Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-29

A New Adaptive Throughput Policing and Shaping Algorithm on Campus IP-based Network

[1,2] Murizah Kassim, [1]Mahamod Ismail and [2]Mat Ikram Yusof

***Abstract*— this paper presents the development of a new scheme called Adaptive Throughput Policing and Shaping (ATPS) algorithm to control internet inbound throughput and burst flow in a Campus IP-based network. Real live throughput collected from a Campus Network with Committed Access Rate (CAR) of 16 Mbps bandwidth speed are simulated and analyzed. New mathematical model with identified parameters on ATPS is derived. Adaptive throughput policies with burst shaping are simulated using Token Bucket theory control mechanism with 16 Mbps threshold policy. Three main adaptive policy conditions called P1, P2 and P3 which is controlled on 110%, 100% and 50% threshold rate are defined as filtered condition. Burst throughputs are shaped into next free bucket capacity for the next flow time. The throughputs are continuously shaped if the next bucket is full until free buckets are available. This new ATPS algorithm is numerically evaluated and analyzed on traffic performance which controlled the bandwidth and burst throughput. Performance results present reduced bucket capacity, reduced bandwidth rate in throughput transfer, no burst throughput and no byte loss in conforming traffic transferred in a network compared to previous implemented ATP algorithm, which held burst throughput and byte loss in the system.**

***Keywords*— Throughput, Internet Traffic, Quality of Service (QoS), Policing, Shaping, Bandwidth, Burst, IP-based Network**

I. Introduction

Quality of Services (QoS) in an IP-based network is an important task in network management. Large IP network may faces the reality of network performance which consists of heterogeneous network's traffic and large users' example like Campus University network. Research proved that unmanaged network traffics in IP-based network cause throughput burst and unreliable network performance especially with the used of heterogeneous protocols, heterogeneous applications and new IP protocols are used in the IP network [1]. Certain QoS issues which impact on traffic performance like flow of throughputs burst. The traffic performances have to be measured in order to support reliability and good network services. One of the scenario is studied in the environment of Campus University Network which faces the issue on controlling the HTTP traffic bandwidth used and measured gain which is subjected to traffic burst[2]. Upgraded internet

line speed is the solution but still the performance matter still occurs. A few methods like policing and shaping are developed in tackling problems on bandwidth management QoS issues especially on traffic performances [3], [4] .

Adaptive Traffic Policing (ATP) algorithm in an IP-based Campus network is developed to tackle traffic performance issues [5]. Performance result presents how bandwidth is saved, faster processing time and reduced the speed rates for byte transferred in the bucket system. But one condition exist during policing is byte loss or non-confirm byte transferred in the network system. In tackling the issue of byte loss and non-confirm byte transferred, therefore shaping algorithm is designed.

This paper presents a development of a new scheme called Adaptive Throughput Policy and Shaping (ATPS) algorithm to control internet inbound throughput and burst flow in a Campus IP-based network. Simulations and analysed are done on real live inbound internet traffics which are collected from a Campus Network with 16 Mbps Committed Access Rate (CAR) to the internet. Token Bucket theory control mechanism are used in both policy and shaping technique. Three main adaptive policy conditions called P1, which is controlled on 110% threshold rate, and P2, which is controlled beyond on 100% threshold rate and P3 which controlled on 50% threshold rate are defined as filtered condition. The three conditions are selected to compare the performance of the traffic. Identified burst throughputs are shaped into next free bucket capacity for the next flow time. The throughputs are continuously shaped if the next bucket is full, then process of shaping is continued until free buckets are available. New mathematical model is derived on the ATPS and numerically analyze the traffic performance. Traffic performance results presents reduced bucket capacity, reduced bandwidth rate in throughput transfer, no burst throughput and less byte loss in conforming traffic transferred in a network compared to previous implemented ATP algorithm.

II. Policy and Shaping

Policing in network traffic is one example of bandwidth management mechanisms in controlling any resource in the network especially network traffic. A good traffic policing scheme should make it easy for nodes inside the network to detect bad flows. Other method of traffic policing is to control

[1]Faculty of Engineering and Built Environment
Universiti Kebangsaan Malaysia
43600 UKM Bangi,Selangor,Malaysia

[2]Faculty of Electrical Engineering
Universiti Teknologi MARA
40450 UiTM Shah Alam, Selangor, Malaysia

bandwidth burst in a network. This activity is sometimes called policing the traffic flow or bandwidth management. Traffic policing detail process use token bucket mechanism which is one of the flow processes in resource management. Research presents traffic policing which identifies a policer that typically drops certain traffic [6]. For example, the network committed access rate (CAR) in IP based network rate-limiting policer will either drop the packet or byte or rewrite its IP precedence, resetting the type of service bits in the packet header or byte flow. One of traffic policing process uses token bucket mechanism which is one of the flow processes in traffic and resource management [7]. All conforming throughput that meets the policy requirement are stayed in the bucket. Bandwidth policing is implemented at various network protocols at a different standard network layers, examples like the packet layer [8].

