LOW BANDWIDTH DDOS ATTACK DETECTION IN THE NETWORK

[1]*L. SHIVAKUMAR,* [2]*G. ANIL KUMAR*
[1]M.Tech CSC Dept, RVRIET, Hyderabad, India,
Email: lsk.10@rediffmail.com
[2]PhD, Professor and H.O.D CSE Dept, RVRIET, Hyderabad, India

ABSTRACT- *A DDoS (i.e., Distributed Denial of Service) attack is a large scale distributed attempt by malicious attackers to fill the users' network with a massive number of packets. This exhausts resources like bandwidth, computing power, etc.; User can't provide services to its clients and network performance get destroyed. The methods like hop count filtering; rate limiting and statistical filtering are used for recovery. In this paper, we explored two new information metrics which have generalized information about entropy metric and distance metric. They can detect low-rate of Distributed Denial of Service i.e., DDoS attacks by measuring difference between the legitimate traffic and the attack traffic. The generalized entropy metric information can detect the attacks on several hops before than the traditional Shannon metric. The proposed information about the distance metric outperforms the popular Kullback–Leibler divergence approach as it has the ability to perfectly enlarge the adjudication distance and gets the optimal detection sensitivity. Further the IP trace back algorithm can find all attackers as well as their attacks through local area networks (LANs) and will delete the attack traffic.*

Index Terms—Attack detection, information metrics, IP trace back, low-rate distributed denial of service (DDoS) attack.

1. INTRUDUCTION

Present in networking we have to provide security to information while accessing and transmitting. Lots of hacking tools are available for getting the information that was transmitted in the network. A standard security mechanism is in need to overcome this thing. The information in the network have to be out of range to intruders. It impacts bandwidth, processing capacity, or memory of a network. It has huge occupying nature on wired and wireless networks. DDoS attack is an intelligent attack and considered as low rate attack. The attacker is capable of sending multiple numbers of attack packets to the user which is out bound to elude detection. Mostly combination of large-scale DDoS attacks and multiple Low-rate attacks are making user uncomfortable in the networking process. So it is becoming difficult to detect and getting solutions to such attacks.

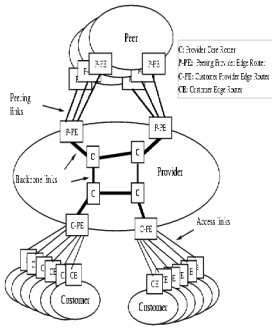

Fig: Networking from provider to customers

Nowadays, several Distributed Denial of Service attacking detection methods of metrics are in use, they are mainly separated into the following categories:

i) the signature-based metric, and
ii) anomaly-based metric.

The signature-based method of metric depends on a technology that deploys a predefined set of attack-signatures like patterns or strings as signatures to match the incoming packets. This anomaly-based detection method of metric typically models the normal network (traffic) behavior and deploys it to compare the differences to incoming network behavior.

Anomaly-based method of detection has many limitations:
i) Attackers can train detection systems to gradually accept anomaly network behavior as normal.
ii) The rate at which the false positives use the anomaly-based detection metric is generally higher than those using the signature-based detection metric. It is difficult to set a threshold that helps us to balance the rate of false positives and the false negatives.

iii) Precisely the extraction of the features like normal and anomalous network behaviors is very difficult. An anomaly-
based detection method of metric uses a predefined as well as specific threshold for example, an abnormal deviation of parameters related to some statistical characteristics that are considered from normal network traffic, to identify abnormal traffic amongst all normal traffic. Hence, it is important to utilize and to be decisive while choosing the statistical methods and tools respectively. It is an acceptable fact that the fractional Gaussian noise function and the Poisson distribution function can be used to simulate the can be used to simulate real network traffic in aggregation and the DDoS attack traffic in aggregation respectively. Many information theory based metrics have been proposed to overcome the above limitations. In information theory, information entropy is a measure of the uncertainty associated with a random variable. Information distance (or divergence) is a measure of the difference between different probability distributions. Shannon's entropy and Kullback–Leibler's divergence methods have both been regarded as effective methods based on IP address-distribution statistics for detecting the abnormal traffic. Time taken for detection as well as detection accuracy of DDoS attacks are the two most important criteria for rating a defense system. Through this paper, we make you aware of two new and effective anomaly-based detection method of metrics that not only identify attacks quickly, but also they reduce the rate of false positives as compared to the traditional Shannon's entropy method and the Kullback–Leibler divergence method.

