TRAFFIC CLASSIFICATION AND MANAGEMENT BASED ON FLOW STATISTICS ON NETFPGA

HAIDER ALI

UNIVERSITI TEKNOLOGI MALAYSIA

Replace this page with form PSZ 19:16 (Pind. 1/07), which can be obtained from SPS or your faculty.

*Replace this page with the Cooperation Declaration form, which can be obtained from SPS or your faculty. This page is **OPTIONAL** when your research is done in collaboration with other institutions that requires their consent to publish the finding in this document.]*

TRAFFIC CLASSIFICATION AND MANAGEMENT BASED ON FLOW STATISTICS ON NETFPGA

HAIDER ALI

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Engineering (Computer and Microelectronic Systems)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

JUNE 2018

Dedicated to my country, Pakistan

ACKNOWLEDGEMENT

I would like to express my profound gratitude to my respectful and wonderful supervisor Dr. Muhammad Nadzir Marsono for his continuous guidance, supervision and support throughout the whole project. His special guidance in conducting engineering research is a lifelong learning experience. I am also thankful to Loo Hui Ru for her help in carrying out this project, especially in the architecture of traffic classifier, and to my friends Munawar Zaman (Master student FKM) and Shahid Zaman (Master student FKM) for encouraging and helping me in proof reading. Furthermore, I am also thankful to my department for giving me scholarship grant for MS, without which I can not proceed this study.

ABSTRACT

The internet bandwidth increased significantly over the past years but the problem of network bandwidth management remained a key issue. One of the major problems associated with bandwidth management is *network bottleneck*, which is the overcapacity of network traffic due to abnormal application bandwidth usage. With the release of new applications every year, especially P2P applications that require high bandwidth, effective network management has become even more important. Congestion can be caused inside a network by numerous flows and high bandwidth applications that may dominate the total bandwidth allocation, affecting normal users. This report presents an approach to detect and manage high bandwidth traffic flows in a congested network, providing fair bandwidth usage to normal users and restricting bandwidth-heavy applications. Flow statistics information is used for classification of network traffic by applying k-means clustering. An inline rate-limiter technique based on queue management is used for controlling high bandwidth flows. The proposed traffic shapping method queues the header packets of flows that are classified as high bandwidth flows. These modules are integrated into the NetFPGA platform, where decision making is carried out with minimal intervention of network administrators by only updating the classifier model when accuracy falls below a threshold line. It ensure zero intrusion of user privacy and at the same time it is able to reduce the high bandwidth rate, providing fair network usage for home users.

ABSTRAK

Lebar jalur internet telah meningkat dengan ketara sejak beberapa tahun yang lalu. Namun, pengurusan rangkaian jalur lebar masih kekal sebagai masalah utama. Antara masalah besar yang dikaitkan dengan pengurusan jalur lebar adalah kesesakan jalur lebar yang disebabkan oleh kapasiti trafik jalur lebar yang berlebihan. Hal ini berlaku apabila penggunaan jalur lebar yang tidak normal. Dengan pengeluaran aplikasi baru setiap tahun, terutama aplikasi P2P yang memerlukan jalur lebar yang tinggi, pengurusan rangkaian yang berkesan menjadi lebih penting.Kesesakan jalur lebah yang berlaka dalam rangkain boleh berlaku disebabkan oleh banyak aliran dan aplikasi jalur lebar yang tinggi. Hal ini akan memerlukan peruntukan bandwidth keseluruhan, akitbatnya memberi kesan kepada pengguna biasa.Laporan ini membentangkan pendekatan untuk mengesan dan menguruskan arus trafik jalur lebar yang tinggi dalam rangkaian sesak, menyediakan penggunaan jalur lebar yang adil kepada pengguna biasa dan menyekat aplikasi jalur lebar berat.Maklumat statistik aliran digunakan untuk klasifikasi trafik rangkaian dengan menggunakan k-means clustering. Teknik pengatur kadar inline berdasarkan pengurusan giliran digunakan untuk mengawal arus jalur lebar yang tinggi. Kaedah pembentukan trafik yang dicadangkan mengetuk paket header aliran yang diklasifikasikan sebagai aliran jalur lebar yang tinggi.Modul-modul ini disatukan ke platform NetFPGA, di mana keputusan dibuat dengan campur tangan pentadbir rangkaian yang minimum melalui pengemas kini model pengelas apabila ketepatan jatuh di bawah garisan ambang sahaja. Ia memastikan pencerobohan sifar privasi pengguna dan pada masa yang sama dapat mengurangkan kadar jalur lebar yang tinggi serta menyediakan penggunaan rangkaian yang adil untuk pengguna di rumah.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AQM	-	Active Queue Management
CHOKe	-	CHOose and keep for responsive flows
DPI	-	Deep Packet Inspection
ECN	-	Explicit Congestion Notification
FRED	-	Flow Random Early Discard
HDL	-	Harware Descriptive Language
IANA	-	Internet Assigned Numbers Authority
NAT	-	Network Address Translation
NS2	-	Network-Semulator-2
P2P	-	Peer-to-Peer
PQM	-	Passive Queue Management
QoS	-	Quality of Service
RED	-	Random Early Discard
SFB	-	Stochastic Fair BLUE
TCP	-	Traffic Control Protocol

