http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (17): 2632-2644, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.2632.2644

Adaptive Throughput Policy Algorithm with Weibull Traffic Model for Campus IP-Based Network

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

Abstract: This study presents a new Adaptive Throughput Policy algorithm with Weibull (ATPWT) Traffic Model. Real live inbound internet throughput from IP-based campus network which supports 16 Mbps Committed Access Rate (CAR) is collected. Throughputs are fitted with four best Cumulative Distribution Function (CDF) which are Normal, Lognormal, Exponential and Weibull. Maximum Likelihood Estimator (MLE) technique is used to measure the best CDF fits which presents the maximum log-likelihood. Analysed throughput found that Day 1 and Day 7 present the minimum and maximum log-likelihood, respectively. A fitted 2-parameter Weibull distribution is identified as the best fit which produced new parameters: Scale, α and shape, β. These parameters are simulated as Weibull traffic model in the ATPWT algorithm. ATPWT performances on min-max MLE produces larger bandwidth saving, reduces bucket capacity and faster processing time. Burst traffic controlled in the system is derived with five different Weibull shape, β parameter. Larger value of shape, β produces less burst traffic while smaller shape, β parameter produces larger burst in the system. Thus, ATPWT algorithm derives burst controlled and better performance on internet throughput traffic for IP-based campus network in this research.

Key words: Throughput, policy, internet, traffic model, Weibull distribution, algorithm, burst, bandwidth management, IP-based network

INTRODUCTION

Traffic modelling in network and engineering communications is gradually being an important research focus. Internet traffic research by analysing and understanding the features of network traffic models are becoming a concerned environment in forecasting the real network situation (Garsva *et al.*, 2014). Not only development of new scheme on traffic management is important but also the identification of best traffic model seems a basic requirement for accurate capacity planning in network communication (Karagiannis *et al.*, 2004). Various network traffic communications which occur in the network produce high volume of traffic capacity and different characteristics exist in the traffics. Among the mechanisms that contribute to high volume of traffics are high user's density, user's ethic in network communication, use of new technology on various network tool, orientation with new applications in the system, network architecture design, virus attacks from internet or intranet and Quality of Service (QoS). QoS are the regular issues in network communications where some network managements are recognized with the real situations in their own network (Pavlou, 2004; Xiaolong *et al.*, 2012). Fast development of network technology either in hardware, software or application medium produce the network traffic challenge where huge traffic needs huge bandwidth capacity. Research presents that high bandwidth used is due to the increase of new technology and new applications especially internet applications. These reasons also contributes to burst traffic and slow accessing (Schudel, 2013; Ahn *et al.*, 2013). Thus, certain network becomes unreliable and traffic congestion occurs. A broad network with huge clients is possible to risk with high traffic load without proper QoS. Thus, bandwidth management is one of the QoS to control throughput in network management (Kassim *et al.*, 2012). There are some network management which are implemented namely users blocking, routers scheduling or embedded with network bandwidth controlled machine but bursting of network traffic still happens (Kassim *et al.*, 2014). This study

Corresponding Author: Murizah Kassim, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

presents that bandwidth management is needed where burst traffic existed in real IP-based network traffic. In order to overcome the problem, some organizations just upgraded their internet line or Committed Access Rate (CAR) with higher bandwidth. Burst traffic and high load bandwidth are examples of bandwidth being gradually upgraded in an IP-based network.

In a broad area of network communications, policing traffic is implemented in many network approaches or techniques. Policing traffic is identified as one technique for bandwidth management which supports the Quality of Services (QoS). Other policing schemes or techniques may be implemented at various network areas such are blocking virus or bad flows, policing on unwanted traffic based on certain criteria, controlled certain traffic, bandwidth controlled, IP-route management, applications blocking and network level policing. Policing techniques or scheme usually control certain identified resource in presenting better performance in a network. One of the examples of better network performances in policing technique is bandwidth saved and delay avoided but certain traffics are dropped. Enhancement of traffic policing is traffic shaping where certain traffics are dropped with policing but shaping takes actions to transmit the dropped traffic into next submission time in a network (Vayias *et al*., 2006). One example of bandwidth policing is identified which implements a packet layer policing in network communication (Caini and Firrincieli, 2004). Bandwidth management or policing on throughput is implemented at byte flow or rate controlled in a network.

This study presents a new Adaptive Throughput Policy with Weibull Traffic Algorithm (ATPWT) based on real live internet throughput for campus IP-based network. First, four best Cumulative Distributions Functions (CDF) which are Normal, Lognormal, Exponential and Weibull are fits to real live traffic by using Maximum Likelihood Estimator (MLE) technique. The CDF Weibull is identified produce the maximum log-likelihood among the four distributions. The analysed traffic has identified fitted 2-parameter CDF Weibull which is scale, α and shape, β. Both parameters are derived and simulated in the new ATPWT and analysed. Result on traffic performances are presented in larger bandwidth save, lower bucket capacity and faster processing time. ATPWT derives burst traffic controlled in the system where larger value of shape, β produces less burst traffic and vice versa. This new model presents new performance on throughput controlled which based on real traffic implemented in campus IP-based network. With this new traffic fits also useful for future prediction of tele-traffic models.

TRAFFIC MODEL STATISTICAL ANALYSIS AND POLICY

Traffic modelling is an important role in identifying and understanding the features of dynamic demands by stochastic or random processes. Accurate traffic models may represent the real situations of real network traffic. Thus, this helps service providers to proper maintain and forecast the Quality of Service (QoS) in a network. Many traffic models are developed based on traffic measurement data and how to improve its performance in a network such as analysis on time distributions (Garsva *et al*., 2014; Choi *et al*., 2014), performance measures on heavy tails (Ramaswami *et al*., 2014), traffic models evaluation (Chandrasekaran, 2009) and traffic predictions (Sang and Li, 2002). Research presented that concepts and requirements of Quality of Service (QoS) and traffic modelling is rapidly changed. Thus, traffic modelling is an important aspect to be considered to meet QoS requirements of services and efficient utilisation of network resources and management. Statistical analysis on identifying real traffic model is also a crucial research area in tele-traffic engineering. Mathematical concept is proved with traffic theory where it is taken as one of the methods in evaluating real traffic data. Previous research presented that Poisson traffic model are used but it failed or becomes inadequate model in certain internet traffic simulations (Karagiannis *et al*., 2004; Willinger *et al*., 1998). Some new traffic distribution is identified as self-similarity process with Weibull Long Range Dependent (LRD) (Thakur *et al*., 2013; Ramaswami *et al*., 2014) and Pareto traffic model (Garsva *et al*., 2014). In probability theory and statistics, the Weibull distribution is a continuous probability distribution. There are a few Weibull properties in evaluating data which depended on certain parameter values (Shuhong *et al*., 2014; Huang *et al*., 2009). Such Weibull properties example like analysis on density which used Probability Density Function (PDF) or analysing hazards to calculate errors in data. This research uses CDF Weibull with two value parameters, scale, α and shape β. Equation 1 presents the mathematical equation for CDF Weibull with two important WT parameters, F (x; α, β):

$$F(x; \alpha, \beta) = \begin{Bmatrix} 1 - e^{-\left(\frac{x}{\alpha}\right)^{\beta}}; x \geq 0 \\ 0; x < 0 \end{Bmatrix} \tag{1}$$