The drawback of traffic policing is byte loss which non-confirmations of bytes transferred in the network. Thus, shaping algorithm is a method on bandwidth management where burst traffic are shaping or scheduling into next process. Benefit of shaping from policing is where byte or packets are still kept in the running process. Fig. 1 presents token bucket shaping method where burst byte are shape into next bucket. The bandwidths are saved in a time where burst or overflow traffic happened and being transmits or forward to next flow time traffic [9]. Shaping used the same token bucket mechanisms. Shaping responds to the identified traffic violations where usually no bytes or packets loss happened in a system [10]. When throughputs are burst, shaping will controlled the throughputs overflow and shapes it into next token tokens. Identified parameters are important in planning shaping scheme and best implementation can be done if evaluations on real traffic are analysed and examined.

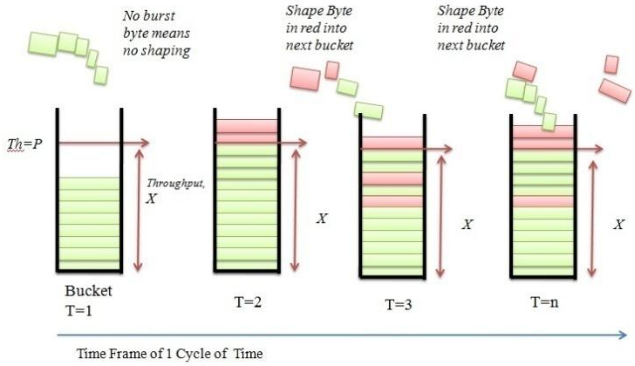

Fig. 1 Token bucket Transitions of Throughput Byte on Shaping

III. Methodology

This section presents method flow on policing and shaping algorithm on a real live IP-based throughput collected in a campus university.

A. *Method Flow*

Fig. 2 shows the proposed method for ATPS algorithm. The input of the model is the byte flow (MByte) inbound throughput of IP-based campus internet traffic. Policy condition is identified as P is chosen before traffic policing is derived on the traffic. Three selected policy conditions of P1, P2 and P3 are identified. P1 is throughput filtered with 110% on threshold, P2 is throughput controlled on threshold, and P3 is 50% throughput on threshold. Policy condition is applied once at a time where if P1 is selected, then all throughput will be applied with P1 conditions, and the same goes for P2 and P3. Real threshold implemented is at 16Mbps speed rate. All throughput tracers are policing and shaping into a bucket which used token bucket mechanism. Shaping is actives when there are bursts throughput in the network. Bursts throughput are forwards into the next available free bucket. Continues process on burst traffics is on until no burst traffics exist in the system. Performance evaluation is identified and present based on the three implemented policies with shaping process. Comparison on throughput performance also is present between real traffics, policing algorithm and shaping algorithm.

