Flow Based Solutions for DoS and DDoS Attack Detection

Noble George[1], Sujitha M[2]

Abstract— **Denial of Service (DoS) and distributed denial-of-service (DDoS) attack is a kind of vigorous behavior caused to online servers that makes a network resources unavailable to its users. Denial of Service attacks are sent by a person or a system and distributed denial-of-service attacks are sent by more than two persons or more systems. Moreover at present, payload based scheme and flow based streaming solutions that detects Denial of Service attacks and Distributed Denial-of-service attacks are executed. Flow momentum algorithm which perform online traffic measurement is truly depended on traffic flows. However flow momentum increase the computational complexity of anomaly detection process due to inefficient splitting of flowset and also it is not considered as TCP Synchronization Flooding attack. In this work, it's been proposed a traffic streaming algorithm *Flow Filter and Syn flood detect* that overcome the limitations of flow momentum algorithm. The main attacks considered are TCP SYN flooding, heavy-hitter (HH) and global iceberg (GI) that sub-parts under denial-of-service and distributed denial-of-service attack.**

Index Terms- Flows, Flowset, Sampling, Syn flooding, Tuples

I. INTRODUCTION

DDoS attacks heavily destroys the connectivity of the victim, also in term of a host, a router or an entire network. They impose intensive computation tasks to the victim by degrading its system unprotected or flooding it with huge amount of useless packets. This process can make a victim to be moved out service or even for days and this can make serious damages to the services running on the victim. Therefore, such solution for DoS attacks are required for the protection of online services. The process on DoS attack detection focuses on the solution as well as the development of network-based detection mechanisms [1].

From times, traffic measurement and monitoring were processed through sampling based techniques. In the above mentioned process, at first, the selected samples were stored in a local limited storage space. Different techniques were used to collect samples [2] then the collected samples are then moved to server storage. There the anomaly detection of the collected samples are done based on rule processing.

Manuscript received Feb, 2013.

Noble George*, Department of Computer Science and Engineering, Mangalam College of Engineering Ettumanoor, India*

,

Sujitha M*, Assistant Professor Department of Computer Science and Engineering, Mangalam College of Engineering, Ettumanoor. India.*

Sampling based process had many limitations in itself hence, they were called its disadvantages and they are accuracy and latency of the anomaly detection. To diminish these limitations many studies were proposed like Programmable measurements, fast sampling [3], [4] but these proposals were not suitable for DDoS attack detection.

Instead of using Payload based technique for identifying SYN flooding attacks, it is more suitable to use Flow based detection process. In Flow based detection process tuple values are considered the most instead of Payload. Tuple values includes protocol field, source IP, source port address, destination IP and destination port address. Packets are grouped on basis of tuple values. A flow occurs when number of packets inculcates together. In a flow, the tuple values are same for all packets.

Here, all flows are considered for rule processing instead or bearing in mind packet samples that makes this process to well known as iterative measurement. In iterative measurement scheme measurement processing in completed through different iterations. Current measurement tools collects traffic statistics based on some rigid concept of flows. These concepts doesn't have that active intelligence to understand the application requirements or to adapt traffic conditions. According to the number of flows and heterogeneity of monitoring applications, the scalability is limited [6]. Due to these inefficiencies attacks like DDoS mainly, flooding large number of small flows and SYN flooding attack were not detected through flow evaluation. Different payload based classification algorithms are used to detect anomalous flow but payload based scheme is more complex compared to flow based streaming solutions.

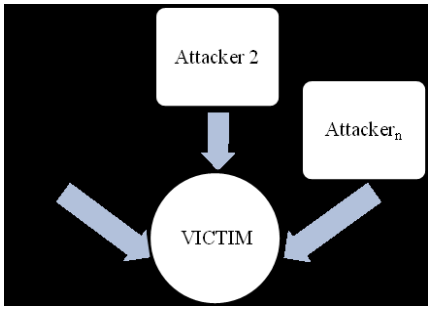

Fig. 1. DDoS attack

Current flow based measurement techniques do not consider the arrival time of packets, where it is the most relevant object considered to find a DDoS attack. Source IPs of incoming packets may be different in DDoS attacks. So the packets are added to different flows while grouping the packets based on the tuple values.

ISSN: 2278 – 1323

In the figure placed (fig.1), the victim may be attacked by different machine or person having different IP address that results packet arrival time is also considered important as tuple values in flows. Based on subject time threshold is defined and further an anomaly can be detected. The basic method used in flow based method uses a concept of grouping flows into flowsets. For attack detection these flowsets are divided into small flowsets and evaluating them using rules that defined previously. These rules are formulated based on anomalies. In this approach the flows with same IP may fall into several flowsets[5]. This may badly affect the attack detection process. Flowset division is an important part of flow based anomaly detection. A new concept of flowset division is discussed over here.

