Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 50 (2015) 30 – 36

Procedia Computer Science

2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

DDoS Attack Detection using Fast Entropy Approach on Flow-Based Network Traffic

Jisa David[1], Ciza Thomas[2]

[1]*Department of Electronics and communication, Rajagiri School of Engineering & Technology, Kochi, 682039, India*
[2]*Department of Electronics and communication, College of Engineering, Trivandrum, 695016, India*

Abstract

Denial of service attack and Distributed Denial of Service attacks are becoming an increasingly frequent disturbance of the global Internet. In this paper we propose improvement in detection of Distributed Denial of Service attacks based on fast entropy method using flow-based analysis. An adaptive threshold algorithm is made use of since both network activities and user's behavior could vary over time. Fast Entropy and flow-based analysis show significant reduction in computational time compared to conventional entropy computation while maintaining good detection accuracy. The network traffic is analyzed and fast entropy of request per flow is calculated. DDoS attack is detected when the difference between entropy of flow count at each instant and mean value of entropy in that time interval is greater than the threshold value that is updated adaptively based on traffic pattern condition to improve the detection accuracy.

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

Keywords: DDoS; Flow-based analysis; Fast Entropy

1. Introduction

As the number of Internet users and network services continuously increase and the dependence on Internet for the critical online services grows, there is a high damage cost due to network attacks. Denial of Service (DoS) attacks has become a growing problem over the last few years resulting in huge loss for the victims regarding the quality of service. In Denial of Service attack, an attacker attempt to prevent legitimate users from accessing information or

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)
doi:10.1016/j.procs.2015.04.007

network resource such as a website, web service, or computer system. In the case of Distributed Denial of Service (DDoS) attack, attackers generate a huge amount of requests to victims through compromised computers (zombies), with the aim of denying the normal service or degrading the quality of services. One good example of DDoS attack which happened on February 2014 is a massive DDoS attack hit EU-US based servers, with security companies reporting it to be a powerful attack. The main reason behind these situations is that the network security community does not have useful traceback methods to trace attackers and detect the attacks efficiently and effectively immediately after the attack.

The one of reasons why the DDoS attacks are very threatening is the automated tool. Because of using the automated attack process, if once the attacker finds the systems with weak security, it does not take above 5 seconds to install the tool and attack the victim. And it takes thousands of hosts only one minute to be invaded. DDoS attack tools like Trin00, TFN, Tribe Flood Network 2000 (TFN2K) and Stacheldraht are being used to launch even stealthier attacks.

Most of DDoS attack detection method is using static threshold approach to detect the attacks [1], where the detection accuracy is less. Some of the work in DDoS attack detection takes more computation time which makes the detection system very complex. The proposed DDoS attack detection method improves detection accuracy by using adaptive threshold algorithm. To improve computational complexity, we use fast entropy approach on flow based data rather than conventional entropy approach.

The organization of this paper is as follows. Section 2 describes the background of DDoS attacks and the related work in the area of DDoS attack detection. The proposed detection method is described in section 3. Detailed analysis and performance evaluation is illustrated in Section 4. Section 5 summarizes the paper giving an outlook on future research in flow-based DDoS detection.

2. Related work

DDoS attack detection mainly considers three approaches: Signature Based Approach (SBA), Anomaly Based Approach (ABA) and Entropy Based Approach (EBA). In SBA system attributes are compared against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to the database. During that period, the new threats will go undetected. SBA is efficient because it is easy to implement. According to Ditcheva and Fowler [2] it is proved that signature based IDS identifies known attacks with low false negatives. But SBA has limitations that updating lag and it is not possible to detect zero day attacks.

Anomaly Based Approach (ABA)[3] has been proposed to overcome the limitations of SBA. It uses distribution analysis approaches, data mining, and statistical approaches. Anomaly based approach will monitor network traffic and compare it against an established baseline. The baseline will identify what is “normal” for that network, what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other and alert the administrator or user when traffic is detect as anomalous, or significantly different, than the baseline. The issue is that it may raise a False Positive alarm for a legitimate use of bandwidth if the baselines are not intelligently configured [4].