Contributions
Some of the main contributions made in this paper are as follows:
1) It highlights the advantages and also it analyses the generalized entropy and information distance compared with Shannon entropy and Kullback–Leibler distance, respectively.
2) It proposes a better technique to the generalized entropy and information distance metrics to perform better than the traditional Shannon entropy and Kullback–Leibler distance method of metrics at low-rate DDoS attack detection in terms of quick detection, low rate of false positives and stabilities.
3) It proposes an effective IP trace back scheme that is based on an information distance method of metric that can trace all the attacks made by local area networks (LANs) and drive them back in a short time.

2. ALGORITHMS FOR DETECTION AND IP TRACEBACK ANALYSIS

In this section, we propose and analyze two effective detection algorithms and an IP traceback scheme. In this paper, we make the following reasonable assumptions:
1) We will have full control of all the routers;
2) We will have extracted an effective feature of network traffic to sample its probability distribution;
3) We will have obtained and stored the average traffic of the normal, as well as the local thresholds and routers on their own in advance;
4) On all routers, the attack traffic obeys Poisson distribution and the normal traffic obeys Gaussian noise distribution.
To illustrate this algorithm, we use the work topology of Fig. 1 as an example. Our algorithm can not only detect DDoS attacks at router via single-point detection, but can also detect the attacks that are made using a collaborative detection at routers. Fig. 2 shows the processing flowchart of the collaborative detection algorithm. Compared with single-point detection, we can detect attacks even before by using a collaborative detection approaches if the traffic can be analyzed before them. The divergence and distance are increasing

simultaneously. By increasing the divergence between legitimate traffic and attack traffic we can distinguish DDoS attacks easily and earlier. Therefore, in DDoS attack detection; we can take full advantage of the additive and increasing properties in of the information divergence and the information distance to enlarge the distance or gap between legitimate traffic and attack traffic. This means we can find and raise alarms for DDoS attacks quickly and accurately with a lower rate of false positives in upper stream routers instead of the victim's router. In information theory, we know that both information divergence and information distance are nonnegative values and the sum of the divergences or distances is always greater.

C. IP Trace back Analysis

IP trace back is the ability to find the source of an IP packet without relying on the source IP field in the packet, which is often spoofed. We combine our DDoS attacks detection metric with IP trace back algorithm and filtering technology together to form an effective collaborative defense mechanism against
network security threats in Internet. In hop-by-hop IP tracing, the more hops the more tracing processes, thus the longer time will be taken.
Listing 1. A collaborative DDoS attack detection

Alogirthm

1. Set the sampling frequency as f , the sampling as T, and the collaborative detection threshold as 0.
2. In routers R1 and R2 of Fig. 1, sampling the network traflic comes from the upstream routers R3, R4 , R5, R6 and LAN1, LAN; in parallel.
3. Calculate in parallel the munbers of packet which have various recognizable characteristics (e.g., the source IP address or the packet's size, etc.) in each sampling time interval 'r('r = 1/ f) within T.
4. Calculate the probability distributions of the network traflic come from R3, R4, LAN 1 and R5, R6, LAN2 in parallel.
5. Calculate their distances on router R1 and R2, respectively, using the formula.

Da(Ps Q) = Da(PllQ) + D¢-(Q||P)-

6. Sum the distances.
7. If the summed distance is more than the collaborative detection threshold 0, then the system detects the DDoS attack, and begins to raise an alarm and discards the attack packets; otherwise the routers forward the packets to the downstream routers.
8. Return to step 2.
In order to convenience for IP trace back algorithm analysis, we classify two types of traffic in Figs. 1 and 3 as local traffic and forward traffic, respectively. The local traffic of is the traffic generated from its LAN, the forward traffic of is the sum of its local traffic and the traffic forwarded from its immediate upstream routers. In this paper, we propose an IP trace back algorithm that can trace the source (zombies) of the attack up to its local administrative network; Listing 2 illustrates this algorithm.

