Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2016, Article ID 2579274, 5 pages
http://dx.doi.org/10.1155/2016/2579274

Research Article

An Algorithm of Traffic Perception of DDoS Attacks against SOA Based on Time United Conditional Entropy

Yuntao Zhao,[1,2] Hengchi Liu,[1] and Yongxin Feng[1]

[1]*School of Information Science and Engineering, Shenyang Ligong University, Shenyang 110159, China*
[2]*College of Information Science and Engineering, Northeaster University, Shenyang 110819, China*

Correspondence should be addressed to Yongxin Feng; fengyongxin@263.net

Received 12 April 2016; Revised 24 September 2016; Accepted 29 September 2016

Academic Editor: Jun Bi

DDoS attacks can prevent legitimate users from accessing the service by consuming resource of the target nodes, whose availability of network and service is exposed to a significant threat. Therefore, DDoS traffic perception is the premise and foundation of the whole system security. In this paper the method of DDoS traffic perception for SOA network based on time united conditional entropy was proposed. According to many-to-one relationship mapping between the source IP address and destination IP addresses of DDoS attacks, traffic characteristics of services are analyzed based on conditional entropy. The algorithm is provided with perception ability of DDoS attacks on SOA services by introducing time dimension. Simulation results show that the novel method can realize DDoS traffic perception with analyzing abrupt variation of conditional entropy in time dimension.

1. Introduction

With the development of network technology, Distributed Denial of Service [1] (DDoS) attack has become a huge threat to today's network service and has aroused great concern in various countries around the world. DDoS attack being easy to implement and difficult to guard and track has become the most common network attack techniques, which has a serious impact on the efficiency of network and service [2]. According to statistics, the number of DDoS attacks continued to rise in recent years. From the latest survey released by the Akamai who is the world's largest CDN service provider, the number of DDoS attacks doubled in the second quarter of 2015. In 4 January 2016, HSBC suffered an unknown DDoS attack, which causes the system to crash and service to interrupt for two days. And a Distributed Reflection Denial of Service (DRDoS) attack is becoming an important novel form [3]. DRDoS is a method by which the hacker uses modified source address to produce a large number of forgery requests instead of directly attacks. A lot of forgery requests will point to the attacked node that would crash due to resource exhaustion at last. In the application layer DDoS attacks gradually shifted the target from the network bandwidth to the server resources of application. With the growth of service-oriented architecture (SOA) and web technology, the attacks in application layer are more destructive.

SOA is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network. The principles of service-orientation are independent of any vendor, product, or technology [4]. Because SOA which has flexible, open, and extensible characteristic is widely used, there is also increasingly great concern over a large number of DDoS attacks against SOA. Jung et al. [5] analyze the difference between the application layer DDoS and Flash Crowd. Lu et al. [6] puts forward the request path and access time of the web server to distinguish between attack flow and normal one. Zhou et al. [7] analyze the characteristics of average access time and page request sequence. Those researchers realize perception of attack with the statistics comparison of normal users and abnormal users.

In this paper, a novel method to traffic perception of the DDoS attack based on SOA is proposed. Because SOA registration centers carry a mass of data traffic that is from many service nodes, it is difficult to distinguish between

DDoS traffic and Flash Crowd (legal flow or normal traffic) on SOA registration centers. In order to effectively perceive the DDoS attacks and distinguish it from Flash Crowd, the time dimension of conditional entropy is considered. The instantaneous jump of conditional entropy is calculated and statistical in the setting time slot, which leads to the sudden traffic from DDoS attacks in the time dimension while normal traffic is smooth. The simulation results show that the algorithm is able to effectively perceive the traffic changes caused by DDoS attacks against SOA.

2. The Vulnerability of SOA under DDoS Attacks

SOA has increasingly popular in all areas of application and rapid developed. A large number of businesses, organizations, government departments, and agencies are setting up and developing their own SOA network. Modern society relies heavily on computer network system under the SOA architecture, which makes it very important to ensure the security of computer and network systems. Otherwise, it will cause not only the waste of manpower and material, but also the loss of competitive advantage, company confidential documents to be stolen. So how to enhance the security of SOA systems and network systems has become the focus of world attention.

Among all the forms of attacks against SOA, the most prominent ones are DDoS attacks. With network systems under SOA with rapid response, distributed collaboration, and reuse of services and other features, it has also undertaken a series of management and security risks brought by public service, especially from DDoS attacks in the process of information exchange.

Under DDoS attacks the vulnerability of SOA is mainly reflected in the following three aspects.

