Out of order packets analysis on a real network environment

René Serral-Gracià, Loránd Jakab, Jordi Domingo-Pascual*
Universitat Politècnica de Catalunya
{rserral, ljakab, jordid}@ac.upc.edu

***Abstract*— As Internet usage grows, more efforts are put in analysing its internal performance, usually such analysis comes through simulation using different models. While simulation can provide a good approximation of network behaviour, modeling such a complex network as the Internet is very difficult if not impossible. This paper studies the network's performance from an experimental point of view using the European Academic Network (EAN) as a testbed.**

In the framework of the EuQoS project, many performance tests have been performed to prove the reliability of data transmissions. The tests show some rough edges which need further analysis, among them the most important being random losses in UDP flows and a great amount of out of order packets.

This paper focuses on the study of such out of order packets, searching for their causes, and more importantly to show the effects on real-time traffic such as VoIP, videoconferencing, video streaming, etc.

I. Introduction

The increase of services available on the Internet shifts the research topics on this area. This change is from a more theoretical point of view towards a more experimental analysis of the network. With this last trend lots of different research efforts for studying the network behaviour are carried on.

This paper presents an analysis of out of order packets in the environment of the EAN. To develop such analysis, a reliable, Europe-wide testbed is needed. For this purpose, we used in this study the EuQoS project's testbed [1], where different companies and universities all over Europe participate in the building of a Quality of Service framework for inter-domain environments.

For modelling the Quality of Service, the project studies the raw performance of the EuQoS network. While performing connectivity tests, some strange results were found, the most important being sporadic packet losses even with low bandwidth and a notorious amount of out of order packets within UDP flows. Those issues were unexpected on a stable and reliable network such as the EAN.

The contributions of this paper are twofold: on one hand the methodology used for detecting such out of order packets, and the techniques for finding their main causes, on the other hand this study focuses both on the user-level impact and on the network performance.

Detecting such out of order packets will help network administrators to have more information about the underlying network, knowing their effect over real-time applications will help configuring all the parts involved on the communication. Such packets have impact on issues ranging from buffer's reception size to the degree of available interactivity.

The rest of the paper is structured as follows, first a discussion of the related work on out of order packets is done. The following section describes the definition we used to determine out of order packets, after such description, the document focuses on the experiments and the results carried on the EAN, while the final section ends with a summary of the conclusions and the proposals for future work.

*This work was partially funded by IST under contract 6FP-004503 (*IST-EuQoS*), MCyT (Spanish Ministry of Science and Technology) under contract TSI 2005-07520-C03-02 and the CIRIT (Catalan Research Council) under contract 2005 SGR 00481.

0-7803-9455-0/06/$20.00 (c) 2006 IEEE

II. Related Work

Out of order packets are a relatively new problem introduced by packet switched networks, on classical circuit switched networks they are not an issue. But since packet switched networks spread it became evident that new problems would arise.

Out of order packets have been studied previously on several different environments. In [2] the methodology used is based on sending ICMP packets and analysing their responses. The main problem with this approach is the different treatment ICMP traffic receive from the network.

A different methodology is used in [3] where end-to-end TCP flows are studied. More recently broader analysis has been performed in [4] where a single capture point is used for detecting such packets, but also with TCP flows. A similar TCP analysis but this time regarding throughput is done in [5], there the study focuses on the impact of such reordering on the TCP window, and thus in the final communication performance.

More closely related to this paper, X. Zhou *et. al.* in [6] study UDP reordering issues in an experimental testbed across several RIPE boxes, their approach however is flow based reordering, while this study focuses in in-flow reordering analysis. Moreover, our analysis is based on relatively long flows, while [6] uses short bursts of traffic for achieving the same goal.

Other studies focus on techniques for the prevention of such packets, more specifically, [7] proposes a methodology for in-order delivery of packets under an adaptive routing environment.

