# DDoS attacks defence strategies based on nonparametric CUSUM algorithm

**Changhong Yan[1*], Qin Dong[2], Hong Wang[3]**

[1]*School of Information Engineering, Yancheng Institute of Technology, No.9 XiWang Avenue Road, Yancheng, China*

[2]*School of Information Engineering, Yancheng Institute of Technology, No.9 XiWang Avenue Road, Yancheng, China*

[3]*YanCheng junior high school, No.199 The liberation of south Road, Yancheng, China*

*Received 1 September 2014, www.cmnt.lv*

**Abstract**

In the Internet network attacks, distributed denial of service (DDoS) has aroused world attention because of its destructive power. It seems particularly difficult to defend against DDoS attacks for they have characteristics such as abrupt attacks, attacking host computer in a very wide distribution, and so on. To guard against network security and defend distributed denial of service attacks (DDoS), research should begin from the detection of DDos attacks. On the basis of deep research of DDoS attacks, the thesis summarizes and analyses the mechanism and principles of intrusion detection firstly. This paper starts with the analysis of the principle of DDoS attacks. Followed by inquiry and analysis of data packet of DDoS attacks detection, the thesis gives out the computation method for detecting DDos attacks based on Flow Connection density and presents a defending model against DDos attacks based on the temporal series of Flow Connection Condensity (Density). With the defending module based on the temporal series of Flow Connection Condensity (Density), data packet can be effectively filtered so that DDos attacks can be effectively defended and prevented. Finally, experiments prove that the module can effectively filter data packet from network.

*Keywords:* network security, distributed denial of service, flow connection density, time series, defence strategies

## 1 Introduction

With the network coming into the Internet era, network security problems appear, of which distributed denial of service attack has great impact on the network security. Distributed Denial of Service, referred to as DDoS, is a kind of denial of service attacks which is offensive and destructive. At present, the Internet is everywhere, and DDoS attacks launched by hackers are everywhere unless we disconnect the network. Distributed denial of service mainly target host node, switch, routers and other network equipment. Tools used by hackers for distributed denial of service are easy to develop. Hackers conduct diversified attacks secretly and the attacking techniques improve day after day which can cause devastating damage even immeasurable losses.

DDoS is widely applied by hackers because it is easy to implement, difficult to prevent and of great harm. In February 2000, unidentified hackers launched a huge-scale distributed denial of service, attacking a series of world-renowned sites such as eBay, yahoo, Microsoft, MSN, Amazon, and so on, and causing numerous system paralyses for several days and significant social economy loss which mounted to billions of dollars. In early 2003, hackers, who will do whatever they can to cause damage, used a new technology of distributed denial of service attacks to damage the Internet in a wide range including North America, Europe and Asia. This not only caused hundreds of thousands of computers nearly paralyzed and nearly one hundred thousand network servers unable to run, but also resulted in incalculable economic losses and adverse social impact. As for China, on May 19, 2009, DNS resolution system of China Telecom was attacked by a large flow of DDoS, causing a massive network paralysis in telecommunications network of six southern provinces and thousands of web services termination [1].

Distributed denial of service, referred to as DDos, is of destructive power. For an analogy, how can you get through when 10000 people call you at the same time? And DDos attacks are like that. DDos mainly take advantage of the loopholes and shortcomings of network transport protocol - TCP/IP protocol. It chooses computers with scattered network locations as its attacking host to send large amounts of data to the target host. This will not only cause the resources or network bandwidth of attacked hosts consume a lot, but also that the attacked host is so overloaded and paralyzed that it will stop providing normal network services. As a result, legitimate users cannot get access to or use the resources, nor can the attacked host provide any services. Schematic diagram for DDos attacking principle is shown in Figure 1.

[*]***Corresponding author*** e-mail: hycit@ycit.cn

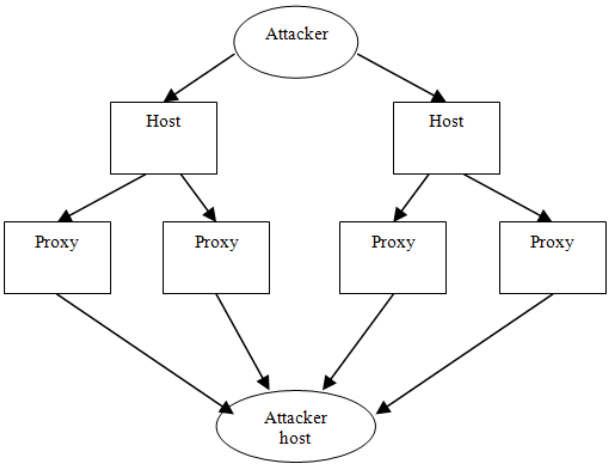


FIGURE1 DDoS attack principle

## 2 Common DDoS defence strategies analysis

The DDoS attacks on the Internet are becoming increasingly fierce and will continually intensify. Only in 2013, DDoS attacks have emerged in an endless stream in the world, and it seems difficult to measure the amount and size by using statistics. A new IDC study found that prevention solution market for DDoS attacks and DoS attacks is expected to grow 18.2 percent from 2012 to 2017 and related spending will reach $870 million [2].