(1) SOA is a central network structure with the registration center as its core. SOA service registration, publish, query, subscription, and so on must go through the service registration center. Once the center suffered from DDoS attacks, the performance of whole network is severely reduced and even the system is paralyzed.

The registration center is taken as the central platform of SOA service release and query, which connects service providers and demanders as shown in Figure 1. So the registration center is more vulnerable to DDoS attacks. It has become a bottleneck and barriers to services system under rapid development of SOA.

(2) In order to maintain the compatibility and extensibility of the cross platform systems, lightweight transport protocols are generally used for SOA, such as SOAP protocol, which can be compatible with and bind to a variety of upper layer protocols. The lightweight protocol is easy to build DDoS attack samples and vulnerable to attacks.

(3) SOA has the characteristics of service integration and data sharing, which inevitably open interface and expose data formats of service models to providers and demanders. This makes the SOA message easy to be monitored, intercepted, and analyzed. An attacker can extract useful information from the acquisition of the SOA message and then launches DDoS attacks.

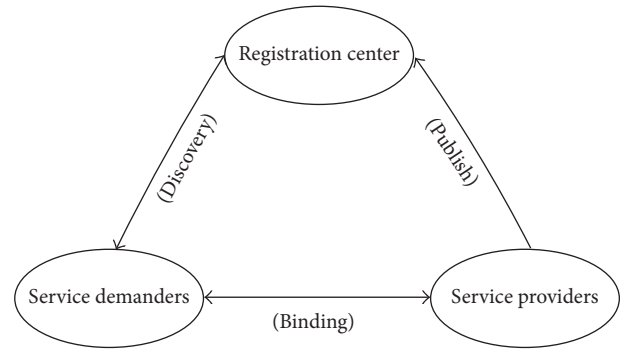

Figure 1: SOA system structure.

Therefore, due to the features such as the central structure, lightweight protocols, and services open, SOA is more vulnerable to DDoS attacks. The perception method of DDoS attacks against SOA, especially registration center of SOA, should be studied.

3. Traffic Perception Method of DDoS Attack Based on Entropy

The most prominent feature of DDoS attacks is the large increase in traffic. And traffic perception means are the most common method to detect DDoS attacks. Xiao et al. [8] carried out the classification of DDoS attack in application layer. According to the authenticity of the host to submit the request, DDoS attack in the application layer is divided into real URL request attacks and forgery ones. The former can be further divided into repeated use of a single URL or of multiple URL.

In terms of information theory, entropy is a measure of uncertainty of the random variable. The conditional entropy [9] represents the uncertainty of the second random variable Y in terms of known first random variables X.

Define information entropy of variable Y as

$$H(Y) = \sum_i p(y_i) \log_2 (p(y_i)). \quad (1)$$

Among them, $p(y_i)$ is the prior probability of each component of variable Y.

The variables X and Y of the conditional entropy are defined as

$$H(Y \mid X) = \sum_j p(x_j) \sum_i p(y_i \mid x_j) \log_2 (p(y_i \mid x_j)). \quad (2)$$

Among them, $p(y_i \mid x_j)$ is x_j about y_i of posterior probability.

4. An Algorithm of Traffic Perception of DDoS Attack against SOA

4.1. Principle. With *sip* and *dip,* respectively, representing the source address and destination address, $H(sip \mid dip)$ is defined as the conditional entropy that is consistent with

multiple to single map of DDoS attacks. The formula directly reflects the divergence and disorder from *sip* to *dip*. By sampling the network data stream, we set the total number of packets arriving at a sampling period as S. The packets from different source address are set to $\{sip_i \mid i = 1, 2, \ldots, N\}$, and those from different destination addresses are set to $\{dip_i \mid i = 1, 2, \ldots, N\}$. By the definition of M-dimensional matrix $A[M]$, $A[i]$ is the number of packets of the destination address. We define N-M-dimensional matrix $B[M] : B[i]$ to represent the number of packet source addresses as sip_i and the destination address as dip_i. Equation (3) can be obtained:

$$\begin{aligned} &H(sip \mid dip) \\ &= -\sum_j p(dip_j) \sum_i p(sip_i \mid dip_j) \log_2 \left(p(sip_i \mid dip_j)\right) \\ &= -\sum_{j=1}^{M} \frac{A[j]}{S} \sum_{i=1}^{N} \frac{B[i][j]}{A[j]} \log_2 \left[\frac{B[i][j]}{A[j]}\right]. \end{aligned} \tag{3}$$

In the above formula, $p(dip_j)$ represents the proportion of the number of packets arriving at dip_j in S, which is the total number of packets arriving at a sampling period. And the expression of $p(sip \mid dip_j)$ represents the proportion of the number of packets arriving at dip_j from sip_i in the total number of packets dip_j.