More on the standardising side of the research, IP Performance Metrics (IPPM) is on the way of standardising a metric related to out of order packets. The last draft available to date can be found at [8], which will complete a series of RFCs related to internet measurement metrics, such as *One-Way Delay* [9] or *IPDV* at [10], altogether forming a stable framework for network performance and Quality of Service (QoS) analysis.

The study done in this paper is novel in the sense of analysing the out of order packets inside UDP flows, along with proposing actual tools and methodology for their computation in experimental environments, this analysis is somewhat more important in currently available services, because usually such flows carry real-time traffic which needs to be delivered under tighter One-Way Delay, jitter and packet loss conditions than standard bulk TCP transfers.

III. Out of order packets

The reordering issue of Internet packets is a subject under study as said before. This section is devoted to detail the definition of out of order packets used in this paper along their possible causes and effects.

A. Definitions

The definition of out of order (OOO) packets used on this paper is similar to the one used on the Standards Track draft found at [8]. This draft defines *reordered packets* as arriving packets with sequence numbers smaller than their predecessors. For example, if sequentially numbered packets arrive 1,3,2,4,5, then packet 2 is reordered. This is consistent with different definitions like Paxon's reordering [11], where *late* packets were declared reordered.

[8] determines the actual *reordering metric* by defining a `Type-P-Reordered` Type-P packet. For further information of Type-P packets refer to [12] where the full standard IETF framework for network parameters is described.

Differently to other sources, this paper will seamlessly use out of order packets, reordered packets or late packets.

The above definition permits to define several dependent metrics for computing the degree of reordering. Given that our analysis will focus on Active Measurements, all the data sent will contain the aforementioned sequence number, this will help to detect out of order packets, but more importantly will permit to compute other metrics too.

All analysis is done on separate flows, so all of the following definitions consider the packets belonging a given flow. Let us denote R as the packet's sequence number. Being R_{MAX} the highest received sequence number, R_i (where $0 \leq i \leq R_{MAX}$)

the i-th received packet's sequence number. We define R^i_{MAX} as the current highest received sequence number, when parsing through the flow, where:

$$R^i_{MAX} = max(R_k), \qquad 0 \leq k \leq i \ . \tag{1}$$

Consider the following equation:

$$\begin{cases} L_i = 1, & R_i < R^i_{MAX} \\ L_i = 0, & otherwise \end{cases} \qquad 0 \leq i \leq R_{MAX} \ . \tag{2}$$

Thus L_i will define whether a packet i is really an out of order packet or not, this definition is the base formula for the rest of computed metrics:

- *Total out of order packets:* Will be the result of

$$OOO_{TOTAL} = \sum_{i=1}^{N} L_i \tag{3}$$

  Where N is the finite number of samples (packets in our case).
  This metric is computed on a per flow basis.
- *Out of order ratio:* given a single test, with a known N the out of order ratio is

$$OOO_{RATIO} = \frac{OOO_{TOTAL}}{N} \tag{4}$$

  Which is also computed per flow.
- *Out of order Distance:* refers to the difference between the current packet's position (j) and the position the sample should be (i). It is represented by:

$$\begin{cases} \Delta_i = j - i & , \quad L_i = 1 \\ \Delta_i = 0 & , \quad otherwise \end{cases} \tag{5}$$

  where $\Delta_i \geq 0$. This metric permits to know the maximum distance, which could be used for inferring the buffer size at reception for ensuring proper packet delivery. Moreover when transmitting real-time traffic, if this distance is too big the packet may be considered as lost by the application.
  The results on this metric will bound the one-way delay results obtained by the measurement.
- *Out of order Burst Length:* refers to a series of consecutive out of order packets. Let k_1 be a number in the interval $[0, N)$. Suppose R_{k_1-1} is the sequence number of an in-order packet followed by an out of order packet (R_{k_1}). And k_2 which $k_1 \leq k_2 < N$, complying with the conditions:

$$\begin{cases} L_k = 1 \\ L_{k_2+1} = 0 \end{cases} \qquad \forall k : k_1 \leq k \leq k_2 \ . \tag{6}$$

  We have:

$$OOO_{BL_{k_1}} = k_2 - k_1 \ . \tag{7}$$

  Which gives the burst length starting at packet k_1.

