ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 7, No. 2, 2012, *pp*. 143-150

Probing Packets Efficiency and Effectiveness on Network Performance and Measurements

Yazeed A. Al-Sbou[1]

Computer Engineering Department, Faculty of Engineering, Mu'tah University, Karak, P.O. Box 7, Postal Code 61710, Jordan

(*Received February13, 2012, accepted March 2, 2012*)

Abstract. Quality of Service (QoS) has become more widely recognized as an important issue since network applications with real-time requirements have started to spread on a larger scale. Measuring QoS in the internet today is difficult as notions of what constitutes QoS vary. Additionally, service Level Agreements (SLA) between customers and network service providers are often poorly defined. Therefore, all the information needed to infer the network performance must be monitored in order to extract the network QoS parameters: latency, jitter, packet loss and throughput. This paper presents a direct estimation of active one-way delay, throughput, and losses measurements precision compared to the actual user measurements. This evaluation allows us to objectively evaluate the network applications performance for delivering user acceptable quality.

Keywords: Active measurements, monitoring, Quality of Service, Biasness, Network performance.

1. Introduction

Measurements, monitoring and estimation of IP networks performance and Quality of Service (QoS) are becoming imperative for today's network operators, service providers, network diagnosis, etc... Additionally, measuring QoS parameters such as the delay and loss for network is also important since these are used as key parameters in service level agreements (SLAs) between an Internet service provider (ISP) and its customers. Therefore, these information are very crucial for controlling, managing, and provisioning the network. Any monitoring system must support a daily operation, traffic control and planning of an operator's network with relevant and timely measurements and estimates [2].

Many tools have been developed to measure network performance or QoS like [3], [4], and [5]. Generally, Monitoring and measurement network performance/QoS schemes usually fall into two categories: passive and active methods. The idea behind passive techniques is to capture packets in order to store and collect information from various fields of the packet header within a flow of application packets. Passive measurement is mainly used to monitor and track the volume and the behaviour of traffic flow but can be used to measure the per-flow QoS as well because it allows the properties of carried traffic to be observed [1], [5]. Moreover, it is a traditional technique used to obtain measurements of QoS parameters related to a certain network element [6], [7], [8] and [9]. This is based on monitoring the performance of packet streams through a network (element) by tracking the traffic passing by a measurement point without creating or perturbing it. These measurements can be done by collecting traffic flow data, from routers, switches or end-point hosts or by adding a stand-alone server at the location of interest (e.g., core or edge) of the network, which acts as a traffic meter or a monitoring device for the crossing traffic. This can be done using either two-point monitoring or one-point monitoring [10].

On the other hand, active measurement measures network performance and/or QoS by injecting probe packets into a network path and monitoring them [11], [12], [13]. Active measurement method is a very

[1] Tel. 00962 799 613 566, Email: yazeed@mutah.edu.jo

popular mean for estimation of the network performance and it becoming increasingly important due to its great flexibility, ability to achieve end-to-end measurements, and freedom from the need of accessing the core of network. In this method, QoS and the performance of a network are measured by inserting of some artificial probing packet streams into the network and monitoring them from a source to a destination. Active measurements can determine the QoS experienced by the probe flow for a particular path and then measure the QoS as it is seen by applications. The purpose of these probing packets is to provide some insight into the way the user traffic is treated within the network. The QoS and performance of the probe-packet stream are monitored to infer the performance of the user's packets and the network directly. There are several tools which are based on active methods like, the Internet Control Message Protocol (ICMP) Echo Reply/Request messages (ping) which is defined in RFC 729 [14], traceroute [15], Service Monitoring Management Information Base (SMMIB) [16], Cisco Internet Performance Monitor (IPM) [17], [18], The Active Measurement Program (AMP) [19], and [20] .

