Signature-based network traffic shaping

Eng. Asaad Jamous [*]

Dr. Nawar Al-awa [**]   **Dr. Maher Suleiman** [***]

Abstract

This research aims to study signature-based network traffic shaping systems, to manage the bandwidth of network link among different packets of applications according to the priority and importance per application , and building QoS classes.

In this research, we investigate the different methods of packets classifications, string matching algorithm, regular expression, traffic shaping algorithms and techniques.

A generic model to match the application signatures was developed, and integrated with QoS. The system components implemented at Linux operating system using the open sources units and programs.

Experiments of the effects of various metrics and their overall performance have been undertaken and evaluated, and the limitations found in the study are also discussed.

References:

[1] Subhabrata Sen, Oliver Spatscheck, and Dongmei Wang, "Accurate, scalable in-network identification of p2p traffic using application signatures" In Proceedings of the 13th international Conference on World Wide Web, Pages:512 – 521, 2004.

[2] Cisco Systems. Cisco Adaptive Security Appliance. http://www.cisco.com..

[3] "Snort", the. http://www.snort.org/.

[4] "SpamAssassin:Open-Source Spam Filter ", http://spamassassin.apache.org/.

[5] Leonardo Balliache, Differentiated Service on Linux, http://www.opalsoft.net/qos/DS.htm, 2003.

[6] Netfilter, Iptables, packet filtering framework, http://www.netfilter.org/

[7] L7-filter, Application Layer Packet Classifier for Linux, http://l7-filter.sourceforge.net/

[8] TC, Linux man page, traffic control Tc, http://linux.die.net/man/8/tc.

[9] R. Boyer and J. Moore, A fast string searching algorithm, Communications of the ACM, Pages: 762 –772, 1977.

[10] Ipp2p project, http://www.ipp2p.org.

[11] Niccol Cascarano, Luigi Ciminiera, Fulvio Risso, Computer Networks Group (NetGroup), "Accelerating DPI Traffic Classifiers", 2009.

[12] Fang Yu, Zhifeng Chen, Yanlei Diao, T. V. Lakshman, Randy H. Katz, "Fast and memory efficient regular expression matching for deep packet inspection", ANCS '06: Proceedings of the 2006 ACM/IEEE symposium on Architecture for networking and communications systems, 2006.

[13] Fang Yu, Zhifeng Chen, Yanlei Diao, T. V. Lakshman, Randy H. Katz, "Fast and memory efficient regular expression matching for deep packet inspection", ANCS '06: Proceedings of the 2006 ACM/IEEE symposium on Architecture for networking and communications systems, 2006

[14] Sailesh Kumar, Sarang Dharmapurikar, Fang Yu, Patrick James Crowley, Jonathan Turner," Algorithms to accelerate multiple regular expressions matching for deep packet inspection", Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications, Pages: 339 - 350 , 2006.

[15] Danhua Guo, Guangdeng Liao, Laxmi N. Bhuyan, Bin Liu, Jianxun Jason Ding, "A Scalable Multithreaded L7-filter Design for Multi-Core Servers", Proceedings of the 4th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, Pages: 60-68, 2008.

[16] LSI Tarari Content Processor, http://www.lsi.com/networking_home/networking_products/tarari_content_processors/index.html.

[17] Abhishek Mitra, Walid Najjar, Laxmi Bhuyan ,"Compiling PCRE to FPGA for Accelerating SNORT IDS", Proceedings of the 3rd ACM/IEEE Symposium on Architecture for networking and communications systems, Pages: 127-136, 2007.

[18] Jeffrey Erman, Martin Arlitt, Anirban Mahanti, "Traffic Classification Using Clustering Algorithms", Proceedings of the 2006 SIGCOMM workshop on Mining network data, Pages: 281-286 , 2006.