LIST OF SYMBOLS

d	-	Number of flow features
k	-	Number of clusters
N	-	Total number of instances
R	-	Cluster's radius
T	-	Time stamp
t	-	Number of iterations
U	-	Accumulated direction of cluster's centroid movement
μ	-	Cluster's centroid
y	-	Class of instance
x	-	Flow instance

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Problem Background

From the early era of networking, traffic classification remained a key research area for monitoring and managing bandwidth. With the classification of network traffic, the data obtained can be utilized by network operators for giving differentiated services to end users (e.g. QoS), along with having a better understanding of the network usage, which could help in link capacity planning and network traffic engineering.

At the early stage traffic classification was carried out using well-known ports. These ports were defined by IANA. The emergence of P2P applications, which consume large amounts of bandwidth, migration to using dynamic ports was observed [2][3] as many applications started using dynamic and unpredictable port numbers. As a result, classification using port numbers was deemed ineffective. Researchers proposed approaches aiming at inspecting packet payload, which is better known as Deep Packet Inspection (DPI). This type of analysis was used to identify the type of traffic directly from the payload or to infer patterns which can make a protocol distinguishable. Classification based on DPI requires intensive CPU computations and is time-consuming, thus discouraging its usage in large networks.

Machine Learning algorithms were applied successfully for the classification of Internet traffic [3][4][5]. These algorithms make statistical analysis of flow attributes to identify the applications, which allow the creation of models to split traffic among classes. Most of the Internet traffic relies on the client-server model which give rise

to other proposals exploiting this behavior [6]. In general, all the proposed techniques poses strong and weak points. The current tendency, however, is to combine different classifiers in order to cover the drawbacks of one technique with the benefits of other.

1.2 Network Traffic Classification and Management

Internet traffic can be categorized into three types 1) Sensitive, 2) Best Effort and 3) Undesired. Sensitive traffic has an expectation to deliver on time and this type of traffic deem sensitive to QoS metrics such as jitter, packet loss, latency. Best-effort are the non-detrimental traffic.

The bandwidth management is important for monitoring the internet traffic growth in order to give the best services to end users, because the highest speed networks may not satisfy the demand of internet applications that require huge bandwidth. This leads to the congestion in network traffic.

Traffic flows passing through a typical network consists of flows from multiple applications and utilities, many of which are unique and have their own requirements. Classification of Internet traffic is a technique that identifies different applications and protocols that exist in a flow. It can broadly be divided into two approaches: classifying the packets based on the payload, and classification based on a statistical method that uses statistical analysis of the traffic behaviour e.g. inter-packet arrival, session time, and total number of bytes in a flow.