For every measurement based on probing experiment, the sender generates and transmits a probe stream, which traverses some route in the network and terminates at the receiver (the sink). Together with the probe sequence numbers available from the payloads, the packet arrival and departure timestamps are recorded. They are recorded by the sender monitor and the receiver monitor, respectively. By selecting particular properties at the sender (like packet size, departure time, bit rate, etc.), it is potential to compute metrics by analyzing the probe flow characteristics (e.g. arrival time) at the destination so, one can determine end-to-end metrics (from the source to the destination) [23]. Examples of measured metrics that can be derived from the active measurement methods are: connectivity, delay, delay variation (jitter), packet losses, link bandwidth (capacity), bottleneck bandwidth, and available bandwidth.

It is implicitly assumed that the QoS and performance of the user/network are the same as the values measured (obtained) from the active probe packets. Sometimes, the measurements of the probing packets do not accurately represent and estimate the performance experienced by the actual traffic [5]. This accuracy depends on the specifications of both the probe traffic and the actual user traffic. Therefore, in order to produce accurate results, the active probe traffic pattern must have the same pattern of the user traffic pattern being measured [23]. The accuracy of the measurements depends on many factors: packet size of the probe packet, generation rate (i.e. number of injected probe packets), and its packet type. Excessive probe packets generation produce a significant load which can disturb the operation of the network. On the other hand, low probing rates can not reveal the performance accurately [5]. So, underestimation or overestimation of the user performance and application QoS will occur if probe packet properties are very different than the user packet properties under estimation. Therefore, the active monitoring schemes may suffer from the following problems [24]:

- If a probe packet stream is used to simulate an actual user traffic:
    - The probe packet incurs non-negligible extra traffic into the network and it affects QoS and the performance of user's traffic, and
    - The QoS and performance obtained from the probe packets will not be equal to the unbiased one i.e. the results obtained without the presence of the probe packet stream.
- If probe packets of small length have been used and sent periodically, the extra traffic may be negligible, but the QoS and performance results obtained from the probe packets are not exactly equal to the QoS and performance experienced by the user.

In [2], monitoring and estimating the performance of the user traffic parameters has been done based on using Operation, Administration, and Maintenance (OAM) packets. The basic idea is to use these OAM probe packets in conjunction of the user traffic to infer the network performance. OAM packets are inserted between blocks of the user packets (e.g. one OAM packet for every N user packets).

In some cases, it is very hard to specify a probe packet pattern, which will represent the user traffic being measured without degrading its performance. In this paper, the throughput, delay and losses QoS parameters of the user traffic will be estimated based on injecting the network with 1, 5, 10, 20% probe packets of the user traffic. In addition to that, sensitivity calculations will be presented to measure the degree of influence of the intensity of probe packets inserted to the network on the user traffic performance.

2. Active Measurements Precision Evaluation

Active measurement methodology provides efficient tools to infer the network QoS/performance. On the other hand, it perturbs the actual traffic running over the network. Therefore, it is important to glimpse to what extent this perturbation is. In this paper, the intrusiveness, which means the effect of adding probe packets to the network on the user QoS parameters being measured, i.e. the biasing, which will be presented to the measured probing, will be examined. In addition, because the actual traffic will depend on parameters from the active measurements results to represent the performance of the actual application, the precision of the probing measurement will be illustrated. To perform that, a comparison process will be performed. In comparison between *X* and *Y*, which must be identical, the following distance measure will be used:

$$\varepsilon(X,Y)=|X-Y| \tag{1}$$

where ε is the absolute difference (error) between *X* and *Y*. The closer the difference to 0 the better of the measurement. This concept will be applied to estimate the effectiveness of the active-based QoS measurements. Two quantities will be used for this comparison, intrusiveness and precision.

2.1. The Intrusiveness (Biasness)

Here, intrusiveness means the influence of presence of the probe traffic on the actual user traffic. This effect appears on the monitored QoS parameters: throughput, delay, and loss ratio of the user traffic. If it is not possible to detect any change in these parameters for the user traffic with and without the presence of the probe packets, this means that the probe injecting process has no effect on the actual user performance.

In order to check this, the distance in throughput, delay, and loss ratio in the cases of presence and no presence of the probing packets is calculated using equation (1) as follows:

$$\varepsilon(Th,Th_w)\ ,\ \varepsilon(D,D_w)\ ,\ \varepsilon(L,L_w) \tag{2}$$

where *Th, D,* and *L* are the throughput, delay and losses, respectively, observed without the presence of probe packets, and Th_w, D_w, and L_w are the throughput, delay and loss, respectively, observed in the presence of probe packets.

