Output: Th_{t+1}

(1) If $P_t^d > Th_t$

(2) freeze $S_{t,i}$, Th_t

(3) While $P_{t+1}^d < Th_t$

(4) calculate the P^d value of the next time interval $P_{t+1}^d = P^d\left(S_{t+1,i}, S_{t-1,i}\right)$, continue to compare P_{t+1}^d and Th_t

(5) End while

(6) Else

(7) calculate the P_{t+1}^d and Th_{t+1} value of the next time interval, continue to compare Th_{t+1} and P_{t+1}^d

(8) End if

(9) unfreeze *Th*, calculate the Th_{t+1} value of the next time interval and $P_{t+1}^d = P^d\left(S_{t+1,i}, S_{t,i}\right)$, compare P_{t+1}^d and Th_{t+1}

Suppose that at time interval t, $P_t^d > Th_t$, which means that attacks occur at time interval t. The signal $S_{t,i}$ and threshold Th_t are frozen as line (2). Next, calculate the energy percentage P^d_{t+1} at time interval t+1. P^d_{t+1} is obtained by the divergence between the signal of the time interval t+1 and that of the time interval t-1, instead of the signal of the time interval t as line (4). Compare P_{t+1}^d and Th_t to distinguish whether P_{t+1}^d is an anomaly. Suppose that until the time interval $t+q$, $P_{t+q}^d < Th_t$, the network state returns normal. At this time, the cyclic of lines (3)-(5) finishes. Then, the threshold is updated again to obtain Th_{t+q+1}. At the same time, unfreeze $S_{t,i}$. Instead of $S_{t-1,i}$, S_{t+q} is used to calculate $P_{t+q+1}^d = P^d\left(S_{t+q+1,i}, S_{t+q,i}\right)$ as line (9).

3.5 Parameter configuration

LDDM contains multiple parameters, and appropriate parameters will improve the ability of detecting LDDoS attacks. This section describes the ways of parameter configuration. The parameters of LDDM includes the following parts: parameters *H* and *K*, parameters α, β and λ, and the detection time interval ΔT.

1）Parameters *H* and *K*

In Sketch, *H* is the number of hash functions and *K* is the size of the hash table. Parameters *H* and *K* determine not only the detection accuracy but also the data storage complexity. For the parameter *H*, it is set to 4, 8, and 5 in the reference (Tang et al., 2009), the references (Wang et al., 2018; Tang et al., 2014), and the reference (Tang et al., 2012), respectively. Summing up different references, the value of parameter *H* is not obviously different. In Section 3.3, there is a definition that the sketch with more than *H*/2 abnormal hash tables is as an abnormal sketch. Therefore, when *H* is an odd number, it is more conducive to determine the abnormal sketch. In addition, in sketch, there exist parameters (ε, δ) to ensure the storage accuracy (Cormode et al., 2012). $K = [e/\varepsilon]$, $H = [\ln 1/\delta]$, in which ε is the expected accuracy, and δ is the certainty of the expected accuracy. It can say that the *K* determines the expected accuracy of the storage. The *H* determines the certainty of achieving the expected accuracy. When $H = 5$, the certainty is 0.99. When $H = 7$, the certainty is 0.999. Since our method does not need to strongly consider the requirement of storage accuracy, there is no difference whether *H* is 5 or 7. When $H = 5$, the storage of sketch structure is smaller. Hence, *H* is set as 5 in this paper. The value of parameter *K* greatly varies among different references. In the reference (Wang et al., 2018), *K* is set as 2^{12}. However, in the reference (Tang et al., 2014), it is set as 32. This is largely due to different hash functions and different network environments. Considering the

applied hash function, the parameter K determines the proportion of free buckets in a hash table. Hence, the parameter K will be set based on our hash function and the real network environment.

2）Parameters α, β, and λ

The improved exponent weighted moving average method has three parameters: α, β, and λ. α is the damping coefficient, β is the variance damping coefficient, and λ is the threshold damping coefficient. The parameter α determines the relationship between the predicted value and historical values.

$$\begin{aligned}\hat{P}^d_{t+n} &= \alpha P^d_{t+n-1} + (1-\alpha)\hat{P}^d_{t+n-1} \\ &= \alpha P^d_{t+n-1} + (1-\alpha)\alpha P^d_{t+n-2} + (1-\alpha)^2 \hat{P}^d_{t+n-2} \\ &= \alpha P^d_{t+n-1} + (1-\alpha)\alpha P^d_{t+n-2} + (1-\alpha)^2 \alpha P^d_{t+n-3} + (1-\alpha)^3 \hat{P}^d_{t+n-3} \\ &= \cdots\end{aligned} \tag{14}$$

According to formula (14), the larger α indicates that the recent values are more important for estimating the threshold of the next time. In the reference (Wang et al., 2018), this parameter is suggested as 0.2 to 0.3. The parameter β is used to smooth the estimated value. Like the parameter α, the larger the parameter β *is*, the more important the recent values are. In the reference (Wang et al., 2018), the parameter β is suggested to less than 0.5. The parameter λ is different from parameters α and β, which directly determines the threshold. Therefore, the parameter λ is more important and is suggested as 3 or 1.96 in the reference (Wang et al., 2018). For the better detection effect, three parameters α, β, and λ are determined by a large number of experiments.

3）The detection time interval ΔT

The detection time interval ΔT determines both the detection granularity and the response time. Smaller detection granularity cannot ensure enough data to reflect statistical characteristics of network traffic and may result in a higher false positive rate. Meanwhile, it also increases the challenge of the response time. Larger detection granularity possibly conceals the statistical information of LDDoS attacks in a large amount of network traffic, which leads to a high false negative rate. The detection time interval is set as 10s in the reference (Tang et al., 2014). In this paper, numerous experiments are conducted to set a more appropriate detection time interval.

3.6 Algorithm description of the LDDM

This section describes the overall execution process of the proposed LDDM. Since LDDM is a real-time online detection method, and the three components are executed by a linear way within a single detection interval. However, this method spirals forward in the entire time domain. The detailed description is shown in algorithm 3.

Algorithm 3 The proposed LDDoS attacks detection method (LDDM)

Input: flow set F, m, σ, β, λ
Output: detection R
(1) *Anomaly_flag* = 0 // *Anomaly_flag* is the anomaly flag, which indicates whether the previous time was an anomaly.
(2) *Before_Th*, *Before_S* = *getInitBaseline*(F, m, σ, β, λ)
(3) $t = m+1$
(4) While t is continued do
(5) S_t = ø //the multi-dimensional sketch of the current time interval
(6) Summary F_t into S_t
(7) Calculate P^d_t according to Algorithm 1
(8) If *Anomaly_flag* == 0
(9) Calculate Th_t according formulas (8-11)
(10) If P^d_t in the range of Th_t
(11) r = 0 // the detection result is normal.
(12) R.add(r)
(13) *Anomaly_flag* = 0
(14) Update *Before_Th*, *Before_S* according to Th_t, S_t preparing for next time interval
(15) else

(16) r = 1 // the detection result is abnormal.
(17) R.add(r)
(18) *Anomaly_flag* = 1
(19) Start the freezing mechanism according to Algorithm 2
(20) End if
(21) Else
(22) If P^d_t in the range of Th_t
(23) r = 0
(24) R.add(r)
(25) *Anomaly_flag* = 0
(26) Update *Before_Th*, *Before_S* according to Th_t, S_t preparing for next time interval
(27) else
(28) r = 1
(29) *Anomaly_flag* = 1
(30) R.add(r)
(31) End if
(32) End if
(33) End while
Produce 1: *getInitBaseline*(F, m, σ, β, λ)
(1) For i = 1:m do
(2) S_i = ø //the sketch of the current time interval
(3) Summary F_i into S_i
(4) Calculate P^d_t according to Algorithm 1
(5) Calculate Th_t according formulas (8-11)
(6) End for
(7) *Before_Th* = Th_m
(8) *Before_S* = S_m

In Algorithm 3, line (1) sets the *Anomaly_flag* to indicate whether an attack has occurred in the past time interval. *Anomaly_flag* = 0 indicates that the previous time interval is normal, and then execute lines (8)-(20). Otherwise, execute lines (21)-(30). The difference between the two parts is the process of updating the threshold as line (9). If the previous time interval is an abnormal time, the freezing mechanism is started as line (19). The threshold does not need to be updated again as lines (21)-(30). Line (2) performs the *getInitBaseline* which generates the network baseline of the initial threshold and initial sketch according to normal traffic of the previous m time intervals. This condition that the first m time intervals are normal is easy to realize in network environment. In this paper, m is set as 10.