The substantial harm of DDOS attacks is forcing people to defend against DDOS attacks to minimize the loss. To defend against DDOS attacks, people have explored a variety of DDOS defence strategies from various prospective based on the principle of DDoS attacks. From the DDoS attack principle in Figure1, we can see that core router of the attacked host is the proxy host and it forwards data through the intermediate network routers. Thus, when analysing distributed denial of service, we can divide the whole network into three parts, involving the attacking end of the network, the middle layer and the attacked end. Correspondingly, DDoS attack defence strategies are also divided into the attacking end defence, the middle layer defence and the attacked end defence.

### 2.1 THE NET WORK DEFENCE IN THE ATTACKING END

In this process, defence node is deployed on the ingress router of the network, then the node counts and analyses the flow based on packet information, which is monitored by the ingress router. Finally, through repeated comparisons between statistics and the normal flow model, dangerous abnormal packets will be filtered out. In this way, we cannot only track information about the attacking end, but also to avoid further damage from outside to the network. There are of course some shortcomings in the attacking end, for instance, if the attacking flow in the attacking end does not converge, it will be difficult to establish normal flow model, which will cause misjudgement rate of packet increase, resulting in a loss of legitimate data information. Currently, the most typical source-side defence strategy is D-WARD model proposed by Jelena Mirkovic and others [3].

### 2.2 THE NETWORK DEFENCE IN THE MIDDLE LAYER

Currently, the network defence in the middle layer mainly depends on intrusion detection systems on the network. Intrusion detection systems detect attacks by capturing and analysing network packets. If the network is attacked, it will take measures to correspondingly limit the rate of the attacking data flow. The benefit of this defence strategy is that once an attack is detected, you can quickly suppress the traffic, thus greatly reducing the harm to the attacked end. Disadvantage of network defence strategies in the middle layer is that the data flow on the middle tier network router is large which will not only consume more resources, but also make it difficult to decide whether the data flow is legitimate, ultimately causing damage to legitimate network traffic, and even to the performance of the whole network.

### 2.3 THE NETWORK DEFENCE IN THE ATTACKED END

The attacked end is direct victim of the DDoS attacks, and it is most immediate, most accurate and most effective to deploy defence system in the attacked end. Thus, it is effective to deploy defence system in the attacked end to defend against DDoS attacks, which is the outstanding advantage of attack end defence. Of course, there are some shortcomings in the attacked end defence strategy. For example, the attacked end is the main attacking target. If the attack is fierce, resulting in paralysis in storage and processing system on the defence node, it may not be able to respond to the defence system deployment to locate the position of the fiercest attack, which will lead to limited response to attacks. To balance its advantages and disadvantages, it is a good choice to deploy the defence system in the end network. The challenge is to find a good defence strategy, making the DDoS attacks dysfunctional so as to defend against DDoS attacks and to secure the attacked host.

## 3 DDoS attacks defence module and strategies based on nonparametric CUSUM algorithm

To design DDoS defence module based on nonparametric CUSUM algorithm and then make a better defensive strategies to effectively defend against DDoS attacks on the victim port. It is more timely and accurate to detect DDoS attacks by counting and testing traffic of attacked port, so as to defend against DDoS attacks.

### 3.1 THE DEFENCE BASIS OF NETWORK TRANSMISSION

The data transmission is carried out in the form of data packets on the network. In the Internet, in order to overcome the heterogeneity of the network, and to ensure the correct data transmission, IP protocol defines a unified packet format, which is called an IP datagram. The structure is shown in Figure 2.

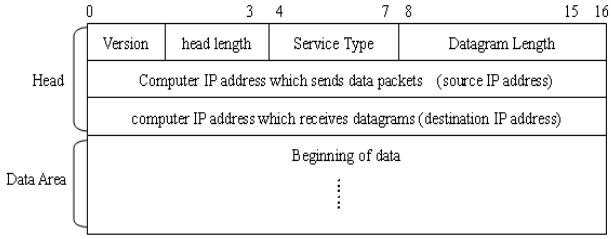


FIGURE 2 IP datagram structure

In the Internet network, any packet transmission, including that is attacked by DDoS, must be organized in the form of IP datagrams. IP datagram must indicate the specified data to be transmitted, the IP address of the computer that sends datagrams and that receives the datagram.