Algorithms for classification of Internet traffic generally falls into two groups: stateless and stateful. In stateless classier (also referred to as packet classier), the required features are extracted from individual packets. The extracted features distinguish traffic classes from one another. In stateful classifier, the required features are extracted from traffic flows instead of packets which are more complicated, slower but accurate compared to stateless classifiers. Therefore, for an effective in-line traffic classification, features from the transport layer must be computed in real-time for stateful flow classication.

Machine Learning (ML) techniques [5] have been proposed to identify patterns of applications in IP traffic. ML techniques are able to identify encrypted traffic and application that use dynamic port. However, there are several limitations of ML techniques. One of these limitation is that ML algorithms that are implemented in software are not fast enough to keep up with line-rates in real-time traffic classification [7]. A compact implementation of a system (running in some recofigurable hardware) is required, which can manage to keep up with high-bandwidth and high-speed networks.

A hardware-assisted decision tree classifier implemented in NetFPGA 1G was proposed by [8]. The proposed traffic classifier is based on DT C4.5 ML algorithm running on the NetFPGA platform and the classifier is able to classify the Iternet traffic at 8Gbps line rate without packet loss, which is the maximum speed of the NetFPGA platform. The problem associated with it, however, is the requirement of a training data-set for building classifier model. The method used for building classifier is batch learning method and has to be done offline. Also, it is unable to react to changes in traffic behavior, called concept drift. The accuracy of classification process becomes low with changes in traffic behavior (concept drift) or with the release of new applications. A semi-supervised online k-means classifier with incremental learning was proposed by [9] and was successfully implemented in reconfigurable hardware, overcoming the problem of concept drift.

A traffic control mechanism is required for optimizing performance, improving latency, or increasing usable bandwidth for some kinds of packets by delaying other kinds. Some of the approach uses large queues that leads to delay in the network as the queues are full most of the time. It is important to have the mechanisms that keep the throughput high but average queue sizes low. Some of traffic control mechanisms are discussed here.

1.3 Problem Statement

One of the problems associated with stateful classifier is the difficulty in maintaining the information of flow. Working with high-bandwidth network make it worse as the statistical features of a larger number of active flows must be maintained. In adition to maintaining flow information, it must also be able to be reconfigured in order to suit various traffic classifications and keep up with the current high-speed networks. To meet these requirements, a specialized hardware is needed in some parts of the classifier such as feature extraction. The proposed specialized hardware is NetFPGA with the architecture which can be made parameterizable to work with various number of features. NetFPGA can classify multiple full-duplex flows without packet loss and with minimal delay at 8Gbps line-rate.

There are two types of router algorithm to control the congested traffic: schedulling algorithm and queue management algorithm. The scheduling algorithm implements buffer at each output of a router which needs to be partioned into multiple queues. Each queue receive packet from one of the flows. Packets from the output buffers are then placed on the outgoing line by a scheduler. Packets belonging to different flows can easily be differentiated from each other because of per flow queueing, and hence a specific flow cannot reduce the quality of another flow. The difficulty associated with this approach, however, is the requirement of maintaining complicated state information for each flow, making it too expensive to be widely used. Hence, although scheduling algorithms can provide a fair bandwidth allocation yet they are often very complex to be deployed in high-speed implementations. Besides, these algorithms do not scale well to a large number of users [10].

On the other hand, the queue management algorithms, posses a simple design architecture. Queue management mechanism utilizes a single queue for managing bandwidth. This type can be further divided into Passive Que Management (PQM) and Active Que Management (AQM). The PQM technique waits for the queue to become full before starting to drop packets. Drop-tail is an example of PQM, which admits packets into the queue until there is enough spcae. Once queue is full it starts dropping packets. Drop-tail has two major disadvantages associated with it, which

are 1) lock-out (global synchronisation) and 2) full-queue problem [11]. An AQM mechanism, on the other hand, does not wait for the queue to become full. It starts dropping packets earlier or notifies the end-hosts about congestion in the network using Explicit Congestion Notification (ECN). RED is an example of this type of flow control mechanism.