4、Experiment and performance evaluation

The overall experiments are conducted in the Windows 7 PC, Intel® Pentium® CPU G2020 @2.90GHz, 4.00GB RAM, and the LDDM is implemented in the software of matlab2017b.

4.1 Dataset

(1) 3%, 10% and 30% DDoS dataset

The network traffic dataset combines normal network traffic and DDoS attack traffic. Normal network traffic is obtained in the real campus LAN environment of School of information science and engineering. This environment includes several PCs of windows 7 and windows 10 system as well as Ubuntu system servers. DDoS attack traffic is obtained via attacking the specific victim host by IP spoofing and pseudo randomization technology of Hping3 tool. The DDoS attacker system runs Kali Linux system which is a Linux distribution based Debian. Kali Linux system is a practical security test kit, including as many penetration and audit tools as possible. Hping3 tool in Kali Linux system is as an attack tool to generate

various DDoS attacks. Hping3 is usually used by system administrators and moral hackers for pinging tasks or advanced tasks. It can use multiple protocols and a route tracking mode to transfer files between two mutually contained channels. The victim system runs window 7 system.

This dataset contains DDoS attack traffic (ICMP, UDP and TCP SYN Flood attacks) with different attack rates. The attack rate refers to the rate of the number of attack packets to the total packets per unit time in the attack scenario as formula (15) (Sagar, 2018). The detailed attack mode is shown in Table 1. The detailed description of the generated three network traffic datasets is shown in Table 2.

$$Attack_{rate} = \frac{P_{attack}}{P_{total}} * 100\%, \quad (15)$$

Where P_{attack} is the number of attack packets, and P_{total} is the number of total packets.

Table 1 Details of simulated DDoS attacks

Attack type	Attack rate
ICMP Flood	3%, 10%, 30%
UDP Flood	3%, 10%, 30%
TCP SYN Flood	3%, 10%, 30%

Table 2 Information description of 3%, 10% and 30% DDoS dataset

Dataset name	Dataset description	Number of total packets	Number of abnormal packets	Duration time	Attack time
Dataset1	This dataset contains normal network traffic and DDoS attack traffic with an attack rate of 3%.	2,667,367	23,956	1810s	1070s~1180s 1280s~1400s 1570s~1710s
Dataset2	This dataset contains normal network traffic and DDoS attack traffic with an attack rate of 10%.	1,856,280	72,475	1290s	510s~600s 710s~850s 960s~1100s
Dataset3	This dataset contains normal network traffic and DDoS attack traffic with an attack rate of 30%.	2,071,413	179,902	1660s	790s~870s 1060s~1160s 1330s~1420s

(2)SUEE8 dataset

SUEE8 dataset includes network traffic in and out the network server of the electronic engineering student union in Ulm University lasting for 8 days (2017). The attack traffic is generated by slowloris, slowhttptest and slowloris-ng tools. The specific information is as follows: ①50 attackers (IP address from 10.128.0.1 to 10.128.0.50) run the slowloris tool; ②50 attackers (IP address from 10.128.0.50 to 10.128.0.100) run the slowhttptest tool; ③50 attackers (IP address from 10.128.0.100 to 10.128.0.150) run the slowloris-ng tool. In this paper, some of SUEE8 datasets (called Dataset4) are selected, and the details are shown in Table 3. According to formula (15), the attack rate of Dataset4 is about 50%. To obtain a low-rate DDoS attack traffic, some attack packets were replaced by normal packets to get a dataset with 10% and 50% attack rates.

Table 3 Information description of SUEE8 dataset

Dataset name	Dataset description	Number of total packets	Number of abnormal packets	Duration time	Attack time
Dataset4	This dataset contains normal network traffic and DDoS attack traffic with attack rates of 10% and 30% on HTTP protocol.	3,518,706	17,258	69,620s	3630s~3935s

(3)MAWI_BOUN DDoS dataset

The dataset is a hybrid dataset consisting of MAWI20200501 dataset (202005011400.pcap) (MAWI, 2020) and BOUN DDoS dataset (Erhan, 2020). In MAWI20200501 dataset, normal network traffic of TCP and UDP protocol are extracted as background traffic. DDoS attack traffic in BOUN DDoS dataset is extracted as attack traffic. The MAWI20200501 dataset

is obtained from traffic traces of the MAWI Working Group of the WIDE Project. The traffic data traces at the transit link of WIDE to the upstream ISP every day. This link is 1Gbps with 150Mbps committed access rate. MAWI20200501 dataset contains 15 minute network traffic captured on May 1, 2020, which contains a large number of packets transmitted between tens of thousands of active hosts (50 million to 200 million packets per 900 seconds). Hence, MAWI20200501 dataset is a representative ISP network traffic dataset. BOUN DDoS dataset is recorded on the campus backbone network of Bogazici University with more than 2000 active hosts. This dataset includes normal traffic and attack traffic, in which attack traffic is generated by the random spoofing IP technique of Hping3. The victim is a server connected to the campus backbone router. For simplicity, this dataset is called Dataset5 in the following. According to formula (15), attack rates of this dataset are about 1%~15%.

Table 4 Information description of MAWI_BOUN DDoS dataset

Dataset name	Dataset description	Number of total packets	Number of abnormal packets	Duration time	Attack time
Dataset5	This dataset contains normal network traffic and DDoS attack traffic with attack rates 1%~15%.	32,511,624	386,203	900s	160s~182s 260s~283s 359s~383s 460s~483s

4.2 Data preprocessing

This section mainly describes data preprocessing which involves the traffic packet capture and the traffic flow generation. The detailed steps are as follows.

(1) Capture and analyze network packets by Wireshark to obtain attributes: timestamp, source IP address, destination IP address, source Port, destination Port, protocol and bytes.

(2) Convert the IP address into the numerical value.

(3) Aggregate traffic packets to traffic flows in time interval ΔT. In this paper, the traffic flows are not summarized on the maximum constraint group (source IP address, destination IP address, source Port, destination Port, and protocol), but only on the constraint condition of source IP address and destination IP address.