A. TCP SYN flooding attack.

The goal in a modern SYN flooding attack is simply to throw hundreds or thousands of packets to a server to disable system resources. A person, specially an attacker who sets up a SYN flood, may not complete the three-way handshake and establish the connection. For the completion of TCP connection establishment, three-way handshake is required. May be the attackers goal is to over pass the limits set for the number of connections waiting to be established for a given service. The attacker do not send the final acknowledgement to the server for completing the connection process [6]. For the establishment of new connection a server has to wait until the value of wait queue become below the threshold.

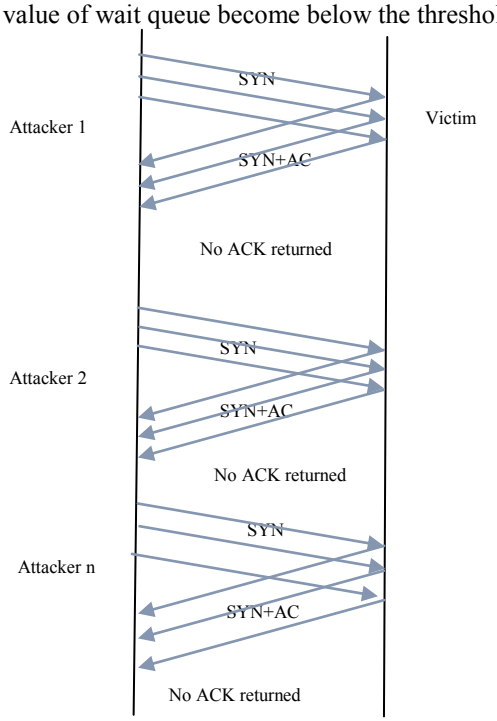

Fig. 2.TCP SYN flooding attack

The above figure explains, when an attacker is sending a large number of requests to a server, the victim accepts it and sends back SYN+ACK, but there the process of three way hand shake becomes incomplete due to the 'No response' in acknowledgement area by the attacker.

Some implementations of TCP have strategies to alleviate the effect of a SYN attack. Some have imposed a limit of connection requests during a specific period of time. Others try to sort out datagrams sourced from unwanted source addresses. A new strategy is to postpone resource allocation until the server can identify that requested connection is from a valid IP address, by using cookie. Probably, this process resulted latency and complexity in detection. But, the deed can be solved by using flow evaluation under schedule of packet arrival. Hence, this is the proposed idea in this work.

The rest of this paper proceeds as follows. In section II the related works are discussed. The Flowset and rule evaluation is discussed in section III. Section IV discusses the implementation. Section V discusses the experimental evaluation the paper concluded in section VI

II. RELATED WORKS

There is a considered work which focuses on identifying HH at single node which sub-parts under DoS attack [7]. In the work there are two novels and scalable algorithms to identify large flows: *sample and hold* and *multistage filters* which uses a small amount of memory and takes a constant number of memory reference per packet. But, the process becomes insufficient due to lack of accuracy when considering DDoS attack.

Idea of using additional sketches to solve the global iceberg problem has been proposed [8]. These sketches were used to aggregate distributed data. The problem is the study only works when the data is only available as a stream at the distributed nodes and also it fails to identify Heavy Hitters. Another study [9] related to DDoS proposes anomaly detection in distributed dataset with minimum communication overhead. Here sampling based approach is used which reduces accuracy. Hence, this is a major problem.

Many works were proposed for flow based network monitoring and one of them is cSAMP, a system which monitors whole network by analyzing flow[10]. CSAMP is a network monitoring module which uses available resources efficiently and eliminates recurring evaluation. In previous works streaming solutions were available for monitoring fine-grained networks which also introduced different algorithms named flow momentum, equilibrium roll-back and directed momentum. But packet arrival times are not considered and flowset division method used insufficient due to false positives and false negatives attack detection here. Hence, attack detection is not accurate here. Worst case running time of these algorithms is high.

Many studies were introduced for detecting SYN Flooding attack and one of them is Counting Bloom Filter. This technique was a very good sensitivity to identify IP spoofing [11]. This work was far better than the works previously introduced. Therefore, in this work it out performs the study such as Counting Bloom Filter and it's been considered light weight flows only and packet arriving time too.

ISSN: 2278 – 1323

For identifying TCP SYN Flooding attack many payload based works were also introduced. This attack can be detected according to the values of IP header and TCP header of incoming packets [12]. Flow based technique is much more effective than Payload technique. In other words, Payload based technique is complex

III. FLOWSET AND RULE EVALUATION

Critics were really described when TCP based communication was indulged with SYN Flooding attack and thus fine-grained network with real time monitoring. SYN Flooding attack was proposed when the connection establishment procedure in TCP was susceptible. The problem was occurred when one or more malicious attackers send huge number of SYN segments to a server with a pretention of each of them to have a different client and by faking the IP addresses in datagrams. Meanwhile, we need to detect the possible number of attacks.