Many estimators on fit distributions theories are developed based on mathematical calculations. MLE is one of the identified methods in fitting theories based on

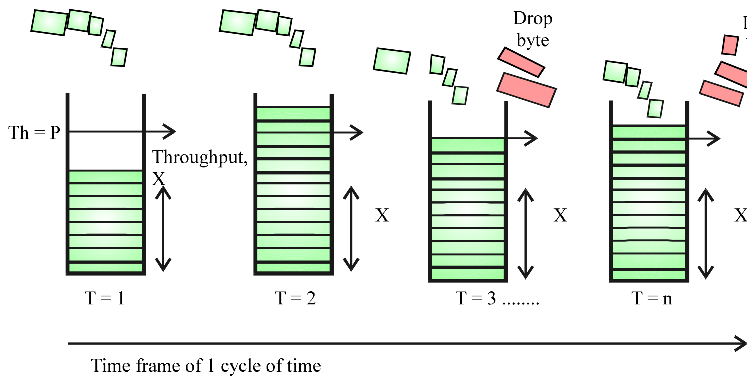

Fig. 1: Token bucket transitions of throughput on policy

identified maximum log-likelihood value. A few researches in many areas have utilised this MLE method in their implementation method which are proved with successful results (Cao *et al*., 2008; Gu *et al*., 2005). Maximum Likelihood Estimation (MLE) is a procedure of finding the value of one or more parameters for a given statistic which makes the known likelihood distribution maximum. Example MLE for a parameter mu is denoted as max-mu (Weisstein, 2014; Myung, 2003; Harris and Stocker, 1998).

Policing in network traffic is one example of bandwidth management mechanisms in controlling any resources in the network especially network traffic. A good traffic policing scheme should make it easy for nodes inside the network to detect bad flows. This activity is sometimes called policing the traffic flow. One of traffic policing process uses token bucket mechanism which is one of the flow processes in traffic and resource management (Dashdorj *et al*., 2010). Figure 1 presents the Token bucket Transitions of Throughput, X on Policy. Threshold, Th acts like the CAR service rent by an organization. Thus, Th is the maximum possible transmission rate in bytes/second or identified as Policy, P. The maximum burst time is the time where the rate of throughput, X is fully utilized. Bytes as token are discarded from the bucket if it goes beyond the threshold, Th or policy, P and per Bucket size, B_K. The incoming throughput is put in bucket according to identified policy condition, P. All conforming throughput that meets the policy requirement are stayed in the bucket.

Other mechanisms of bandwidth management are shaping and scheduling which differ in the way they respond to the identified traffic violations (Simion, 2012). Traffic policing identifies certain technique to block or police certain traffic which typically drops the unwanted traffic or above certain rate threshold (Vayias *et al*., 2006). Policing traffic mechanism helps to improve traffic performance in network. Policing on speed or rate controls is a techniques uses in bandwidth management. Certain bandwidth is by limiting or controlling within the traffic. Many researchers presented the improved performance on bandwidth management. This study identifies a continuing research needs as new traffic features and technology used shows a burst rate on speed from time to time.

MATERIALS AND METHODS

Figure 2 presents the methodology flow of the new Adaptive Throughput Policy with Weibull Distribution (ATPWT) algorithm modelling that fits with the real live internet traffic. Daily internet traffic is collected in 7 days and traffic is fitted with the best existing theory distribution which is Normal, Lognormal, Exponential and Weibull. Maximum Likelihood Estimator (MLE) is used to fit all theories and identified maximum log-likelihood is chosen as the best result. Weibull is identified as the best fit distribution with the real live data that presents two mains Cumulative Distribution Function (CDF) parameter which is the Scale, α and Shape, β. Among the best MLE log-likelihood, day 7 Weibull is identified the best fitted CDF. Besides that two days comparison between minimum and maximum MLE log-likelihood is identified. The fitted 2-parameter Weibull is used as random distribution or traffic model in the new algorithm called Adaptive Throughput Policy with Weibull Traffic (ATPWT).

Figure 3 presents the ATP method which is adapted in ATPWT. Three policies conditions are applied according to percentage level filtering on implemented threshold. The new ATPWT derives sample on one policy condition as real implementation for Committed Access Rate (CAR) in real network situations. Token bucket theory is used in the policing algorithm. New mathematical model on the new ATPWT is presented according to