One caveat in most descriptions of out of order packets is the effect of packet losses. Here, taking into account the previous definitions, the packet losses will be ignored. That doesn't pose a problem given that all the tests done in this work are based on periodic flows. With such traffic, the inter-packet generation times are constant, thus, the fact that a packet is dropped doesn't conditionate the reordering of the flows, neither the one-way delays.

More statistical data can be deducted from the above metrics, such as *Maximum Distance*, *Minimum Delay* or *Average Distance*, which will be very useful on our final study later on this paper.

B. Causes of out of order packets

Once the out of order packet's definition is done, it is important to analyse the possible causes which bring out of order packets to the network.

The first reason is due to Border Gateway Protocol *(BGP)* route changes while the protocol is converging: it is possible to find a burst of reordered packets on the stream. These changes are easily noticeable because are usually short and contain packet losses.

Another reason is load balancing: there are paths with redundancy where the flow is split among two or more interfaces. This kind of reordering can be divided on two different possibilities: first link layer load balancing, which is often undetectable without proper access to the direct equipment responsible for the reordering. The other option is network layer reordering, easier to detect because the route the packets follow varies, moreover, in those cases, the number of hops may vary also giving a higher degree of packet reordering, thus easier detection.

This paper will focus on the latter case, being a typical and detectable behaviour on the EAN.

IV. Testbed and Results

This section will describe the main contribution of this paper, for such description, first we explain the testbed used for our tests in deep detail. Later the paper focuses on the software tools developed and used for this work, finally there is the description of the obtained results.

A. Testbed

As said before, the testbed used for this work is the EAN, more specifically, the overlay network used for the EuQoS project, where different testbeds on each partner's premises permit us to run different set of tests.

The whole testbed forms an overlay network among the involved partners, this is accomplished currently through IP tunnels which connect all the local testbeds in a full mesh fashion. The routing on the overlay network is based on BGP, where each partner has their own Autonomous System (AS) number assigned. In later stages of the project, this full mesh connectivity will be reduced to emulate a real network where end-to-end packets must cross several domains until their destination.

Figure 1 shows a part of EuQoS testbed, where several partners comunicate over Géant and their respective National Research and Education Networks (*NREN*).

Is important to notice that even using an overlay network doesn't affect the final results of the tests. This is due to the fact that the only overhead introduced is due to the extra IP Tunnel header, but the packets keep being routed by the Géant nodes, competing with standard traffic for the network's resources.

The methodology used for computing the network parameters is through actively generate controlled flows between two different end-points. The main problem when facing such distributed tests is the synchronisation among the machines involved. This is an issue because some parameters need an accurate timestamping for determining the quality of the network. Further information on simple methodology for verifying the synchronisation can be found at [13].

This permits to compute several parameters such as:

- *One-Way Delay:* which affects interactivity and the quality of the transmission.
- *Inter Packet Delay Variation:* is related with the quality of the communication.
- *Packet Losses:* also affecting the quality.
- *Out of order packets:* relates to the reception buffers and to the quality because too late out of order packets can be considered lost depending on the application. This paper will never consider late packets as lost.

As can be noted, all of the above parameters determine the good behaviour of the network, and in the case under study, the user's perception quality of the communication when dealing with real-time applications.

B. Working environment

The main tool used for the tests is NetMeter [14]. This tool has been developed under the GPL by the Advanced BroadBand Communications Centre (*CCABA*) at Universitat Politècnica de Catalunya (*UPC*). Lately this tool was greatly improved thanks to the shared efforts of different partners involved in EuQoS.

The main goal of this tool is to be used as a frontend for traffic generation tools. This permits to schedule, control and remote launch a set of tests from a couple of stations connected to the network under study in a non intrusive way.