According to the principle of DDoS attacks, DDoS attacks are carried out by a large number of hosts that are geographically dispersed on the network, which send plenty of packets to attack the victim host. Therefore, we can analyse the source IP address, destination IP addresses and port numbers of IP datagram that reaches computers. If large amounts of datagram are from several hosts that are in geographically dispersed network, then it is DDoS attack, which we should guard against.

### 3.2 FLOW CONNECTION DENSITY

Firstly, in a certain time period, we intercept a collection of identical network data package that contains the same port number of the source address, destination port, and destination port number, and this is called a flow connection, and the amount of the flow connection in this period is called flow connection density. It can be showed in the following form.

We assume that in unit time, the collection of data packets within network traffic is $R = \{p_1,\ldots, p_i,\ldots,p_M\}$, of which, collection of related data packets is $\{R_1,R_2,\ldots,R_N\}$, then we define that in this network traffic, the flow connection density is the amount of related data packets collection, that is $N$ [4-5].

Then we take the following table as an example. Table 1 indicates the obtained IP data packets collection within a unit of time on a certain network.

TABLE 1 Information collection of IP data packets within a unit time on a certain network

| Data packets | Source IP address | Destination IP address | Destination port number |
|---|---|---|---|
| P0 | s1 | D1 | port1 |
| P1 | s1 | D1 | port1 |
| P3 | s3 | D2 | port1 |
| A | s3 | D1 | port1 |
| P4 | s2 | D2 | port2 |
| C | s2 | D2 | port2 |
| B | s3 | D2 | port2 |
| R | s3 | D2 | port1 |

Through analysis, we conclude that by comparing the same set of IP packets within this network flow per unit time, relevant set of data packets are $\{p_0, p_1\}$, $\{p_4, C\}$, $\{p_3, R\}$. According to the definition, in a time unit, the flow connection density is 3, because there are 3 relevant data packets collection within the time unit of the network. Then, we can decide whether the network traffic is normal based on the flow connection density, so as to determine whether there is distributed denial of service attack.

### 3.3 CALCULATION FOR IMPROVING FLOW CONNECTION DENSITY BASED ON NON-PARAMETRIC CUSUM ALGORITHM

Through the study of non-parametric CUSUM algorithm [6-8], we can better improve the calculation method of flow connection density. We no longer count the collection of identical network data packages in the unit time, but we calculate the added source IP address in a $\Delta t$ time to get flow connection density. Then we get a time series $\{Z\}$, which consists of flow connection density sequences within multiple $\Delta t$ time. The basic idea based on nonparametric CUSUM algorithm to improve flow connection density can be showed by the following Equations (1)-(3):

$$\begin{aligned} Y_0 &= 0, \\ Y_n &= (Y_{n-1} + Z_n)^+, \end{aligned} \tag{1}$$

$$x^+ = \begin{cases} 0, & x \le 0 \\ x, & x > 0 \end{cases}, \tag{2}$$

$Y_n$ is the cumulatively positive value of $Z_n$, and the decision functions are:

$$d_N(Y_n) = \begin{cases} 1, & Y_n > M \\ 0, & Y_n \le M \end{cases}, \tag{3}$$

where the constant value of detection threshold of DDoS is $M$, the function $d_N(Y_n)$ represents the judgment result for $M$ in a certain generating time. Through the judgment result, we define that, when the result of function $d_N(Y_n)$ is 1, there are a large number DDoS attacks; when the result is 0, there are no DDoS attacks and the network is normal.

### 3.4 CALCULATION DDoS ATTACKS DEFENCE MODEL BASED ON NON-PARAMETRIC CUSUM ALGORITHM TO IMPROVE FLOW CONNECTION DENSITY

The DDoS attacks defence model based on nonparametric CUSUM algorithm to improve flow connection density consists of three modules, respectively are acquisition module, time series module and filter module.

- Acquisition module: In this module, IP data packets received by the host are collected in every certain time of $\Delta t$, then it comes to data format conversion according to required data format in time series module and filter module and then the data is transmitted to the time series module and filter module in different levels.
- Time series module: In this module, we use the additional received IP data packets within a certain time of $\Delta t$ to calculate the abstract flow connection density. Then send the final judgment result of function $d_N(Y_n)$, which is based on the judgment result of Equations (1), (2) and (3) to the filter module by combining with the time series of $\{Zn\}$ composed of flow connection density data received in previous time periods of $(n\text{-}1)\ \Delta t$.
- Filter module: whether to receive or discard the data packets based on the data information results from processing a data packet and judgment results of function $d_N(Y_n)$ passed from time series module.