Listing 2. An IP traceback algorithm in DDoS attacks detection

The proposed IP trace back algorithm based on a sample scenario of low-rate DDoS attacks on a victim. When the proposed attacks detection system detects an attack on a victim, the proposed IP traceback algorithm will be launched immediately. On router , the proposed traceback algorithm calculates information distances based on variations of its local traffic and the forward traffic from its immediate upstream routers; in this paper, we set LAN of router include the victim. If the information distance based on its local traffic is more than the specific detection threshold, the proposed detection system detects an attack in its LAN

```
IP_Traceback_Algorithm ()
{
while(true)
call Check_ForwardTraffic(0)//check attacks on
router R0 (or victim)
}
Check_ForwardTraflic (i)
{
calculate infommtion distance D I-( R,-)
i1°D:(Ri> > arm)
```

call Check_LocalTrafic
for j = 1 to n
k = the ID of the jth immediate upstream router of router Ri
call Check_ForwardTraflic (Ic)
end for
end if I
}
Check_LocalTraflic (xi)
{
calculate infomlation distance D1,-
if Du > 01¢
stop forwarding the attack trafic to downstream routers (or destination), label the zombie
end if
}

This means that the detected attack is an internal attack. If the information distances based on the forward traffic from its immediate upstream routers and are both more than the specific detection threshold and, respectively, the proposed detection system has detected attacks in routers and , then on and the proposed trace back algorithm calculates information distances based on variations of their local traffic and the forward traffic from their immediate upstream routers, and Will find that there are no attacks in LAN and LAN and ; therefore, on routers , and the proposed algorithm calculates continually information distances based on variations of their local traffic and the forward traffic from their immediate upstream routers, then can find there is an attack (zombie) in LAN so the router will stop forwarding the traffic from the zombie immediately.

3. RELATED WORK

The metrics of an anomaly-based detection have been the focusing on the intense study years together in an attempt to detect the intrusions and attacks done on the Internet. Recently, this information theory is being used as one of the statistical metrics that are being increasingly used for anomaly detection. Feinstein et al present methods to identify DDoS attacks by computing entropy and frequency-sorted of selected packet attributes. These Distributed Denial of Service attacks show their characteristics of the selected packet attributes to its anomalies, and its detection accuracy and performance can be analyzed with the help of live traffic traces among a variety of network environments. However, because of the proposed detector and responder there will be a coordination lack with each other, then the impact of its responses on legitimate traffic and expenses for computational analysis may increase. Yu and Zhou applied a special technique for information theory parameter to discriminate the Distributed Denial of Service attack against the surge legitimate accessing. That technique is based on the shared regularities along with different Distributed Denial of Service attack traffic, which differentiates it from real surging accessing over a short period of time. However, the proposed detection algorithm will be helpful to us in predicting a single directions or a limited number of directions but the real problem comes when these attackers adopt a multiple attack package generation function in one attack to fool us. Lee and Xiang used various information-theoretic measures like entropy, conditional entropy, relative conditional entropy, information gain, and information cost for anomaly detection, etc. yes it is true that for some extent measures like mentioned above can be used to evaluate the quality of anomaly detection methods and to build the appropriate anomaly detection models but we find a tough time to build an adaptive model that can dynamically adjust itself to different sequence lengths or time windows that are based on run-time information. A low-rate Distributed Denial of Service attack is substantially different from a high-rate Distributed Denial of Service attack which is considered to be the traditional type of Distributed Denial of Service attack. A few number of researchers have proposed several detection schemes against Distributed Denial of Service type of attack. Sun et al. proposed a distributed detection mechanism that is used as a dynamic time warping method for identifying the presence of the low-rate attacks, then a fair resource for the allocation mechanism will be used to minimize the affected flows in number. However, this method can lose the legitimate traffic to some extent Shevtekar et al. gave a light-weight data structure to store the necessary

flow history at edge routers to detect the low-rate TCP DoS attacks. Although this method can detect any periodic pattern in the flows, it may not be scalable and can be deceived by the IP address spoofing. Chen et al. Present a collaborative detection of DDoS attacks. While focusing on detection rate, it is difficult for this scheme to differentiate the normal flash crowds and real attacks. As it heavily relies on the normal operation of participating routers, the false positives will increase if the routers are compromised. Zhang et al. propose to use self-similarity to detect low-rate DDoS attacks. While the approach is claimed to be effective, the paper does not use real scenario data to evaluate it.Kullback–Leibler divergence, as a well-known information divergence, has been used by researchers to detect abnormal traffic such as DDoS attacks.

The difference between previous work and our research is that we are the first to propose using information divergence for DDoS attack detection. Information divergence, as the generalized divergence, can deduce many concrete divergence forms according to different values of order. For example, when, it can decipher the Kullback–Leibler divergence. It is very important and significant that we can obtain the optimal value of divergence between the attack traffic and the legitimate traffic in a DDoS detection system by adjusting the value of order of information n divergence. In addition to this, we also study the properties of Kullback–Leibler divergence and information divergence in theory and overcome their asymmetric property when used in real measurement. We successfully convert the information divergence into an effective metric in DDoS attack (including both low-rate and high-rate) detection.

