International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-5 Issue-6, August 2016

Prevention of Denial-of-Service Attacks using Multimatch Packet Classification

Kiran Mohan M. S, Jayasudha J. S.

Abstract: ***The growth of enterprise networks demands better security and quality of service. The denial of service attacks mainly focuses on the network resources or a service of a host, thereby prevent the service is being available to the normal users. This paper contains a method that effectively prevents the denial of service attack with the help of multimatch packet classification. The method uses multimatch packet classification for identifying the multiple matches and thereby determines the different flow of traffic. The packet migration is enforced to limit the flow of suspected packets and thus the attacking packet flow can be limited while the normal users unaffected. The method effectively prevents denial of service attack. The multimatch classification works at high speed by identifying and isolating the attacking flows.***

Keywords: Routers, packet classification, multiple match, denial of service

I. INTRODUCTION

As a result of the rapid expansion of size and complexity of enterprise networks, packet classification have significant role for providing better security and Quality of Service (QoS). The packet classification is necessary to identify different traffic and isolate them if necessary. The optimal requirement for a packet classification is its searching speed. The denial of service attacks usually targets a host machine and interrupts service of a host temporarily or indefinitely. Security and QOS are the two major concerns need to be considered for a denial of service prevention scheme. In denial of service attacks, the attacker will generate unwanted traffic to the targeted host and thereby consume the network resources heavily to interrupt the service. The packets are anomalous and the header is either spoofed or not.

The newer network applications require all matching rule from a set of rules for each of the incoming packet. For an incoming packet, the packet header is processed and the necessary fields are retrieved. The multimatch classification can be used to find out all matched rules from a set of rules. Based on the matched rules appropriate actions can be taken. Multimatch packet classification can be considered as an initial stage for choosing some set of actions for an incoming packet. The network applications like SNORT require multimatch packet classification for its working [1].

Manuscript published on 30 August 2016.
* Correspondence Author (s)
Kiran Mohan M. S*, Department of Computer Science and Engineering, Sree Chitra Thirunal College of Engineering, Thiruvananthapuram, (Kerala) – 695018, India.
Dr. Jayasudha J. S, Department of Computer Science and Engineering, Sree Chitra Thirunal College of Engineering, Thiruvananthapuram, (Kerala) – 695018, India.

II. RELATED WORKS

Different packet classification methods are used based on the applications. The best classification scheme provides better searching speed and has the ability to handle large rule base. Software based approaches are less efficient during its operation. Linear search is a simple method but the complexity increases as the number of rules increases. In two dimensional method, one of the dimension is limited and the other is having no limitations so it can possess any range [2].

The Grid of tries method further reduces the storage requirement of a classification scheme [3]. Recursive Flow Graph uses heuristic approaches for classification on multiple fields[4]. Hicuts and Hypercuts are decision tree based approaches [5][6].The TCAM is well known for its searching speed. So TCAMs are used in packet classification. Multimatch using discriminators is a TCAM based approach [7] which uses a discriminator field along with each entry of rules in the rule base. The TCAM based approach [8] uses a prioritizer circuits for its operation. The TCAM will natively support single match from a set of rules. The improvements made to TCAM approaches to address multimatch classification will also increases the implementation cost and power consumption [9-11].

B2PC is a two stage classification scheme that uses bloom filters for its operation [12][13]. The Distributed and pipelined hash tables approach is also a two stage classification scheme that can be used to find multimatch [14]. The existing method reports multimatch. The flows need to be identified for preventing denial of service attacks. The AVANT-GUARD uses packet migration to prevent saturation attack [15]. The method addresses prevention of TCP based saturation attacks. The method does not address other protocols. FLOOD GUARD addresses saturation attacks of all protocols using packet migration [16].

III. DENIAL OF SERVICE PREVENTION SCHEME

The proposed method prevents denial of service by identifying the flows from multimatch packet classification. The overall work flow is shown in figure 1.