The first step is to focus on main possible DoS and DDoS attacks and they are TCP SYN flooding attack, Heavy Hitter(HH) and another most commonly occurring distributed denial-of-servicing (DDoS) attacks viz., global iceberg(GI). So here the presentation has got solution with flow based solutions with an aim to address the challenges related with application-aware rule-based on-line traffic measurements, to achieve highly volatile traffic with accurate response.

In this proposed study the case is denotes the number of SYN packets as SYNc, and the number of SYN/ACK packets as SYN/ACKc. For identifying HI and GI traffic were grouped into flows. About flow, it is the set of packets of header fields which has the same n-tuple values. 5-tuples included in the flow are {prt, sip, spt, dip, dpt}, where prt represents protocol, sip is source IP address and dip is the destination IP address, spt is source port address and dpt is destination port address. In proposed system additionally tuple time and TCP flag is added. The main challenge in the process of identifying anomaly is determining its optimal set of rules that can accurately answer the user query in reasonable time while connecting to computational and storage budgets. Here it is been introduced a flowset based traffic measuring algorithm named *Flow Filter Algorithm* and *Syn flood Detect Algorithm*.

Flow Filter Algorithm initially group the incoming packets based on the tuple value. The same tuple valued packets are in same flow. Flows are combined to form flowset. For anomaly detection flow filter algorithm split flowset into sub flowset based on flowsize. Then flows are evaluated according to the given ruleset. Further divisions of sub flowset depends upon the rule evaluation. Flow weight is calculated according to bandwidth consumption and number of packets in the flow. In *Flow Momentum Algorithm* the flowset are divided into sub flowset until the finite granularity is obtained. Here the packets with same IP may belong to different sub flowset, it leads to numerous number of flowset divisions thus increases time complexity. It can also lead to false negatives detecting anomaly. The proposed algorithm initially group flows in flowset based on sip before first division of flowset, which reduce number of flowset divisions in anomaly detection process. The pseudocode for *Flow Filter Algorithm* provided in section A. *Syn flood Detect Algorithm* uses the tuple values :{sip,dip,dpt,time,flag} for identifying the TCP Syn flooding attack detection. The pseudocode for *Syn flood Detect Algorithm* is provided in section B.

A. Flow Filter Algorithm

```
Input  1  : trace file at time t
Input  2   : flowset at time t
Input 3    : ruleset Rset

Output 1 : identified HI set {}
Output 2 : identified GI set {}

1.      F ← set of flows
2.      Group flows in F into P based on tuple sip
3.      P← partition of F
4.      if  t ≥ time interval ti
5.      repeat
6.       for F in P
7.         if weight of flowset is >threshold θ
8.            if further division is possible
9.               divide P into another equal partitions with
                 partition coefficient β
10.               P = sub partition(P)
11.               iteratively apply rules from rule set Rset
12.            else
13.             append to heavy hitters set
14.         else
15.         initialize counter cn =0
16.         increment cn for each flow
17.          check if counter value is > threshold Th at interval
            ti append to GI set
```

B. Syn flood Detect Algorithm

```
Input 1 : Flowset at time t

Output 1 : identified flooding attack set {}

1.      F ← set of flows
2.      if  t ≥ time interval ti
3.      P1 ← set of flows with same dip and dpt
4.      S1 ← SYNc-SYN/ACKc (P1)
5.      P2← set of flows with same sip and dip
6.      S2 ← SYNc-SYN/ACKc (P2)
7.      P3 ← set of flows with same sip and dpt
8.      S3 ← SYNc-SYN/ACKc (P2)
9.      if  S1 or S2 or S3 > Threshold n
10.          Flooding attack set ← common packets from
             P1,P2,P3
```

Syn flood Detect Algorithm additionally need tuple flag for identifying synchronization and acknowledgement packets. Difference between number of synchronization packet and acknowledgement packet are compared against the previously defined threshold(n). If the difference exceeds threshold, then further process of selecting the common packets from different packet set and create the flooding attack set.

ISSN: 2278 – 1323

IV. Implementation

The implementation procedure use Server: Apache/1.3.3.7 (Unix) (Red-Hat/Linux) as victim server with port address 2020. Server machine having core i7 Intel processor and 8 GB RAM. Attack is generated artificially from client machine using Colasoft packet builder, which is a Windows compatible packet building tool. *WinPcap* is the Windows version of the libpcap used as packet capturing library and *JPcap* network packet library for application written in Java.

V. Experimental Evaluation

This section describes analysis results of the implemented results in terms of time complexity in DoS and DDoS attack detection.

