KNOM Review '15-01 Vol.18 No.01
https://doi.org/10.22670//knom.2015.18.1.1

Network Neutrality Violation Detection for Streaming Media Traffic in Wired and Wireless Networks

Ramneek*, **, Patrick Hosein*, Wonjun Choi*, Woojin Seok****

* Korea University of Science and Technology, Daejeon, Korea

** Korea Institute of Science and Technology Information, Daejeon, Korea

***The University of the West Indies, Trinidad and Tobago

ramneek@kisti.re.kr, patrick.hosein@sta.uwi.edu, cwj@ust.ac.kr, wjseok@kisti.re.kr

Abstract

Network Neutrality principle states that all the network users are entitled to access all the content on the Internet, without any kind of unfair blocking or degradation of access to the contents of a particular application provider by the Internet Service Providers (ISP). The Network Neutrality conflict has been in the limelight for several years due to political, economic, and technical implications. While the proponents, including the end users and the content providers, argue that enforcing Network Neutrality by law is essential to preserve the openness of the Internet and promote innovation, the opponents, including the ISPs, counter this argument by asserting that such rules provide disincentives for them to invest in their network. We focus on the technical aspects of Network Neutrality and detect whether or not an ISP is Network Neutral. In this paper, we propose a method for monitoring ISPs to ensure that the network neutrality is not violated. We monitor the packet loss statistics for users of each content provider, and determine if the rate adaptation in case of streaming media is being influenced by the throttling of the service at the ISP, and prove the novelty of the proposed method through simulations.

Keywords: Network Neutrality, Network Management, Resource Management, Content Provider, ISP, Streaming Media.

1. Introduction

Over the past decade, the Network Neutrality debate has been in the spotlight due to its political, economic, social and technical aspects. Many government organizations in different parts of the world including the United States, Europe, Canada and Japan have been engaged in framing the laws and regulations for enforcing this design principle [1][2]. The debate has been triggered by a number of events in the past, such as the case of Comcast blocking, throttling Bit torrent traffic on its network and slowing down the peer-to-peer applications [3], the case where France Telecom asked Apple and Google to pay in return for the rise in the network traffic due to their content, and the case in which British Telecom slowed down the video content delivery over their network.

The proponents of network neutrality, including the content providers and the user support groups, argue that the Internet was intrinsically born to be neutral, with the sole aim of transferring the packets from source to destination, and any kind of paid prioritization should be prohibited. They assert that if nondiscrimination, and non-blocking is not enforced by law, the Internet Service Providers (ISPs) might ask for compensation from the service providers differently for access to dedicated bandwidth and Quality of Service (QoS). In addition to charging the content providers differently for provision of different levels of QoS, they may also block certain applications and content which can hinder the innovation and growth of new internet applications as the startups may not be able to pay for large bandwidths. On the other hand, the opponents, including the ISPs, disagree with the above arguments and assert that if they are not allowed to charge for providing enhanced QoS then they may not be able to afford network upgrades. In addition, if all the data on the Internet is transmitted equally, without

논문번호 : KNOM2015-01-01, Received April 18, 2015; Revised May 30, 2015; Accepted July 1, 2015

any kind of blocking, then the ISPs might not be lawfully permitted to block viruses and spam emails and other objectionable content on the Internet.

Although there is no current globally accepted definition of network neutrality, we focus on the definition provided in [4], according to which, Network Neutrality represents the idea that Internet users are entitled to service that does not discriminate on the basis of source, destination, or ownership of Internet traffic. Although some minimum QoS guarantees can be provided to different applications based on the implicit requirements, there should be no discrimination based on the online service providers or websites. Note that this does not restrict ISPs from providing different subscription plans and providing differential levels of service based on these plans. A number of tools and algorithms have been proposed in the literature to detect the violation of network neutrality. For instance, Glasnost [5] is a tool that is capable of detecting traffic discrimination that is triggered by transport protocol headers (e.g. ports) or packet payload, ShaperProbe [6] is an active probing tool which detects whether an ISP uses a token bucket method to apply traffic shaping, and examines the port blocking.

