# DDoS Attack Detection Algorithm Based on IP Entropy Model

Wang xintong[1], Liu guqing[3], Yang jungang[2], Ran jinzhi[3]

[1]Administration Office for Graduate Students, Xi’an Communications Institute, Xi’an 710106, China;

[2]Department of Information service, Xi’an Communications Institute, Xi’an 710106, China;

[3]Department of Information Transmission, Xi’an Communications Institute, Xi’an 710106, China;

Email: wxt0645@qq.com

**Keyword:** DDoS detection; destination IP entropy; unexpected traffic; membership function

**Abstract.** Put forward a DDoS (Distributed Deny of Service) attack detection algorithm based on IP entropy model. Through the establishment of destination IP Entropy model, setting flow and entropy threshold with membership function, checking conditions of DDoS attacks step by step. The experimental results show that the algorithm can accurately detect DDoS attacks, and it can accurately distinguish DDoS flow and unexpected traffic, which has improved the detection rate and detection efficiency.

## Introduction

DDoS/DoS attack is to point to attackers malicious disturb the network by sending a large number of data packets request to exhaust host or network resources. It will lead to a host or network paralysis, and refuse normal user's request. Some serious DoS/DDoS attack can cause huge economic losses, and even affect the safety of state secret information.

There have been many research for the detection of DDoS attacks[1][2][3], which are generally in view of the network traffic statistical analysis[4][5][6][7]. Those methods are through analyzing the characteristics of network traffic, and find out the DDoS attack traffic characteristics, so as to achieve the aim of detecting attacks. These methods have a certain detection effect, but do not perform well in the distinction of DDoS attacks and unexpected traffic, and some detecting way are not rigorous, which leads to false positives and omission.

In order to distinguish DDoS attacks and network attack flow, this paper puts forward the DDoS attack detection algorithm based on IP entropy model. Establishing destination IP entropy detection model, structuring the membership function to judge the flow, with the change of entropy to distinguish the DDoS attack flow and unexpected traffic, achieve the purpose of accurately detecting DDoS attacks.

## Design of the DDoS detection algorithm

### A. Entropy

If there are multiple events in a system $S$={1,2,…,$m$}, the probability distribution of each event $P$={$p_1$,$p_2$,…,$p_n$}, the entropy of event $i$ is defined as $E_i$=-$p$∑ln $p_i$.

Definition 1: $IP\_all=\{ip_1,ip_2,\cdots ip_i,\cdots,ip_n\}$, *IP_all* show destination IP address set per unit time.

Definition 2: $P=\{p_1,p_2,\cdots,p_i,\cdots,p_n\}$, $p_i$ show the probability of the IP address $i$.

Definition 3: $E=-p_i\sum_{i=1}^{n}\ln p_i$, $E$ show the entropy of the destination IP address per unit time.

DDoS attacks and unexpected traffic will lead to abnormal increase of network traffic. Assuming that $E_N$, $E_D$, $E_U$ respectively according to the change of the IP entropy of normal flow, DDoS attacks flow and unexpected traffic. Under normal circumstances, due to different visitors won't be too big and different users to access different services, network traffic is normal and the destination IP address is dispersion at this time, $E_N$ keep in the general level; When DDoS attacks occurred in the network, network traffic increases, and IP address is intensive, $E_D$<$E_N$; When there is a unexpected traffic, the network traffic increases, but because is a normal access of a large number of normal users, so IP address is decentralized, $E_N \approx E_U$.

## B. Threshold Settings

Assuming that network instantaneous flow is $L(t)$ at time $t$, average flow rate is $L\_avg(t)$, destination IP entropy is $E(t)$, average entropy is $E\_avg(t)$. In order to determine the flow of "big and small" boundaries, using entropy maximization method[8] in fuzzy mathematics constructing membership function to measure the magnitude of the network traffic, define $u(t)$:

$$u(t)=\begin{cases}0 & , \ \mathrm{L}(t)\le m\times L\_avg(t)\\ \dfrac{(L(t)-m\times L\_avg(t))^2}{(n\times L\_avg(t)-m\times L\_avg(t))^2}, & m\times L\_avg(t)\le \mathrm{L}(t)\le n\times L\_avg(t)\\ 1 & , \ \mathrm{L}(t)\ge n\times L\_avg(t)\end{cases} \tag{1}$$

$u(t)$ defined the membership function of network flow, when of instantaneous flow rate is $m$ times less than average flow, the degree of $L(t)$ belong to "big" is 0; In the same way, when $m\times L\_avg(t)\le L(t)\le n\times L\_avg(t)$, network traffic belongs to the "big", the degree of $L(t)$ belong to "big" is $(L(t)-m\times L_avg(t))^2/(n\times L_avg(t)-m\times L_avg(t))^2$when of instantaneous flow rate is $n$ times more than average flow, the degree of $L(t)$ belong to "big" is 1.