2.2. Precision

As mentioned above, the probe packets should estimate the user traffic performance in the network. In order to verify the precision in the probe estimate, the distance in delay and loss ratio observed by the probe traffic and the user traffic is calculated based on equation (1) as follows:

$$\varepsilon(D_p,D_w)\ ,\ \varepsilon(L_p,L_w) \tag{3}$$

where D_P and L_P are the delay and the losses, respectively, observed by the probe packets. D_w and L_w the delay and losses, respectively, of the actual user packet.

3. Experimental Procedure

In order to illustrate the effectiveness of the probing technique in estimating the network QoS/performance, a few simulation runs have been conducted in terms of biasness and precision of the throughput, delay, and losses parameters. The NS-2 [25] simulator is used to perform the experiments with a simple topology as shown in Figure (1). The system is loaded by two different sources: probing packet traffic and the user traffic.

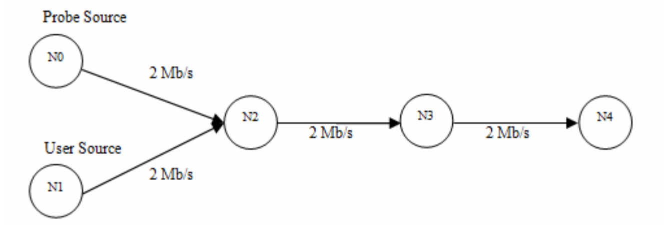


Fig. 1: Network topology used in the simulations

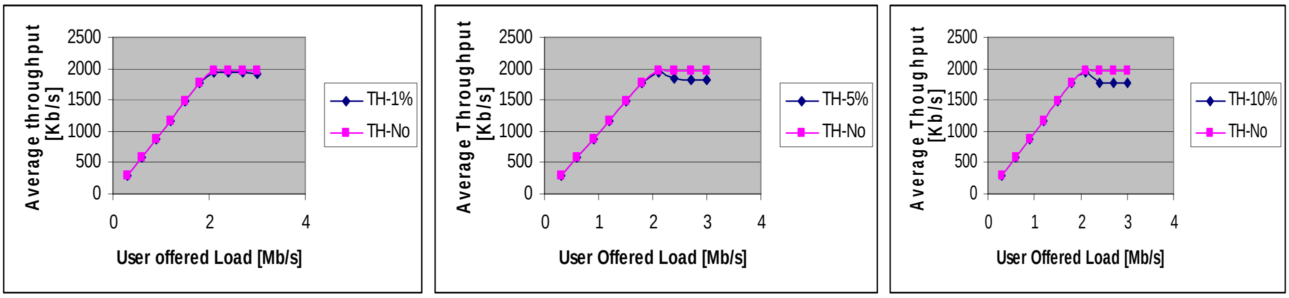
The packet sizes of the probe packets and user packets used in the simulations are 64 byte and 600 byte, respectively. The simulations have been performed with varying the offered traffic load over different experiments to observe how the precision and the influence (intrusiveness) of the probe traffic depends on the traffic load level. This load is varied from light load to heavy load over the 2Mb/s bottleneck. The loads of the user traffic applied in the simulations are {0.3, 0.6, 0.9, 1.2, 1.8, 2.1, 2.4, 2.7, and 3} Mb/s and the probe traffic intensities have been selected to be 1%, 5%, and 10% of the user traffic. The transport protocol used for both traffics is UDP protocol and the buffer size is selected to be 20 packets with SFQ queuing algorithm.

The measurement of QoS parameters has been done as follows, increasing the offered load of the user traffic from 0.3 Mb/sec to 3Mb/s in a step of 0.3Mb/s and then injecting the network by probe traffic of 1%, 5%, and 10% of the user load (i.e. for user traffic of 2.4Mb/s the 1% probe traffic is 24Kb/s will be injected) and then for each step the average throughput, average delay, average loss are calculated.