Although these tools are capable of discovering certain types of discrimination, they have a number of limitations. They focus on one particular parameter or application, such as peer-to-peer applications, and hence are not capable of identifying other factors that may cause a difference in performance. In addition, the ISPs can bypass the detection mechanisms that are based on the information obtained by sending probe packets, by identifying such packets and giving them preferential treatment. Furthermore, such tools cannot guarantee whether the variation in the performance is due to the service provider discrimination or other network conditions such as congestion.

In this paper, we propose a novel mechanism for monitoring network neutrality conformance by Internet Service Providers. We monitor the packet loss statistics to determine if the adaptation rate in case of multi-bitrate streaming is being affected by throttling at the ISP. In the case of wireless networks, the proposed mechanism is based on the scheduling information in addition to packet losses at the base station, due to time variant nature of such networks. The rest of the paper is organized as follows: Section 2 provides a review of various violation detection mechanisms that have been proposed in the literature; Section 3 includes the proposed mechanism and the network architecture; Section 4 provides the simulation results and discussion and finally we conclude our work in Section 5.

2. Literature Review

In this section we will describe some of the existing algorithms for monitoring the net neutrality violation, discussing the advantages and drawbacks of each one of them.

Glasnost [5] is a client-server based tool where end user hosting the Glasnost client connects to the Glasnost server to download and execute various performance tests. Each of these tests generates flows containing application-level data to measure the path between the client and the server. It emulates two identical flows on the same path and compares their performance to determine the presence of any differentiation. The strength of Glasnost lies in its accuracy and simplicity of usage for the end user. However, the Glasnost is focused on the end user differentiation and might not be capable of detecting the discrimination between the different content providers by the ISP. In contrast, we are focus on detecting the discrimination between the different CPs in the current work.

Another system that gathers data passively from the end users, running the agents, and establishes a causal relationship between the ISPs policies and the observed deterioration in performance is NANO [7]. It infers the differentiation in the achieved performance, by comparing the performance achieved through a particular ISP to the other ISPs, for a particular service. In addition, the information regarding the end user host, operating system, etc. is also collected by the agents. The inferences produced by NANO system takes the impact of a number of confounding factors into consideration. However, there are a vast number of such confounders that may affect the results and might not have been taken into consideration, which can lead to erroneous results in some cases. Also, it focuses on performance differences between different ISPs and between different types of applications, but does not take the performance difference between same applications from different sources or content providers into consideration.

NeuBot [8] is software for distributed network measurements, where an agent periodically monitors the QoS provided to the user and stores the results on a centralized server. The agents run active transmission tests in the background, emulating different types of applications and the master server coordinates these tests and collects the results, which are made available publicly, allowing the interested users to monitor the state of

internet continuously. NeuBot currently supports two main types of tests, including speed test and Bit Torrent test, emulating HTTP traffic and Bit Torrent traffic respectively. The strength of NeuBot lies in the fact that it continuous monitors the end user connection rather than sending probe packets to the ISPs. However, the variation in performance might be a result of other factors such as network congestion, and not always because of the ISP discrimination or throttling.

There are number of other tools related to network neutrality, however they mainly focus on one particular type of interruption. For instance, ShaperProbe [6] detects if the ISP is employing any kind of traffic shaping, by actively probing the network flow paths. It measures the time taken for the traffic shaping hardware to make a level shift to lower speed limit. By gathering this data repeatedly and from different users, this tool can estimate the token bucket parameters being used for differentiation. Another example is NetPolice [9], earlier known as NVLens [10] that detects traffic differentiation on the basis of routing information, contents of packet header, and application layer information. Its inferences on the network neutrality violation among the backbone ISPs are based on the comparison of the aggregate loss rated between different flows. In addition to the above techniques that are based on technical parameters and statistics, there are some others that are based on the concept of crowd-sourcing, including [11] and [12].

3. Proposed Method to Detect Network Neutrality Violation

3.1 The Network Model

The proposed network framework takes three basic network entities into consideration: the last-mile or the access internet service provider (ISP), the content/application providers (CP) and the end user. The end user accesses the services/applications provided by the content providers via their broadband ISPs. Figure 1 shows the basic network model. We consider two sets of n users each, subscribed to the last-mile ISP for internet access. The end users from the set1 and set2, access the content/services from the CP1 and CP2 respectively. If the ISP is network neutral, then the last mile bottleneck capacity should be shared equally among all the users and there should be no discrimination based on the origin of the traffic. However, if the ISP is not neutral, then a better treatment can be given to the traffic coming from a particular CP as compared to others. For this work, we will primarily focus on the last-mile or the access ISP and ignore the backbone providers as the bottleneck for the internet traffic, in both wired and wireless, is often the last mile, and most of the discrimination occurs there [13].