In the same way, define $s(t)$:

$$s(t)=\begin{cases}1 & , \ \mathrm{E}(t)\le x\times E\_avg(t)\\ \dfrac{(E(t)-x\times E\_avg(t))^2}{(y\times E\_avg(t)-x\times E\_avg(t))^2}, & x\times E\_avg(t)\le \mathrm{E}(t)\le y\times E\_avg(t)\\ 0 & , \ \mathrm{E}(t)\ge y\times E\_avg(t)\end{cases} \tag{2}$$

$s(t)$ defined the membership function of entropy, when $\mathrm{E(t)}\ge y\times E\_avg(t)$, the degree of $E(t)$ belong to "small" is 0; when $x\times E\_avg(t)\le E(t)\le y\times E\_avg(t)$, the degree of $E(t)$ belong to "small" is $(E(t)-x\times E\_avg(t))^2/(y\times E\_avg(t)-x\times E\_avg(t))^2$; when $E(t) \le x\times E\_avg(t)$, the degree of $E(t)$ belong to "small" is 1.

## C. The key parameter selection

Through Formula (1) see that the parameter $m$ determines when the procedure judge traffic belongs to the "big", $m$ determines the accuracy and sensitivity of the algorithm. When $m$ is too big, can lead to omission, too small will lead to false positives.

In this paper select the parameter m through the experimental simulation of the normal network flow. In order to ensure that simulation closer to the real network condition, the selection of parameter $m$ more accurate, use DARPA 1999 Monday data set[9] as the experimental data for the selection of parameter $m$. The real-time change of instantaneous flow and average flow is shown in Figure 1. At the beginning, average network traffic is not stable, but as time goes on, the average flow tends to be stable gradually. Calculate the ratio of instantaneous flow and average flow of every second, represented as Formula (3). The distribution graph is shown in Figure 2.

$$f(t)=\frac{L(t)}{L\_avg} \tag{3}$$

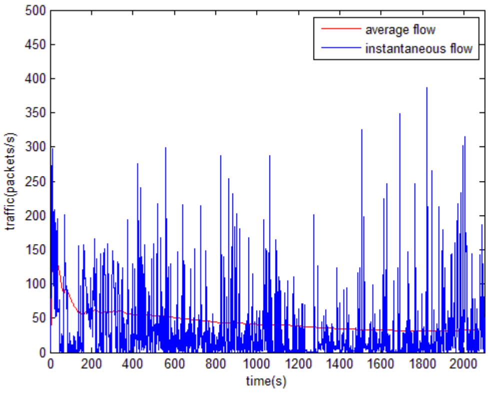


Fig.1. The changes of simulation traffic

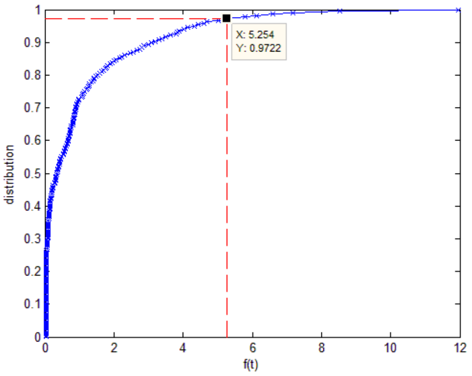


Fig.2. The distribution map of $f(t)$

It can be seen from the Figure 2 that 97.22% of instantaneous flow value is 5.254 times less than of the average flow. So the parameter m value is set to 5.254 which represent when the instantaneous flow rate is 5.254 times less than of the average flow, it may be the beginning of the attack. Use the same method to get parameter *y*.

### D. Algorithm implementation

When $u(t)$=0, the degrees of network flow belong to "big" is 0, consider there is no attack; when $u(t)$>0, network flow belong to “big”, consider it is the suspect points of attack, start the attack process. DDoS attack detection process is shown in Figure 3.