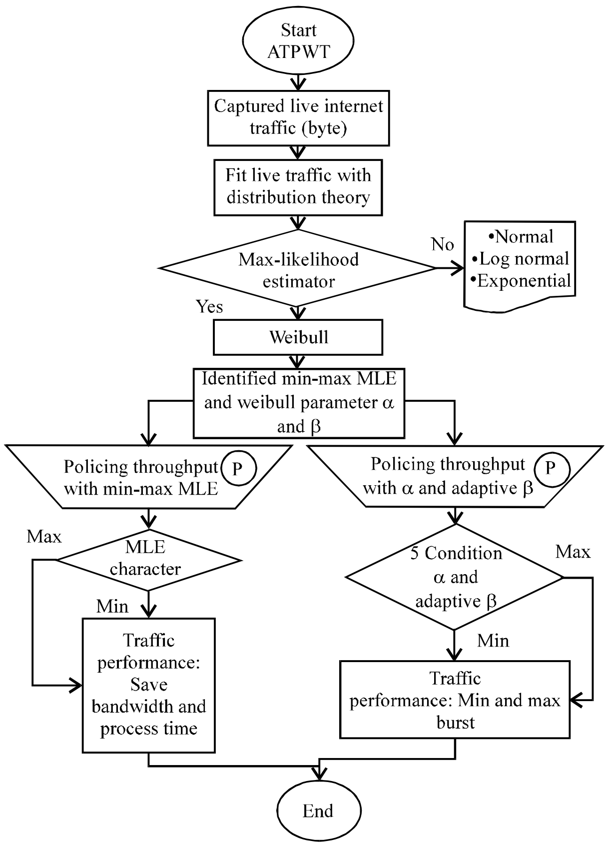

Fig. 2: Method flow on ATPWT

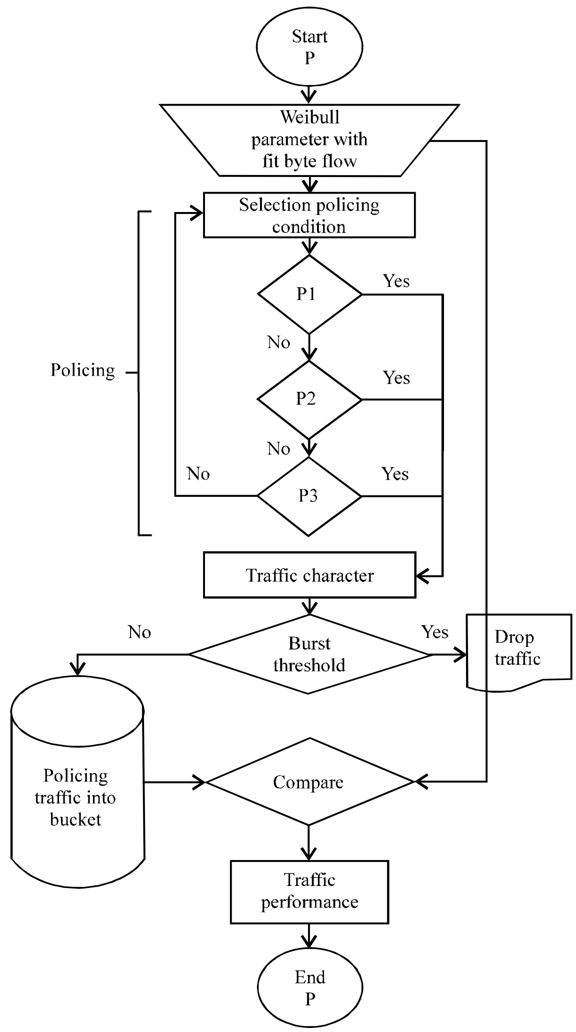

Fig. 3: Adaptive policy on throughput flow

police implementation and evaluation on the traffic performance. The performance evaluation result is derived by presenting bandwidth save, processing time and burst throughput traffic between the two identified days selected which is day 1 and day 7. Comparison on performance with control burst traffic is also identified based on Weibull fit parameter scale, α in five difference conditions of parameter shape, β.

Analysis on real internet traffic: Distribution on Daily Internet Traffic has identifies two conditions which is burst traffic and fitted CDF. Real live internet traffic throughput is identified as byte flow, B_T. Allocation bandwidth, B_A Committed Access Rate (CAR) is 16 Mbps and Inter-arrival Time, T_A is captured in every 10 min traffics throughput. Throughput captures time started at 00:00 to 23:50 on each day. One day traffic tracers are 144 times and 7 days captures traffic tracers are accumulated to 1008 times. Equation 2 presents the equation for Max throughput, B_{Max} for the byte flow collections in 10 min time with Bandwidth Speed, B_A at 16 Mbps. This maximum throughput per time is taken as Bandwidth threshold, B_{TH} in the new Adaptive Throughput Policy with Weibull Distribution (ATPWT) algorithm.

$$B_{max} = B_A \times T_A = 1200 \text{ MByte} \tag{2}$$

Empirical CDF throughput: Figure 4 shows daily live internet traffic which is captured in 7 days. Every tracer shows in the figure presents 10 min time which derives the throughput traffic in MBytes. Traffic shows burst exists in captured real live traffic where throughput goes beyond the CAR rate, 16 Mbps which is 1200 MByte threshold. Figure 5 presents the comparison of Cumulative Distribution Function (CDF) on seven daily real live throughput traffics. The graph presents the difference of empirical CDF plots for throughput rate at each tracer. All days traffics are measured using the Maximum Likelihood

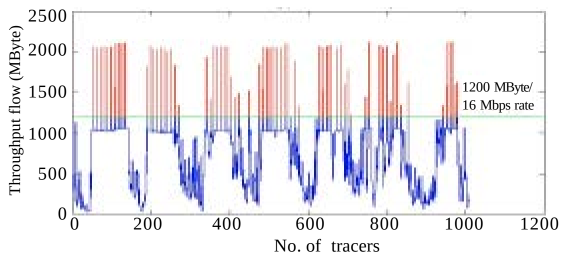

Fig. 4: Real live throughput internet traffic in 7 days

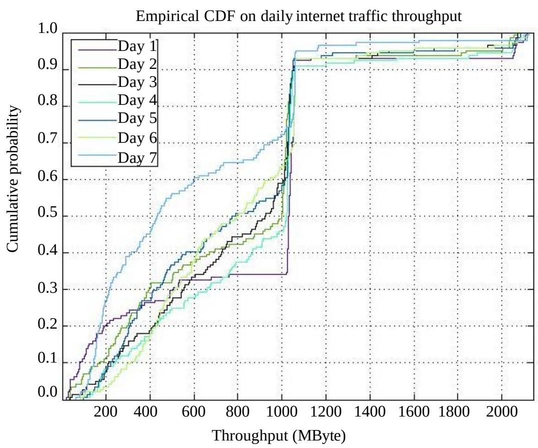

Fig. 5: Comparison on 7 days empirical CDF throughput

Estimators and log-likelihood is identified. Parameters are presented based on best fits CDF distribution to implement in Adaptive Throughput Policy with Weibull Traffic (ATPWT) algorithm.

Captured real live throughputs are fitted to the best four CDF distributions to identify the best fits for traffic model. Figure 6 shows an example of day 1 CDF distribution fits to the four best distributors. Among many distribution theories that fit to this throughput, the identified 4 best distributions are Normal, Lognormal, Exponential and Weibull distribution. MLE is used to identify the best distributions which among four distribution.

Maximum likelihood estimation: Table 1 presents MLE with log-likelihood of day 1 to day 7 traffics for four difference distribution. Maximum value of log-likelihood is the best result that fits to the live traffic. Tabulated log-likelihood value presents that all the values are in negative points. Therefore, the best log-likelihood is the value which is nearest to 0. From the derived table, Weibull distribution is identified as the best fit which shows the maximum log-likelihood among Normal, Lognormal and Exponential in day 1 to day 6. However, only day 7 shows the best fits on Lognormal which present maximum log-likelihood which is -1050.93. It is only 1.03 point different from the Weibull maximum log-likelihood. Because of the small different for a day, this research identifies the best result for best fit is Weibull distributions. Thus, analysis traffic shows day 1 is the minimum MLE log and day 7 is the maximum MLE log-likelihood values. Both these two days are taken as sample to run the new ATPWT algorithm. Thus, fitted 2-parameter Weibull is identified in simulating a new ATPWT for both days.

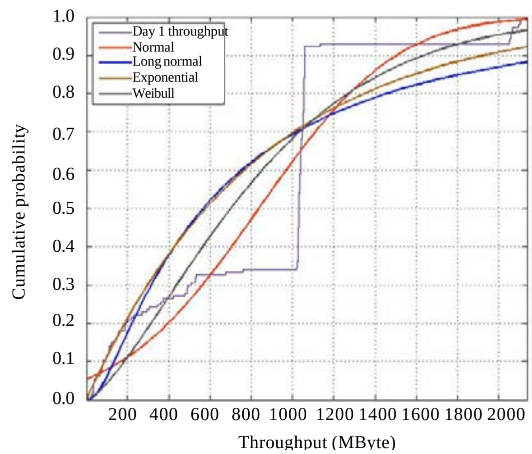

Fig. 6: Empirical CDF day1 throughput fit to four best distributions

Weibull CDF: Figure 7a and b present the comparison of real live internet traffic on day 1 and day 7 which fits to Weibull distributions after the maximum log-likelihood for MLE is identified. With minimum MLE log as in Fig. 7a shows there is quite a high range of difference to real live empirical CDF traffic compared to Fig. 7b which shows the fit Weibull distribution is close to real live empirical CDF traffic. After analysed the fitted throughput, important 2-parameter CDF Weibull are identified whcih are the scale, α and shape, β. This parameter is used as Weibull traffic distribution model on the Adaptive Traffic Policy algorithm.