4. Experimental Results

4.1. Throughput Measurements

Throughput is measured as how many bits received at the destination per unit of time. The aim is to observe the effect of adding probe packets on the user throughput. Figure (2) shows the user average throughput in the case of no presence of the probe traffic and in the case of presence of probe traffic with different intensities. From this Figure, it can be seen that there is an obvious effect of the existence on the user traffic and as its percentage increases, the effect will be higher. This means that increasing the probe packet intensity will reduce the number of user packets received at the destination which will consequently reduce the throughput, specially when traffic over the link between node2 (N2) and node3 (N3) exceeds the link capacity (2 Mb/s). This due to the fact that some packets will be dropped because the SFQ queue will be overwhelmed by the applied traffic from both user and probe sources.



(a) (b) (c)

Fig. 2: The user average throughput of different injecting probe traffic intensities: (a) 1% of the user traffic, (b) 5% of the user traffic, and (c) 10% of the user traffic

To examine how much that effect is, equation (2) has been used. Figure (3) illustrates the biasness (intrusiveness) results from injecting the probe traffic at different percentages. From this Figure, it is clear that the intrusiveness of the throughput measurement from its actual value due to the probing packets is minimum as the intensity of the probe is minimum and as the intensity increases the influence will increase (i.e. at 1% probe traffic intensity the biasness was minimum and at 10% is the maximum for our measurements). This is not applicable when the network is in the light load conditions because from the Figure, sooner than the offered load of 2Mb/s, the biasness is zero for all probing intensities, but after that biasness starts to become visible and it becomes clear as the probe intensity increases.

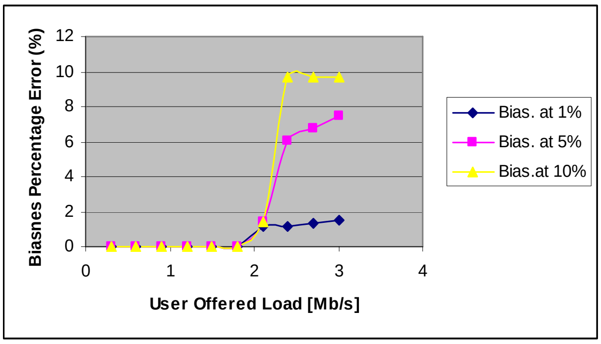
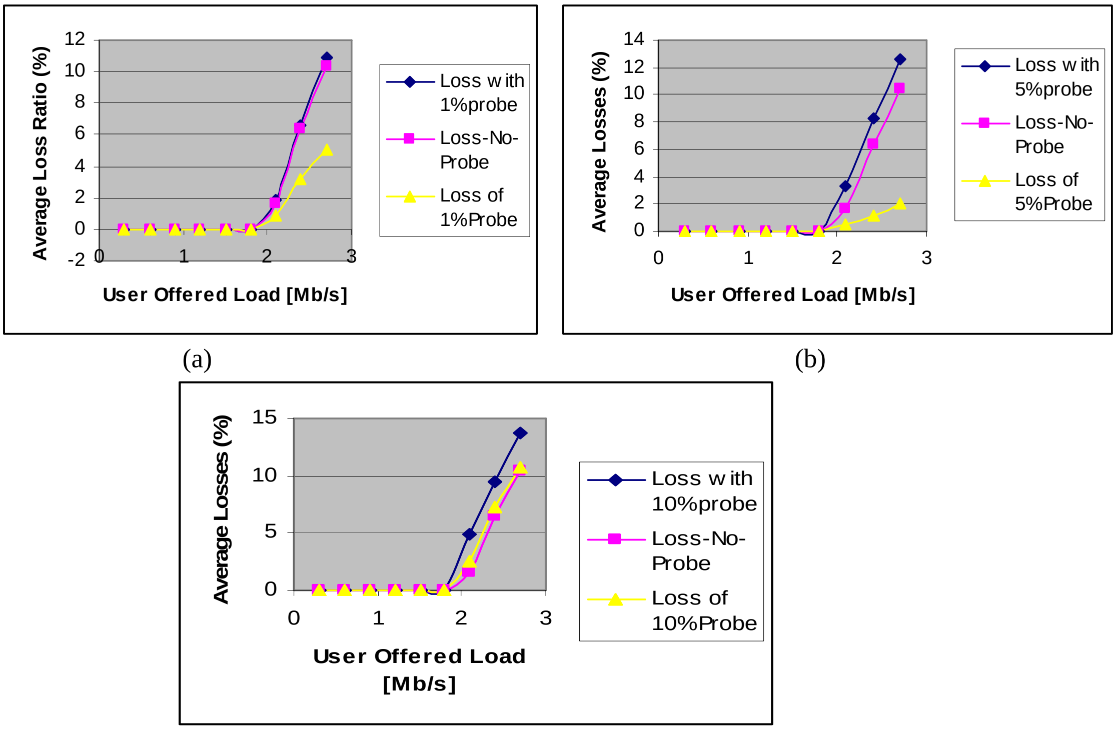