4.3 Performance evaluation index

To evaluate the detection effect of the LDDM, *Acc* (Accuracy), *TPR* (True positive rate), *FPR* (False positive rate) and *FNR* (False negative rate) are adopted in this paper (Wang, 2018). *Acc* refers to the proportion of normal and attack behaviors identified correctly in the total flow behaviors. *TPR* refers to the proportion of the number of attacks correctly identified as attacks in the total attacks. *FPR* refers to the proportion of the number of normal behaviors that are mistakenly identified as attacks in the total normal behaviors. *FNR* measures the proportion of the number of attacks that are wrongly identified as normal behaviors in total attacks. The whole formulas are as follows.

$$Acc = \frac{n_{normal}+n_{attack}}{N_{total}}, \tag{16}$$

$$TPR = \frac{n_{attack}}{N_{attack}}, \tag{17}$$

$$FPR = \frac{n_{normal\to attack}}{N_{normal}}, \tag{18}$$

$$FNR = \frac{n_{attack\to normal}}{N_{attack}}, \tag{19}$$

Where, N_{total}=N_{normal}+N_{attack}, N_{total} is the number of total flows, N_{normal} is the number of total normal behaviors, N_{attack} is the number of total attacks, n_{normal} is the number of normal behaviors correctly identified, n_{attack} is the number of attacks correctly identified, $n_{normal\to attack}$ is the number of normal behaviors mistakenly identified as attacks, and $n_{attack\to normal}$ is the number of attacks wrongly identified as normal behaviors.

4.4 Experiment result

This section evaluates the proposed LDDM by a lot of experiments and the above evaluation indexes. The experiment process is mainly divided into the following parts. Firstly, the information (number of bytes, number of packets) of five traffic datasets is globally analyzed and visualized to better understand the overall distribution of network traffic. Next, the parameter configuration is discussed via several experiments, and the parameter values with best detection results are selected. Next, the effectiveness of three components is analyzed, respectively. Then, the time feasibility is discussed. Finally, compare with other algorithms to further illustrate the detection effect of the proposed LDDM.

A. Network traffic analysis and visualization

The first experiment mainly analyzes and visualizes network traffic changes (number of packets, and number of bytes) with time. Taking 10s as a time interval, traffic changes with time in Datasets1, 2, 3, 4 and 5 are as shown in Figures 3 and 4. By comparing the ordinate of Figure 3(a)-(e), we find that the network scale of Dataset5 is the largest and far larger than that of the other two kinds of datasets. Dataset4 represents the smallest network scale. Next, network traffic changes are analyzed. It can be seen that the network traffic has a great volatility with time. Even in the normal network state, the network traffic still abruptly reduces or increases, such as Figure 3(a). In the attack network state, the network traffic also does not display an obvious increase as Figure 3(e). We note that the network traffic does not show a significant change with the occurrence of DDoS attacks, especially in LDDOS attacks. Only when the attack rate is 30%, it shows a slight fluctuation. However, the boundary between attack traffic and normal traffic is not clear. Therefore, DDoS attacks cannot be identified only by traffic changes. It is impossible to judge whether traffic changes are caused by normal traffic fluctuation or DDoS attacks. Therefore, only via network traffic changes, it is difficult to detect DDoS attacks.

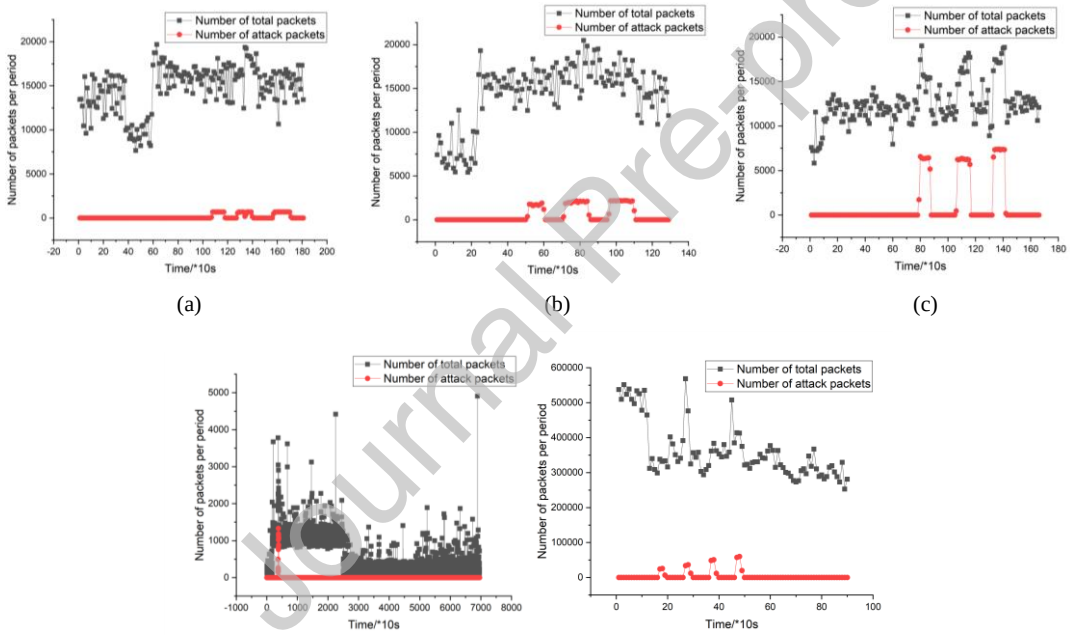
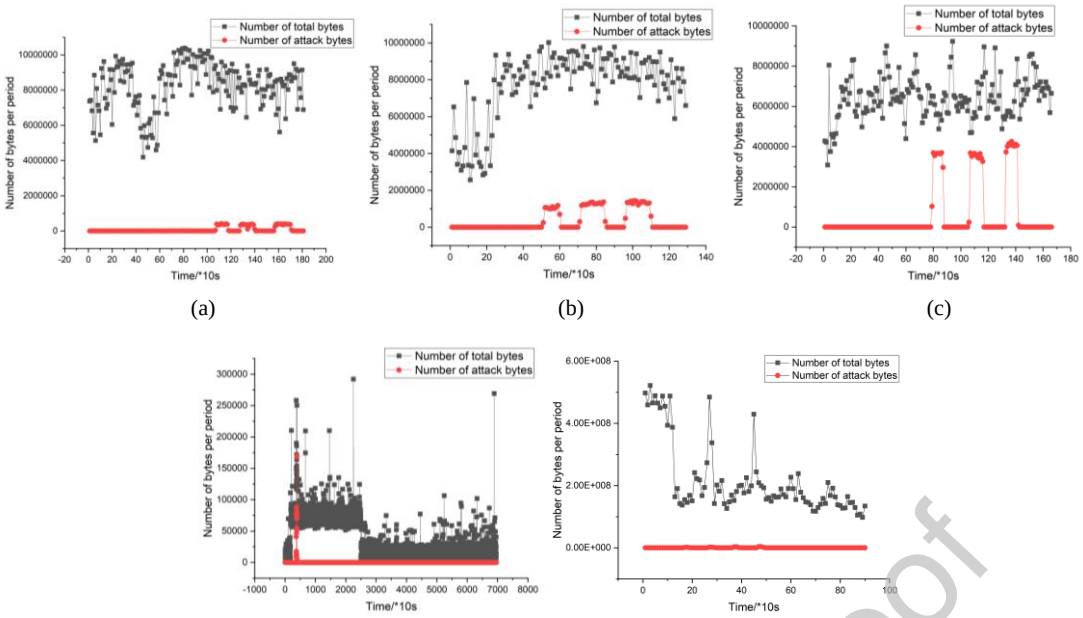


Figure.3 Changes of total traffic packets with time (a) Dataset1 (b) Dataset2 (c) Dataset3 (d) Dataset4 (e) Dataset5