ATP mathematical model with identified Weibull traffic: This section presents the mathematical model for ATPWT whcih is based on fitted 2-parameter values of Cumulative Distribution Function (CDF) for Weibull Traffic (WT) as the incoming throughput. Parameter Scale, α and Shape, β are presented. Real live internet traffic, x is used as scheme values with the fitted distribution. Token bucket theory is used in simulating the algorithm.

Table 1: Comparison of MLE log on daily throughput internet traffic

Parameters	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
Normal	-1104.95	-1091.96	-1076.00	-1083.68	-1082.40	-1071.78	-1081.58
Lognormal	-1133.39	-1107.83	-1093.73	-1093.75	-1076.50	-1068.98	-1050.93
Exponential	-1113.23	-1103.10	-1107.44	-1118.52	-1099.15	-1104.79	-1061.50
Weibull	-1102.92	-1084.17	-1071.37	-1077.83	-1069.42	-1061.98	-1051.96

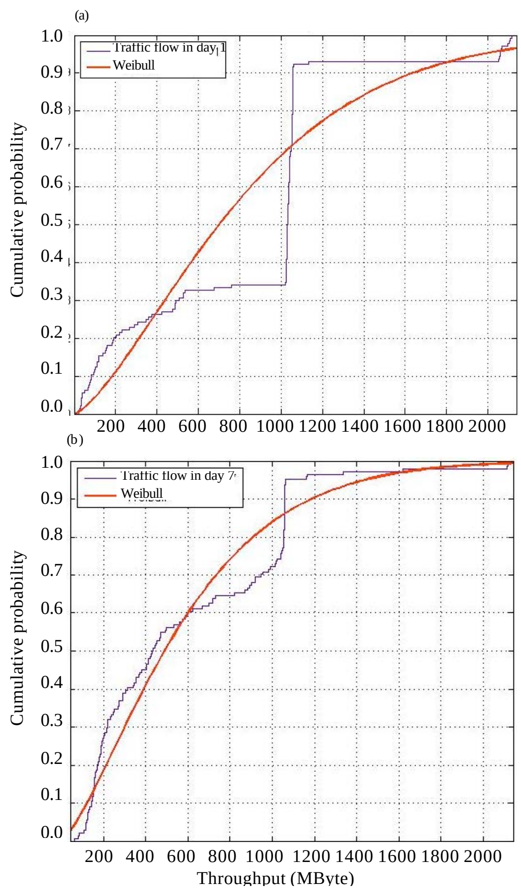

Fig. 7(a-b): Weibull distribution CDF fit to real live traffic (a) Day 1 and (b) Day 7

Modeling parameter identification: Table 2 presents the identified modelling parameters based on the throughput captured including with the fitted 2-parameter Weibull for day 1 and day 7 which is scale, α and shape, β. Performance comparison based on the new implementation of ATPWT algorithm is compared between the two days.

Mathematical model: Mathematical model with ATPWT algorithm is derived. Performance analysis on the new algorithm is produced a mathematical model on larger bandwidth, reduced processing and comparison of burst traffic control on the scalar of parameter α and β used in the model. The real bandwidth threshold, B_{Th} is used in the simulation. Maximum throughput, B_{max} is taken as value of maximum Bucket Size, B_{KMax}. ATPWT presents sample used on one policy condition, p_1B_{Max} which acts exactly like the real live implementation in the campus network. ATPWT algorithm simulates condition when the throughput traffic larger than the policy condition, p_1B_{Max}, than throughput is filtered or cut-off. The incoming throughput, are put in bucket with bucket capacity as bucket size, B_k. B_k is the original bucket size before policy implementation. New traffic after policing is put in new bucket, B_{Kn}. Maximum bucket is identified as BK_{Max}. Equation 3 presents the total of bucket size, B_k in a daily cycle, D_t. Let's, throughput, $B_T = F(x; \alpha, \beta)$ which uses two parameters Weibull CDF. In formulating the mathematical model, symbols are address as Bandwidth allocation, B_A = Z, Speed, S, Policy Condition = P and bandwidth threshold, B_{TH} = Y for all presented equations. Algorithms models the Bucket Size, B_K according to real live parameter throughput captured, B_T. Daily inter-arrival, D_t time is from i to n which is 114 times.

$$\sum_{i=1,\, j=1}^{n,\, m} Bk = \sum_{i=1,\, j=1}^{n,\, m} 1-e^{-\left(\frac{x_i}{\alpha_j}\right)^{\beta_3}}, \; x\geq 0 \qquad (3)$$

Equation 4 derives a mathematical model on ATP algorithm based on Weibull Traffic. Policing action derives the total throughput and put in a new bucket as bucket size, B_{kn}. Daily throughput numbered from i to n is processed with policing according to p_1B_{Max}. The equations present a condition where B_T is filtered and if B_T is found under policy threshold which is py than it is put in B_{kn} and if B_T which is greater than policy threshold, py and then it is put in a new bucket, B_{kn}. This model also controls traffic burst by using the different value of Shape, β by using the token bucket mechanism for bandwidth management. Performance result also presents burst and bandwidth controlled:

$$\sum_{i=1,\, j=1}^{n,\, m} Bkn = \begin{cases} \sum_{i=1,\, j=1}^{n,\, m} (1-e^{-\left(\frac{x_i}{\alpha_j}\right)^{\beta_3}} - \left(1-e^{-\left(\frac{x_i}{\alpha_j}\right)^{\beta_3}} - py\right), 1-e^{-\left(\frac{x_i}{\alpha_j}\right)^{\beta_3}} > py, x\geq 0 \\ 1-e^{-\left(\frac{x_i}{\alpha_j}\right)^{\beta_3}}, 1-e^{-\left(\frac{x_i}{\alpha_j}\right)^{\beta_3}} \leq py \end{cases} \qquad (4)$$

Performance of this model presents by two mathematic models which are Bandwidth Save, B_s and

Table 2: ATPWT parameter used on real live internet traffic

Parameters	Symbol	Values
Committed access rate, speed (Mbps)	S	16
Inter-arrival time (min)	T_A	10
Daily and weekly captured time	min	00:00-23:50
Daily tracers	Dt	144 times
Threshold (MByte)	B_{Th}	1200
Maximum bucket (MByte)	P	1200
Scale of day 1 and day 7	a1, a7	$\alpha_{j=1}^{j=2}$ 908.501, 641.04}
Shape of day 1	β	$\beta_{5=1}^{k=5}$, {0.5, 1, 1.41765, 1.7, 2}
Shape of day 7	β	$\beta_{5=1}^{k=5}$ {0.5, 1, 1.3575, 1.7, 2}
Minimum throughput of day 1 (MByte)	Bmin1	22.04
Minimum throughput of day 7 (MByte)	Bmin7	63
Maximum throughput of day 1 (MByte)	Bmax1	2116.2
Maximum throughput of day 7 (MByte)	Bmax7	2120.8