Fig. 3: Biasness measurement of throughput for different probe traffic intensities.

4.2. Packet Losses Measurement

Packets loss is measured as the ratio of the lost packets compared to the sent packets. Here, we aim to observe the effect of adding probe loads on the user average loss. Figure (4) shows the user average losses in cases of no presence (Loss-No-Probe), presence of the probe traffic with different intensities (Loss with x% probe) and the losses experienced by the probe traffic (Loss of x% Probe). From this Figure, it can be clearly seen the effect of the existence of probe on the user traffic. As the probe traffic intensity increases, the effect on user traffic will be higher due to the same reasons explained above for the throughput.



(a)

(b)

(c)

Fig. 4: The user average losses with different injecting probe traffic intensities: (a) 1% of the user traffic, (b) 5% of the user traffic, and (c) 10% of the user traffic

To observe that effect is, equation (2) has been used. Figure (5) illustrates the average losses biasness error results from injecting the probe traffic at different percentages. Ideally, the intrusiveness of the loss measurement from actual values because of the probing process is minimum as the intensity of the probe is minimum and as the probe traffic intensity increases the influence will increase (i.e. for example at 1% probe traffic intensity the biasness should be minimum and at 10% should be maximum for our measurements). When the network is in the light load conditions, ahead of offered load of 2Mb/s, the biasness is zero for all probing processes, but after that biasness starts to occur and it becomes clear as the probe intensity increases. As shown in the Figure below, the maximum biasness and the minimum biasness are in the case when the probing is 10% and 1% respectively and the intensity of 5% has a moderate biasing value.

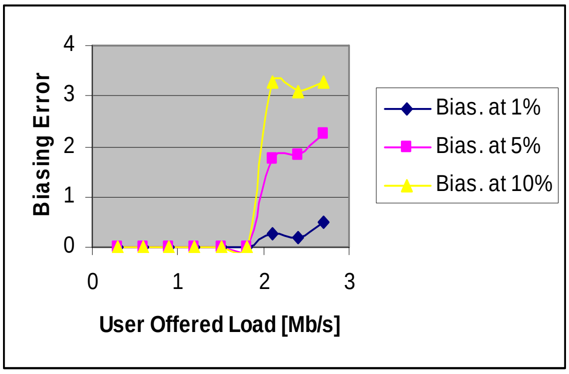


Fig. 5: The biasing error in the average user losses based on different probing intensities.

In order to examine the precision of different probing process estimates of the user losses, the error in the average losses between the values observed by the probe packets and the user packets is calculated using equation (3). The precision error results for the three different probing intensities are given in Figure (6). From the Figure, the error with the highest probe intensity (10%) produces the minimum precision error and shows good performance for high and low offered loads.