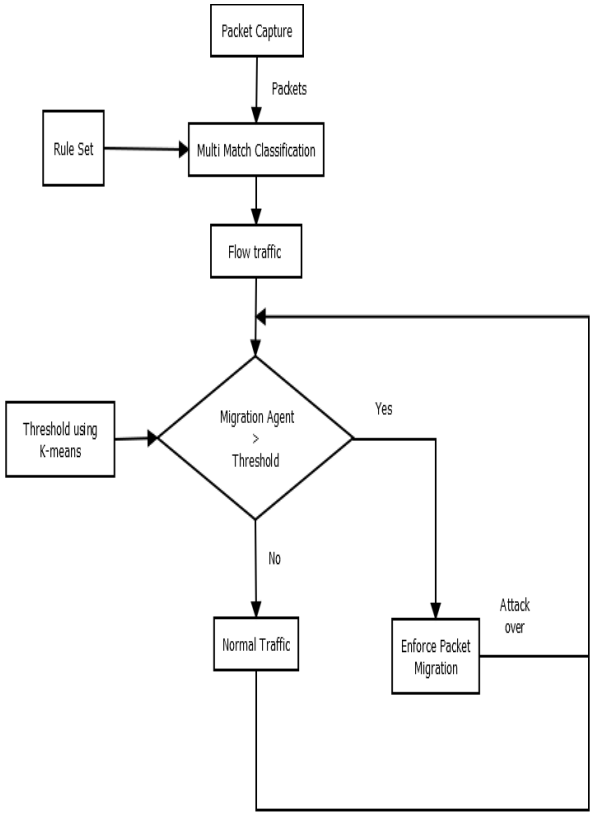

Figure 1. Overall work flow

The method will capture packets continuously and process the packet to retrieve necessary header information. The multimatch packet classification is used to identify the multiple matches and the flow of traffic is identified. The migration agent continuously monitors the traffic for denial of service. The packet migration is used to control the suspected flow and thereby denial of service attack can be prevented.

The packet classification uses a rule set and it is converted into corresponding encoded counterpart. The encoded rule set is stored in a data structure called signature tree. Each of the distinct value in a rule is assigned a distinct encoded value. For each of the incoming packet, the signature tree is traversed to find out the number of matches. The edge in the signature tree represent a character and node represents prefix of strings in the encoded rule set. The leaf node contains the identifier of a rule in the rule set. The number of leaf nodes represents the number of matched rules while traversing through the signature tree.

The traversal speed through the signature tree can be increased by utilizing an asynchronous pipeline architecture. The architecture divides the signature tree into d-1 partitions and distributes the partitions into d processing modules. Each of the processing modules has its own hash table, character FIFO, output FIFO and active FIFO. Character FIFO provides set of matching characters from single dimensional searches to the processing module. Each active FIFO provides active node identifier to the next processing module. The distributed and pipelined hash table approach ensures high traversal speed through the signature tree. A counter is associated with each of the incoming flow and the counter is updated based on the flow of incoming packets. The single dimensional search will update the counter for each of the flow.

The denial of service attacks will temporarily or permanently interrupt the services of a host. The attackers usually sent unwanted packets to the targeting host and thereby interrupt the service to the normal user. The denial of service prevention method will treat traffic without any restriction in normal conditions. Whenever there is an attack, it will employ packet migration to certain flow and thereby control the overall flow. The attack can be determined by using a threshold value. The attacking and non attacking situations are monitored and k- means clustering is used to cluster the different flows. The k-means clustering will give two clusters that represent attacking and non attacking clusters. The threshold value can be obtained from cluster average of the attacking cluster. Thus the obtained threshold can be used to identify the attacking conditions. The various states during denial of service attack prevention is shown in figure 2.

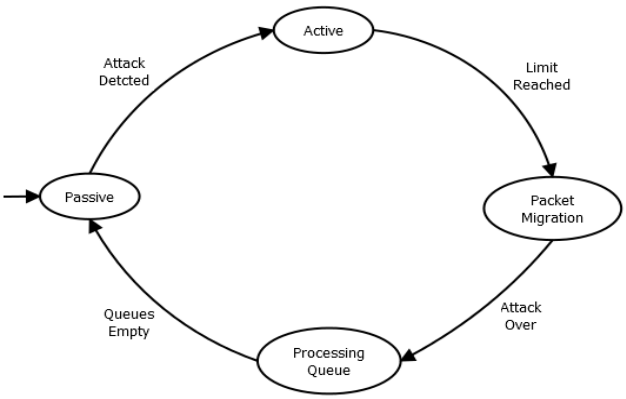

Figure 2. States of packet migration

Whenever an attack is identified, the denial of service prevention scheme will enforce packet migration. In packet migration, packets from each suspected flow is assigned a separate queue. After the packet migration is enforced, normal traffic is treated separately and the packets from the suspected flow are cached in its assigned queue. The older cached packets are overwriting if the flow exceeds the corresponding queue size. The packets from the queues have lower priority thus it will ensure better availability for normal users. The normal flow packets are treated with high priority and the suspected attacking packets correspond to certain flow will be having lower priority. The packets from queues are processed using round robin algorithm. After identifying attack is over, the migration is stopped and the packets remaining in the queues are processed. After processing all packets, denial of service prevention method will be operated normally.