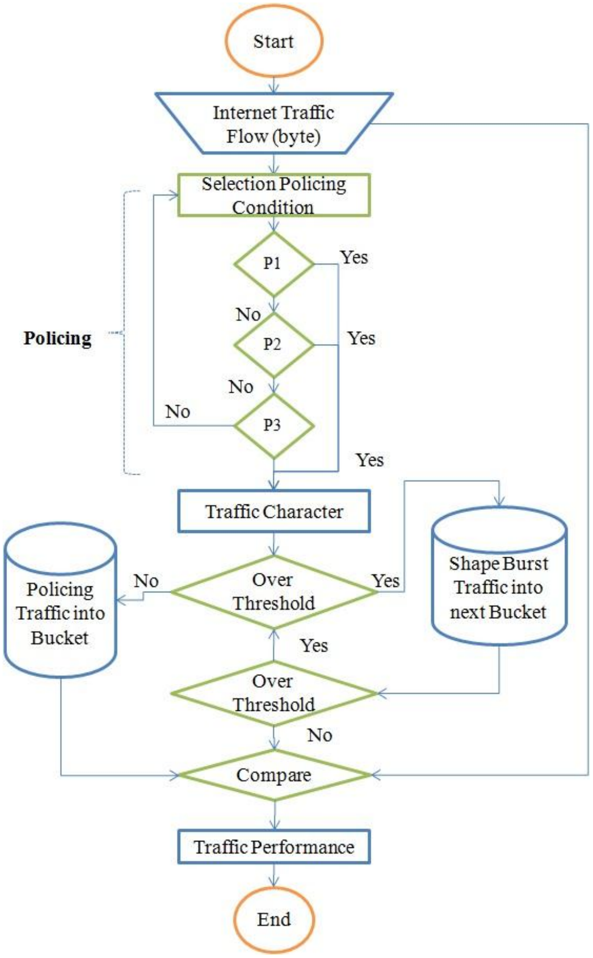

Fig. 2 Method on Policing and Shaping simulate on Live Internet Throughput

B. *Mathematical Model*

The new Adaptive Throughput Policy with Shaping (ATPS) Algorithm presents identified parameters used from the real traffic as in Table 1. These parameters are defined in mathematical model to simulate the new ATPS algorithm.

Table 1: Identified Parameters from Real IP-based Campus Internet Traffic

Parameter	Value
Committed Access Rate, Speed, *S*	16Mbps
Inter-Arrival Time, T_A	10 minutes
Daily and weekly Captured Time	00:00 to 23:50
Daily Tracers, *Cmin*	144 times
Real Live Traffic threshold, *Th*	1200MByte
Maximum Bucket *P1*	1140MByte
Maximum Bucket *P2*	1200MByte
Maximum Bucket *P3*	600MByte
Daily Minimum throughput	36.39 MByte
Daily Maximum throughput	2073.3 MByte
Daily Minimum Speed	0.49Mbps
Daily Maximum Speed	27.64Mbps

The real threshold which is the Committed Access Rate (CAR) and byte throughput per 10 minutes as identified in Eq. (1) also presents the policy threshold used in the algorithm.

$$B_{Max} = B_A \times T_A \quad (1)$$

$$Bmax = \frac{16 \times 1000000\ bps \times 10\ min \times 60\ second}{8\ bits}$$

$$=1200000000 \text{ byte}$$

$$=1200 \text{ MByte}$$

Based on real tracers captured, every 10 minutes throughput captured are put into traffic buckets as in Eq. (2). Minimum and maximum throughputs are identified as traffic functions scope in modelling ATPS.

$$\sum_{i=1}^{n} Bk = \sum_{i=1}^{n} x, 0 < x < Cmin \quad (2)$$

Eq. (3) is the new mathematic algorithm in policing and shaping. The existence of burst traffic in the first time bucket is forwards to the next buckets. This process called throughput shaping. The process is continued if the next bucket is full and process is continued until free available bucket is reached.

$$\sum_{i=1,j=1}^{n,m} Bkn = \begin{cases} \displaystyle\sum_{i=0,j=1}^{n,m} \begin{matrix} x_1 = x_1 - p_j y, \quad 0 < x < C_{Min}, B_{Min} < y > B_{Max} and x > py \\ (x_{i+1} + (x_i - p_j y), 0 < x < C_{Min}, B_{Min} < y > B_{Max} and x > py \end{matrix} \\ x_i, 0 < x < C_{Min}\ and\ x < py \end{cases} \quad (3)$$

Process time is identified as P_{T1} referred how long the byte in the bucket is transferred to the other bucket. The process time depends on how large the byte flow in the bucket. Thus total of process time is as Eq. (4) which is the existing bucket and before policing and shaping. Eq. (5) present the process time after policing and shaping. Shaping algorithm avoid byte loss compared to policing algorithm unless the throughput is too large to fits into next free bucket. If the throughput is too large possibility the next bucket is full all the time. This algorithm simulated based on the 144 tracers. Assuming the last bucket is transferred into the next cycle time.

$$\sum_{i=1}^{n} P_{T1} = \frac{\sum_{i=1}^{n} Bk \times S}{z} \quad (4)$$

$$\sum_{i=1,j=1}^{n,m} P_{T2} = \frac{\sum_{i=1,j=1}^{n,m} Bkn \times S}{z}, 0 < x < C_{Min}, B_{Min} < y > B_{Max}\ and\ x > py \quad (5)$$

IV. Analysis and Result

Analysis and result compares between real throughput, policing and shaping performance based on real collected campus traffic.