Entropy-based approaches have significant benefits in DDoS detection. When the monitored network runs in normal way, the entropy values are relatively smooth. Otherwise, the entropy value of one or more features would change significantly [5]. The use of entropy can increase the sensitivity of detection to uncover anomalous incidents. Even though using Entropy has several advantages, it still needs an efficient algorithm to reduce computational time and memory usage in a high speed network. In the work of No et. al [6] developed fast entropy approach to reduce computation time. Here fast entropy of packet count is calculated.

3. Proposed DDoS Attack Detection

The proposed DDoS attack detection method is based on three objectives. This section describes each objective in detail.

1. Flow aggregation for doing flow based attack detection.
2. Fast Entropy computation to detect DDoS attack with less computation time.
3. Adaptive Threshold Algorithm to improve detection accuracy.

3.1. Flow Aggregation

Flow is a unidirectional series of IP packets of a given protocol travelling between a source and a destination IP/port pair within a certain period of time [7]. Flow aggregation techniques are used to aggregate flows into a single flow with a larger granularity of classification giving a flow count for each connection is shown in Fig. 1. Aggregated flows have a larger number of packet information that dramatically reduces the amount of monitoring data. Hence, Internet traffic flow profiling has become a useful technique in the passive measurement and analysis field. Instead of considering the packet count of each connection, the proposed method takes the flow count of each connection at particular time interval for detecting the flooding attacks, increasing the speed of analysis.

Source IP	Destination IP	Source Port	Destination Port	Protocol	Flow Count

Fig. 1. Flow Aggregation

3.2. Fast Entropy Approach

In this detection approach, fast entropy of flow count is calculated for each connection as shown in Fig. 2. When there is an attack, entropy drops drastically, because there is one flow count that is dominating. In the non-attack case, the entropy will be in a constant range. Let a random variable $x_{(i,t)}$ represent the flow count of a particular connection i over a given time interval t. The fast entropy for a particular interval and particular connection is calculated as follows:

$$H"_{(i,t)} = -log\frac{x_{(i,t)}}{\sum_{i=1}^{n} x_{(i,t)}} + \tau_{(i,t)} \tag{1}$$

where

$$\tau_{(i,t)} = \begin{cases} \left|log\frac{x_{(i,t+1)}}{x_{(i,t)}}\right|, & x_{(i,t)} \geq x_{(i,t+1)} \\ \left|log\frac{x_{(i,t)}}{x_{(i,t+1)}}\right|, & x_{(i,t)} < x_{(i,t+1)} \end{cases} \tag{2}$$

t1					t2					t3					t4				
i1	i2	i3	i4	i5	i1	i2	i5	i4	i3	i2	i1	i3	i4	i5	i1	i3	i2	i4	i5
H1	H2	H3	H4	H5	H6	H7	H8	H9	....	....	....	...	...	....	....	....	....	....	Hn

t – Time Interval
i – Flow Connection
H – Fast Entropy

Fig. 2. Pictorial representation of fast entropy calculation

3.3. Adaptive Threshold Algorithm

In flooding attack detection, threshold value is very important. Threshold value needs to be updated according to the packet traffic condition. On one hand, if an attacker sends malicious traffic with small change in traffic when the channel is stable, the detector cannot detect the attack with high value of β, where β is the threshold multiplication factor. Because of the steady channel condition and stealthy attack pattern, the detection facility does not work properly with highly set β. On the other hand, if the channel is burst but the detector has small β, the detector works very sensitively in this situation. As a result, the detector yields many false positives, which are not severe but a bad characteristic of the detector. In the proposed method β value is updated based on entropy value. The detection algorithm is shown in fig: 3. The β will be changed under the following rules:

$$If\ H''_{(i,t)} > 1.5\mu_t\ \ then\ increase\ \beta \text{ by } 1$$

$$If\ .5\mu_t\ \leq H''_{(i,t)} < 1.5\mu_t\ \ then\ maintain\ current\ \beta$$

$$If\ H''_{(i,t)} < .5\mu_t\ \ then\ decrease\ \beta \text{ by } 1$$

$H''_{(i,t)}$ refers to the fast entropy, μ_t and σ_t is the mean and standard deviation of flow count during a particular time interval. $D_{(i,t)}$ is defined as the difference between the mean value μ_t and the fast entropy $H''_{(i,t)}$. While applying adaptive threshold algorithm, if $D_{(i,t)}$ is greater than the product of β and σ indicates flooding attack.

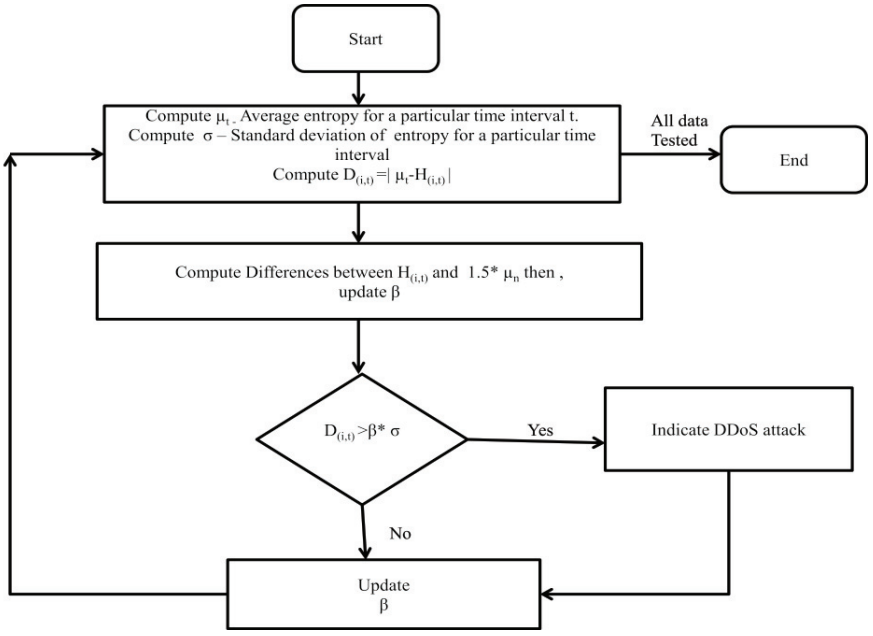

Fig. 3. Adaptive Detector algorithm flow

4. **Performance Evaluation**

Experiments are carried out on a subset of CAIDA dataset [8] used in DDoS detection evaluation program. In this section, we evaluate the effectiveness and efficiency of the proposed DDoS detection based on fast entropy mechanism with adaptive threshold algorithm. The proposed method is based on flow based analysis which requires only packet header information. In flow aggregation, the header information was aggregated in a particular time interval, which belongs to identical 5 tuple (Source IP address, Destination IP address, Source port, Destination

port, Protocol Number). By flow aggregation, processing overhead is reduced and speed of analysis is increased. The subset of flow count obtained during particular time interval is shown in Table 1 in descending order.

Table 1. Flow Aggregation

Connections	Source IP Address	Destination IP Address	Protocol	Flow Count
C_1	192.95.27.190	71.126.222.64	ICMP	2605
C_2	192.120.148.227	71.126.222.64	ICMP	1831
C_3	202.1.175.252	71.126.222.64	ICMP	1786
C_4	40.75.89.172	71.126.222.64	ICMP	1743
C_5	51.173.229.255	71.126.222.64	ICMP	1023
C_6	51.81.166.201	71.126.222.64	ICMP	295
C_7	195.198.120.238	71.126.222.64	ICMP	204