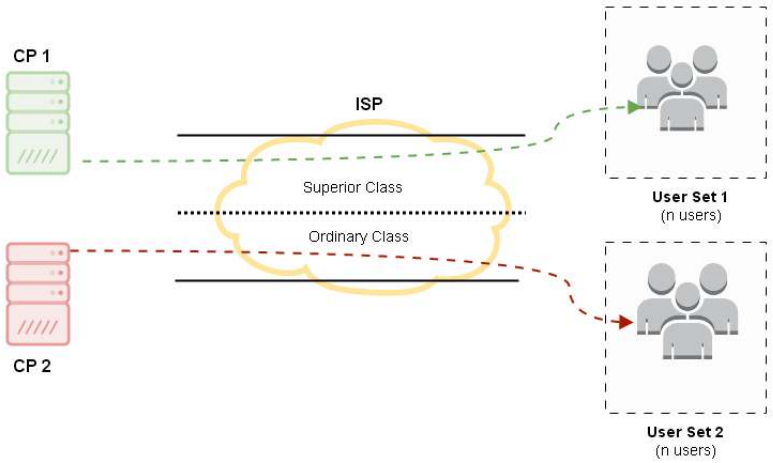


Figure 1. Network Model

3.2 Problem Statement

With the introduction of advanced network technologies, and the increase in the number of smart devices on the Internet, data traffic has increased rapidly over the last few years, and it has been predicted that the demand for data will exceed available capacity in the near future. Due to the increase in the connection speeds in fixed and mobile networks, the average bit rate of the content accessed over such networks is also expected to increase. This has resulted in an increase in the proportion of video and streaming media content over the

internet, as compared to the other best effort content, as shown in Figure 2. The forecasted data traffic (in Exabytes per month) has been plotted as a function of time, using data provided in the Cisco visual networking index (2014-2019)[14], according to which, the mobile video traffic will dominate all other forms of traffic with a CAGR of 63% by the end of 2019. Video traffic is different from web traffic due to its higher bit rate and delay constraints, and hence, the most common form of discrimination by the ISPs is to throttle the content from the CPs hosting such streaming media. Therefore, in this work, we aim to detect if an ISP throttles traffic from of a particular CP as compared to other CPs, with the focus on streaming media applications.

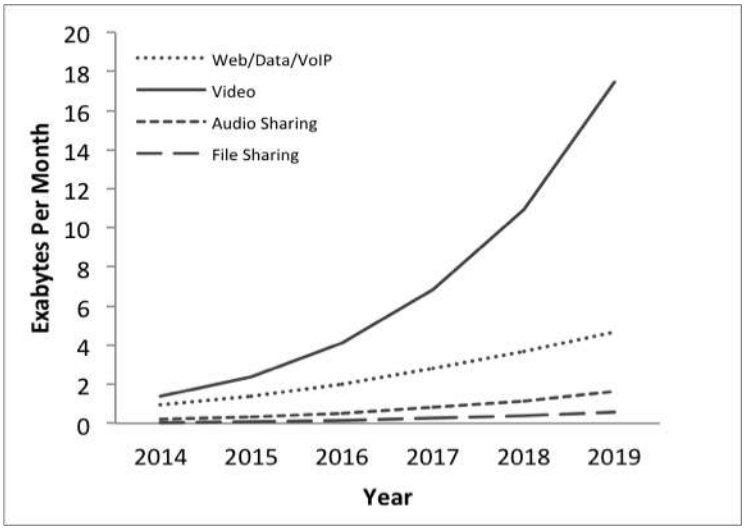


Figure 2. Global Mobile Data Traffic Growth (2014-2019) Per Application

3.3 Proposed Method

As discussed previously, the amount of video traffic is expected to increase rapidly and will dominate all other forms of traffic in next few years. Therefore, in the case of such streaming media applications, reliable and uninterrupted content delivery is of prime importance for maintaining the Quality of Experience (QoE). Due to varying characteristics of the network channels, the packet arrival rate can vary over time. As a result, a number of techniques have been deployed to avoid the interruption in playback, Adaptive Bit Rate (ABR) being the most common one as it automatically adapts to the changes in the network. It works by estimating the available bandwidth for the user, and adjusting the quality of the stream accordingly, as shown in Figure 3. The content from the source is encoded at different bit rates, which are known to the source. The source rate can be adapted dynamically depending on the network condition or the download rate at the end user.