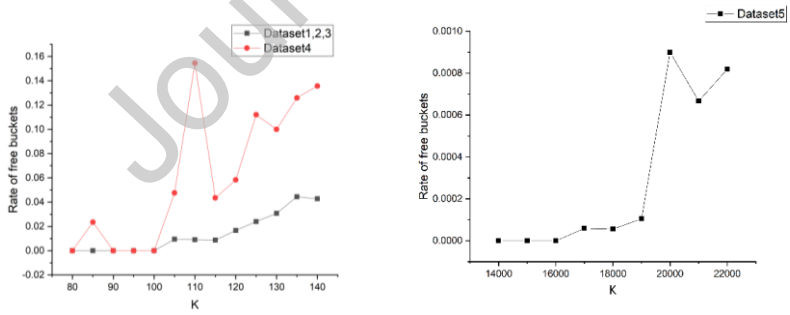
(a) (b) (c)

(d) (e)

Figure.4 Changes of total traffic bytes with time (a) Dataset1 (b) Dataset2 (c) Dataset3 (d) Dataset4 (e) Dataset5

B. Experiment parameter configuration

Experiment 2 is mainly used to set various parameters, including the size of hash table *K*, parameters of the improved weighted exponential moving average method α, β, λ and the detection time interval ΔT. It is worth noting that in different network environments, parameter values are different. Therefore, three kinds of datasets in this paper correspond to three groups of parameter values. For the parameter *K*, it is set according to the proportion of free buckets in the sketch. Because the network scale would affect the size of hash table, the *K* values in three kinds of datasets are different. Figure 5 shows the relationship between the *K* value and the rate of free buckets in five datasets. Due to the volume of Dataset5 much larger than that of other datasets, the size of hash table is also much larger than that of other datasets. Therefore, for clarity we separately show the relationship between the *K* value and the rate of free buckets about Dataset5. We see that with the increase of the *K* value, the rate of free buckets increases. At the same time, the data conflict is becoming smaller, but the data storage is becoming larger. In Dataset1, 2, 3 and 4, when *K* = 100, the data conflict is the smallest. With the increase of the *K* value, the waste of data storage increases gradually. Therefore, the *K* values of Dataset1, 2, 3 and 4 are set as 100. In Dataset 5, the *K* value is relatively larger as 16000.

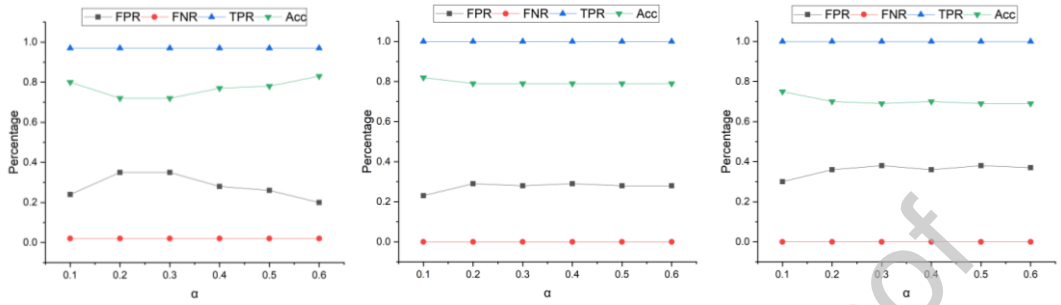


(a) (b)

Figure.5 The proportion of free buckets in the sketch (a) Dataset1, 2, 3, 4 (b) Dataset5

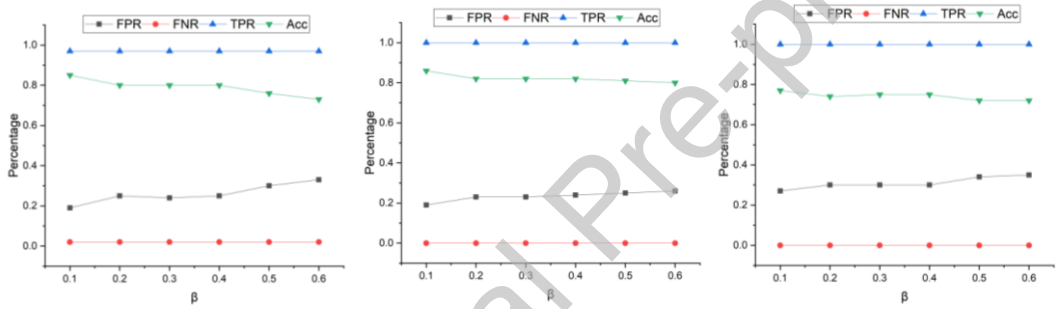
Next, parameters of the improved weighted exponential moving average method are evaluated. According to the detection effect, the optimal parameter values are selected. Considering the above evaluation indexes, the larger the *Acc* and *TPR*, and the smaller the *FPR* and *FNR*, the better the detection results. Take the first kind of datasets as an example,

Figures 6, 7, and 8 show detection effects of the different values of parameters α, β, and λ, respectively. From Figure 6, diverse values of parameter α have a negligible influence for detection effects on *FPR*, *FNR*, *TPR*, and *Acc*. When α=0.1, the evaluation results show a relatively high accuracy and low *FPR*. Hence, the parameter α is set as 0.1. Figure 7 shows evaluation results of parameter β. The parameter β is similar to parameter α on detection effects. Therefore, the parameter β is set as 0.1. Figure 8 displays the impact of different values of parameter λ. Unlike parameters α and β, the parameter λ has a significant influence on detection effects as Figure 8(a). The smaller the attack rate, the greater the impact of parameter λ for evaluation results. In Figure 8(a), when the parameter λ is 2 or 3, detection effects are relatively well. In Figures 8(b) and 8(c), the better evaluation results are obtained when the parameter λ is equal to or greater than 3. Therefore, considering comprehensive detection effects of the three datasets, the parameter λ is set as 3.



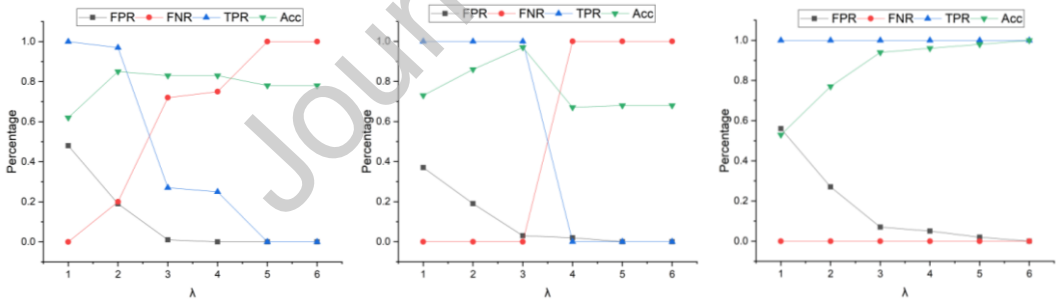
(a) (b) (c)

Figure.6 Impact of the parameter α for detection results (a) Dataset1 (b) Dataset2 (c) Dataset3



(a) (b) (c)

Figure.7 Impact of the parameter β for detection results (a) Dataset1 (b) Dataset2 (c) Dataset3

