On the Use of Traffic Monitoring and Measurements for Improving Networking

Sílvia Farraposo[1], Philippe Owezarski[2], Edmundo Monteiro[3]

[1]Escola Superior de Tecnologia e Gestão de Leiria, Morro do Lena
Alto-Vieiro Apartado 4163, 2401-951 Leiria, Portugal
silvia@estg.ipleiria.pt
[2]LAAS – CNRS 7, Avenue du Colonel Roche
31077 Toulouse Cedex 4, France
owe@laas.fr
[3]Departamento de Engenharia Informática, Pólo II
Pinhal de Marrocos, 3030-290 Coimbra, Portugal
edmundo@dei.uc.pt

Abstract. Several recent traffic monitoring studies proved that traffic is highly variable (sometimes not stationary), and in any cases exhibiting many disruptions in its throughput, that of course are damageable for providing a stable QoS. If some of these disruptions can be legitimate variations of traffic (because a user suddenly generates a big flow or flash crowd), others may be due to DoS attacks. This paper presents the use of monitoring and measurement techniques for improving networking. In particular, it gives examples on how to operate TCP/IP level traffic engineering mechanisms, and how to use monitoring as a countermesure for DoS attacks. All contribute to the provision and maintenance of end-to-end QoS in the presence of traffic disruptions, due to user demand (normal or abnormal) or to malicious behaviour.

1 Introduction

The Internet is nowadays considered as a multi-services network, and as such should be able to provide guaranteed differentiated services. The solutions that the Internet community has offered in the areas of differentiated and guaranteed services have not met the needs of users or operators (Internet Service Providers (ISP), carriers, etc.). Efforts have been stymied by the complexity of the Internet, its myriad systems of interconnections, and by the technological heterogeneity of these systems. They have also run up against poor general knowledge of how to provision networks, based upon traffic characteristics that are largely unknown, and that might deviate significantly from standard suppositions.

Given this poor knowledge of Internet traffic, and this is certainly one of the most important contributions of research activities in Internet networking these past years, recent advances in Internet traffic monitoring seems to provide important missing information. But the idea defended in this paper is that monitoring is not just a tool for network administrators to know the average throughput of traffic on their network for

charging users. Monitoring and measurements have also to be integrated on the network engineering process as the new knowledges on Internet traffic should help to design more suited architectures, protocols, and mechanisms for the Internet. Going further, the paper also defends the idea of network mechanisms reacting according to real time measurements of the traffic and QoS. This new measurement based approach of networking appears as particularly well suited given the high variability of current Internet traffic, which makes network conditions change very frequently.

The remainder of the paper then starts by a short presentation of traffic characteristics, especially focusing on its high variability and disruptions (section 2). It then presents the measurement based architecture (MBA) which has been defined to cope with the Internet structure (section 3). Based on this architecture, section 4 shows how it is possible to use the measurement based networking approach for traffic engineering and DoS countermeasures. Finally, section 4 is a conclusion with the main ideas defended by this paper.

2 Issues in the Internet Traffic and MBN Goals

Network monitoring and measurements proved to provide network operators, administrators, designers, engineers as well as researchers with very interesting and important information on the real nature of the traffic, on the way the network is working, as well as on the Quality of Service (QoS) it is providing. In particular, many recent research projects across the globe have shown that Internet traffic is very far from being regular, and presents large variations in its throughput at all scales [1]. These projects have shown that Internet traffic exhibits characteristics such as self-similarity [2], (multi-)fractality [3], and long-range dependence (LRD) [4], which is to say in all cases that traffic can vary significantly. These phenomena are due to several causes and in particular to congestion control mechanisms, especially the ones of TCP that is the dominant protocol in the Internet [1]. To summarize, it has been demonstrated that TCP congestion control mechanisms are not suited for the transmission of long flows on high speed networks [5], being responsible for the increase of oscillations.

An important consequence of such variability of traffic is related to the complexity of providing stable and guaranteed QoS which is one of the main goals of researches lead during the last decade. Actually, guaranteeing QoS means providing the requested QoS under all circumstances, including the most difficult ones. Among the most difficult circumstances, Internet QoS is highly sensitive to traffic variability, and to a wide variety of disruptions, often designated as unexpected traffic, be they induced by failures, by the Byzantine behaviors of some network elements, or more simply by the significant, though not abnormal, increase in traffic levels related for instance to the live diffusion of some popular event. Traffic disruptions more generally include all events that provoke a large change in network traffic characteristics, and that can badly impact the QoS provided by the network.