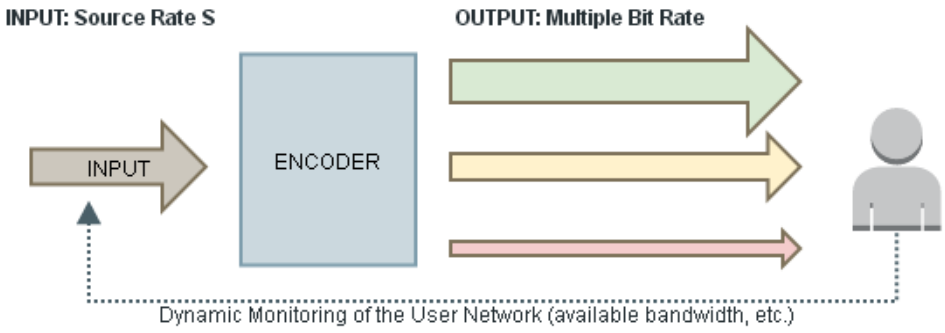


Figure 3. Adaptive Bit Rate Streaming

Detecting discrimination in such cases is particularly challenging. For example, consider the case where a content provider is generating a video stream at source rate S. In this case, the receive rate must be equal to the source rate for acceptable performance. However, if the network is congested, and there is a high packet loss, the source rate S will be adapted to the available capacity of the end user. Consider the case where the ISP

provides a service rate R (where R < S). The CP will decrease the source rate according to the feedback and once the source rate is adapted the packet loss rate is reduced and so violation cannot be detected. To overcome these challenges, we propose the following: Consider two Content Providers CP1 and CP2 each capable of transmitting with a source rate S. Now suppose that the ISP is not neutral, and provides rate R1 and R2 to CP1 and CP2 respectively, where R1 << R2. This means that the ISP will throttle the performance of the CP1 more than CP2. Initially, both the content providers, CP1 and CP2, will start transmitting with source rate S. The ISP drops some packets arriving from CP1 and CP2, and the clients will feed back the loss information so that the CPs drop the source rate to R1 and R2 respectively. As R1 << R2, the number of packets dropped will be more for CP1 than for CP2. We will monitor the loss rate and the throughput over time for the clients of each CP. If Li denotes the packet loss rate (PLR) for CPi during the transient period, it can be defined as $L_i = (1-R_i/S)$.

We will monitor the packet loss rate Burstiness at the start of the streaming and when the channel conditions vary, in addition to throughput Ri and the PLR Li, for each CP. If the ISP provides differential service rates to each CP, then the one with the lower service rate should experience more packet losses. Hence the rate of packet loss should indicate if one CP is being unfairly treated. Therefore, if the long term throughput R of two CPs is different, then we can conclude that they are being treated differentially, by monitoring the loss rate. If the loss rate is small, then the ISP might not be at fault since the source rate is low (close to the service rate R). However if the difference in the loss rate is high, then it indicates that one CP was penalized more and ended up at a lower service rate than the other. Therefore, if there is a bursty packet loss at the beginning of the streaming, and R1 << R2, while L1 >>L2, we can conclude that the CP1 is being unfairly treated as compared to the CP2.

The proposed method provides a more robust mechanism as compared to monitoring just the average throughput or average PLR over time. Note that if the ISP drops the packets of a CP to bring down its adaptive rate, then from thereon, there might be no more packet loss as the ISP can easily provide the streaming rate R, and there will be no negative feedback to the CP. In this case, the average packet loss will still be low, and hence is not a robust mechanism to indicate the discrimination. This mechanism can be applied to both wired and wireless networks. However, due to the time-variant nature of the wireless networks, we might need additional information for auditing the network neutrality conformance. In wireless networks, there are a number of factors such as fading, shadowing, handoffs, etc, due to which the number of active users and the amount of available resources keep on changing dynamically. Therefore, we propose an enhanced mechanism based on the scheduling information, in addition to the parameters discussed above.