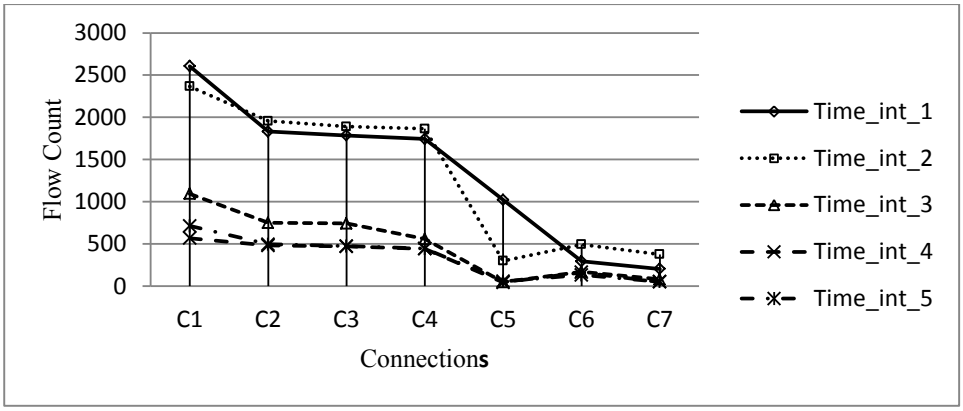

Fig. 4. Flow Information

Fig. 4 shows flow count information of each connection at different time intervals. Flow count is a distinguishing property which shows the severity of the flooding attack. During flooding attack the flow count will increase. As shown in Fig:4 the connections C_1 and C_2 its flow count is very large value. Here Instead of analysing the dataset based on the captured packet header information, the flow count of each connection in the dataset is being used for fast entropy calculation. This increases the speed of analysis.

The next objective is to show that the flow entropy drops drastically for attack case and it is stable for non attack cases. Table 2 shows the fast entropy value of each connection at particular time intervals. Here entropy value is drastically decreased for a connection with large flow count. Table 3 summarises the fast entropy value and flow count at different time intervals.

DDoS attack detection is characterised by the fact that if the difference between the fast entropy and mean is greater than the threshold value. This adaptive threshold algorithm improves the detection accuracy and the fast entropy calculation reduces the computation time compared to conventional entropy. Table 4 presents variation of entropy value with mean for different connections. Table 5 shows variation of $|H''_{(i,t)} - \mu_t|$ |with flow count of each connection at different time interval. It indicates the variation is significantly large for a large flow count of particular connection. For example the connection between 192.95.27.190 and 71.126.222.64, entropy variation is very large value (7.46) compared to other connections as shown in Table 4.

Table 2. Fast Entropy

Source IP	Destination IP	Protocol	Flow Count	Fast Entropy
192.95.27.190	71.126.222.64	ICMP	2605	1.386761887
192.120.148.227	71.126.222.64	ICMP	1831	1.726403333
202.1.175.252	71.126.222.64	ICMP	1786	1.74718696
40.75.89.172	71.126.222.64	ICMP	1743	1.776358775
51.173.229.255	71.126.222.64	ICMP	1023	2.814050051
51.81.166.201	71.126.222.64	ICMP	295	3.748148199
195.198.120.238	71.126.222.64	ICMP	204	4.158931561

Table 3. Fast Entropy and flow count at different time interval

Time Interval	Time_int_1		Time_int_2		Time_int_3		Time_int_4		Time_int_5	
Connection	Flow Count	Fast Entropy	Flow Count	Fast Entropy	Flow Count	Fast Entropy	Flow Count	Fast Entropy	Flow Count	Fast Entropy
C_1	2605	1.387	2367	1.776	1094	2.497	1891	2.967	713	2.743
C_2	1831	1.726	1956	2.047	751	2.782	946	3.049	497	3.160
C_3	1786	1.747	1890	2.071	743	2.799	238	3.062	475	3.209
C_4	1743	1.776	1865	2.203	559	2.984	238	3.115	445	3.294
C_5	1023	2.814	299	4.304	48	5.377	238	5.539	57	5.418
C_6	295	3.748	495	3.465	172	4.086	44	4.205	133	4.459
C_7	204	4.159	377	3.946	81	5.025	42	5.332	54	5.370