The relation between *sip* and *dip of* DDoS attacks is many-to-one mapping relationship. The more dispersed the source address, the greater the value of conditional entropy of $H(sip \mid dip)$. Conditional entropy is able to detect DDoS attack under normal circumstances and network environment. Also conditional entropy can reflect the traffic growth of DDoS attacks. But in the SOA systems, the detection method on the usual conditional entropy is not able to find abnormal traffic of DDoS attacks, especially in registration center of SOA. Because in the legal flow (Flash Crowd), the service registration center still has a strong many-to-one mapping relationship, the value of the conditional entropy will become very large. Therefore, it is difficult to distinguish Flash Crowd and the flow of DDoS attacks only by the conditional entropy.

In this paper, the novel method of instantaneous transition of condition entropy is able to make up for this shortfall by introducing timeline Z. In a short time, the emergence of a range of regional conditional entropy change, which can help to determine the occurrence of abnormal traffic of DDoS attacks, makes the SOA anomaly traffic aware method become efficient.

4.2. Select the Test Data Set. In this paper, three data sets are used in the experiment, including an attack data set, a normal flow data set and the set of SOA registration center traffic. The first two sets come from MIT Lincoln Laboratory in the 2000 DDoS data set LLDoS1.0 [10]. With the TCP flood attack traffic, the packets of source address and destination address of attack are randomly generated carrying flag ACK. Another SOA data set is from the laboratory network structures of typical SOA applications. The computers run in a shared LAN environment of 100 Mbps. A typical system consists of SOA applications from eight computers. IP addresses are from 10.166.178.101 ~ 10.166.178.108. IP address of application system of SOA registry center is 10.166.178.105. When multiple publishers simultaneously release services, the data is sampled from network traffic. In order to test the proposed method on perception capability of the small-scale attacks, under normal flow selected nodes suddenly launched a large data flow attack, which makes the registry center be denial of service. The experimental environment adopts the real source address and the fixed destination port. WIRESHARK software is used to capture the entire packets in all process on the LAN.

4.3. Experiment Result. In this paper, experiments are conducted on three data sets by conditional entropy method. 500 traffic samples are collected in each cycle time, starting from the fiftieth samples to calculate the value of the conditional entropy. And the conditional entropy is recalculated each additional 10 samples. With the advance of time, each distribution of conditional entropy is, respectively, sought out. The traffic matrix is generated based on the previous 50 samples of LLDoS1.0 data set. The matrix reflects features of many-to-one on 50 samples. There are 50 source addresses and 3 destination address.

By (3) the conditional entropy can be calculated as shown in Figure 2.

Then the distribution of conditional entropy can be obtained on the flow of normal data set as shown as Figure 3.

Finally, a kind of typical applications in SOA registration center for publishing services with the previous experimental environments is tested. The difference is that services from multiple nodes simultaneously release to a single node, which belongs to the normal process of interaction with many-to-one way. When attackers send a large number of data packets in an instant by DDoS method, the target node received abnormal traffic. The traffic data is statistical and analyzed to obtain value of conditional entropy, which helps us to judge its unusual traffic. The experimental results are shown in Figure 4.

Through the introduction of conditional entropy on axis Z, the instantaneous transition to study of the distribution of conditional entropy can be drawn as shown in Figure 5.

By extracting conditional entropy in time dimension, it can generate instantaneous jump of entropy condition shown in Figure 6.

4.4. Analysis of the Experimental Results. As shown, by comparison of Figures 2 and 3, we can see that the value of conditional entropy is relatively large by the attack data sets calculated, which is much larger than the value of 5, while the normal flow is calculated in 0 to 1 range. This reflects the definition of entropy: the greater the value of the conditional entropy, the stranger the uncertainty of the source address. The conditional entropy is able to effectively distinguish the DDoS attack traffic from normal traffic in non-SOA architecture.