In order to schedule multiple users over a shared packet data networks, a number of scheduling techniques have been proposed [15]. In order to explain the proposed algorithm for the wireless networks, we will first provide a brief overview of the scheduling problem. As described by Kelly [16], the scheduling problem over a shared channel can be formulated as follows:

$$\text{maximize} \quad F(\vec{r}) \equiv \sum_{i=1}^{k} U_i(r_i)$$

$$\text{subject to} \quad \sum_{i=1}^{k} r_i < C$$

$$\text{over} \quad r_i \geq 0, \;\; 1 \leq i \leq k.$$

Where,

k = the number of active users competing for the channel,
ri = the average throughput of user i,
Ui(ri) = the utility function of user i,
C = the channel capacity.

The above formulation can also be defined in terms of other performance parameters such as delay, packet loss rate, etc. If we assume that the utility function is strictly concave and differentiable, then the same will be valid for the objective function F as well. Since the feasible region is compact, the unique optimal solution can be computed using the Lagrangian Methods. However, in the case of wireless networks, we cannot move to the optimal allocation at once due to the time-variant nature of the network. Therefore, at every scheduling step, that user is chosen, who if served, results in the maximum value of the gradient of the objective function. Therefore,

the dual-ascent algorithm reduces to finding the maximum gradient direction and serving the corresponding user.

If the ISP is neutral or non-discriminating, then we can assume that the underlying scheduler used for scheduling the traffic received from different content providers, to the end users, must be based on the principle of the proportional fair scheduling, so that there is no prioritization of the content based on the source. If the well known Proportional Fair utility function is used then $U(r) = \log(r)$ and hence the resulting scheduler picks the user for which $U_j(n)/r_j(n)$ is the maximum. When a user is served (allocated more resources), its gradient (Priority Function) decreases and when it is not served, its gradient increases. The net result is that all users approach some common gradient (the optimal point for convex optimization) [17]. The aim of providing this description is to emphasize on how the scheduling information can be used to infer non neutral behavior of the ISP.

In a wireless network we can assume that the streaming bottleneck is the air interface. Therefore the only way a wireless provider can treat one CP better than another is to give the users of the favored CP higher priority and hence a higher throughput leading to a higher streaming rate, after adaptation. Therefore, we can compute the average priority over all users of each CP and compare this for violation. Although the instantaneous priority may vary, depending on the channel condition and the past throughput of a user, the average priority over all users of all the CPs should converge to a common value over time [18].

The main factor that differentiates our proposed work from the current mechanisms is that we primarily focus on detecting the application/content provider discrimination, done by the access providers or the last-mile ISP. Instead of just monitoring the network performance parameters such as throughput, delay or PLR, we provide a more robust mechanism, based on the packet loss trend and the scheduling information, for detecting the net neutrality infringement by the ISPs.

4. Performance Evaluation

In this section, we will describe the general framework used for simulation, followed by the results and discussion. The proposed work was divided into two parts for simulation. In first part, we will illustrate the novelty of our proposed approach in a wired network scenario and the second part focuses on the wireless networks, for which the proposed mechanism is based on the scheduling information and packet losses at the base-station. All the simulations were performed using the Network Simulator-3 (NS3)[19], which is a discrete event simulator, designed to support realistic replication of various networking protocols. The simulation parameters have been summarized in Table-I.

For the first part of the simulation, we created a point-to-point network topology, in which the CP is linked to the end user by a point-to-point link, with a router in-between, representing the ISP. As described earlier, we focus on the last mile or the access ISP only. A large sized streaming application flow was transferred from the CP to the end user via the ISP, with a fixed source rate of 10 Mbps. The throughput, or the data rate of the actual flow was then decreased dynamically, and the corresponding packet loss burst size was monitored using the flow monitor module of NS-3 [20]. The results are shown in Figure 4. As the ISP increases the throttling rate, the number of packets it drops at the beginning of the stream increases in order to reach the lower throughput value. After the source rate gets adapted according to the achievable throughput value, there is little or no packet loss on the link. Hence, if the ISP is non neutral, and different throughput assigned to different CPs, then the amount of packet loss at the beginning of the stream clearly indicates if one CP is being unfairly treated with respect to the others.