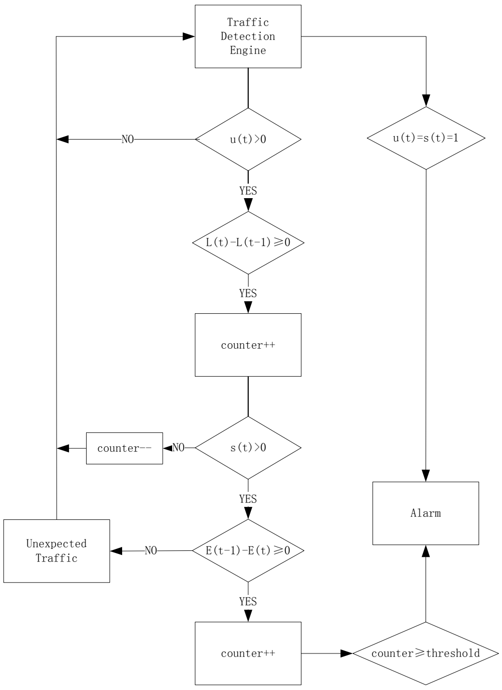


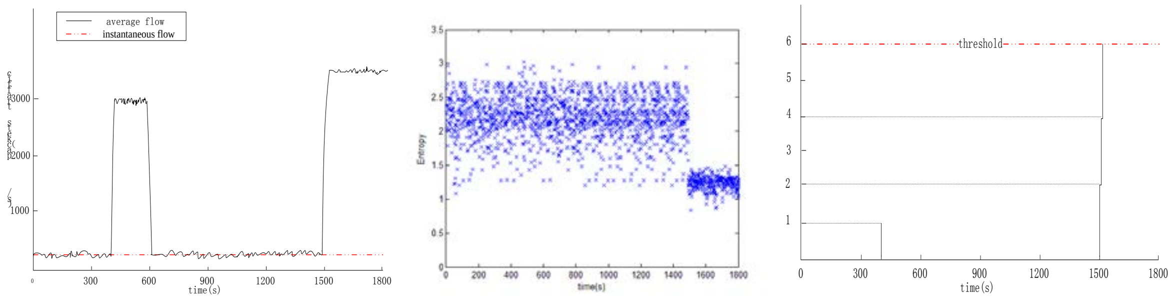
Fig.3. DDoS detecting process

## Experimental analysis

Using the network analyzer simulate network background traffic, the changes of network flow is shown in Figure 4(a), the changes of IP entropy is shown in Figure 4(b) and the test result is shown in Figure 4(c). Network flow configuration and parameter selection is shown in Table 1.

Table1 Network flow and parameter configuration

| parameter<br>traffic | start time(s) | duration (s) | intensity (packets/s) | m | n | x | y | threshold |
|---|---|---|---|---|---|---|---|---|
| background traffic | -- | -- | 200 | 5.254 | 10 | 0.3 | 0.6345 | 6 |
| unexpected traffic | 400 | 200 | 3000 | | | | | |
| SYN-Flood | 1500 | 300 | 3300 | | | | | |



(a) Curves of network traffic (b) The changes of IP entropy (c) Curves of parameter *counter*

Fig.4. The experimental results

Through curves of network traffic in Figure 4(a) and curves of parameter *counter* in Figure 4(c), we got when *t*=400, network traffic increases suddenly, *L*(*t*)≥*L*(*t*-1), the traffic continued to increase or stable in a larger value, consider it is the suspect points of attack, *counter*+1. And then calculate the IP entropy membership function *s*(*t*), because the increased of traffic is due to the increase of normal users, *s*(*t*)=0. Consider it is the normal traffic, *counter*-1 and continue to monitor the flow; when t=1500, the network is attacked by SYN-Flood, network traffic increases suddenly and *L*(*t*)≥*L*(*t*-1), *counter*+1.Then calculate the IP entropy membership function *s*(*t*), we got *s*(*t*)>0 and *E*(*t*)≤*E*(*t*-1), the IP entropy continues to reduce or maintain at the smaller level, attack possibility increase again, *counter*+1. When *counter*≥*threshold*, alarm.

Through Figure 4(b) we got that when *t*=400, network traffic increases, but the unexpected traffic's IP address is as scattered as normal traffic, they have some IP entropy graph; when *t*=1500, the network is attacked by SYN-Flood, IP address is concentrated, IP entropy decreased greatly. The DDoS detection algorithm based on IP entropy can accurately distinguish DDoS attacks and unexpected traffic.

## Conclusion

On the basis of the destination IP entropy a DDoS attack detection algorithm is proposed in this paper. Through the establishment of destination IP Entropy model, setting flow and entropy threshold with membership function to determine whether there is a DDoS attacks. Through the experiment proved that the DDoS attack detection algorithm based on destination IP entropy, not only can accurately detect DDoS attacks, and can clearly distinguish the DDoS attack and unexpected traffic.

## References

[1] Sunqin Dong, Zhangde Yun, Gao Peng. Detecting Distributed Denial of Service Attacks Based on Time Series Analysis[J]. CHINESE JOURNAL OF COMPUTERS, 2005,28(5):767-773.

[2] Liuxiao Hu, Zhangming Qing, Tang Jun, Konghong Shan. Design of Distributed DDoS Attack Source Traceback Model[J]. Journal of Information Engineering University, 2014,15(2):242-247.

[3] Huchun An, Huangjiang Hua. Detecting DDoS attacks based on improved D-S evidence theory[J]. COMPUTER ENGINEERING AND DESIGN, 2014,35(4):1198-1206.

[4] Yushuang Cheng. RESEARCH ON DDOS ATTACKS DETECTION TECHNOLOGY[D]. Beijing: Beijing University of Post and Telecommunications, 2013.

[5] Yanruo Yu. DDoS Attacks Detection Method Based on Traffic Matrix and Kalman Filter[J]. Computer Science, 2014,41(3):176-180.

[6] Zhuying Wu, Yangjia Hai, Zhangjin Xiang. Anomaly Detection Based on Traffic Information Structure[J]. Journal of Software, 2010,21(10):2573-2583.

[7] Xuxiao Dong, Fanyan Hua, Zhushi Rui. DDoS Attack Detection Based on Correlation of Macro Network Flow[J]. Computer Engineering, 2011,37(10),133-136.

[8] H. D. CHENG, JIM-RONG CHEN. Automatically Determine the Membership Function Based on the Maximum Entropy Principle. Information Science, 1997, 96:163~182.

[9] MIT Lincoln Lab, DARPA 1999 intrusion detection scenario specific dataset[EB/oL].