Under the normal flow of SOA, there is many-to-one mapping relation between the source address (service

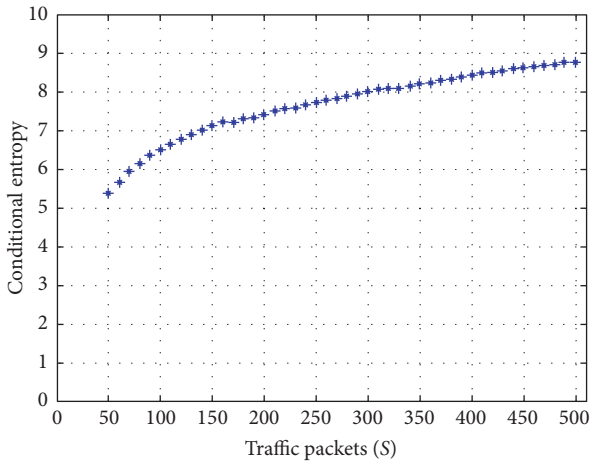

Figure 2: Conditional entropy on LLDoS1.0 attack set.

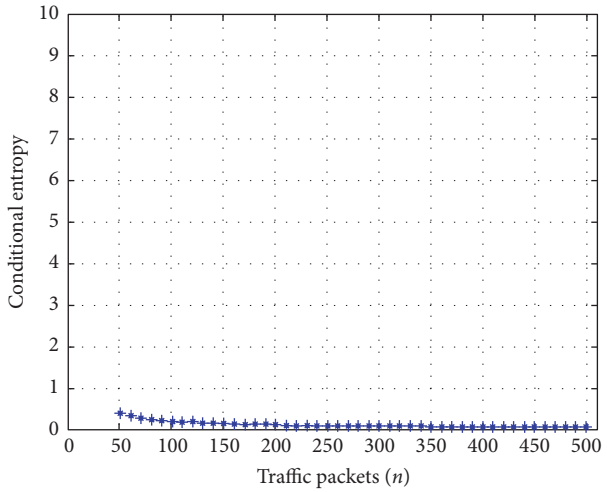

Figure 3: Condition entropy on normal traffic set.

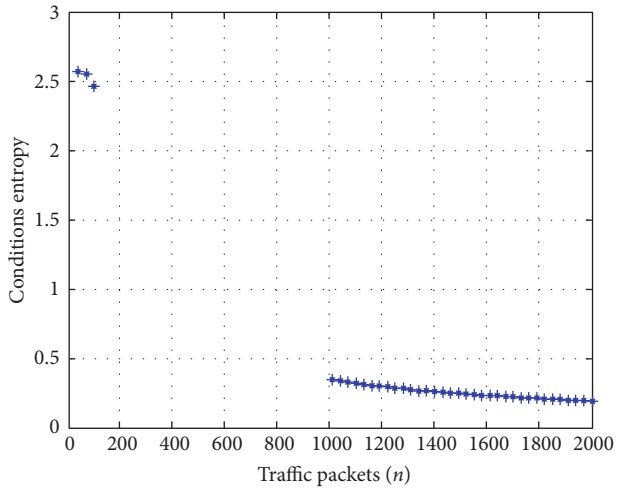

Figure 4: Conditional entropy of DDoS traffic on SOA publishing service.

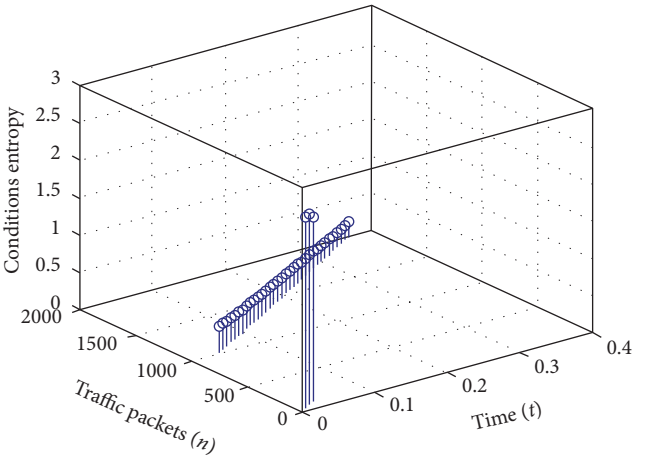

Figure 5: Three-dimensional plot of conditions entropy of DDoS on SOA.