Jointly with NetMeter come a series of helper applications which help to plot different graphical representations of the network parameters, and some statistical data extracted from the obtained traces.

C. Results

Before the description of the obtained results, it is important to explain the details of the generated traffic in the tests.

For detecting the threshold where out of order packets were found, we did some series of tests,

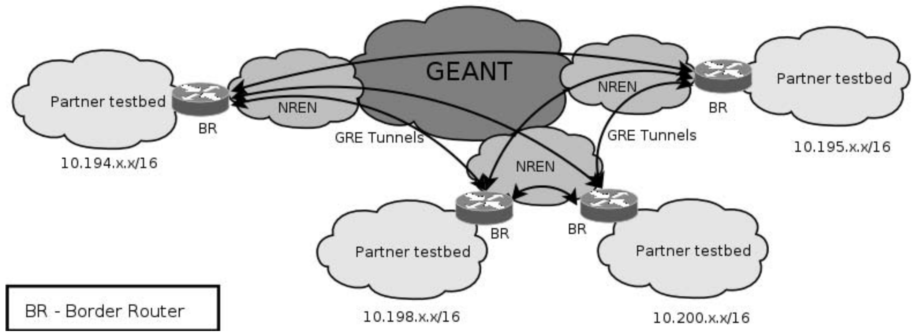

Fig. 1. Partial EuQoS architecture

TABLE I
TRAFFIC CHARACTERISTICS

Name	*Rate*	*Packet Size*	*Bandwidth*
VoIP	60	20	$16Kbps$
UDP - 1	1420	96	$1Mbps$
UDP - 2	160	897	$\sim 1.4Mbps$

each one with different traffic characteristics as shown in Table I.

It is important to notice that the specified packet sizes are at application level, so for having the actual *Physical layer* sizes all the headers must be taken into account. Moreover, given that EuQoS works through IP Tunnels the size of the tunnel encapsulation has to be counted.

The three series of tests permit us to know the degree of out of order packets in three different scenarios:

1) Low bandwidth and low packet rate
2) Medium bandwidth and low packet rate
3) Medium bandwidth and high packet rate

The results shown here are the most representative of a series of 5 rounds of tests. Unless noted otherwise, the results are the arithmetic mean of the different tests.

The tests involved several partners, specifically from Portugal, Spain and Switzerland, each round of tests was composed by a couple of runs of VoIP, UDP-1 and UDP-2, the first run in daily hours and the second at night.

The Table II shows the summary of out of order packets between two partners (from Spain and Portugal). Looking at the results can be noted that the amount of reordered packets is very high, taking into account ITU Rec. Y.1540 [15]. When the out of order ratio is higher that $5.0 \cdot 10^{-3}$ the network cannot be considered reliable.

Investigating the obtained traces, and the way the reordered packets arrive at destination, the only possible reason for such packets is load balancing as will be shown later.

TABLE II
OUT OF ORDER RATIO

Name	*VoIP*	*UDP - 1*	*UDP - 2*
Test1 (Night)	0	$1.44 \cdot 10^{-1}$	$2.38 \cdot 10^{-1}$
Test2 (Day)	0	0	$4.72 \cdot 10^{-4}$
Test3 (Night)	0	$2.45 \cdot 10^{-3}$	$1.91 \cdot 10^{-2}$
Test4 (Day)	0	$8.68 \cdot 10^{-5}$	$2.65 \cdot 10^{-3}$

The above tests are done at different hours, Tests 1 and 3 were done at nighttime hours (starting at 19:00), while Tests 2 and 4 were daytime tests (starting at 9:00), the duration of the tests, instead of being composed of short bursts as in [6] last for ten minutes each, this way, any transcient state on the network can be easily detected.

As it can be seen, nigthly and dayly results are pretty different, which indicates a trend of the backbone to balance the same flow over different interfaces. This happens more often when the network is underloaded (usually night hours).