In the case of wireless networks, the simulations were performed using the LTE module of Network Simulator-3 (NS-3), which has been designed to support the evaluation of various aspects of LTE systems including Radio Resource Management, QoS-aware Packet Scheduling, Inter-cell Interference Coordination and Dynamic Spectrum Access, etc. In order to investigate the feasibility of average priority as a metric to monitor the network neutrality conformance, the Proportional Fair MAC scheduler, of the LTE model of NS-3[21] was used. In case of this algorithm, the perceived user throughput is compared to the channel quality index and a user is scheduled if the channel quality index is higher than the perceived user throughput. On the basis of the network model described in Figure 1, a set of n (n=20) users were associated to each of CP1 and CP2, with the ISP represented by the eNodeB or the base station. To simulate the non-neutral behavior of the ISP, the traffic originating from CP2 was throttled and the average priority over all users of CP1 and CP2 was monitored over time.

Part A	
Source Rate (S)	10 Mbps
Throughput	0.5-5 Mbps (Varied Dynamically
Maximum Packet Size	1024 Bytes
Simulation Time	20 seconds
Part B	
Number of UEs in each Set	20
Cell Radius	50 meters
Propagation Model	Friis Spectrum Propagation Model
Scheduling Algorithm	Proportional Fair
Mobility Model	Constant Position Mobility Model
Simulation Time	20 seconds

Table 1. Simulation Parameters

The results are shown in Figure 5. We can clearly see that although the average priority fluctuates periodically due to the proportional fair characteristics of the scheduler, the average priority over all users of CP2 is less than that of CP1 over time. This clearly indicates that the ISP is violating the net neutrality by giving higher priority to the traffic originating from CP1, as the quality of service perceived by the users of CP1 is higher than those of CP2. Hence, from the above results, we can clearly see that the proposed mechanism is effective in the net neutrality violation detection in both the wired and wireless scenarios. In addition, the proposed method provides a more robust mechanism as compared to just monitoring the average throughput or average packet loss rate over time.

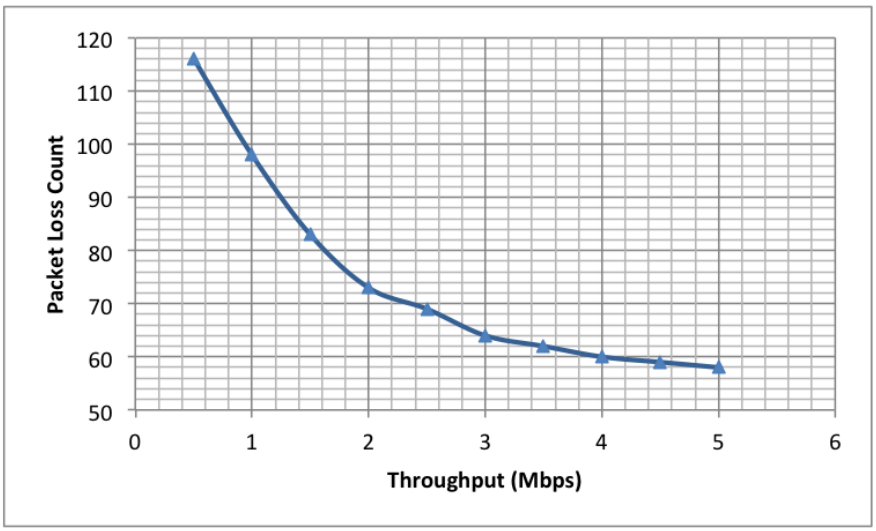


Figure 4. Packet Loss Count Vs. Throughput

5. Conclusion

Network neutrality is a an important issue for the development of policies and functioning of the future internet. In order to support the rapid growth and innovation, it is important to preserve the openness of the Internet, and hence, the net neutrality violation detection is a critical issue. In the current work, we focused on the technical aspects of network neutrality and proposed a simple framework for the monitoring the network

neutrality conformance by the ISP. We proposed a mechanism for detecting whether an ISP is discriminating between different content providers, by studying the packet loss trend when a large streaming media is transferred from the content provider to the end user via the ISP. In case of the wireless networks, there are additional challenges due to the time variant nature of such networks, and external factors such as interference and noise. In this case, the proposed mechanism is based on the scheduling information, in addition to the packet loss pattern at the base station.