In this context, it is important to be able to develop methods and methodologies for global monitoring of the network. These methods are essential for detecting and reacting to “disruptions”. But, the main challenge for network and traffic monitoring and

measurement deals with helping improving networks and networking architectures protocols, and mechanisms. This paper then proposes to use monitoring techniques and to take advantage, in real time, of monitoring results for proposing a new Measurement Based Architecture (MBA) and mechanisms suited to adapt to frequent changes in the traffic. The MBN proposal whose main principles are presented in section 3 deals with providing a new solution for networking able to take into account non-stationary traffic and huge variations on a link, as well as the large differences that appear on the traffic from one link to the other in the network. In our work we will particularly address network routers mechanisms at IP level (routers and routing mechanisms). The main goal addressed in our work deals with avoiding large variations of the traffic on some particular links, through the limitation of all kinds of variability in the traffic for making it as smooth as possible and thus avoiding traffic variations at some points to have an impact on network QoS. This is especially the case for DoS and DDoS attacks that create generally very strong disruptions in the traffic. Actually, by limiting the variations of the traffic on any of the network links, we expect the network to continue providing a good QoS even in the presence of attacks, i.e. the network to be more robust to DoS attacks. However, increasing the robustness of network in the presence of disruptions, and more specifically attacks, implies to perform a very accurate and deep analysis of the impact of disruptions on traffic characteristics, to explain how they work and how they can decrease the network QoS.

3 Traffic Monitoring and the MBN Approach

The contribution of this work being on the use of monitoring and measurement for improving networking, the first requirement deals with being able to monitor and measure the network and its traffic with both local and global points of view. This monitoring and measurement system is one of the key components of the MBA architecture we plan to design, and of course, it directly depends on the network structure, particularly of the Internet. In fact, the Internet can be more and more considered as a global worldwide network but split in several domains (also called AS), administratively independent and independently designed and managed. In particular, the peering links interconnecting the different AS are generally under-provisioned, and the source of huge QoS and performance decrease in end-to-end communications.

The first requirement of MBN is then to be aware of the network and traffic changes. It is then necessary to measure traffic and QoS parameters locally, as well as on long distances when the connection crosses several domains. So, MBN is designed that way: even if on some points measurement information is not present, the network should continue to work with good performance and QoS. But performance and QoS can be much improved, and even become optimal, if measurement information is available.

Thus, given the administrative topology of the Internet, we propose to use different measurement techniques. Then, intra-domain measurements as loss ratio, used and available bandwidth, number of flows, etc. can be made using passive equipments.

On the other side, for inter-domain measurements it is impossible to use passive techniques as the other domains are not managed the same way, and their administrators may not use measurement techniques, or not necessarily the same techniques. In addition, even if they are performing measurements on their domain, in an open market where ISP have to compete to each other, they may not be willing exchanging such measurement information. So, in that case, it is required to address a measurement technique with a user point of view. Therefore, if we want to get information on other domain, the best solution consists in measuring what we need with active techniques, i.e. sending packet through the other domains, and measure what happens to these probe packets. Then, all these measurements performed in real time and signaled to traffic sources (i.e. service users), can give an accurate knowledge of network and traffic state, and allow them to perfectly adapt their sending rate (for instance) to available resources. Note however that one important aspect of MBN deals with the design of a protocol for signaling measurement information. Such protocol has necessarily to work in intra-domain, but can also be extended for inter-domain signaling.

Given such topological structure of the Internet, in addition of all the issues related to current traffic as un-stability, non-stationary nature, huge oscillating nature, correlation, dependence, and a huge versatility of traffic types during time, it is easy to understand that it is impossible to find an optimal solution suited for all connections in the Internet. This statement leads us proposing MBN in order to react in real time to some events on the network. We do believe that MBN can be a universal solution for managing the Internet and its traffic. In particular, MBN has been designed in order to be able to provide a suited solution that can adapt to any kinds of networks, any traffic nature and conditions, etc. In particular, MBN should have applications in many domains as traffic control, traffic management, traffic engineering or QoS optimization (cf. section 4).

4 Examples of MBN contributions for improving networking

4.1 Measurement Based Traffic Engineering

Network capacities are being deliberately overengineered in today's commercialised Internet in such a way that there be virtually no data loss, even during the worst possible network utilisation scenario. Thus, the service delivered by today's end−to−end wide area Internet would be perfect − if it wasn't for the inter−domain connections, such as Internet access links to the ISP or peering points between ISPs. Those points are carefully rate limited and their capacity is controlled by SLAs and Peering Arrangements. It is at these points that data packets will experience delays and loss due to deliberate reductions in network bandwidth.

Knowing exactly how Internet traffic behaves is a major step to define accurately how to act on traffic, and improve Traffic Engineering (TE) functions which major goal involves adapting the routing of traffic to the network conditions, with the joint goals of good user performance and efficient use of network resources. Particularly, we are interested in improving TE in such a way that any decision taken will be done based on current traffic monitoring and analysis.

So, we argue that through a deep knowledge of Internet traffic characterization it will be possible to define what are the major factors responsible for traffic variations at low frequencies (type of flows, rush hours, DoS attacks), and then to limit the degree of LRD, and the range and amplitude of variations in the traffic.