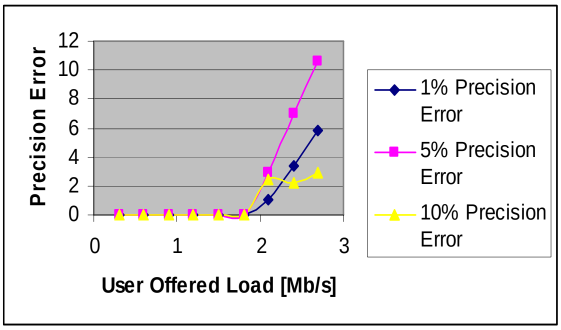
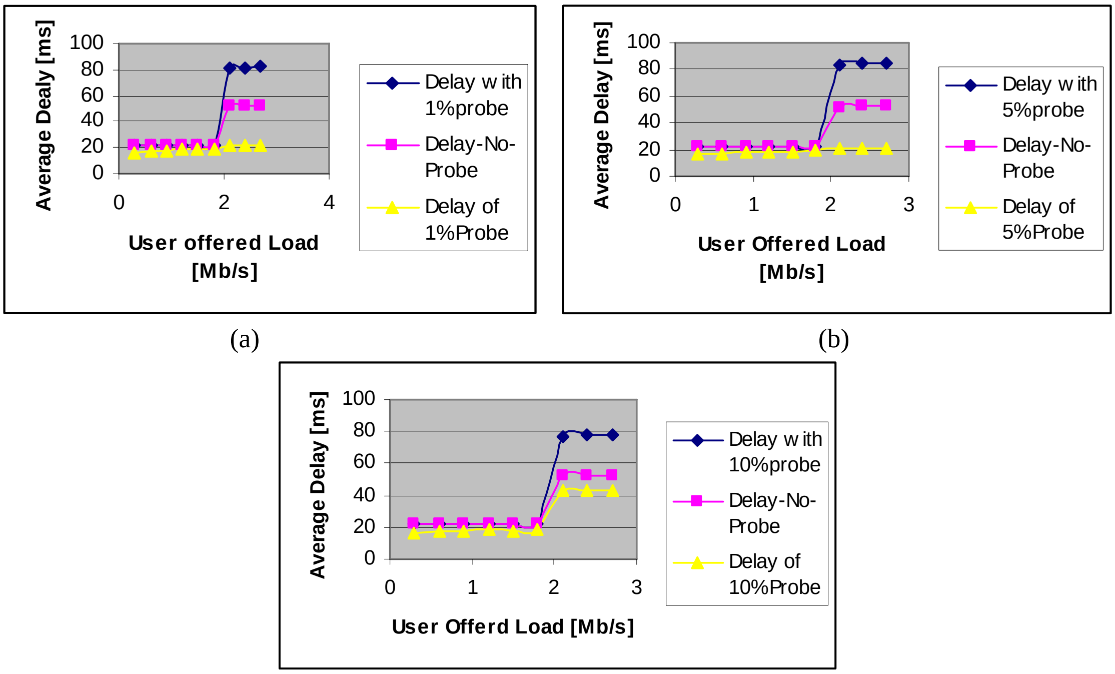


Fig. 6: The precision error in the average user losses based on different probing intensities

4.3. Delay Measurement



(a) (b)

(c)

Fig. 7: The user average delay with different injecting probe traffic intensities: (a) 1% of the user traffic, (b) 5% of the user traffic, and (c) 10% of the user traffic.

Delay is measured for each packet as the difference between the timestamps of that packet at the destination and the source. In this subsection, we aim to observe the effect of adding probe loads on the user average delay. Figure (7) shows the user average delay in cases of no presence and presence of the probe traffic with different intensities. From this Figure, it can be clearly seen the effect of the existence of probe on the user traffic and as its percentage increases, specially when the total traffic over the bottleneck link between N2 and N3 surpass its available capacity. Moreover, it is clear that the measured delays by the probe packets is an accurate value to depend on to estimate the actual user traffic delays. That is because the probe packets size is very small compared to the user packets size which will experience higher delays compared to the probe packets delay values and for all the probe traffic intensities.