A. *Real Live Throughput Analysis*

Fig. 3 presents the throughput traffic in a day where 144 tracers data traffic are captured. The red plotted graph shows that burst traffics exist in the internet inbound flow. Fig. 4 presents the histogram distributions on daily throughput where burst traffics are identified in the network which goes beyond 16 Mbps rate which is 1200 Mbyte or 1.2Gbyte. The minimum and maximum throughput is identified as 36.39 Mbyte/0.49Mbps and 2073.3 Mbyte/27.64Mbps.

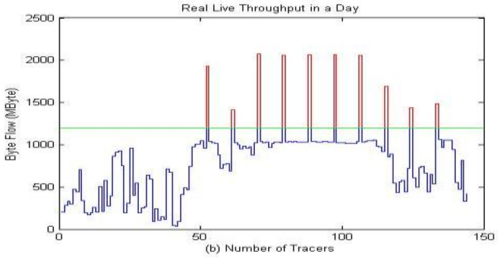

Fig. 3: Real Live Daily Throughput

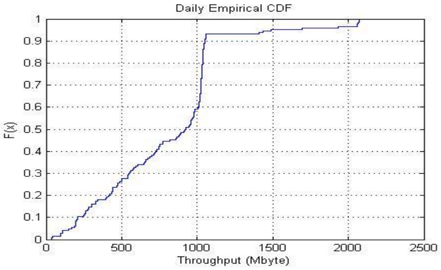

Fig. 4: Real Live Daily Throughput Distribution

B. *Performance after Policing*

Fig. 5 (a) – (c) presents comparison on real live throughput policing at 110%, 100% and 50% on threshold of 16Mbps or 1200Mbyte. The red graph presents the burst traffic which are policing and bandwidth is kept. Thus, time processing is reduced after policing implementation. Performance on policing P1, P2 and P3 are compared in processing time and bandwidth Save. Fig 6 shows comparison of reduced process time between (a) real traffic without policing and after policing in Fig.6 (b) – (c). Without policing present high process time which is longer compared to P1, P2 and P3. P3 presents the fasters processing time in throughput transfers in the network system. Fig. 7 presents the comparison of bandwidth save (a) Real Throughput and after policing (b) – (c). There is no bandwidth save before policing compared to P1= 67.82, P2=83.82 and P3=561.4 Mbps. P1 shows less bandwidth saved compared to P2 and P3. P3 shows the highest bandwidth save compared to all.

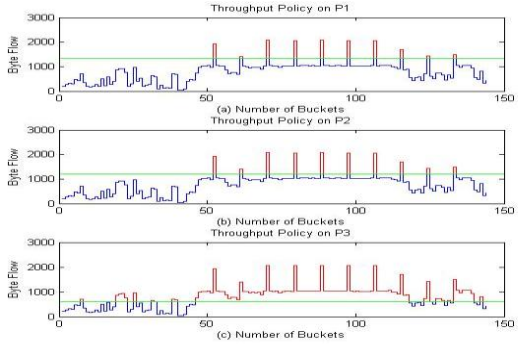

Fig.5 Policing On Throughput (a) P1 (b) P2 (c) P3

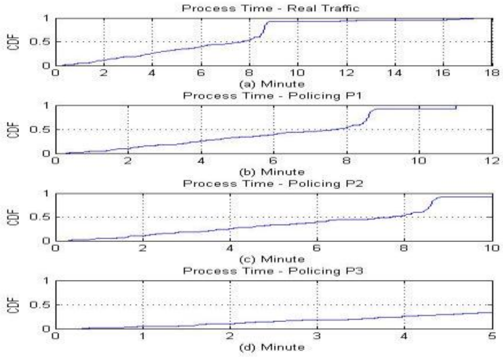

Fig. 6 Reduced Processing Time (a) Real Traffic (b) P1 (c) P2 (d) P3

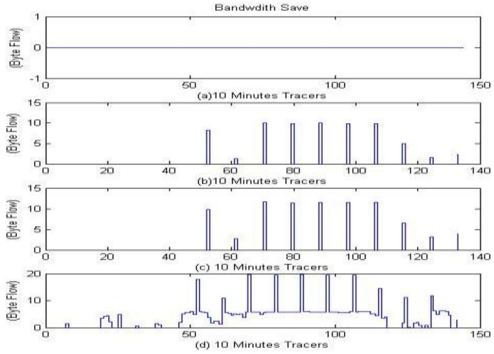

Fig.7 Bandwidth Save after Policing (a) Real Throughput (b) P1 (c) P2 and (d) P3

Figure 8 shows comparison on byte loss with policing throughput on P1, P2 and P3 condition. P1 shows the lowest byte loss compared to P3 which has the highest byte loss.