Processing Time, P_T. Bandwidth Save is calculated as in Eq. 5 and total of B_s is derived based on Eq. 6. Byte Burst, B_b in the equation also is equal to byte loss, Ᵽ .

$$D_s = B_b \times S \tag{5}$$

$$\sum_{i=1,\, j=1}^{n,\, m} Bkn = \left\{ \sum_{i=1,\, j=1}^{n,\, m} \left(1 - e^{-\left(\frac{x_i}{\alpha_j}\right)^{\beta_5}} - py \right) \times S,\ B_{Min} < y > B_{Max} \text{ and } 1 - e^{-\left(\frac{x_i}{\alpha_j}\right)^{\beta_k}} > py,\ x \geq 0 \right. \tag{6}$$

Processing time presents network performance of the developed model. There are two main processing times calculation which is total time before and after implemented policy. Equation 7 presents mathematical calculation before policy action. It presents the total Process Time, P_{T1} before Policing. Traffic before policy is multiplied with parameter speed and divided with Bandwidth Allocation, B_A in the implemented system where z. P_{T1} is considered one cycle processing time which is a day. Result presents a comparison on daily and weekly basis in the result section:

$$\sum_{i=1}^{n} P_{T1} = \frac{\sum_{i=1}^{n} Bk \times S}{z} \tag{7}$$

Equation 8 derives the Total Process Time after Policing, P_{T2} for the internet traffic:

$$\sum_{i=1}^{n} P_{T2} = \frac{\sum_{i=1}^{n} Bkn \times S}{z} \tag{8}$$

Equation 9 presents the different of total difference of Processing Time between after and before implementation of adaptive throughput policy algorithm:

$$\sum_{i=1}^{n} D = \sum_{i=1}^{n} P_{T1} - \sum_{i=1}^{n} P_{T2} \tag{9}$$

Equation 10 presents burst throughput if the throughput flow is larger than the policy condition. Burst throughput is controlled on the value of shape, α. When larger value of parameter shape, β, is used, it generates the smaller burst throughput in the system:

$$\sum_{i=1,\, j=1,\, k=1}^{n,\, m,\, o} \text{Burst} = \begin{cases} \sum_{i=1,\, j=1,\, k=1}^{n,\, m,\, o} (1 - e^{-\left(\frac{x_i}{\alpha_j}\right)^{\beta k}} - py, 1 - e^{-\left(\frac{x}{\alpha}\right)^{\beta}} > py,\ x \geq 0 \\ 0, 1 - e^{-\left(\frac{x}{\alpha}\right)^{\beta}} \leq py \end{cases} \tag{10}$$

RESULTS

Result presents the performance evaluation with ATPWT. ATPWT presents sample on one policy condition, p_1B_{Max} which acts exactly like the real live implementation in the campus network. Four performance conditions which are bandwidth save, bucket capacity, process time and burst controlled on identified fitted 2-parameter Weibull are presented. Based on the maximum MLE log value, day 7 is selected in the analysis of the traffic performance on the bandwidth save, bucket capacity and processing time. The identified α and β parameters on fit day 7 are used for traffic simulation. The analysis presents only one sample of adaptive policy controlled which is 16 Mbps. Result also presents burst traffic controlled using parameter α and β. Burst traffic are evaluated based on five different shapes, β value in the ATPWT which differentiate the volume of burst traffic.

Bandwidth save: Figure 8 and 9 present the fitted CDF Weibull of day 1 which identify the value of α = 908.501, β = 1.41765 and day 7 which identify the value of α = 641.04, β = 1.3575 on threshold, P1 in 144 tracers incoming traffic. Figure 8a and 9a present throughput flow with policy which is put in buckets every 10 min of

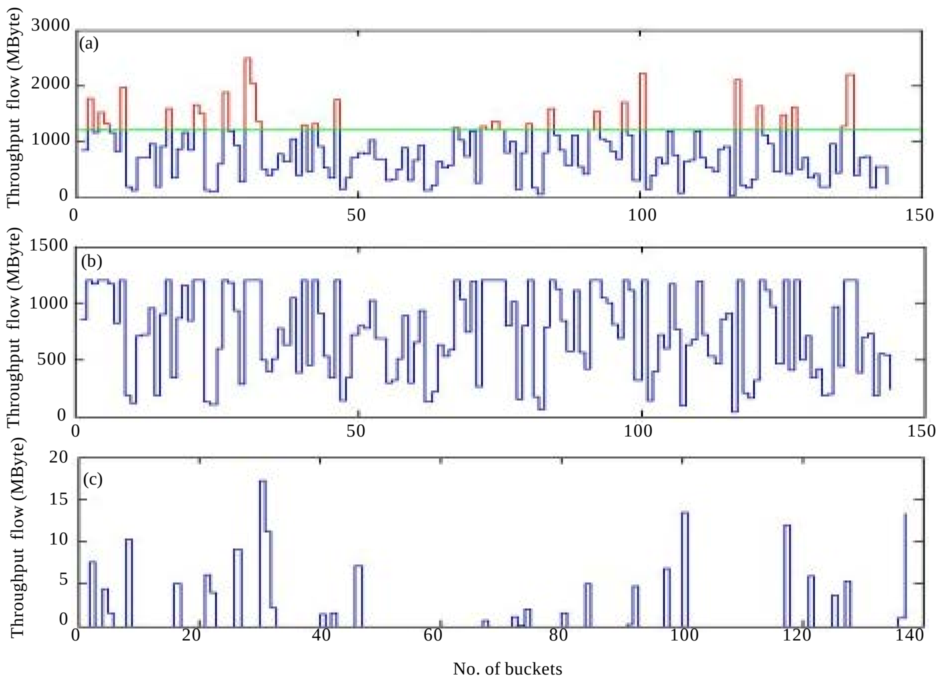

Fig. 8(a-c): Day 1 policing with α = 908.501, β = 1.41765 on 144 tracers (a) Throughput flow with policy, (b) Throughput flow after policy and (c) Bandwidth save after policing