4. CONCLUSION

In this paper we described different techniques which are for the prevention of the denial of service attacks. A new methodology along with the existing packet marking technique was proposed. The information contains the lifetime of the packet. The traceback process an accurate one. As the proposed metrics can increase the information distance among attack traffic and legitimate traffic. Those lead to detect low-rate DDoS attacks fast and reduce the false positive rate accurately. This information distance metric overcomes the properties of asymmetric of both Kullback-Leibler and information divergences. IP traceback scheme based on information metrics can effectively trace all attacks including LANs (zombies). Our proposed information metrics improve the performance of low-rate DDoS attacks detection and IP traceback over the traditional approaches.

5. REFERENCES

[1] A. Chonka et al., “Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks,” J. Netw. Comput. Applicat. Jun. 23, 2010 [Online]. Available: http://dx.doi.org/10.1016/j. jnca.2010.06.004

[2] X. Jin et al., “ZSBT: A novel algorithm for tracing DoS attackers in MANETs,” EURASIP J. Wireless Commun. Netw., vol. 2006, no. 2, pp. 1–9, 2006.

[3] A. Shevtekar, K. Anantharam, and N. Ansari, “Low rate TCP Denial- of-Service attack detection at edge routers,” IEEE Commun. Lett., vol. 9, no. 4, pp. 363–365, Apr. 2005.

[4] G. Carl et al., “Denial-of-service attack-detection techniques,” IEEE Internet Comput., vol. 10, no. 1, pp. 82–89, Jan./Feb. 2006.

[5] P. Du and S. Abe, “IP packet size entropy-based scheme for detection of DoS/DDoS attacks,” IEICE Trans. Inf. Syst., vol. E91-D, no. 5, pp. 1274–1281, 2008.

[6] S. Ledesma and D. Liu, “Synthesis of fractional Gaussian noise using linear approximation for generating self-similar network traffic,” Comput. Commun. Rev., vol. 30, no. 2, pp. 4–17, 2000.

[7] E. Perrin et al., “ th-order fractional Brownian motion and fractional Gaussian noises,” IEEE Trans. Signal Process., vol. 49, no. 5, pp. 1049–1059, May 2001.

[8] E. Perrin et al., "Fast and exact synthesis for 1-D fractional Brownian motion and fractional Gaussian noises," IEEE Signal Process. Lett.vol. 9, no. 11, pp. 382–384, Nov. 2002.

[9] Y. Bao and H. Krim, "Renyi entropy based divergence measures for ICA," in Proc. IEEE Workshop on Statistical Signal Processing, 2003,pp. 565–568.

[10] Y. Gu, A. McCallum, and D. Towsley, "Detecting anomalies in network traffic using maximum entropy estimation," in Proc. ACM SIGCOMM Conf. Internet Measurement (IMC 2005), 2005, pp. 32–32.

[11] R. Sekar et al., "Specification based anomaly detection: A new approach for detecting network intrusions," in Proc. ACM Conf. Computer and Communications Security (CCS 2002), 2002, pp. 265–274.

[12] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends, Comput.Netw" vol. 51, no. 12, pp. 3448–3470, 2007.
[13] C. E. Shannon, "A mathematical theory of communication," Bell Syst. Tech. J., vol. 27, pp. 379–423 and 623–656, 1948.

[14] K. Zyczkowski, "Rényi extrapolation of Shannon entropy," Open Syst.Inf. Dynamics, vol. 10, no. 3, pp. 297–310, 2003.

L. SHIVA KUMAR is an M.Tech student in PVR Institute of Engineering and Technology, Hyderabad. He received B.Tech Degree in Computer Science and Engineering from JNTU, Hyderabad. His research interested areas are Computer Networks and Network Security.

G. ANIL KUMAR received M.Tech (COMPUTER SCIENCE AND TECHNOLOGY) from Andhra University. B.Tech (Computer Science And ENGINEERING) From JNTU. Pursuing PhD from Andhra University. Presently working as Professor, Head Department of Computer science and Engineering. He is a member in International Association of Computer science and Information Technology, International Association of Engineers. His research areas include Data mining applications in image processing, Medical image processing.