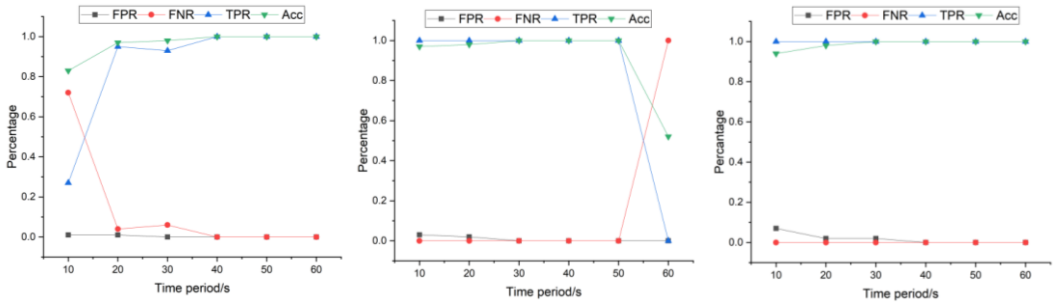


(a) (b) (c)

Figure.8 Impact of the parameter λ for detection results (a) Dataset1 (b) Dataset2 (c) Dataset3

The following experiment illustrates the influence of the time interval ΔT for detection results. When the detection time interval is too short or too long, it is mostly possible to product negative detection effects. Therefore, it is very important to select an appropriate detection time interval. Take the first kind of datasets as an example, Figure 9 depicts detection effects of different time intervals on the three datasets. As shown in Figure 9(a), when the attack rate is low, the

short detection time interval cannot be helpful to effectively detect network attacks. However, if the detection time interval is too long, attacks may be buried as Figure 9(b). Combining detection results of three datasets, ΔT is set as 20s.



(a) (b) (c)

Figure.9 Impact of the time interval ΔT for detection results (a) Dataset1 (b) Dataset2 (c) Dataset3

The parameter configuration of SUEE8 and MAWI_BOUN DDoS datasets is similar to the above experiments. Table 5 shows the parameter values of these five datasets. According to the parameter values, Table 6 demonstrates the final detection results. It can be seen that our method has excellent detection effects on all five datasets. The accuracy and *TPR* are close to 100%, *FPR* and *FNR* are very low. Only there is a slightly higher *FNR* on Dataset1. This is that fewer attack packets per time interval (when the attack rate is less than 3%) cannot make the sketch show a significant deviation. The *FPR* of Dataset5 is slightly higher as 5%. This is due to great changes of network traffic in a certain time interval, normal network traffic is mistakenly identified as attack traffic. The 10% attack packets in Dataset4 are well detected. Detection results of Dataset5 illustrate that our method can identify DDoS attacks with the attack rate as low as 1% in backbone network. Therefore, the proposed LDDM is very excellent, which can detect low-rate DDoS attacks in different network environments.

Table 5 Setting values of the related parameters

Items	Parameters	Description	Values of Dataset1,2,3	Values of Dataset4	Values of Dataset5
Sketch	H	Number of hash functions	5	5	5
	K	Size of hash table	100	100	16000
IEWMA	α	Damping coefficient	0.1	0.7	0.7
	β	Variance damping coefficient	0.1	0.1	0.3
	λ	Threshold damping coefficient	3	3	4
Other parameters	ΔT	Detection time interval	20s	20s	20s

Table 6 Overall effects of the proposed LDDM

Dataset	Dataset1	Dataset2	Dataset31	Dataset4	Dataset5
Acc	0.97	0.98	0.98	0.98	0.95
TPR	0.95	1	1	1	1
FPR	0.01	0.02	0.02	0.02	0.05
FNR	0.04	0	0	0	0

C. Availability analysis of multidimensional sketch structure

The validity analysis of multidimensional sketch includes two parts: storage validity and detection validity. Storage validity means that the consumption of sketch mode is far less than that of traditional per-item-state model. Figure 10 shows comparison results of five datasets in traditional per-item-state mode and sketch summary mode. In traditional per-item-state mode, because the duration and packet number of first three datasets are approximately same, the storage size basically increases with the increase of the attack rate. The network scale of Dataset4 is smaller than that of first three datasets, and the number of unique IP addresses also is smaller. Therefore, even the duration and attack rate of Dataset4 are relatively large, the storage size is not larger than that of first three datasets. The network scale of Dataset5 is much larger than that of other datasets. In traditional per-item-state mode, its storage size also is far greater than the storage size of other datasets. In sketch summary mode, the sketch size is same as other four datasets. The storage size of this mode slightly

changes with the duration. Because the sketch size of Dataset5 is much larger than that of other four datasets, its storage size is also larger than the storage size of other four datasets in sketch summary mode. In generally, the storage size of traditional per-item-state mode is much larger than that of sketch summary mode. Therefore, sketch summary mode can greatly reduce the storage consumption, especially in a larger network environment or a higher attack rate.

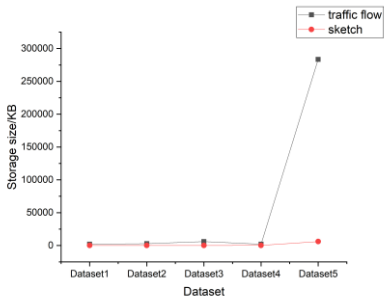


Figure.10 Comparison results of storage size between traditional per-item-state mode and sketch summary mode

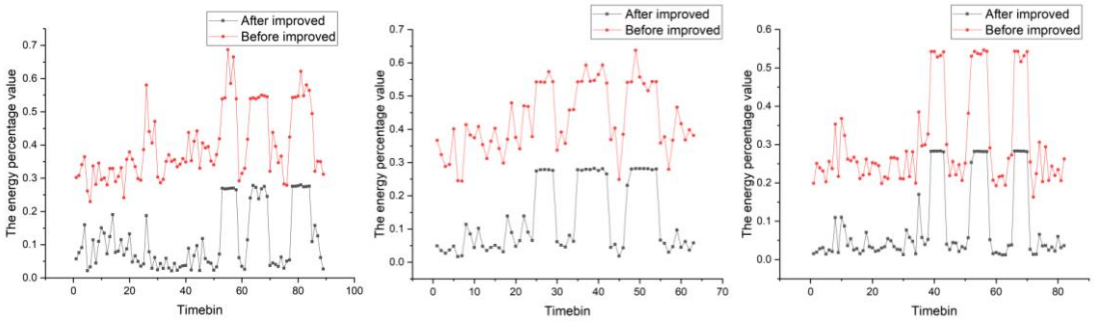
Table 7 demonstrates the influence of single dimensional SIP sketch structure and multidimensional sketch structure for attack detection effects. SIP sketch refers to the sketch mapping result with source IP address as the key. The optimal detection results of this structure are shown in Table 7. It can be seen that the detection results of single dimensional sketch are lower than that of multidimensional sketch. This is because when DDoS attacks occur, comprehensive distributions of source IP addresses and destination IP addresses can better reflect the anomaly of network flows. From first three datasets, the higher the attack rate, the better the attack detection effects based on SIP sketch. However, it is still lower than the detection results of multidimensional sketch structure. In Dataset4 and Dataset5, the distribution of the source IP address cannot discover the attack information and leads to a high *FNR* or *FPN*. Therefore, according to detection results of these five datasets, the multidimensional sketch structure is very effective for improving detection effects. In conclusion, multidimensional sketch structure helps to reduce the complexity of traffic flow storage and improve detection effects of LDDoS attacks.