In order to check how much that effect is, equation (2) has been used. Figure (8) illustrates the delay biasness results from injecting the probe traffic at different percentages. Ideally, the intrusiveness of the delay measurement from its actual value due to the probing process is minimum as the intensity of the probe is minimum and as the intensity increases the influence will increase (i.e. for example at 1% probe traffic intensity the biasness should be minimum and at 10% should be maximum for our measurements). This is not applicable when the network is in the light load conditions because from the Figure, before offered load of 2Mb/s, the biasness is zero for all probing processes, but after that biasness starts to appear and it becomes clear as the probe intensity increases. In addition to this, it is clear that the average delay biasing of the user traffic is miss leading because theoretically, the 10% and 1% probing intensities should cause the maximum and the minimum biasing respectively. However, as shown, the maximum biasing error is at 5% and the minimum is at 10%, the reason for that is due to the fact that as the traffic increases the number of dropped packets is increased at the queue and so the average delay will decrease and due to that the biasing will decrease.

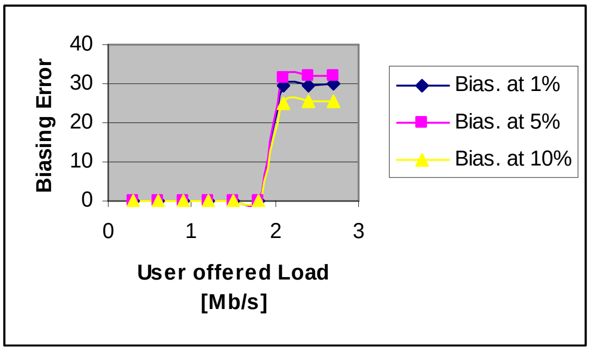


Fig. 8: Biasing Effect on the average delay of the user traffic.

As mentioned before, the probing process should estimate the performance of the user QoS parameters. To examine the precision of the different probing process estimates, the error in the average delay between the values observed by the probe packets and the ones of the user packets using equation (3). The precision error results for the three different probing intensities are given in Figure (9). From the Figure, the error with the highest probe intensity produces the minimum precision error and shows good performance for high and low offered loads.

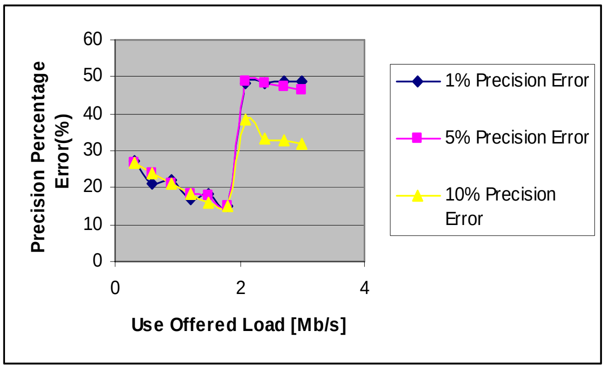


Figure (9): The Precision Error in the Average User Delay based on different probing intensities.

5. Conclusions

In this paper, the emphasis is placed on active measurement method and its application to network monitoring. We present an overview of passive and active monitoring techniques, point out their strengths and weaknesses in terms of reliability and accuracy in the estimation in different network traffic parameters. We also provide the motivations for active measurement on high-speed network links. The purpose of this paper has been to present an implementation of the accuracy that the active measurement can provide to estimate the actual network QoS/performance. From the obtained results, active measurements can provide accurate information about the performance of the targeted user traffic in case of light loaded networks and some insights when the network is moderately loaded. On the other hand, misleading results may be obtained in case of heavily loaded networks. In conclusion, the degree of biasness and precision of the active measurements estimations depends on the type of the information required and the traffic load intensity in the network.

6. References

[1] A, Masaki, M, Naoto and I, Keisuke I. A Change-of-Measure Approach to Per-Flow Delay Measurement Combining Passive and Active Methods: Mathematical Formulation for CoMPACT Monitor. *IEEE Transactions on Information Theory*. 2008, **54**(11).

[2] T, Lindh. A New Approach to Performance Monitoring in IP Networks-Combining Active and Passive Methods. In Proceedings of the Passive and Active Measurements 2002 Workshop, Colorado, USA, 2002.

[3] CAIDA. The Cooperative Association for Internet Data Analysis [Online]. Last accessed on 09th January 2012. URL available at: http://www.caida.org, 2011.