1.4 Objectives

This research focuses on the architecture on NetFPGA approach for detecting and controlling the high bandwidth flows in the network to provide fair bandwidth allocation for all flows in the congested network and keep the network condition stable. The needs for timeliness and accuracy of detection are the main consideration in this research. The proposed hardware is built by implementing three modules in hardware: a netflow probe module which is able to provide statistical information about flows for both endpoints, a feature extractor unit which is parameterizable to work with different features list and a programmable k-means classier. The proposed hardware architecture also includes the module for controlling high bandwidth flows.

Specifically, this reseach aims to achieve the following goals.

1. To develop a high bandwidth detector based on semi-supervised learning technique which is capable to detect high bandwidth flows with high accuracy and to make decision without the intevention of administrator on the netFPGA platform.
2. To develop a high bandwidth controlling (throttling) units to network infrastructure to perform fair bandwidth allocation.

1.5 Scope of Work

This report focuses on classification and mangement of high bandwidth network traffic flows, which include the architectural implementation of network traffic classifier and network traffic scheduler. Both architectural models can be implemented on NetFPGA platform. The architectural implementation of high throughput network traffic classification is scoped down to the following.

1. Verilog-HDL is used to model the hardware architecture of the proposed high throughput network traffic shaper. The proposed traffic shaper includes a network traffic classifier and a network traffic scheduler. Both hardware architectures are synthesized for Xilinx Virtex-2 Pro 50 available on NetFPGA platform.
2. The flow and feature extraction implemented in this work, for the network traffic classifier, are based on the original work by [9]
3. The architecture is designed such that it can be implemented in NetFPGA 1G [1], is a flexible hardware platform that comes with reference design for network switch and router. In addition, it can process network packet at 1 Gigabit per second (Gbps) throughput.

1.6 Organization

The reminder of this project report is organized as follows. Chapter 2 provides a detail background about the traffic classification and traffic control mechanism. Related work on traffic classification and traffic control mechanism are also discussed in this chapter. Chapter 3 discuss about the research methodlogy and experimental set-up. Chapter 4 introduces the proposed model for traffic classification. Chapter 5 introduces the proposed model for traffic scheduling. Chapter 6 concludes all the research work and point out potential future direction of this work.

REFERENCES

1. Lockwood, J. W., McKeown, N., Watson, G., Gibb, G., Hartke, P., Naous, J., Raghuraman, R. and Luo, J. NetFPGA–an open platform for gigabit-rate network switching and routing. *Microelectronic Systems Education, 2007. MSE'07. IEEE International Conference on*. IEEE. 2007. 160–161.

2. Mula-Valls, O. *A practical retraining mechanism for network traffic classification in operational environments*. Ph.D. Thesis. Master Thesis in Computer Architecture, Networks and Systems, Universitat Politecnica de Catalunya. 2011.

3. Nguyen, T. T. and Armitage, G. A survey of techniques for internet traffic classification using machine learning. *IEEE Communications Surveys & Tutorials*, 2008. 10(4): 56–76.

4. Li, W. and Moore, A. W. A machine learning approach for efficient traffic classification. *Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, 2007. MASCOTS'07. 15th International Symposium on*. IEEE. 2007. 310–317.

5. Soysal, M. and Schmidt, E. G. Machine learning algorithms for accurate flow-based network traffic classification: Evaluation and comparison. *Performance Evaluation*, 2010. 67(6): 451–467.

6. Baldi, M., Baldini, A., Cascarano, N. and Risso, F. Service-based traffic classification: Principles and validation. *Sarnoff Symposium, 2009. SARNOFF'09. IEEE*. IEEE. 2009. 1–6.