Table 7 Comparison of detection results between SIP sketch and multidimensional sketch

Item	Dataset1		Dataset2		Dataset3		Dataset4		Dataset5	
	SIP sketch	multi-dim sketches	SIP sketch	multi-dim sketches	SIP sketch	multi-dim sketches	SIP sketch	multi-dim sketches	SIP sketch	multi-dim sketches
Acc	0.64	0.97	0.90	0.98	0.91	0.98	0.99	0.98	0.80	0.95
TPR	0.96	0.95	0.90	1	1	1	0.14	1	0.90	1
FPR	0.53	0.01	0.09	0.02	0.10	0.02	0.01	0.02	0.22	0.05
FNR	0.03	0.04	0.09	0	0	0	0.86	0	0.11	0

D. Availability analysis of the improved behavior divergence measurement method based on daub 4 wavelet transform

The following experiment analyzes the availability of the improved behavior divergence measurement method based on daub 4 wavelet transform. The improvement of this method mainly points to the reordering of the signal divergence that identifies low-frequency and high-frequency components of the signal divergence more effectively. Take the first type of datasets as an example, Figure 11 shows the energy percentage of the sketch divergence before and after improved on three datasets, respectively. On normal network, the improved P^d value is more stable and keeps at a lower level. When attacks occur, it is stable at a high level. The improved P^d value is significantly higher than that of normal traffic, which is very beneficial to distinguish normal traffic and attack traffic. Compared with the trend of the P^d value before the improvement, there is an obvious boundary between normal traffic and attack traffic in the improved P^d value as Figure 11. Therefore, based on the P^d value before the improvement, it is difficult to distinguish normal network and abnormal network by an effective threshold. This situation leads to a large *FPR* or *FNR* in the process of DDoS attack detections. Therefore, the improved behavior divergence measurement method based daub 4 wavelet transform is very effective for detecting DDoS attacks.



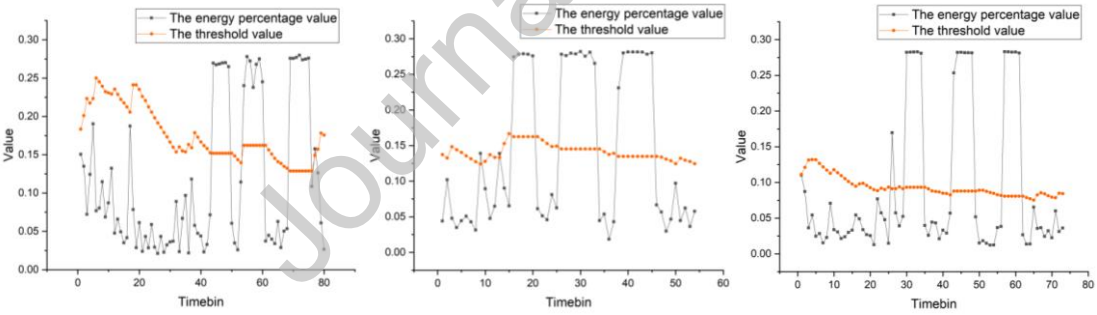
(a) (b) (c)

Figure.11 Comparison of P^d values before and after the improved behavior divergence measurement method based on daub 4 wavelet transform (a) Dataset1, (b) Dataset2, (c) Dataset3

E. Availability analysis of dynamic threshold mechanism

This experiment will analyze the effectiveness of dynamic threshold mechanism, including two parts: the effectiveness of dynamic threshold mechanism and the effectiveness of freezing mechanism. Take the first kind of datasets as an example, Figure 12 displays the changes of the P^d value and threshold in three datasets, respectively. From the longitudinal perspective, when the P^d value of normal traffic is large, the threshold is also large. The P^d value of normal traffic in Figure 12(a) is higher than that in Figures 12(b) and 12(c). Like the P^d value, the threshold displays the same trend. Therefore, it means that the threshold changes with network traffic. It is very necessary to set the dynamic threshold. From the horizontal perspective, in Figure 12(a), the P^d value and the threshold value are relatively high at the initial time interval. When the P^d value becomes small, the threshold also decreases. Therefore, it can be seen that network traffic is not fixed and has a certain fluctuation. Moreover, dynamic threshold mechanism is effective and can well reflect the real network traffic.

The freezing mechanism is an important part of dynamic threshold mechanism. It ensures that the network threshold stays in the standard state and is not affected by attack traffic. Figure 13 shows changes of the P^d and threshold without freezing mechanism. With the occurrence of attacks, the threshold sharply increases due to the abnormal P^d value. Even if attacks disappear, the threshold does not decrease to the normal level. Hence, attacks cannot be well detected resulting in a high *FNR*. Combining results of Figures 12 and 13, the freezing mechanism keeps the baseline of normal network at a standard level and ensures a low *FPR* and *FNR* for LDDoS attack detections. The detection results with and without freezing mechanism are shown in Table 8. When there is no freezing mechanism, the *FNR* is always 1 and attacks cannot be detected totally. Therefore, the freezing mechanism is very necessary and effective.



(a) (b) (c)

Figure.12 Changes of P^d value and threshold of network flows under dynamic threshold mechanism (a) Dataset1, (b) Dataset2, (c) Dataset3

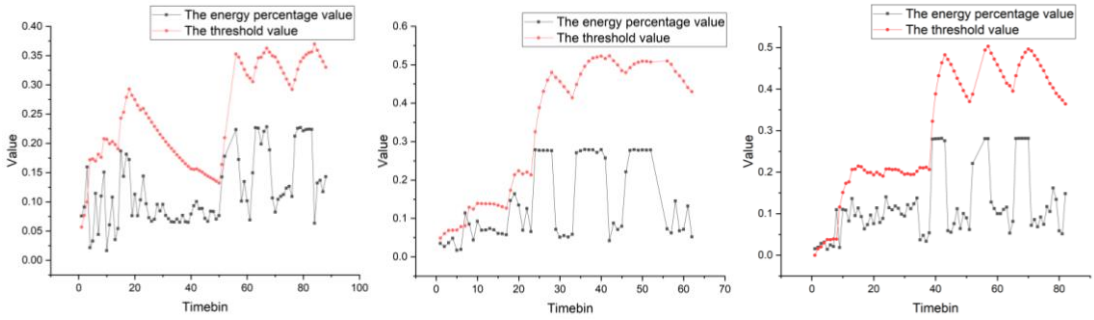


Figure.13 changes of the P^d value and threshold of network flows without freezing mechanism (a) Dataset1, (b) Dataset2, (c) Dataset3

Table 8 Comparison of LDDoS detection effects with and without freezing mechanism

	Dataset1		Dataset2		Dataset3	
	Without Freezing Mechanism	With Freezing Mechanism	Without Freezing Mechanism	With Freezing Mechanism	Without Freezing Mechanism	With Freezing Mechanism
Acc	0.76	0.97	0.67	0.98	0.81	0.98
TPR	0	0.95	0	1	0	1
FPR	0	0.01	0	0.02	0	0.02
FNR	1	0.04	1	0	1	0

F. Time feasibility analysis

For DDoS attack detections, time feasibility is a very important evaluation index. The higher the detection efficiency, the more conducive to timely find attacks and take appropriate measures. The detection time is mainly consumed in multidimensional sketch summary and detection stage. Table 9 displays the consume time of sketch summary and detection in each detection interval. In LAN environment represented by Dataset1, 2, 3 and 4, sketch summary time and detection time are much less than 20s. Dataset4's size is much smaller than the size of other datasets, the process time of this dataset is especially small only 0.04s. On the contrary, in WAN environment, the sketch summary time and detection time of Dataset5 are longer than that of other datasets. Therefore, sketch summary time is related to traffic volume and attack rates. The detection time is related to the size of sketch. In a single detection time interval, the summary time of Dataset4 is the smallest, and the summary time of Dataset5 is the longest. Compared Dataset 1, 2 and 3, Dataset3 has the largest attack rate and the longest sketch summary time. Due to the largest size of sketch of Dataset5, the detection time of Dataset5 is longer. According to the above analysis, the larger the network scale, the higher the attack rate, the longer the sketch summary time and detection time. In general, this method has a perfect time feasibility in low-rate DDoS attack detections. At the same time, the future work will focus on the sampling technology and distributed technology to further reduce the processing time of network flows under high-speed backbone network.

