Proceedings of 2014 International Symposium on Embedded Technology (ISET 2014)
Seocho-gu Seoul, Korea, 22-23 May, 2014.

Explore "Decrease-All-By-One" on DDoS packet Filtering using Counting Bloom Filter

Suk-Young Oh* Shin-Hyung Lee* Chuck Yoo*

*College o f Information and Communication, Korea University, Seoul, Republic of Korea
E-mail: {syoh, shlee, chuckyoo }@os.korea.ac.kr

Abstract

This paper explores a method which can improve bot IP detection rate and reduce false positive rate in DDoS attack packet filtering using counting Bloom filter. False positive occurs due to inherent characteristic of Bloom filter. We examine a technique, "decrease-all-by-one", that can improve bot detection performance without false positive rate increase and we prove a optimized condition in which "decrease-all-by-one" operation should be performed through simulation experiments.

Keywords: DDoS, Counting Bloom Filter, Packet Filtering, False Positive.

1. Introduction

There have been many DDoS attack packet filtering method using a traditional counting Bloom filter(CBF)[1]. the most widely known problem that Bloom filter(BF) inherently has is a presence of false positive(FP). In the view of DDoS security, FP means a fault in which a packet sent from normal user is determined as bot packet.

Ji Hun Ha el al. [2] present a "decrease-all-by-one" technique which can reduce FP rate. It decreases all field of Bloom filter array by 1 at a specific condition in which the probability of FP occurrence become increased. they defined the pre-mentioned condition depend on the following mathematical formula.

$$(1-\frac{1}{m})^{kn} \leq \frac{1}{2}$$

In this formula, k is the number of hash functions, m is BF array size and n is the number of inserted packets. they explain that if the non-zero portion exceeds the 50%(1/2) of the total BF array, the probability of FP become increased over 50%. It, however, is difficult for this premise to be applied into CBF because the non-zero portion doesn't directly affect FP rate in CBF. In fact, a factor affecting FP rate in CBF is the ratio of fields counted up to a count threshold.

In this paper, we experiment on the specific point of time when "decrease-all-by-one" is performed in DDoS attack packet filtering using CBF. After experiments, we analyze a result data so that we estimate a optimized condition.

2. Simulation "Decrease-All-By-One".

We assume a fixed DDoS attack situation for the experiment on bot IP detection performance and FP. Each randomly generated 100,000 bot source IP and 2M normal source IP are added into CBF at 100pps rate and 2000pps rate individually. The size of BF array is 32768byte and the count threshold of each field of array is four. In addition, four hash functions are used. A IP address is hashed by 4 hash functions, each result value from hash functions passes an modulo 32768B operation so that the count values of field of index corresponding with the result value are increased by one. If count values of four corresponding fields exceed threshold(we use 4), the packet is determined as attacking packet.

we examine results following each condition performing "decrease-all-by-one" operation (non-zero portion of total array is 10%, 20%, 30%, ..., 90% ratio). This experiment is performed 10 times with randomly differently generated IP address set while 10000ms. Finally, the average value of ten results is used to analyze these experiments.

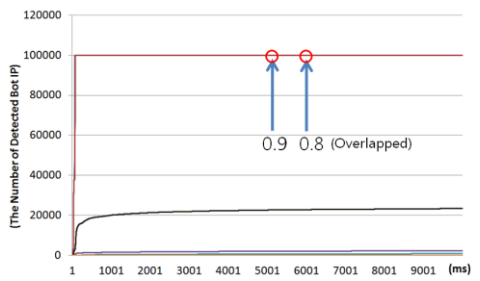

Figure 1. the performance of bot detection

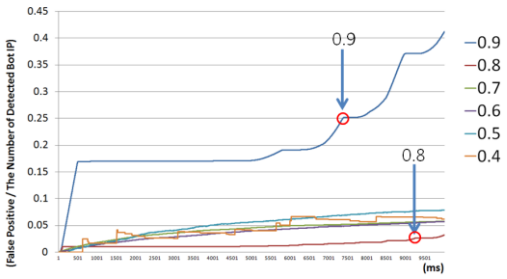

Figure 2. the ratio of false positive per 1 bot detection

In case of 10%, 20%, 30% "decrease-all-by-one", the CBF cannot catch any bot IP. This is because "decrease-all-by-one" is too frequently performed to detect bot IP in which most of the field in CBF cannot reach minimum threshold(we use 4). So, we only examine result from 40% to 90%.

In the Figure 1, in case of performing "decrease-all-by-one" when non-zero portions of total array are 90% and 80%(both are being shown overlapped in Fig. 1), the Bot detection performance is noticeably better than others.

The Figure 2. shows the ratio of FP per one bot IP detection in each "decrease-all-by-one" experiment. we focus on a difference between 90% and 80%. In the Fig. 1, Both 80% and 90% have shown almost same performance. In case of condition that non-zero portion of total array is 80%, FP rate is dramatically more reduced than any other experiments. We conclude that in this pre-assumed situation(array size is 32768B, and the number of bot IP and normal IP, etc.), rather than a fixed "decrease-all-by-one" operation as 50%(1/2), performing "decrease-all-by-one" under the condition that non-zero portions of total array is 80% is more optimistic. Therefore we can choose 0.8(80%) enable to obtain higher performance and low FP.

3. Conclusions

we think that a"decrease-all-by-one" operation is critical method to accomplish high bot IP detect performance and low FP rate. However, if a "decrease-all-by-one" operation occur much frequently, CBF cannot have a enough bot information so that cannot distinguish bot IP among surged traffics. On the other hand, if a "decrease-all-by-one" operation occur too slowly, normal packets cannot pass through CBF(false positive). we prove that there exists a appropriate condition to improve a "decrease-all-by-one" operation. In the future work, we will find a normalized mathematical formula with variety variable in real network system for DDoS attack filtering using the CBF.

Acknowledgement
This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No.2010-0029180) with KREONET.

References

[1] L. Fan, , P. Cao, J. Almeida, and A. Z. Broder. “Summary cache: a scalable wide-area web cache sharing protocol”. IEEE Trans on Networking, 8(3), 281–293, 2000.
[2] Ji Hun Ha, Hyo Gon Kim, "Identifying and Blocking Botnet-based DDoS Attacks Using Counting Bloom Filter". The Korean Institute of Communications and Information Sciences, 2012.