This is a strange behaviour because usually when load balancing is involved, it is done on a per flow basis, permitting this way to balance full connections and not individual packets.

As it can be seen, specially on Test 1 the out of order packets are extremely high, about 23% which means almost one-third of the packets suffered the load balancing.

As the above table shows, the most critical test for packet reordering is when dealing with high packet rates, Table III shows a summary of the whole test set for UDP-2 flows.

For spotting the reason of finding out of order packets, the procedure to follow is to trace the route of the packets from outside the tunnel between the two access routers involved on the communication. The output of two different `traceroute` commands is:

```
# traceroute 193.136.203.143
  1 84.88.39.13 0 ms 0 ms 0 ms
  2 193.147.232.181 100 ms 0 ms 8 ms
  3 130.206.202.1 0 ms 0 ms 0 ms
  4 130.206.240.9 16 ms 16 ms 16 ms
  5 130.206.240.2 20 ms 16 ms 16 ms
  6 62.40.103.61 16 ms 16 ms 20 ms
  7 62.40.96.78 24 ms 28 ms 28 ms
  8 62.40.103.178 24 ms 28 ms 28 ms
  9 193.137.0.13 28 ms 24 ms 28 ms
 10 193.136.1.186 36 ms
    193.136.1.182 36 ms 36 ms
 11 193.136.1.98 36 ms 36 ms 36 ms
 12 193.136.203.17 36 ms 40 ms 36 ms
 13 193.136.203.172 44 ms 36 ms 36 ms
 14 193.136.203.143 36 ms 36 ms 36 ms
```

And the second one:

```
# traceroute 193.136.203.143
  1 84.88.39.13 4 ms 0 ms 0 ms
  2 193.147.232.181 0 ms 0 ms 0 ms
  3 130.206.202.1 4 ms 0 ms 0 ms
  4 130.206.240.9 16 ms 16 ms 16 ms
  5 130.206.240.2 20 ms 16 ms 16 ms
  6 62.40.103.61 16 ms 16 ms 16 ms
  7 62.40.96.78 28 ms 28 ms 24 ms
  8 62.40.103.178 28 ms 28 ms 24 ms
  9 193.137.0.13 28 ms 28 ms 28 ms
10 193.136.1.186 36 ms 36 ms 36 ms
11 193.136.1.98 36 ms 36 ms 36 ms
12 193.136.203.17 36 ms 36 ms 36 ms
13 193.136.203.172 36 ms 36 ms 40 ms
14 193.136.203.143 36 ms 36 ms 36 ms
```

As can be seen in hop 10 of the first attempt there are two different hosts who respond to the same TTL, this states clearly that there are some parts of the network with network layer load balancing. Under an experimental point of view this means that depending on the load balancing policy and the load of each link, the possibility of having reordered packets is pretty high. This Network Layer load balancing is directly related to the maximum out of order packet distance as shown on table IV. The table doesn't show the VoIP results given its lack of reordered packets.

TABLE IV
OUT OF ORDER DISTANCE AND BURST

Name	*UDP - 1*	*UDP - 2*
Distance	3	11
Burst	3	6

Apart from the global data, for finding out if this is an isolate behaviour, or, on the other hand it is a generic trend for the whole test, Figure 2 displays the instantaneous out of order distance for each packet. The figure highlights the fact that the reordering of packets is held all over the test. The graph shows on the X axis the packet's sequence number, and the Y axis holds the distance in packet units.

As it can be deducted from the information gathered, the effect of load balancing is highly influenced by the rate of packets per second, and moreover, it is constant all over the tests, disregarding, this way, any possible transient state on the network. The most critical factor in this analysis is the effect of such high reordering ratio in terms of one-way delay, which is an important parameter to determine the final Quality of Service.