DDoS attacks defence model based on nonparametric CUSUM algorithm to improve flow connection density is shown as follows (Figure 3):

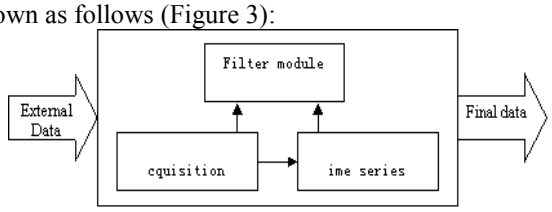


FIGURE 3 DDoS attacks defence model based on nonparametric CUSUM algorithm to improve flow connection density

The mechanism of DDoS attacks defence model based on nonparametric CUSUM algorithm to improve flow connection density is that, the system firstly obtains data within a specified time in the acquisition module, then the data packets received is analysed, including source address, destination address and specific port number of the data packets. Then it comes to data format conversion according to required data format in time series module and filter module, and then the data is transmitted to the time series module and IP packets filter module in different levels. We use the data in time series module and additional received IP data packets to calculate the specific flow connection density. Then we use the additional collected source IP data packets within a certain time of $\Delta t$ in time series module to calculate the abstract flow connection density, and calculate its cumulative positive value by combining with the time series of $\{Z_n\}$ composed of flow connection density data received in previous time periods of $(n - 1)\ \Delta t$. Then it will send the final judgment result of function $d_N(Y_n)$, which is based on the judgment result of Equations (1)-(3) to the filter module. The filter module will compare the cumulative positive value with the threshold value, if the cumulative positive value is greater than the threshold value, then it will decide to receive or discard the data packets based on the data packets information in acquisition module.

We have conducted a series of experiments and obtained evidence for DDoS attacks defence model based on nonparametric CUSUM algorithm to improve flow connection density. According to the analysis of theoretical and experimental value and comparison between them, the error rate of the experimental values is only 3.618%. It is found out that the wrong results are mainly caused by the external factors such as identification delays and network noise. Of course, these external factors can be resolved by a series of measures. As for identification delay, we can take proper means of improving the sensitivity of the system to reduce recognition delays, thereby reducing the risk of errors. To sum up the experimental results, we can see that DDoS attacks defence model, based on nonparametric CUSUM algorithm to improve flow connection density, can effectively detect DDoS attacks and properly filter out malicious attacking data packets, securing the normal operation of the host or network.

## 4 Conclusions

This paper gives an intensive study of the operation mode and principle of DDoS attacks, discusses the simple defence strategies against DDoS attacks. It proposes algorithm to detect DDoS attacks based on flow connection density according to characteristics of network data transmission and DDoS attacking principle. Finally, it gives DDoS attacks defence strategy based on the time series analysis of flow connection density. Based on nonparametric CUSUM algorithm, modules are decided to prevent DDoS, which can lead to good defence strategies, defending against DDoS attacks to a great extent.

## References

[1] Xu C 2012 Research and implementation of DDoS detecting algorithm in application layer *Master thesis Chongqing university:* Chongqing China *(in Chinese)*

[2] Yang Y 2014 Worries of DDoS attacks *Journal of China education network* **2014**(01) 21-2 *(in Chinese)*

[3] *Deleted by CMNT Editor*

[4] Yan C 2009 R*esearch and implementation of DDoS attacking detection and defence strategies based on flow connection density* Master thesis Suzhou University Suzhou China *(in Chinese)*

[5] *Deleted by CMNT Editor*
[6] Takada H, Hofmann U 2004 Application and Analyses of Cumulative Sum to Detect Highly Distributed Denial of Service Attacks using Different Attack Traffic Patterns.Inter-domain *QoS Newsletter* **2004**(7) 414-8
[7] *Deleted by CMNT Editor*
[8] Cai X 2006 Based on the network data acquisition and sequence analysis of the environment of the DDoS attack *Master thesis*, Nanjing university of posts and telecommunications Nanjin China *(in Chinese)*

## Authors

**Changhong Yan, born in May, 1980, Yancheng, Jiangsu Province, P.R. China**

**Current position, grades:** lecturer.
**University studies:** MSc in Computer Science and Technology at Suzhou University.
**Scientific interests:** intermediate lecturer, intelligent control, network security, information processing, remote sensing remote sensing.
**Publications:** more than 19 papers.
**Experience:** teaching experience of 12 years, 3 scientific research projects.

**Qin Dong, born in October, 1974, Yancheng, Jiangsu Province, P.R. China**

**Current position, grades:** associate professor.
**University studies:** MSc in Computer Science and Technology at Nanjing University of Science and Technology.
**Scientific interests:** intermediate lecturer, intelligent control, network security, information processing.
**Publications:** more than 20 papers.
**Experience:** teaching experience of 18 years, 10 scientific research projects.

**Hong Wang, born in October, 1979, Yancheng, Jiangsu Province, P.R. China**

**Current position, grades:** lecturer at the School of Yancheng, China.
**University studies:** BSc in Mathematics at Yunnan University in China. MSc at Qinghai Normal University in China.
**Scientific interests:** education management, mathematics education, network security, information processing.
**Publications:** 10 papers.
**Experience:** Teaching experience of 14 years, 2 scientific research projects.