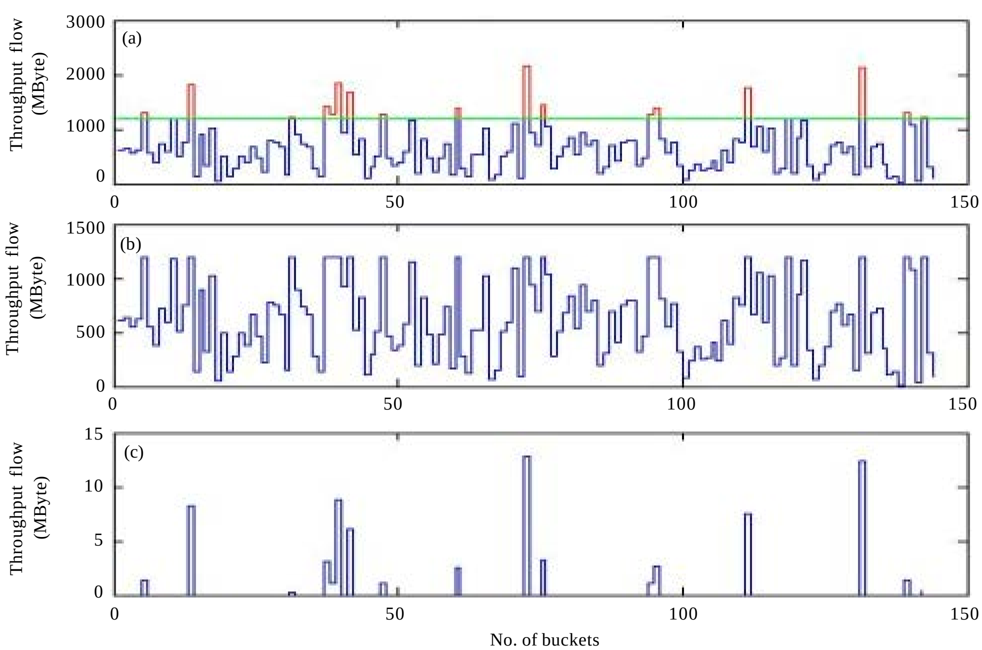

Fig. 9(a-c): Day 7 policing with α = 641.04, β = 1.3575 on 144 tracers (a) Throughput flow with policy, (b) Throughput flow after policy and (c) Bandwidth save after policing

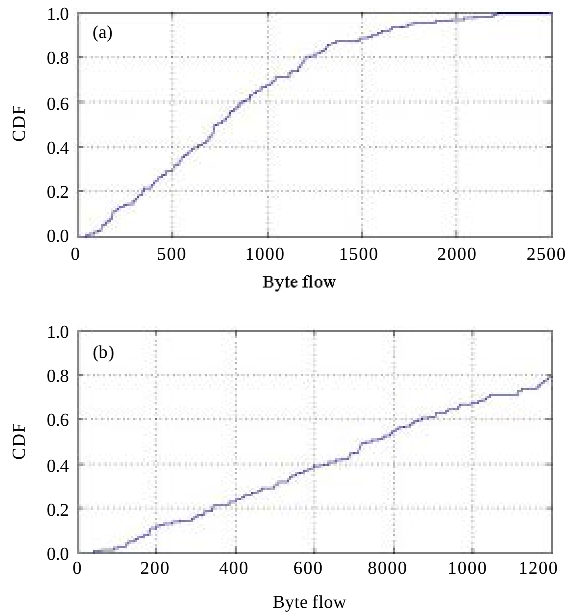

Fig. 10: Day 1 CDF bucket capacity performance (a) Throughput before policing and (b) Throughput after policing

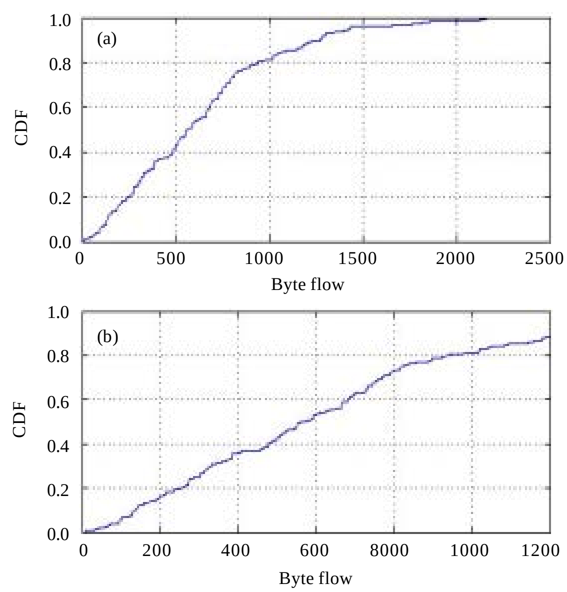

Fig. 11: Day 7 CDF bucket capacity performance (a) Throughput before policing and (b) Throughput after policing

inter-arrival time. Plotted graph presents red throughput which is above threshold and blue throughput is under policy condition. Figure 8b and 9b present throughput flow after applying policy where the max bandwidth allowed is below 16 Mbps. The maximum bucket capacity allows is 1200 MByte traffic. The cut off throughput is identified as bandwidths saved after policing as in Fig. 8c total bandwidth saved is identified as 73.43 Mbps. Figure 9c total bandwidth saved is identified as 165.87 Mbps.

Bucket capacity on byte Flow: Figure 10 and 11 present the comparison of byte flow in bucket of each inter-arrival time between before and after policing. Figure10a shows

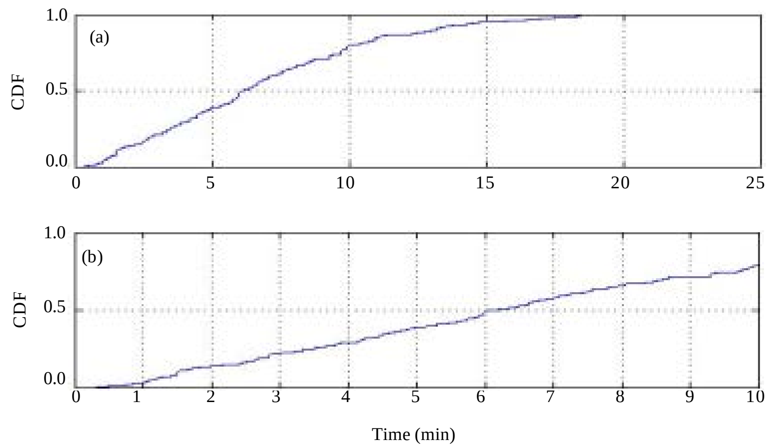

Fig. 12: ATPWT performance on day 1 CDF process time (a) Before policing (b) After policing

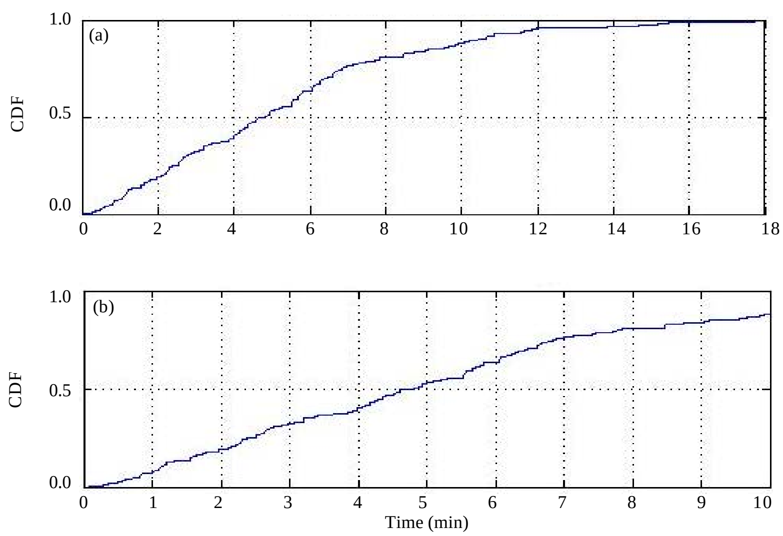

Fig. 13: ATPWT performance on day 7 CDF process time (a) Before policing (b) After policing

CDF Throughput where the maximum traffic is identified as 2488.8 MByte and Fig. 11a more than 2000 MByte. Figure 10b and 11b show CDF Throughput after Policing is reduced with not more than 1200 Mbyte in both days. This policy has cut off the traffic which goes beyond the threshold and avoids burst traffic in buckets.