[4] NLANR. Measurement and operation analysis team [Online]. Last accessed on 09th January 2012. URL available at: http://www.psc.edu/networking/nlanr, 2011.

[5] T, Brekne, M, Clementsn, P, Heegaard, T, Ingvaldsen, and B, Viken. State of the Art in Performance Monitoring and Measurements. Fornebu: Telenor Forskning of Utyikling. R&D Report R 15/2002. 2002.

[6] V, Paxson. End-to-end Internet Packet Dynamics. *IEEE/ACM Transactions on Networking*. 1999, **7**(3): 277-292.

[7] V, Paxson. Measurements and Analysis of End-to-End Internet Dynamics. PhD thesis, University of California, Berkeley, USA, 1997.

[8] V, Smotlacha. QoS Oriented Measurement in IP Networks. CESNET Technical Report Number 17/2001, 2001.

[9] A, Johnsson. Bandwidth Measurements in Wired and Wireless Networks. Licentiate thesis, Mälardalen University Press, 2005.

[10] K, Ishibanishi, T, Kanzawa, M, Aida, and H, Ishii. Active/Passive Combination-type Performance Measurement Method Using Change-of-Measure Framework. *Elsevier Computer Communication.* 2004, **27**(9): 868-879.

[11] G, Almes, S, Kalidindi, and M, Zekauskas. A One-Way Delay Metric for IPPM. *The Internet Society, RFC2679*. 1999.

[12] G, Almes, S, Kalidindi, and M, Zekauskas. A One-Way Packet Loss Metric for IPPM. *The Internet Society, RFC2680*. 1999.

[13] A, Pásztor and D, Veitch. High precision active probing for Internet measurement. In the Proceedings of the 11th Annual Internet Society Conference INET 2001, Stockholm, Sweden, 2001.

[14] J, Postel. Internet Control Message Protocol. RFC 792. [online]. Last accessed on 26 January 2012 at URL: http://www.ietf.org/rfc/rfc0792.txt. 1981.

[15] Traceroute. 2002. [online]. Last accessed on 06 January 2012 at URL: http://www.traceroute.org/ , 2002.

[16] Y.-H, Choi, and I, Hwang. In-service QoS Monitoring of Real-time Applications Using SM MIB. *International Journal of Network Management*. 2005, **15**(1): 31-42.

[17] Cisco Internet Performance Monitor. [online] Last accessed in January 2012 at URL: http:// http://www.cisco.com/en/US/products/sw/cscowork/ps1008/products_user_guide_chapter09186a0080087847.html, 2004.

[18] F, Michaut, and F, Lepage. Application-oriented Network Metrology: Metrics and Active Measurement Tools. *IEEE Communications Surveys & Tutorials*. 2005, **7**(2).

[19] The Active Measurement Program (AMP). [Online]. Last accessed on 9th January 2012. Available at URL: http://sd.wareonearth.com/woe/amp.htm, 2000.

[20] J, Sommers, P, Barford, N, Duffield, and A, Ron. A Geometric Approach to Improving Active Packet Loss Measurement. *IEEE/ACM transactions on networking*. 2008, **16**(2).

[21] M, Luckie. Scamper: a Scalable and Extensible Packet Prober for Active Measurement of the Internet. In the Proceedings of the Internet Measurement Conference 2010, Melbourne, Australia, 2010.

[22] R, Padmalatha and G, Sreedhar. A Novel Algorithm for Improving the End-to-End Active Packet Loss Measurements in Computer Networks. *International Journal of Computer Applications*. 2010, **6**(1).

[23] P, Heegaard. Active Tests for SLA Validation-Correctness, Precision, and Intrusiveness. R&DN 30/2002, 2002.

[24] I, Aad. Quality of Service in Wireless Local Area Networks. PhD Thesis, Joseph Fourier De Grenoble University, France, 2002.

[25] The Network Simulator - NS-2, [Online]. Last accessed on 9th January 2012. Available at URL: http://isi.edu/nsnam/ns/ , 2012.