The one-way average delay of the whole test is about 28ms, if we analyse the packets responsible for maximum burst and distance on the UDP-2 tests

TABLE III

OUT OF ORDER RATIO AMONG ALL THE PARTNERS IN UDP-2 FLOWS

Name	*Portugal*		*Switzerland*		*Spain*	
	Day	Night	Day	Night	Day	Night
Portugal	-	-	$2.61E-01$	$1.86E-06$	$1.30E-01$	$1.19E-01$
Switzerland	$1.66E-01$	$1.94E-01$	-	-	$1.30E-01$	$1.19E-01$
Spain	$2.41E-01$	$2.42E-01$	$8.79E-03$	$8.68E-03$	-	-

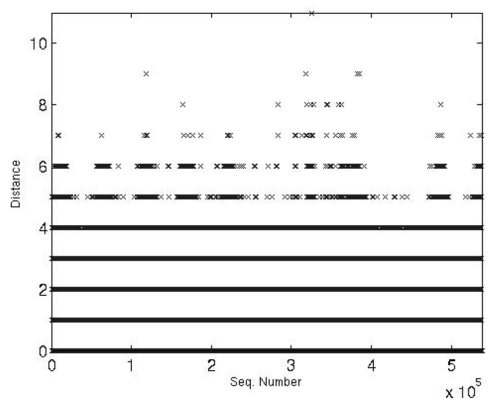

Fig. 2. Distance of out of order packets

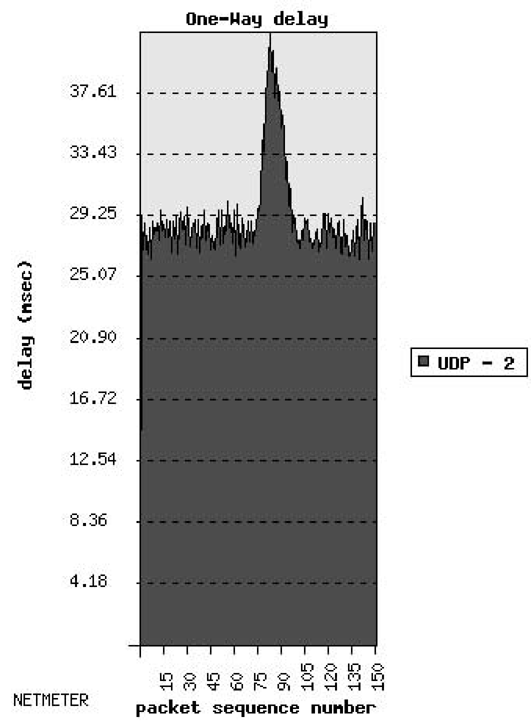

Fig. 3. OOO packet burst effects on one-way delay

we can find out that their delay is 39ms. As it can be seen the difference is important, the user's perception of such behaviour is shown in Figure 3, where the relative instantaneous end-to-end delay of each packet involved on the burst is displayed. This graph displays on the X axis the packet's sequence number, the Y axis shows the one-way delay expressed in milliseconds.

These great distances and bursts in out of order packets forces the reception host to hold a fair amount of packets on its buffer for in-order delivery. This will highly conditionate the final quality of the data transmission given its real-time nature.

V. CONCLUSIONS AND FUTURE WORK

This paper has shown an analysis of the out of order packets found on the EAN. This work's main contribution is to show the effects of such packets on real-time environments. This reordering can be due to several reasons, here, the discussion analyses the case of Network Layer load balancing. The metrics's definition used on this paper are compatible with the proposed standard on the IPPM [8].

The paper reviews the different research approaches to out of order issues. The difference from other papers is the analysis of real-time traffic, along with doing it on a European-wide environment. The effects of this reordering range from one-way delay changes on packet delivery, to the decrease of interactivity level or the possibility of fake packet losses due to late arrival.

Given the low level nature of such packets, the reception services need to control such reordering by having big buffers, given that the packets don't break the usual quality constrains of the traffic, but complicate the packet's delivery.