IV. RESULTS AND DISCUSSION

This method continuously captures the packets and identifies the multiple matches from a set of rules. The asynchronous pipeline architecture effectively traverses the signature tree to identify the matches.

The distributed and pipelined hash tables also utilized to increase the traversal speed. The multimatch packet classification effectively identifies the flows from a certain types of traffic and each flow is accounted. The denial of service prevention scheme dynamically enforces packet migration to control the suspected traffic rate and thereby reduces the risk of attacks. The packet migration effectively prevents the flooding attack irrespective of any type of protocol. The attackers usually flood the network with unwanted packets to the targeted host. The unwanted packet flow is controlled effectively. The queues introduce certain delay during packet processing. But by considering security as a major concern the small delay while processing of packets can be discarded.

V. CONCLUSION

This paper proposes an effective method to prevent denial of service attacks. This method utilizes multimatch packet classification to identify the multiple matches and the traffic flow is identified and accounted. This method effectively identifies multiple matches and the attacks from particular sources will be effectively prevented. The normal users and non attacking flow are unaffected and the attacking flow is limited in order to ensure the security and quality of service. This method is very efficient and effectively prevents the denial of service attacks.

REFERENCES

1. Snort, “A free lightweight network intrusion detection system for UNIX and Windows,” 2013 [Online]. Available: http://www.snort.org
2. P. Gupta and N. McKeown, “Packet Classification on Multiple Fields,” Proceedings Sigcomm, Comp. Commun. Rev., vol. 29, no. 4, pp. 147–60, Sept. 1999.
3. T. V. Lakshman and D. Stiliadis, “High-Speed Policy-based Packet Forwarding Using Efficient Multi-dimensional Range Matching,” Proceedings ACM Sigcomm, pp. 191–202, Sept. 1998.
4. V. Srinivasan et al., “Fast and Scalable Layer four Switching,” Proceedings ACMSigcomm, pp. 203–14, Sept. 1998.
5. P. Gupta and N. McKeown, “Packet Classification using Hierarchical Intelligent Cuttings”, IEEE Micro, vol. 20:1, pp 34-41, Jan/Feb 2000.
6. S. Singh, F. Baboescu, G. Varghese, and J. Wang, “Packet Classification Using Multidimensional Cutting”, ACM SIGCOMM’03, August 2003.
7. K. Lakshminarayanan, A. Rangarajan, and S. Venkatachary, “Algorithms for advanced packet classification with ternary CAMS,” Proceedings ACM SIGCOMM , New York, NY, USA, pp. 193–204, 2005.
8. M. Faezipour and M. Nourani, “Wire-speed TCAM-based architectures for multimatch packet classification,” IEEE Transaction Computer, vol. 58, no. 1, pp. 5–17, Jan. 2009.
9. M. Faezipour and M. Nourani, “Cam01–1: a customized TCAM architecture for multi-match packet classification,” Proceedings IEEE GLOBECOM, pp. 1–5, Dec. 2006.
10. F. Yu, T. V. Lakshman, M. A. Motoyama, and R. H. Katz, “SSA: a power and memory efficient scheme to multi-match packet classification,” Proceedings ACM ANCS, New York, NY, USA, pp. 105–113, 2005.
11. F. Yu, R. H. Katz, and T. V. Lakshman, “Efficient multimatch packet classification and lookup with TCAM,” IEEE Micro, vol. 25, no. 1, pp.50–59, Jan. 2005.
12. I. Papaefstathiou and V. Papaefstathiou, “Memory-efficient 5D packet classification at 40 Gbps,” Proceedings 26th IEEE INFOCOM, pp. 1370–1378, May 2007.
13. S. Dharmapurikar, P. Krishnamurthy, D.E. Taylor, “Longest Prefix Matching Using Bloom Filters”, ACM SIGCOMM’03, August 2003.
14. Yang Xu, Zhaobo Liu, Zhuoyuan Zhang and H. Jonathan Chao, “High-Throughput and Memory-Efficient Multimatch Packet Classification Based on Distributed and Pipelined Hash Tables”,IEEE/ACM TRANSACTIONS ON NETWORKING, vol. 22, no. 3, June 2014.
15. S. Shin, V. Yegneswaran, P. Porras, and G. Gu. AVANT-GUARD:Scalable and Vigilant Switch Flow Management in Software-Defined Networks. In Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS), 2013.
16. Haopei Wang, Lei Xu and Guofei Gu, FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks. In 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2015.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)