Particularly, we are studying a way of adapting path metrics to Internet traffic flows at each moment, in such a way that traffic variations can be smoothed, and LRD reduced and consequently QoS transmissions assured. Obviously, such a method requires real-time collecting information from the network – type of traffic currently on the network and QoS resources, to better balance the increase of traffic among all possible paths. This information is to be collected through the MBN framework.

As we have mentioned at section 2, a deep knowledge of how traffic evolves requires traffic to be continuously measured. Particularly, inter-domain measurements are quite challenging, because of the interaction between different network administrators, and most of the time ISPs. In that sense, we are exploring the advantages of using a modifyed version of QBGP [6], to obtain all the measures taken far away.

Attending the considerations presented above, it seems that a perfect understanding of traffic characteristics is the basis to develop new traffic mechanisms (or adjust the existent) to handle traffic disruptions without significant impact on QoS.

4.2. Measurement Based DoS Attacks Countermeasures

It is important to note that the line between network DoS attacks and legitimate traffic is blurred, and because of that, it is so hard fighting DoS attacks. As far as we know, there exists no broad enough definition of DoS in the literature. With no definition of DoS, it would be difficult to prevent DoS by a general and automatic method that does not involve human judgment, which is, of course, expensive and does not operate on the time scale of electronic packet networks. If it is hard to prevent or quickly cancel the effects of a DoS attack, a network operator might wish to have mechanisms that protect certain traffic that is known to be legitimate. This is also one of the intents of the MBN approach.

Regarding the related work on attack characterization, it clearly appears in recent work that there is an evolution when trying to find characteristics of attacks. Current studies more and more consider spectral parameters for the “signature of an attack”. Previously, it was mostly expected to find a normal profile of the traffic with regard to the classical parameters as throughput, number of packets or connections, parameters which were significantly changing during an attack. Nowadays – and it has been shown by recent traffic monitoring projects (as Sprint IPMON [7] or Metropolis [8] for example) – Internet traffic is highly variable because of flash crowds for instance, or because of transmission protocols as TCP. It is then quite impossible to find a normal traffic profile by just looking at the classical traffic parameters. Monitoring projects nevertheless found that there are invariants in the traffic when looking at the statistical moments of traffic higher than 2 (for which traffic exhibits scale laws) or at traffic spectral properties. That is what Hussain [9] has shown: attacks change the spectral signature of traffic. In particular, the results on spectral analysis or higher level statistical moments are independent from the classical traffic parameter variations.

Possesing non-variant characteristics of DoS attacks, it will be possible through a continuous monitoring and analyzing of traffic, to detect unexpected traffic, analyze it to see if it is associated to a DoS attack, and distribute it among the connections, in such a way that QoS parameters of legitimate traffic are always guaranteed. The MBN approach has all the potential to accomplish this task.

5 Conclusion

The exact state of the research of data traffic characteristics is that traffic is highly variable, and in any cases exhibiting many disruptions in its throughput. While these disruptions are of course damageable for QoS, they can be legitimate variations of traffic, but also due to DoS attacks.

In this context, the ability to observe the dynamic functioning of the network in real-time becomes critical. The complexity of interlocking components at both physical and abstract levels has outstripped the capacity to properly understand how they inter-operate, or to exactly predict the outcome of changes to existing, or the introduction of new components.

The key solution to better understand how the Internet behaves is through the use of network monitoring techniques, where data gathered using network monitoring techniques provides an essential input towards different areas such as: performance tuning, network planning, characterisation of network activities, security, etc.

While the areas presented above are only a few of the possible ones, the main idea to retain is that network monitoring and traffic analysis constitute a powerful toolset to study and to enhance network behaviour.

References

1. Park, Kim and Crovella, “On the Relationship Between File Sizes, Transport Protocols, and Self-Similar Network Traffic”, in Proc. of IEEE ICNP, 1996
2. K. Park and W. Willinger, Self-Similar Network Traffic and Performance Evaluation, Wiley & Sons, 2000
3. A. Feldmann, A. Gilbert, and W. Willinger, “Data Networks as Cascades: Investigating the Multifractal Nature of Internet WAN traffic”, in Proc. of ACM SIGCOMM'98, Vancouver, Canada, 1998
4. A. Erramilli, O. Narayan, W. Willinger, “Experimental Queuing Analysis with Long Range Dependent Packet Traffic”, in IEEE/ACM Transactions on Networking, Vol. 4, No. 2, 1996
5. P. Owezarski, N. Larrieu, “Internet Traffic Characterization - An Analysis of Traffic Oscillations”, in 7th IEEE International Conference HSNMC, Toulouse, France, July 2004
6. G. Cristallo, C. Jacquenet, “An Approach to Inter-Domain Traffic Engineering”, XVIII World Telecommunications Congress (WTC2002), September 2002.
7. Sprint IPMON project, http://ipmon.sprintlabs.com
8. Projet RNRT, Métrologie pour l’Internet et ses services, http://www.lip6.fr/metrologie
9. Ruby B. Lee, “Taxonomies of Distributed Denial of Service Networks, Attacks, Tools and Countermeasures”, Princeton University