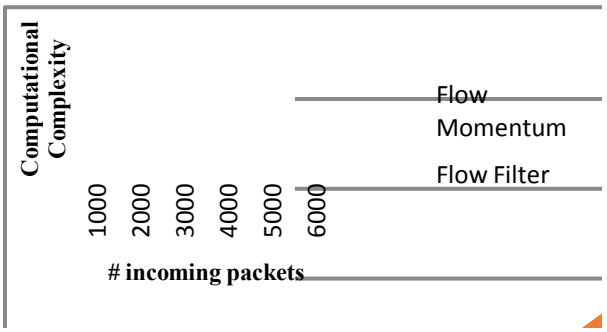

Fig. 3. Computational complexity analysis of flow momentum and flow filter algorithms

The fig 3 depicts analysis report of flow momentum and flow filter algorithms in terms of computational complexity with number of incoming packets, where the flow momentum shows huge difference in worst case scenario. The experiments also done based on number of false negatives, which also shows that flow filter algorithm outperforms flow momentum.

VI. Conclusion

Analysis and measurements of online network traffic is critical for identifying and improving any real-time anomalies in the network. For accounting and detecting DoS and DDoS attacks, accurate network traffic measurement is required. This work deals with Heavy Hitter (HH), Global ice berg and TCP Syn Flooding attack. Anomaly detections are based on flows. For that, traffic is grouped as flows and based on this flows anomaly detection process is held. Time and TCP flag are additionally added tuples in this work for the continuation of the process. There are two algorithms proposed and they are *Flow filter* and *Syn flood detect algorithm. Flow filter* algorithm detects Global ice berg and Heavy Hitter and here computational complexity and accuracy is much better than the current *Flow momentum algorithm.* In implementation, apache web server is used as victim server Apache/1.3.3.7 and an attack is artificially generated from various systems. Thus, it is well shown that both of the algorithms resulted the best way to solve the anomaly detection.

Acknowledgement

For the first, the Author would like to thanks Microsoft, without 'WORD' this work wouldn't be complete. My colleagues for their suggestions and last but not the least thank GOD.

References

[1] N. Brownlee. "Traffic Flow Measurement: Experiences with NeTraMet," RFC 2123, 1997

[2] E. Bertino and R. Sandhu, "Database Security-Concepts, Approaches, and Challenges," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 1, pp. 2-19, Jan.-Mar. 2005.

[3] J. Mai, C.-N. Chuah, A. Sridharan, T. Ye, and H. Zang, "Is sampled data sufficient for anomaly detection?," in *Proc. 6th ACM SIGCOMM IMC*, 2006, pp. 165–176.

[4] Ranjan, S., R. Swaminathan, M. Uysal, A. Nucci, and E. Knightly (2009, February). "Ddos-shield: Ddos-resilient scheduling to counter application layer attacks," IEEE/ACM Trans. Netw. *17*(1), 26–39.

[5] Apache Range Attack (2011). "Apache httpd security advisory," http://httpd.apache.org/security/CVE-2011-3192.txt.

[6] Faisal Khan, Nicholas Hosein, Soheil Ghiasi, Chen-Nee Chuah, Puneet Sharma "Streaming Solutions for Fine-Grained Network Traffic Measurements and Analysis," IEEE/ACM transactions on networking, vol. 22, no. 2, april 2014 pp 377-389.

[7] H. Wang, D. Zhang, and K. G. Shin. "Detecting SYN flooding attacks," In Proc. of IEEE INFOCOM, 2002.

[8] C. Estan and G. Varghese. "New directions in traffic measurement and accounting: Focusing on the elephants, ignoring the mice," ACM Trans. Computer Systems, 2003.

[9] Mark Handley Orion Hodson Eddie Kohler. "XORP: An Open Platform for Network Research," ACM SIGCOMM Hot Topics in Networking, 2002.

[10] G. Huang, A. Lall, C.-N. Chuah, and J. Xu, "Uncovering global icebergs in distributed streams: Results and implications," *J. Netw. Syst. Manage.*, vol. 19, pp. 84–110, 2011.

[11] V. Sekar, M. K. Reiter, W. Willinger, H. Zhang, R. R. Kompella, and D. G. Andersen, "CSAMP: A system for network-wide flow monitoring," in *Proc. 5th USENIX NSDI*, San Francisco, CA, Apr. 2008, pp. 233–246.

[12] H. Wang, D. Zhang, and K. Shin, "SYN-dog: Sniffing SYN flooding sources," in Proc. Conf. IEEE ICDCS'02, July 2002.

[13] J. Lemon, "Resisting SYN Flooding DOS Attacks with SYN Cache," in Proc. Conf. USENIX BSD, February 2001.

Noble George, Department of Computer Science & Engineering, Mangalam college of Engineering, Ettumanoor, Kerala, India.

Sujitha M Assistant Professor, Department of Computer Science and Engineering, Mangalam College of Engineering, Ettumanoor, Kerala, India

ISSN: 2278 – 1323