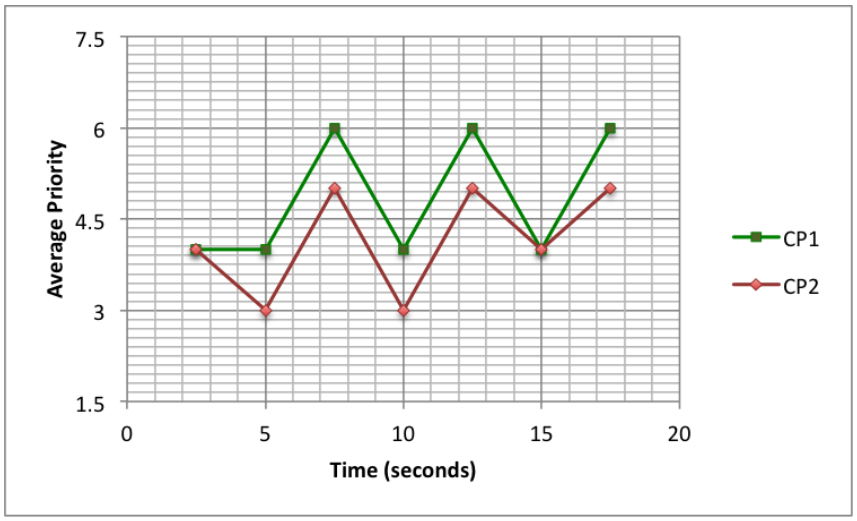


Figure 5. Average Priority Vs. Time for Two CPs

6. Acknowledgement

This work has been supported by the research project: Collaboration Platform Service Technology Development and Application (K-15-L01-C04-S03) of Advanced KREONET Centre, Korea Institute of Science and Technology Information (KISTI), Daejeon, Korea.

References

[1] B. Van Schewick, "Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like", 2014. Available: http://papers.ssrn.com/ sol3/papers.cfm abstractid=2459568.
[2] Fcc.gov, 'Open Internet', 2015, Available: http://fcc.gov/openinternet.
[3] Fei-Yang Ling, Shou-Lian Tang, Miao Wu, Ya-Xian Li and Hui-Ying Du, "Research on the net neutrality: The case of Comcast blocking," Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on , vol.5, no., pp.V5-488,V5-491, 20-22, Aug. 2010.
[4] S. Jordan, 'Implications of Internet architecture on net neutrality', ACM Transactions on Internet Technology, vol. 9, no. 2, pp. 1-28, 2009.
[5] Marcel Dischinger, Massimiliano Marcon, Saikat Guha, Krishna P. Gummadi, Ratul Mahajan and Stefan Saroiu, " Glasnost: enabling end users to detect traffic differentiation", In Proceedings of the 7th USENIX conference on Networked systems design and implementation (NSDI'10). USENIX Association, Berkeley, CA, USA, 27-27, 2010.
[6] Partha Kanuparthy and Constantine Dovrolis, "ShaperProbe: end-to-end detection of ISP traffic shaping using active methods", In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference (IMC '11),
[7] Mukarram Bin Tariq, Murtaza Motiwala, Nick Feamster and Mostafa Ammar, "Detecting network neutrality violations with causal inference", In Proceedings of the 5th international conference on Emerging networking experiments and technologies (CoNEXT '09), ACM, New York, NY, USA, 289-300, 2009.
[8] J.C. De Martin and A. Glorioso, "The Neubot project: A collaborative approach to measuring internet neutrality", IEEE International Symposium on Technology and Society (ISTAS 2008), pp.1-4, 26-28 June 2008.
[9] Y. Zhang, Z. M. Mao and M. Zhang, "Detecting traffic differentiation in backbone ISPs with NetPolice", In

Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference (IMC '09). ACM, New York, NY, USA, 2009.
[10] Y. Zhang, Z. M. Mao and M. Zhang, "Ascertaining the Reality of Network Neutrality Violation in Backbone ISPs", In Proceedings of 7th ACM Workshop on Hot Topics in Networks (Hotnets-VII), Calgary, Alberta. Canada, Oct. 2008.
[11] D. Miorandi, I. Carreras, E. Gregori, I. Graham and J. Stewart, "Measuring net neutrality in mobile Internet: Towards a crowdsensing-based citizen observatory," IEEE International Conference on Communications Workshops (ICC), pp.199-203, 9-13 June 2013.
[12] "Herdict: Help spot web blockages", Available: http://www.herdict.org.
[13] J. Crowcroft, "Net neutrality: the technical side of the debate: a white paper", ACM Computer Communication Review, 2007.
[14] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012-2017", Cisco Whitepaper, www.cisco.com.
[15] G. Song and Y. (G). Li, "Cross-layer optimization for OFDM wireless network: part I and part II", IEEE Trans. Wireless Commun., vol. 4, no. 2, pp. 614-634, March 2005.
[16] F. Kelly, "Charging and rate control for elastic traffic", European Trans. On Telecommunications, vol. 8, pp. 33-37, 1997.
[17] P. Hosein, "QoS Control for WCDMA High Speed Packet Data", IEEE Conference on Mobile and Wireless Communications Networks, Stockholm, Sweden, Sept. 2002.
[18] Ramneek. P. Hosein and Woojin Seok, "Load Metric for QoS-enabled cellular networks and its possible use in pricing strategies", 2014 IEEE Symposium on Wireless Technology and Applications (ISWTA), pp. 30-35, Sept.28-Oct.1, 2015.
[19] http://www.nsnam.org
[20] https://www.nsnam.org/docs/release/3.18/models/html/flow-monitor.html
[21] http://www.nsnam.org/docs/release/3.18/models/singlehtml/index.html# document-lte

Ramneek

She received B.Tech (Computer Science and Engineering) and M.Tech (Information Technology) from Guru Nanak Dev University (G.N.D.U) Amritsar, India in 2010 and International Institute of Information Technology (IIITB), Bangalore, India in 2013 respectively. She is currently a student researcher at Korea Institute of Science and Technology Information (KISTI), pursuing Ph.D. at the University of Science and Technology (UST), Daejeon, Korea. Her research interests include Networking and Communication (Congestion Management in Wireless and Cellular Networks, QoS and Pricing for Cellular Networks, Network Neutrality) and Cloud Computing (Openstack, IaaS, Cloud federation, Cloud Networking, SDN).

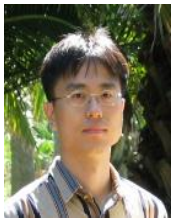
Patrick Hosein

He attended the Massachusetts Institute of Technology (MIT) where he obtained five degrees, a BSc degree in Electrical Engineering and one in Mathematics, an MSc degree in Electrical Engineering and Computer Science, an Engineer's degree and a PhD in Electrical Engineering and Computer Science.

He has worked at Bose Corporation, Bell Laboratories, AT&T Laboratories, Ericsson and Huawei. He is presently a Professor of Computer Science at the University of the West Indies, St. Augustine, Trinidad. He has published extensively with over 75 refereed journal and conference publications. He holds 38 granted and 42 pending patents in the areas of telecommunications and wireless technologies. His present areas of research include radio resource management, QoS and pricing for 5G cellular networks.

Wonjun Choi

He received his Bachelor's degree in Mathematics from Wonkwang University in 2006. He is currently enrolled in the integrated course in Grid and Supercomputing in the Korea University of Science and Technology. His research interests include Network Engineering, Network Communication, TCP, Cloud Federation, CCNx, NDN, SDN, and Computer Science.



Woojin Seok

He received B.E, M.S, and Ph.D. from Kyungpook National University, University of North Carolina at Chapel Hill, and Chungnam National Univerysity, respectively. He currently works for Korea Institute of Science and Technology Information(KISTI) Advanced KREONET center. He is also adjunct professor of University of Science and Technology(UST). He is a society member of KICS and KIPS, and also committee member of Future Internet Forum (FIF) Korea and Asia Pacific Network Operation and Management (APNOM). His interesting research areas are network testbed, federation, SDN, and so on.