Table 9 Detection time of the LDDM (unit: second)

Item	Dateset1	Dateset2	Dateset3	Dateset4	Dateset5
Sketch summary	2.17	4.29	7.50	0.03	59.95
Detection stage	0.01	0.01	0.01	0.01	6.22

G. Comparative analysis of detection effects

In order to better illustrate detection effects of the proposed LDDM, it is compared with three popular algorithms (Hellinger Distance (Tang et al., 2014), Shannon Entropy (Callegari et al., 2017), Tang et al. (2011)). Similar to our method, the method (Tang et al., 2014) uses Hellinger distance to calculate sketch differences. The methods (Callegari et al., 2017) and (Tang et al., 2011) utilize entropy and wavelet analysis on a single period sketch to detect DDoS attacks. The comparison results are shown in Figure 14. On the whole, the proposed LDDM has a significant detection effect on all datasets. For 3% LDDoS attacks, our method is the best. The *FNR* is significantly lower than other methods, the accuracy and *TPR* are also significantly better than other methods, and only the *FPR* is slightly higher than other methods. For 10% and 30% DDoS attacks, the *TPR*, accuracy, and *FNR* of LDDM are slightly better or equal to that of other three methods.

Specially, our method has the lowest *FNR*. In Dataset4, our method is slightly better than the method (Tang et al., 2014). The detection results of methods (Callegari et al., 2017) and (Tang et al., 2011) are obviously worse than the LDDM. For Dataset5, LDDM has a good accuracy and *TPR*, and is significantly better than other methods in *TPR* and *FNR*. In WAN network environment, our method can accurately detect low-rate DDoS attacks of attack rates 1%~15%. Therefore, there is a conclusion that sketch divergences in continuous time intervals can better reflect attacks than sketch of a single time interval. The wavelet transform method is more sensitive to detect LDDoS attacks than other metrics. In summary, the LDDM can effectively detect LDDoS attacks in different network environments (LAN or WAN environment) and has an excellent detection effect in hidden and lower rate DDoS attacks.

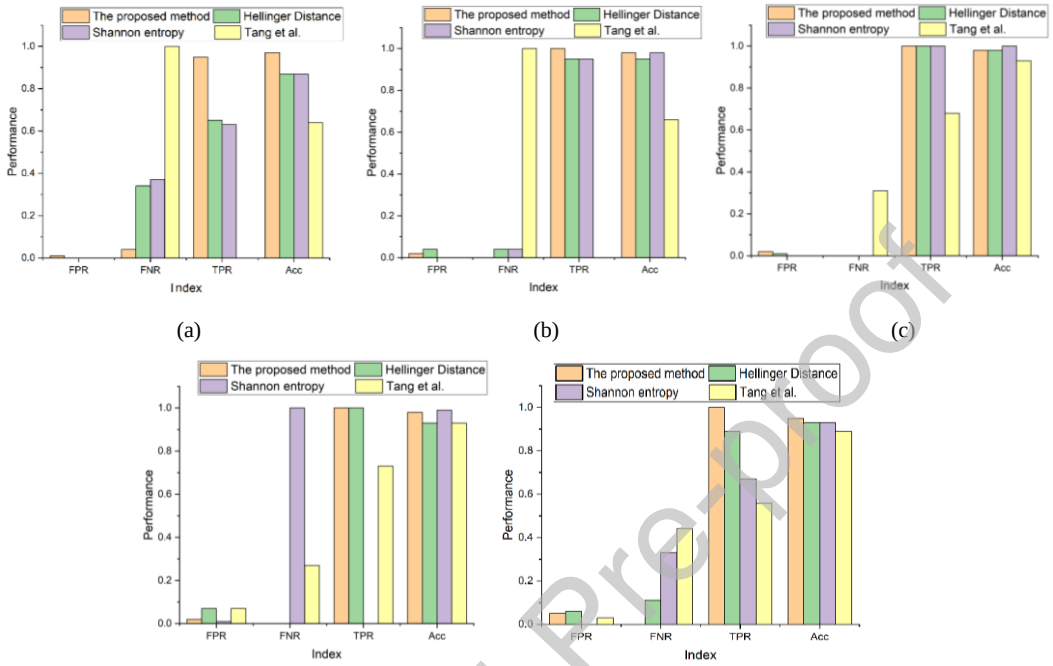


Figure.14 Comparison of detection effects between the LDDM and other methods (a) Dataset1 (b) Dataset2 (c) Dataset3 (d) Dataset4 (e) Dataset5

Conclusion

This paper proposed an effective and real-time attack detection method to detect low-rate DDoS attacks in LAN and WAN environment. We firstly designed multidimensional sketch structure according to network traffic attributes (SIP and DIP). The storage and compress abilities of this sketch structure were tested and compared with the traditional per-item-state mode. Multidimensional sketch structure greatly reduces the storage complexity of network flows. In addition, this structure effectively improves detection effects of LDDoS attacks via comparing with SIP sketch. Next, behavior divergences between normal sketch and attack sketch were measured by an improved behavior divergence measurement method. This method applied a reordered daub 4 wavelet transform method to calculate the energy percentage of the signal divergences. This method enables to maintain the stability of network traffic baseline and effectively distinguish the difference between DDoS attack traffic and normal traffic. Furthermore, we designed an improved exponential weighted moving average method to realize dynamic threshold mechanism. Based on real network traffic changes, the dynamic threshold is more coincident with the real network environment and network inherent dynamic. In addition, for calculating the normative dynamic threshold, we proposed the freezing mechanism. Via comparing with and without freezing mechanism, we can say that the freezing mechanism avoids the threshold polluted by attack traffic and effectively reduces the false positive rate and false negative rate. Further, through computing the run time of each component, the proposed

LDDM has a good time feasibility. Finally, compared with other methods, our results show that LDDM has a superior performance, such as the higher accuracy and *TPR*, as well as the lower *FPR* and *FNR*, especially in more hidden and low-rate DDoS attack detections. Meanwhile, the proposed LDDM has a good adaptability to different network environments.

Credit Author Statement

Xinqian Liu: Methodology, Writing, Experiment. Jiadong Ren: Conceptualization, Supervision. **Haitao He**: Conceptualization, Supervision, Reviewing. **Qian Wang:** Data curation, Investigation. **Chen Song**: Reviewing, Guidance.

Comment [COMP1]: CE: Please check `Credit Author Statement'.

Declaration of competing interests

None

Acknowledgements

This work was supported by the National Natural Science Foundation of China (61572420, 61772449, 61807028, 61802332), and Graduate Innovation Research Assistant Support of Yanshan University (CXZS202008).

References

Vidal J M et al. Adaptive artificial immune networks for mitigating DoS flooding attacks. Swarm and Evolutionary Computation 2017; 38: 94-108. https://doi.org/10.1016/j.swevo.2017.07.002.

Behal S, Kumar K. Detection of DDoS attacks and flash events using information theory metrics–An empirical investigation. Computer Communications 2017; 103:18-28. https://doi.org/10.1016/j.comcom.2017.02.003.

Singh K J et al. Detection and differentiation of application layer DDoS attack from flash events using fuzzy-GA computation. IET Information Security 2018; 12(6): 502-512. https://doi.org/ 10.1049/iet-ifs.2017.0500.