The total existing bucket before policing for the 144 tracers is 118850 MByte and new bucket is 106410 MByte in day 1. The day 7 derives of the total existing bucket is 91936 MByte and after policing bucket is 86429 MByte. The different is about 12440 MByte in day 1 and 5507 MByte in day 7 which are identified as byte loss or burst traffic. The performance produces low bucket capacity and reduce burst throughput according to the implemented threshold in ATPWT algorithm.

Processing time: Processing time is another performance criterion which is derived in this new traffic model algorithm. Figure 12 and 13 present the ATPWT simulation analysis on performance of processing time in day 1 and day 7. Figure 12 shows processing time performance in day 1 (a) Which is before policing. It present the maximum process time per bucket is 20.7 min compared to (b) After policing where the maximum process time is 10 min per bucket. The different graph plotted that time processing is reduced after policing implementation. The total process time before policing is equal to 990.45 min and after policing is equal to 886.78 min. Thus, it presents a different process time of 103.67 min for the whole 1 cycle process. Figure 13 present the performance process time in day 7 (a) Before policing which resulted the maximum process time per bucket is 18 min compared to (b) After policing where the maximum process time is 10 min per bucket. The different graph plotted that time processing is reduced after policing implementation. The total process time before policing is equal to 766.14 min and after policing is equal to 720.24 min. Therefore, performances result presents a different process time of 45.89 min for the whole 1 cycle process. Thus, the new ATPWT algorithm produces time saving and faster process in time.

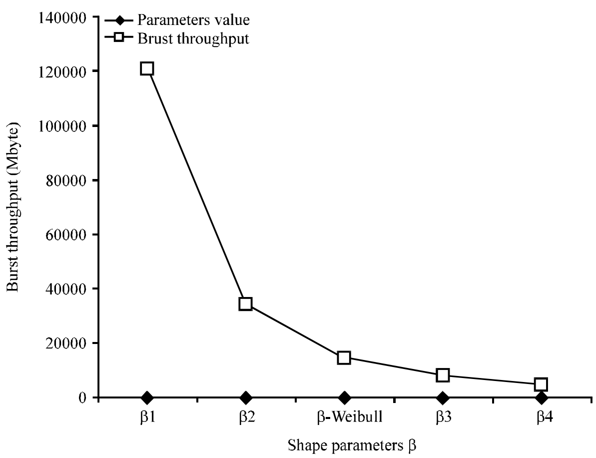

Fig. 14: Day 1 throughput burst with shape-β and scale-908.5

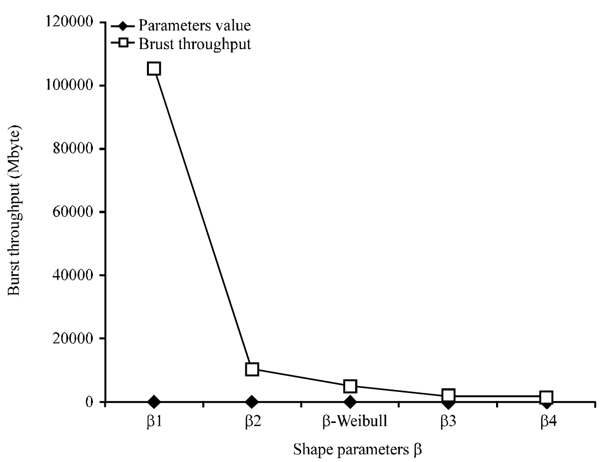

Fig. 15: Day 7 throughput burst with shape-β and scale-641.04

Burst throughput control: This section presents how adaptive used of parameter shape, β can control the burst traffic simulated in ATPWT algorithm. Fitted 2-parameters CDF Weibull are shown which represents for day 1 which is minimum MLE log-likelihood and day 7 which having the maximum MLE log-likelihood. Parameter scale, α presents the scale of fitted distribution to the real live internet traffic while parameter shape, β presents the shape of the Weibull distribution on the fits data. Table 3 presents the difference of five value parameters shape, β included with original fits value of Weibull distribution. Burst throughput is compared between the two days with fix scale but different shapes are derived. Result presents that low β would produce higher burst throughput in both days. The higher the parameter value of β, the lower burst traffic is identified.

Figure 14 and 15 present the slope of shape parameter versus burst throughput in day 1 and day 7. Both days analysis derived the down slope from left to right which present the higher of parameter value shape, β, the lower burst traffic goes down. Thus with Weibull parameter traffic modelling in the adaptive throughput policy can control the burst traffic by adaptive shape parameter, β.

DISCUSSION

Successful results with new parameters identifications on new ATPW algorithm based on real IP-based network internet traffic is analysed and presented. This study is going beyond conventional models and is looking Long Rage Dependence (LRD) in

Table 3: ATPWT performance on burst traffic by shape parameter

	Day 1 with Weibull scale 908.5		Day 7 with Weibull scale 641.04	
Shape parameter	B value	Burst throughput (MByte)	β value	Burst throughput (MByte)
β1	0.5	121460.00	0.5	105020.00
β2	1	34571.00	1	10127.00
β-Weibull	1.41765	14527.00	1.3575	4424.40
β3	1.7	8297.10	1.7	1633.10
β4	2	4858.50	2	1050.70

tele-traffic with CDF Weibull distribution compared to few previous research done by Chandrasekaran (2009) and LSD with self-similarity (Karagiannis *et al*., 2004). This research is similar with Garsva *et al*. (2014) and Ramaswami *et al*. (2014) in modelling and identified performance from a fitted traffic but both of them using a different test which is Kolmogorov-Smirnov fit test for packet inter-arrival time distributions and LogPH fit to wireless mobility network data. A few research which used Weibull distribution model traffic which is similar to this research but implementing in a different approach are by Huang *et al*. (2009) and Shuhong *et al*. (2014) which identifies reliability evaluation on a historical data by combination of empirical methods and statistical methods.

Quite similar algorithm on traffic policing and shaping is done by Daian and Giura (2011) but results presented the effect of traffic shaping and traffic policing on aggregate traffic dynamics especially stochastic properties on traffic time series which is different for this research which present performance comparisons. Moreover, Daian and Giura (2011) tested the algorithm on OPNET Modeler simulation program with synthetic traffic generated by chaotic dynamic systems compared the result produce in this research is based on real IP-based internet traffic. Further shaping algorithm is presented by Vayias *et al*. (2006) using token bucket mechanism which is similar with this research but exponential distribution is used in the algorithm. Thus, recent research on internet traffic would shows most important direction to explore for future understanding of traffic and related with real network traffic phenomena. Deep inspection or particular other internet traffic will produces even more intriguing behaviour which need to be thoroughly explored and new tele-traffic algorithm for QoS should be presented to the International research community.