7. Williams, N., Zander, S. and Armitage, G. A preliminary performance comparison of five machine learning algorithms for practical IP traffic flow classification. *ACM SIGCOMM Computer Communication Review*, 2006. 36(5): 5–16.

8. Monemi, A., Zarei, R. and Marsono, M. N. Online NetFPGA decision tree statistical traffic classifier. *Computer Communications*, 2013. 36(12): 1329–1340.

9. Loo, H. R. and Marsono, M. N. Online network traffic classification with incremental learning. *Evolving Systems*, 2016. 7(2): 129–143.

10. Demers, A., Keshav, S. and Shenker, S. Analysis and simulation of a fair queueing algorithm. *ACM SIGCOMM Computer Communication Review*. ACM. 1989, vol. 19. 1–12.

11. Baker, F. and Fairhurst, G. *IETF recommendations regarding active queue management*. Technical report. 2015.

12. Kim, H., Fomenkov, M., Claffy, K., Brownlee, N., Barman, D. and Faloutsos, M. Comparison of internet traffic classification tools. *IMRG WACI*, 2007. 2007.

13. Sen, S., Spatscheck, O. and Wang, D. Accurate, scalable in-network identification of p2p traffic using application signatures. *Proceedings of the 13th international conference on World Wide Web*. ACM. 2004. 512–521.

14. Riley, M. C. and Scott, B. Deep Packet Inspection: The end of the internet as we know it. *Online] März*, 2009.

15. Ou, G. Understanding deep packet inspection (dpi) technology. *Internet: http://www. digitalsociety. org/files/gou/DPI-Final-10-23-09. pdf*, 2013.

16. Kotsiantis, S. B., Zaharakis, I. and Pintelas, P. Supervised machine learning: A review of classification techniques. *Emerging artificial intelligence applications in computer engineering*, 2007. 160: 3–24.

17. Erman, J., Arlitt, M. and Mahanti, A. Traffic classification using clustering algorithms. *Proceedings of the 2006 SIGCOMM workshop on Mining network data*. ACM. 2006. 281–286.

18. Floyd, S., Fall, K. and Tieu, K. Estimating arrival rates from the RED packet drop history. *Draft paper, April*, 1998.

19. Floyd, S. and Jacobson, V. Random early detection gateways for congestion avoidance. *IEEE/ACM Transactions on networking*, 1993. 1(4): 397–413.

20. Komatsu, T. and Namatame, A. Defending against high-bandwidth traffic aggregates. *IJCSNS International Journal of Computer Science and Network Security*, 2007. 7(2): 243–250.

21. Pan, R., Prabhakar, B. and Psounis, K. CHOKe-a stateless active queue management scheme for approximating fair bandwidth allocation. *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. IEEE. 2000, vol. 2. 942–951.

22. Mahajan, R., Bellovin, S. M., Floyd, S., Ioannidis, J., Paxson, V. and Shenker, S. Controlling high bandwidth aggregates in the network. *ACM SIGCOMM Computer Communication Review*, 2002. 32(3): 62–73.

23. Lin, D. and Morris, R. Dynamics of random early detection. *ACM SIGCOMM Computer Communication Review*. ACM. 1997, vol. 27. 127–137.

24. Brakmo, L. S., O'Malley, S. W. and Peterson, L. L. *TCP Vegas: New techniques for congestion detection and avoidance*. vol. 24. ACM. 1994.

25. Doar, M. B. A better model for generating test networks. *Global Telecommunications Conference, 1996. GLOBECOM'96.'Communications: The Key to Global Prosperity*. IEEE. 1996. 86–93.

26. Zegura, E. W., Calvert, K. L. and Bhattacharjee, S. How to model an internetwork. *INFOCOM'96. Fifteenth Annual Joint Conference of the IEEE Computer Societies. Networking the Next Generation. Proceedings IEEE*. IEEE. 1996, vol. 2. 594–602.

27. Albert, R. and Barabási, A.-L. Topology of evolving networks: local events and universality. *Physical review letters*, 2000. 85(24): 5234.