To solve this load balancing issue, the proper behaviour should be to use this balancing on a per flow basis, and not on a per packet fashion, this way, is easier to guarantee similar delivery times for all the packets involved on the communication.

For future work many issues are left for further study. Once seen this OOO packet problem, it would be interesting to study the effects of the sizes and the behaviour of the reception buffers, along with the effect of different data encodings, such as H.323 for video, PCM for audio and such. For doing this work, another metric must be taken into account, that is the packet interarrival times at destination.

On the network layer is interesting more detailed study to find where is the threshold for the reordered packets which don't affect the QoS, and being able to distinguish on the fly, which reordering is caused by "*light*" reordering (i.e. load balancing) against the "*more severe*" case which is due to route changes.

On the other hand, an analysis of other paths to cover more countries and to analyse potential links where such balancing is done would be useful for detecting potential problems on the network. This will lead to a methodology which would permit to know a priori the reason which causes the out of order packets, having only end-to-end information.

REFERENCES

[1] "[IST] EuQoS - End-to-end Quality of Service support over heterogeneous networks," Sept. 2004. [Online]. Available: http://www.euqos.org/

[2] J. Bennett, C. Partridge, and N. Shectman, "Packet reordering is not pathological network behavior," in *IEEE/ACCM Transactions on Networking*, 1999, pp. 789–798.

[3] V. Paxson, "End-to-end internet packet dynamics," in *IEEE/ACCM Transactions on Networking*, 1999, pp. 277–292.

[4] S. Jaiswal, G. Iannaccone, C. Diot, J. Kurose, and D. Towsley, "Measurement and Classification of Out-of-Sequence Packets in a Tier-1 IP Backbone ," in *Internet Measurements Workshop (IMW)*, 2002.

[5] M. Laor and L. Gendel, "The effect of packet reordering in a backbone link on application throughput," in *IEEE Network*, 2002.

[6] X. Zhou and P. V. Mieghem, "Reordering of IP Packets in Internet," in *C. Barakat, I. Pratt (Eds.): Fifth annual Passive and Active Measurement Workshop PAM2004, LNCS 3015, pp. 207-218, 2005. Springer-Verlag Berlin Heidelberg 2004. ISBN 3-540-21492-5*, 2004.

[7] J. Martínez, J. Flich, A. Robles, P. López, J. Duato, and M. Koibuchi, "In-order packet delivery in interconnection networks using adaptive routing," in *IEEE International Parallel and Distributed Processing Symposium (IPDPS'05)*, 2005.

[8] A.Morton, L.Ciavattone, G.Ramachandran, S.Shalunov, and J.Perser, "Packet Reordering Metric for IPPM - draft-ietf-ippm-reordering-11.txt," Draft 11, Dec. 2005.

[9] G. Almes and S. Kalidindi and M. Zekauskas, "A One-way Delay Metric for IPPM," RFC 2679, Sept. 1999.

[10] C. Demichelis and P. Chimento, "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)," RFC 3393, Nov. 2002.

[11] V. Paxson, "Measurements and analysis of end-to-end internet dynamics," Ph.D. dissertation, U.C. Berkeley, 1997.

[12] V. Paxson, G. Almes, J. Mahdavi, and M. Mathis, "Framework for IP Performance Metrics," RFC 2330, May 1998.

[13] A. Cabellos-Aparicio, R. Serral-Gracià, L. Jakab, and J. Domingo-Pascual, "Measurement Based Analysis of the Handover in a WLAN MIPv6 Scenario," in *C. Dovrolis (Ed.): Passive and Active Measurements 2005, LNCS 3431*, 2005, pp. 207–218.

[14] René Serral-Gracià and Roberto Borgione. (2004) NetMeter a NETwork performance METER - http://www.ccaba.upc.es/netmeter. [Online]. Available: http://www.ccaba.upc.es/netmeter

[15] ITU-T Recommendation Y.1540, "Internet protocol data communication service - IP packet transfer and availability performance paramteters," 12/2002.