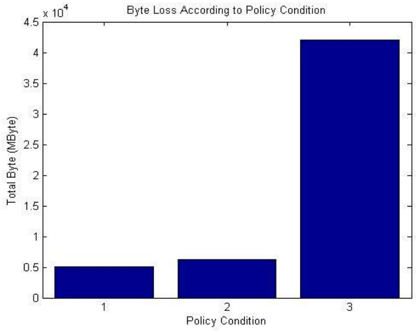

Fig.8 Comparison of Byte Loss after Policing between P1, P2 and P3

C. *Performance after Shaping*

Fig. 9 (a) presents the policing and shaping burst traffic into next buckets when burst traffic exists at previous time bucket with P1 condition. Fig. 9 (b) presents all buckets capacity after shaping process. The maximum rate possible to pass through is controlled to 1320 Mbyte/17.6Mbps compared to policing throughput where those byte losses are saved 100% when shaping take place. Fig. 10 (a) presents the policing and shaping burst traffic into next buckets with P2 policing and shaping condition. All buckets capacity on after P2 are controlled to 1200 MByte/16Mbps speed rate. Byte losses are also saved 100% when shaping take place. All throughputs are transferred with P1 and P2 which total process time before and after policing is 962.23 minutes and 0 byte loss.

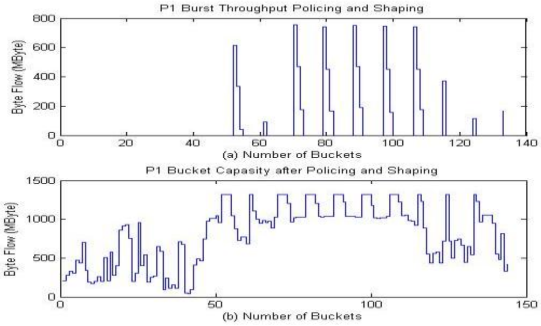

Fig. 9PS on P1 (a) Burst PS Throughput (b) Bucket Capacity after PS

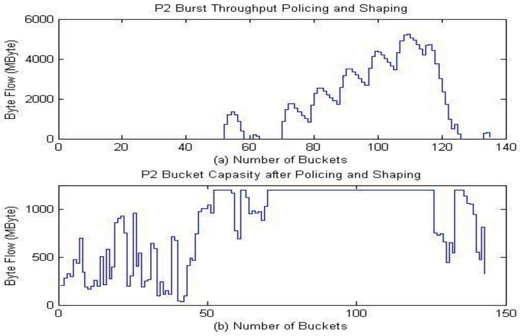

Fig. 10 PS on P2 (a) Burst PS Throughput (b) Bucket Capacity after PS

Fig. 11 (a) presents the P3 policing and shaping on burst traffic into next buckets and Fig. 11 (b) presents all buckets

Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-29

capacity after shaping process at P3 where maximum throughput in buckets are at 600MByte/8Mbps only. Fig. 11(c) shows those byte losses are saved into next bucket when shaping take place. Seems the policy P3 condition is about 50 % of the threshold, there are more burst traffics to police and shapes. With condition shaped to the next available bucket presents that they are still byte loss but smaller burst traffic exist. P3 present reduced byte loss in 10% from previous policing condition. Fig. 12 shows all byte loss with P1, P2 and P3. No byte loss happened in P1 and P2 with same total process time. P3 identified of 10% reduced burst throughput compared to Fig. 8. Thus, policing and shaping helps guarantee of transferred throughput in certain threshold condition with same process time or reduced process time. Both policing and shaping controlled byte flow and speed which produced better performance in the network system.