Table 4. Fast Entropy variation with mean

Source IP	Destination IP	Protocol	Flow Count	Difference of Entropy with Mean
192.95.27.190	71.126.222.64	ICMP	2605	7.461027848
192.120.148.227	71.126.222.64	ICMP	1831	7.121386403
202.1.175.252	71.126.222.64	ICMP	1786	7.100602776
40.75.89.172	71.126.222.64	ICMP	1743	7.07143096
51.173.229.255	71.126.222.64	ICMP	1023	6.033739685
51.81.166.201	71.126.222.64	ICMP	295	5.099641537
195.198.120.238	71.126.222.64	ICMP	204	4.688858175

Table 5. Fast Entropy variation with mean at different time interval

Time Interval	Time_int_1		Time_int_2		Time_int_3		Time_int_4		Time_int_5	
Connection	Flow Count	Difference of Entropy with mean	Flow Count	Difference of Entropy with mean	Flow Count	Difference of Entropy with mean	Flow Count	Difference of Entropy with mean	Flow Count	Difference of Entropy with mean
C_1	2605	7.461	2367	7.069	1094	4.846	1891	4.326	1756	4.697
C_2	1831	7.121	1956	6.798	751	4.561	946	4.244	878	4.280
C_3	1786	7.101	1890	6.774	743	4.545	238	4.231	248	4.231
C_4	1743	7.071	1865	6.643	559	4.359	238	4.178	248	4.146
C_5	1023	6.034	299	4.541	48	1.967	238	1.755	248	2.022
C_6	295	5.100	495	5.380	172	3.257	44	3.088	36	2.981
C_7	204	4.689	377	4.899	81	2.318	42	1.961	36	2.070

5. **Conclusion**

We propose an efficient DDoS attack detection method using Fast entropy approach. The flow count is calculated for each connection at particular time interval. From the observation it is clear that the fast entropy value is considerably reduced for particular connection and particular time interval of which flow count is large value compared to rest. DDoS attack is detected, when the difference between entropy of flow count at each instant and mean value of entropy in that time interval is greater than the threshold value. Since the threshold value is updated adaptively based on traffic pattern condition, the accuracy of detection is improved. After detecting DDoS attack, as a future work it is possible to find out attacker and agents of DDoS attack using IP traceback mechanism, as the detection system can performed efficiently based on flow aggregation method.

References

[1] Petar Cisar, “A Flow based algorithm for Statistical Anomaly Detection”, *In Proceedings of the 7th International Symposium of Hungarian Researches on Computational Intelligence*.

[2] T. Ditcheva and Lisa Fowler, “Signature-based Intrusion Detection” class notes for COMP290-040, University of North Carolina at Chapel Hill, Feb. 2005

[3] Stephen M. Specht, Ruby B. Lee “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures”, *In Proceedings of the International Conferences on Parallel and Distributed system*, pp. 543-550, September 2004.

[4] B. Song, J Heo, and C. S. Hong, “Collaborative Defense Mechanism Using Statistical Detection Method against DDoS attacks”, *IEICE TRANS. COMMUN E90-B*, 2007, pp. 2655-2644

[5] J. Wang, X. Yang, and K. Long, “A new relative entropy based app-DDoS detection method", *In Proceedings of the IEEE symposium on Computers and Communications* , pp. 966- 968, Riccione, Italy 2010.

[6] Giseop No, Ilkyeun Ra, “Adaptive DDoS Detector Design Usin g Fast Entropy Computation Method”, *Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing,* 2011, pp. 86 – 93

[7] Jisa David and Ciza Thomas, “Intrusion Detection using Flow based Analysis of Network Traffic”, *First International Conference on Computer Science and Information Technology*, pp.393-399 Jan 2011

[8] P. Hick, E. Aben, K. Claffy, and J. Polterock, “The caida "ddos attack 2007" dataset.