28. Ahammed, G. and Banu, R. Analyzing the performance of active queue management algorithms. *arXiv preprint arXiv:1005.1992*, 2010.

29. Li, D., Xu, X., Xin, Y. and Hu, Z. Dynamic online traffic identification scheme based on data stream clustering algorithm. *Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on*. IEEE. 2011. 329–334.

30. Mingliang, G., Xiaohong, H., Xu, T., Yan, M. and Zhenhua, W. Data stream mining based real-time highspeed traffic classification. *Broadband Network*

& Multimedia Technology, 2009. IC-BNMT'09. 2nd IEEE International Conference on. IEEE. 2009. 700–705.

31. Erman, J., Mahanti, A., Arlitt, M., Cohen, I. and Williamson, C. Offline/realtime traffic classification using semi-supervised learning. *Performance Evaluation*, 2007. 64(9-12): 1194–1213.

32. Zhou, Z., Song, T. and Fu, W. RocketTC: a high throughput traffic classification architecture. *Computing, Networking and Communications (ICNC), 2012 International Conference on*. IEEE. 2012. 407–411.

33. Gama, J. *Knowledge discovery from data streams*. CRC Press. 2010.

34. Maruyama, T. Real-time k-means clustering for color images on reconfigurable hardware. *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*. IEEE. 2006, vol. 2. 816–819.

35. Estlick, M., Leeser, M., Theiler, J. and Szymanski, J. J. Algorithmic transformations in the implementation of K-means clustering on reconfigurable hardware. *Proceedings of the 2001 ACM/SIGDA ninth international symposium on Field programmable gate arrays*. ACM. 2001. 103–110.

36. Laskov, P., Düssel, P., Schäfer, C. and Rieck, K. Learning intrusion detection: supervised or unsupervised? *International Conference on Image Analysis and Processing*. Springer. 2005. 50–57.

37. Karagiannis, T., Broido, A., Faloutsos, M. *et al.* Transport layer identification of P2P traffic. *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*. ACM. 2004. 121–134.

38. Moore, A. W. and Papagiannaki, K. Toward the Accurate Identification of Network Applications. *PAM*. Springer. 2005, vol. 5. 41–54.

39. Park, S. K. and Miller, K. W. Random number generators: good ones are hard to find. *Communications of the ACM*, 1988. 31(10): 1192–1201.

40. Ahmad, K. and Begen, A. C. IPTV and video networks in the 2015 timeframe: The evolution to medianets. *IEEE Communications Magazine*, 2009. 47(12).

41. Bernaille, L., Teixeira, R., Akodkenou, I., Soule, A. and Salamatian, K. Traffic classification on the fly. *ACM SIGCOMM Computer Communication Review*, 2006. 36(2): 23–26.

42. Crotti, M., Dusi, M., Gringoli, F. and Salgarelli, L. Traffic classification through simple statistical fingerprinting. *ACM SIGCOMM Computer Communication Review*, 2007. 37(1): 5–16.

43. Erman, J., Mahanti, A. and Arlitt, M. Qrp05-4: Internet traffic identification using machine learning. *Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE*. IEEE. 2006. 1–6.

44. Li, J., Zhang, S., Li, C. and Yan, J. Composite lightweight traffic classification system for network management. *International Journal of Network Management*, 2010. 20(2): 85–105.

45. IANA. *https://www.icann.org/ (Retreived on feb. 02, 2018)*.

46. tcpdump. *http://www.tcpdump.org/ (Retreived on feb. 02, 2018)*.

47. mining software, W. D. *http://www.rulequest.com/Personal/ (Retreived on feb. 02, 2018)*.

48. wireshark: Network analyser. *https://www.wireshark.org/ (Retreived on feb. 02, 2018)*.

49. Vivado, X. *https://www.xilinx.com/ (Retreived on feb. 02, 2018)*.

50. ModelSim. *https://www.mentor.com/ (Retreived on feb. 02, 2018)*.