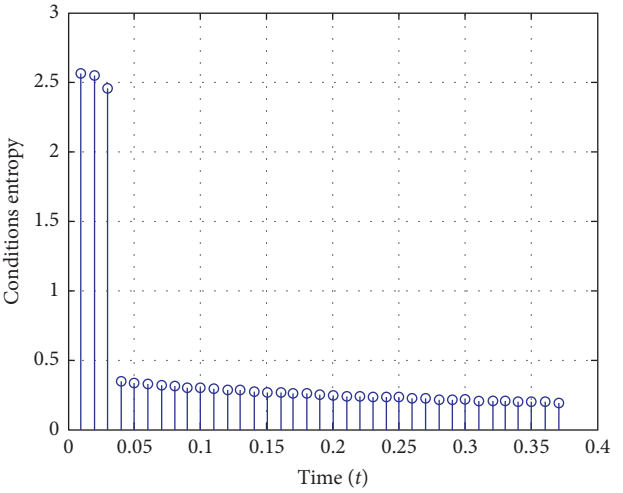

Figure 6: Instantaneous jump of conditional entropy on DDoS attacks.

provider and service demander) and destination address (service registry center). Therefore, the normalized SOA architecture also has a higher value of the conditional entropy. From Figures 3, 4, and 5 in the first half part of the curve it can be seen that in normal SOA architecture the value of entropy condition is about 2.5, far greater than the normal flow of non-SOA framework (entropy is far less than 1). If the traditional flow entropy method is used, it would produce a miscarriage of justice where the reasonable, legitimate traffic of SOA is interpreted as attack traffic. Therefore, the time dimension is referenced to the calculation of the conditional entropy and an algorithm of time united conditional entropy is used to distinguish the DDoS attacks. From Figures 3, 4, and 5 it can be seen that when DDoS attacks occur, the conditional entropy changes from a larger value of a sudden small. This is because the DDoS attack makes the traffic from the source to the destination node suddenly increase, while the number of source addresses is not significantly increased. The value of $p(sip \mid dip_j)$ (the proportion of the number of

packets arriving at dip_j from sip_i in the total number of packets dip_j) becomes larger; that is, the system becomes more ordered. Therefore, conditional entropy becomes smaller. The instantaneous jump of conditional entropy makes DDoS attacks be effectively perceived, while the normal traffic is smooth. The simulation results show that the algorithm is able to effectively perceive the traffic changes caused by DDoS attacks against SOA.

5. Conclusions

The traffic perception of DDoS attacks is an important supplement to traditional network security. It plays an indispensable role in protecting network security. Due to the wide application of SOA architecture, the abnormal behavior perception method of DDoS attacks against SOA is urgently needed. Conditional entropy instantaneous jump perception method provides such a way with finding DDoS attacks behavior under SOA based network system. It is believed that the novel algorithm with instantaneous jump perception will greatly improve the performance of the current abnormal detection for DDoS attacks against SOA.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this article.

Acknowledgments

This work was supported by China Postdoctoral Science Foundation (2016M590234) and the Open Foundation of Key Laboratory of Shenyang Ligong University (4771004kfs32).

References

[1] Z. Y. Yuan, *Distributed Denial of Service Attack Tracking Technology Research*, Central South University, Changsha, China, 2009.

[2] S. Rajesh, "Protection from application layer DDoS attacks for popular websites," *International Journal of Computer and Electrical Engineering*, vol. 5, no. 6, pp. 555–558, 2013.

[3] G. Chen, *DDoS Attacking Countermeasures*, Xi'an University of Electronic Science and Technolog, Xi'an, China, 2005.

[4] Chapter 1: Service Oriented Architecture (SOA), May 2014, https://msdn.microsoft.com.

[5] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: characterization and implications for CDNs and web sites," in *Proceedings of the 11th International Conference on World Wide Web (WWW '02)*, pp. 293–304, Honolulu, Hawaii, USA, 2002.

[6] Y. L. Lu, Y. Zhang, and C. L. Sun, "Distributed denial rebound analysis and prevention service," *Computer Engineering*, vol. 2, article 22, 2004.

[7] W. Zhou, L. N. Wang, H. G. Zhang, and J. M. Fu, "A new DDoS attacks and countermeasures," *Computer Application*, vol. 1, article 144, 2003.

[8] J. Xiao, X.-C. Yun, and Y.-Z. Zhang, "Defend against application-layer distributed denial-of-service attacks based on session suspicion probability model," *Chinese Journal of Computers*, vol. 33, no. 9, pp. 1713–1724, 2010.

[9] C. F. Yang, G. Wang, and J. H. Si, "Construction of a new generation of enterprise application integration based on SOA," *Computer Applications and Software*, no. 10, 2005.

[10] MIT Lincoln Laboratory, 2000, http://www.ll.mit.edu/ideval/data/2000data.html.