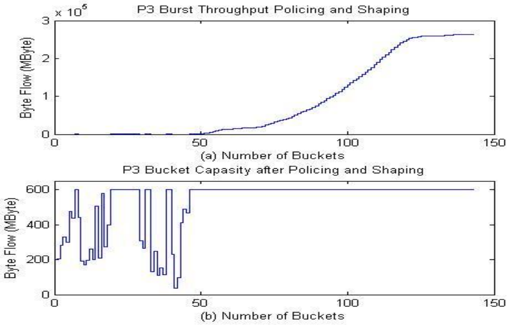

Fig. 11 PS on P3 (a) Burst PS Throughput (b) Bucket Capacity after PS

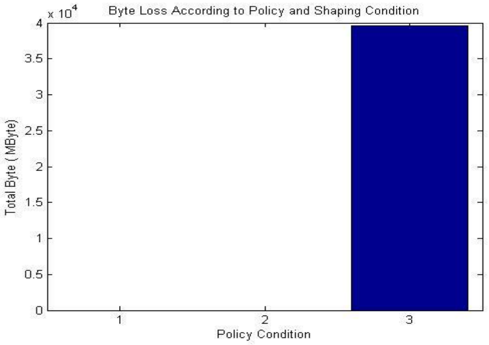

Fig.12 Comparison of Byte Loss after Policing and Shaping between P1, P2 and P3

V. Conclusion

This research presents a new scheme called Adaptive Throughput Policy and Shaping (ATPS) algorithm to control internet inbound throughput and burst flow in a Campus IP-based network. Successfully simulations and analyzed on real internet traffic are done with new driven mathematical ATPS model. Token bucket theories mechanisms are used with three policy implementations called P1, P2 and P3. Both conditions are compared on traffic performance which controlled the bandwidth and burst throughput. Traffic performance results present reduced bucket capacity, reduced bandwidth rate in throughput transfer, no burst throughput, no and less byte loss in conforming traffic transferred in a network compared to rela traffic characterization and previous implemented ATP algorithm, which held burst throughput and byte loss in the system.

Acknowledgment

Authors would like to thank Universiti Kebangsaan Malaysia, for support grant number LRGS/TD/2011/UKM/ICT/02/02 for this research. Authors also would like to express deep appreciation to Ministry of Education Malaysia (MOE) and Universiti Teknologi MARA for the financial funds and supports for the research student.

References

[1] Y. Won, M. J. Choi, B. Park, and J. W. K. Hong, "An approach for failure recognition in IP-based industrial control networks and systems," *International Journal of Network Management,* vol. 22, pp. 477-493, 2012.

[2] M. Kassim, M. Ismail, K. Jumari, and M. I. Yusof, "Bandwidth gain analysis for HTTP and HTTPs traffic on IP based network," in *Wireless Technology and Applications (ISWTA), 2012 IEEE Symposium on*, 2012, pp. 303-308.

[3] K. Kim, D. Niculescu, and S. Hong, "Gateway strategies for VoIP traffic over wireless multihop networks," *KSII Transactions on Internet and Information Systems,* vol. 5, pp. 24-51, 2011.

[4] J. Liu, P. Gao, J. Yuan, and X. Du, "An Effective Method of Monitoring the Large-Scale Traffic Pattern Based on RMT and PCA," *Journal of Probability and Statistics, Hindawi Publishing Corporation,* vol. 2010, 2010.

[5] M. Kassim, M. Ismail, M. I. Yusof, and A. Idris, "A New Adaptive Throughput Policy Algorithm on Live Internet Traffic of IP-based Network," *Submission to be published in 'Journal of Computer Networks and Communications', In Review Progress.*, July 2014.

[6] E. Vayias, J. Soldatos, and G. Kormentzas, "Traffic shaping based on an exponential token bucket for quantitative QoS: implementation and experiments on DiffServ routers," *Computer communications,* vol. 29, pp. 781-797, 2006.

[7] Y. Dashdorj, N. Chuluunbaatar, B. Batzul, and S. Lee, "Characteristics of the token bucket parameters with self similar network traffic," in *Strategic Technology (IFOST), 2010 International Forum on*, 2010, pp. 198-202.

[8] C. Caini and R. Firrincieli, "Packet spreading techniques to avoid bursty traffic in long RTT TCP connections [satellite link applications]," in *Vehicular Technology Conference, 2004. VTC 2004-Spring. 2004 IEEE 59th*, 2004, pp. 2906-2910 Vol.5.

[9] D. S. Daian and D. H. Giura, "Traffic shaping and traffic policing impacts on aggregate traffic behaviour in high speed networks," in *Applied Computational Intelligence and Informatics (SACI), 2011 6th IEEE International Symposium on*, 2011, pp. 465-467.

[10] D. D. Simion, "Traffic Shaping And Traffic Policing Impacts On Aggregate Traffic Behavior In High Speed Networks," *International Journal of Advanced Computer Science,* vol. 2, 2012.