Worldwide Infrastructure Security Reoprt, Arbor Network. http://www. arbornetworks.com/images/documents/wisr2016 enweb.pdf, 2015 (accessed 01 April 2016).

Alzahrani S, Hong L. Generation of DDoS Attack Dataset for Effective IDS Development and Evaluation. Journal of Information Security 2018; 09(4):225-241. https://doi.org/10.4236/jis.2018.94016.

Jisa David, Ciza Thomas. Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic. Computers and Security 2019; 82: 284-295. https://doi.org/10.1016/j.cose.2019.01.002.

Toklu S. Two-Layer Approach for Mixed High-Rate and Low-Rate Distributed Denial of Service(DDoS) Attack Detection and Filterin. Arabian Journal for Science & Engineering 2018; 43: 7923-7931. https://doi.org/10.1007/s13369-018-3236-9

Al-Yaseen W L et al. Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system. Expert Systems with Applications 2017; 67:296-303. https://doi.org/ 10.1016/j.eswa.2016.09.041.

Tang Jin, Cheng Yu. Quick detection of stealthy SIP Flooding Attacks in VOIP Network, 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 2011. https://doi.org/10.1109/icc.2011.5963248.

Wang F et al. A new multistage approach to detect subtle DDoS attacks. Mathematical and Computer Modelling 2012; 55(1-2):198-213. https://doi.org/10.1016/j.mcm.2011.02.025.

Park J et al. Network anomaly detection based on probabilistic analysis. International Conference on Computer Science & Its Applications. Springer Singapore, 2016. https://doi.org/10.1007/978-981-10-3023-9_107.

Behal S, Kumar K. Detection of DDoS attacks and flash events using information theory metrics-An empirical investigation. Computer Communications 2017; 103:18-28. https://doi.org/10.1016/j.comcom.2017.02.003.

Kumar P et al. SAFETY: Early Detection and Mitigation of TCP SYN Flood Utilizing Entropy in SDN. IEEE Transactions on Network and Service Management 2018. https://doi.org/10.1109/TNSM.2018.2861741.

Tang J et al. Sketch-Based SIP Flooding Detection Using Hellinger Distance. IEEE Conference on Global Telecommunications. IEEE Press, 2009. https://doi.org/10.1109/GLOCOM.2009.5426267.

Wang C et al. SkyShield: A Sketch-Based Defense System Against Application Layer DDoS Attacks. IEEE Transactions on Information Forensics and Security 2018; 13(3):559-573. https://doi.org/ 10.1109/tifs.2017.2758754.

Vidal J M et al. Adaptive artificial immune networks for mitigating DoS flooding attacks. Swarm and Evolutionary Computation 2017; S2210650216304679. https://doi.org/10.1016/j.swevo.2017.07.002.

Indraneel S, Venkata P K V. HTTP Flood attack Detection in Application Layer using Machine learning metrics and Bio inspired Bat algorithm. Applied Computing and Informatics 2017; S2210832717301655. https://doi.org/10.1016/j.aci.2017.10.003.

Callegari C et al. Combining sketches and wavelet analysis for multi time-scale network anomaly detection. Computers & Security 2011; 30(8):692-704. https://doi.org/10.1016/j.cose.2011.08.006.

Jiang D et al. Multi-scale anomaly detection for high-speed network traffic. Transactions on Emerging Telecommunications Technologies 2015; 26(3):308-317. https://doi.org/10.1002/ett.2619.

M. Attig, G. Brebner. 400 Gb/s programmable packet parsing on a single FPGA. Archit Netw Commun Syst 2011; 12-23. https://doi.org/10.1109/ANCS.2011.12.

Tong D, Prasanna V K. Sketch Acceleration on FPGA and Its Applications in Network Anomaly Detection. IEEE Transactions on Parallel and Distributed Systems 2017; 99:1. https://doi.org/ 10.1109/TPDS.2017.2766633.

Jazi H H et al. Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. Computer Networks 2017; 121:25-36. https://doi.org/ 10.1016/j.comnet.2017.03.018.

Cormode G, Muthukrishnan M. Approximating Data with the Count-Min Sketch. IEEE Software 2012; 29(1):64-69. https://doi.org/ 10.1109/ms.2011.127.

Tang J et al. SIP Flooding Attack Detection with a Multi-Dimensional Sketch Design. IEEE Transactions on Dependable and Secure Computing 2014; 11(6):582-595. https://doi.org/ 10.1109/TDSC.2014.2302298.

Callegari C et al. An Information-Theoretic Method for the Detection of Anomalies in Network Traffic. Computers & Security 2017; 70:351-365. https://doi.org/10.1016/j.cose.2017.07.004.

Sagar S K, Deepak P, Mayank T, et al. An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. Future Generation Computer Systems, 2018, 89:685-697, https://doi.org/ 10.1016/j.future.2018.07.017.

[dataset] Thomas Lukaseder, https://github.com/vs-uulm/2017-SUEE-data-set, 2017.

Bingdong Li, Jeff Springer, George Bebis, George Bebis, and Mehmet Hadi Gunes, A survey of network flow applications, Journal of Network and Computer Applications, 2013, 36: 567-581, https://doi.org/ 10.1016/j.jnca.2012.12.020.

Sahoo K S, Puthal D, Tiwary M, et al. An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. Future generation computer systems, 2018, 89: 685-697. https://doi.org/ 10.1016/j.future.2018.07.017.

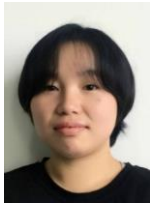
B B Gupta, Kriti Bhushan, Hypothesis Test for Low-rate DDoS Attack Detection in Cloud Computing Environment, Procedia Computer Science, 2018, 132: 947-955. https://doi.org/ 10.1016/j.procs.2018.05.110.

Tang Jin, Cheng Yu, Hao Yong. Detection and prevention of SIP flooding attacks in voice over IP networks, Infocom, IEEE. IEEE, 2012. https://doi.org/ 10.1109/INFCOM.2012.6195475.

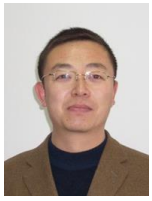
Agrawal N, Tapaswi S. Low rate cloud DDoS attack defense method based on power spectral density analysis, Information Processing Letters, 2018, 138:44-50. https://doi.org/ 10.1016/j.ipl.2018.06.001.

[dataset] MAWI, http://www.fukuda-lab.org/mawilab/v1.1/2020/05/01/20200501.html, 2020.

[dataset] Derya Erhan, https://ieee-dataport.org/open-access/bo%C4%9Fazi%C3%A7i-university-ddos-dataset, 2020.



Xinqian Liu, born in 1992. She is currently a Ph.D in Yanshan University. She received her B.S. degree in Education and Technology from Yanshan University in 2015. Her research interests include social network analysis and network security.



Jiadong Ren, born in 1967, PhD. He is a professor in the School of Information Science and Engineering, Yanshan University. He received his doctor's degree in Harbin Institute of Technology. His current research interests include data mining and software security.

Haitao He, born in 1968. PhD. He is a professor in the School of Information Science and Engineering, Yanshan University. She received her doctor's degree in Yanshan University. Her current research interests include data mining and software security.

Qian Wang, born in 1977. PhD, lecture. She is currently a lecture in the School of Information Science and Engineering, Yanshan University. She received her doctor's degree in Yanshan University. Her current research interests include data mining and software security.

Chen Song, born in 1988, Ph.D. She received both her B.S. and M.S. degree in computer science and engineering from Tianjin University of Science Technology in 2016. Her currently research fields are evolution of complex network, random walk algorithm and air quality.