CONCLUSION

This study presents new research based on the recent and real live collected and best fitted CDF Weibull measured on internet throughput traffic from an IP-based campus network. Analysed throughput on real traffic supports with a 16 Mbps speed rate on a campus IP-based traffic is done using four best fitted distributions. New fitted 2-parameters Weibull are identified as the best parameter using MLE technique. By using the identified parameter, a new ATPWT algorithm is successfully simulated, analysed and presented. Internet traffics may change regularly in time which produced different parameters value. Previous traffic model on policing are imposed based on Poisson traffic, self-similarity traffic model, Exponential traffic model, Pareto traffic model, Normal traffic model and others. Thus, this research presents it novelty with an implemented controlled policing using new identified parameters which are difference from others traffic model in a broad network. Traffic performance and burst traffic are controlled in the system where larger value of shape, β parameter produced less burst traffic. Smaller shape, β parameter produced larger burst in the system. Different value of measured parameter may affect with different research results which are important in network performance. The rate speed can be taken as measured benchmark in future algorithm. Thus, modelling Weibull traffic in Adaptive Throughput Policy (ATP) algorithm presents a new result in controlling traffic burst and traffic performance in bandwidth management of IP-based network.

ACKNOWLEDGMENT

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

REFERENCES

Ahn, S.W., H.S. Jung, C. Yoo and Y.W. Lee, 2013. NARS: Network bandwidth adaptive scalable real-time streaming for smart ubiquitous middleware. J. Int. Technol., 14: 217-230.

Caini, C. and R. Firrincieli, 2004. Packet spreading techniques to avoid bursty traffic in long RTT TCP connections. Proceedings of the IEEE 59th Conference on Vehicular Technology, Volume 5, May 17-19, 2004, Milan, Italy, pp: 2906-2911.

Cao, J., A. Chen and T. Bu, 2008. A quasi-likelihood approach for accurate traffic matrix estimation in a high speed network. Proceedings of the 27th Conference on Computer Communications, April 13-18, 2008, Phoenix, AZ., USA.

Chandrasekaran, B., 2009. Survey of network traffic models.http://www.cse.wustl.edu/~jain/cse567-06/traffic_models3.htm.

Choi, M.J., J.S. Park and M.S. Kim, 2014. An integrated method for application-level internet traffic classification. KSII Trans. Int. Inform. Syst., 8: 838-856.

Daian, D.S. and D.H. Giura, 2011. Traffic shaping and traffic policing impacts on aggregate traffic behaviour in high speed networks. Proceedings of the 6th International Symposium on Applied Computational Intelligence and Informatics, May 19-21, 2011, Timisoara, pp: 465-467.

Dashdorj, Y., N. Chuluunbaatar, B. Batzul and S. Lee, 2010. Characteristics of the token bucket parameters with self similar network traffic. Proceedings of the International Conference on Strategic Technology, October 13-15, 2010, Ulsan, pp: 198-202.

Garsva, E., N. Paulauskas, G. Grazulevicius and L. Gulbinovic, 2014. Packet inter-arrival time distribution in academic computer network. Elektronika Elektrotechnika, 20: 87-90.

Gu, Y., A. McCallum and D. Towsley, 2005. Detecting anomalies in network traffic using maximum entropy estimation. Proceedings of the 5th Conference on Internet Measurement, October 19-21, 2005, Berkeley, CA., USA., pp: 32-32.

Harris, J.W. and H. Stocker, 1998. Handbook of Mathematics and Computational Science. Springer, USA., ISBN-13: 9780387947464, Pages: 1028.

Huang, Z.L., F.X. Yu, S.T. Zhang, Y. Zheng and J.X. Liu, 2009. A novel approach for mmic reliability testing based on weibull distribution. Infom. Technol. J., 8: 1080-1083.

Karagiannis, T., M. Molle and M. Faloutsos, 2004. Long-range dependence ten years of internet traffic modeling. IEEE Internet Comput., 8: 57-64.

Kassim, M., M. Ismail, K. Jumari and M.I. Yusof, 2012. A survey: Bandwidth management in an IP based network. Proceedings of the International Conference on Computer, Communication and Information Sciences and Engineering, February 19-21, 2012, Thailand, Phuket.

Kassim, M., M. Ismail and M.I. Yusof, 2014. A new adaptive throughput policy algorithm on campus IP-based network internet traffic. Letter of Acceptance for Submitted Research Paper ID 25420-JATIT, Journal of Theoretical and Applied Information Technology.

Myung, I.J., 2003. Tutorial on maximum likelihood estimation. J. Math. Psychol., 47: 90-100.

Pavlou, G., 2004. Traffic engineering and quality of service management for IP-based next generation networks. Proceedings of the 10th Symposium on Network Operations and Management, April 23, 2004, Seoul, South Korea.

Ramaswami, V., K. Jain, R. Jana and V. Aggarwal, 2014. Modeling Heavy Tails in Traffic Sources for Network Performance Evaluation. In: Computational Intelligence, Cyber Security and Computational Models, Krishnan, G.S.S., R. Anitha, R.S. Lekshmi, M.S. Kumar, A. Bonato and M. Grana (Eds.). Springer, New York, USA., ISBN: 978-81-322-1679-7, pp: 23-44.

Sang, A. and S.Q. Li, 2002. A predictability analysis of network traffic. Comput. Networks, 39: 329-345.

Schudel, G., 2013. Bandwidth, packets per second and other network performance metrics. http://www.cisco.com/web/about/security/intelligence/network_performance_metrics.html

Shuhong, J., S. Abdalmajeed, L. Wei and W. Ruxuan, 2014. Totally blind image quality assessment algorithm based on weibull statistics of natural scenes. Inform. Technol. J., 13: 1548-1554.

Simion, D.D., 2012. Traffic shaping and traffic policing impacts on aggregate traffic behavior in high speed networks. Int. J. Adv. Comput. Sci., 2: 389-393.

Thakur, G.S., P. Hui and A. Helmy, 2013. On the existence of self-similarity in large-scale vehicular networks. Proceedings of the 9th International Conference on Wireless Communications and Mobile Computing, July 1-5, 2013, Sardinia, pp: 1756-1761.

Vayias, E., J. Soldatos and G. Kormentzas, 2006. Traffic shaping based on an exponential token bucket for quantitative QoS: Implementation and experiments on DiffServ routers. Comput. Communic., 29: 781-797.

Weisstein, E., 2014. Maximum likelihood. MathWorld-A Wolfram Web Resource.http://mathworld.wolfram.com/MaximumLikelihood.html.

Willinger, W., V. Paxson and M.S. Taqqu, 1998. Self-Similarity and Heavy Tails: Structural Modeling of Network Traffic. In: A Practical Guide to Heavy Tails: Statistical Techniques and Applications, Adler, R., R. Feldman and M.S. Taqqu (Eds.). Birkhauser Inc., Boston, USA., ISBN-13: 9783764339517, pp: 27-53.

Xiaolong, J., M. Geyong, S. Velentzas and J. Jianmin, 2012. Quality-of-service analysis of queuing systems with long-range-dependent network traffic and variable service capacity. IEEE Trans. Wireless Commun., 11: 562-570.